COMPUTATIONAL ASPECTS OF CURVES OF GENUS AT LEAST 2

BJORN POONEN

Abstract. This survey discusses algorithms and explicit calculations for curves of genus at least 2 and their Jacobians, mainly over number fields and finite fields. Miscellaneous examples and a list of possible future projects are given at the end.

1. Introduction

An enormous number of people have performed an enormous number of computations on elliptic curves, as one can see from even a perfunctory glance at [29]. A few years ago, the same could not be said for curves of higher genus, even though the *theory* of such curves had been developed in detail. Now, however, polynomial-time algorithms and sometimes actual programs are available for solving a wide variety of problems associated with such curves. The genus 2 case especially is becoming accessible: in light of recent work, it seems reasonable to expect that within a few years, packages will be available for doing genus 2 computations analogous to the elliptic curve computations that are currently possible in PARI, MAGMA, SIMATH, apecs, and the "Elliptic Curve Calculator." As evidence of the growth of the literature, we note that the first book devoted to the explicit study of genus 2 curves has just appeared [22].

Applications requiring computations with curves of genus at least 2 have existed for well over a century. The oldest (but which has also acquired new relevance since the advent of symbolic integration packages) is that of the integration of algebraic functions: according to a theorem of Risch, the problem of deciding whether the integral of an algebraic function is elementary can be reduced to the problem of deciding whether divisors on algebraic curves represent torsion points on the Jacobian. (See [30] for a detailed discussion.) More recently, the ability to deal with curves of large genus explicitly has had applications in coding theory: to construct efficient algebraic-geometric codes, one needs curves over finite fields having many points [46], [113]. Also, algorithmic aspects of Jacobians of genus 2 curves play an important role in Adleman and Huang's proof that the primes are recognizable in random polynomial time [3]. Finally, Jacobians of hyperelliptic curves over finite fields have been suggested for use in cryptosystems [56]. The security of such systems is dependent on the alleged difficulty of solving the discrete logarithm problem in these algebraic groups.

Date: April 10, 1996.

This is an extended abstract for an invited talk to be presented at the Second Algorithmic Number Theory Symposium (ANTS II) in Bordeaux, May 18–23, 1996. The author is partially supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

After a short discussion of the explicit representation of curves, we discuss the explicit solution to the Riemann-Roch problem (computing a basis for $L(D)$), and how it can be used to compute the group law in Jacobians. Next we consider the problems of counting points on curves and Jacobians over finite fields, and the related problem of computing the characteristic polynomial of Frobenius. This is followed by a discussion of practical methods for finding all the rational points on curves and their Jacobians over number fields. Various other topics related to curves over number fields are then discussed: constructing curves with many rational points, constructing curves whose Jacobians have rational torsion points of large order, computing special fibers of genus 2 curves, and listing all curves with good reduction outside a specified finite set of primes. We conclude with an eclectic collection of examples, and a list of possible future projects.

If the relevant work of any people has been neglected in this survey, it is a reflection of the present author's ignorance, and it is hoped that such people will inform the author of their work.

2. Explicit models of curves

If we are to have algorithms for curves, we must first specify how the curves are to be represented concretely. We will assume that our base field k is perfect, but not necessarily (and usually not!) algebraically closed. Also we assume our curves are smooth, projective and geometrically irreducible, although it will often be convenient (especially for hyperelliptic curves) to use singular models.

In general, curves will be represented as the zero locus of homogeneous polynomials in $\mathbb{P}^n$. By linear projection, we may assume $n = 2$, at the expense of introducing singularities. From a computational point of view, it often seems simpler to work with such a singular plane model, given by a single homogeneous equation $f(x, y, z) = 0$, than to work with a nonsingular curve embedded in $\mathbb{P}^n$, $n \geq 3$. But when we speak of divisors, etc., on such a curve, we implicitly mean divisors on its nonsingular model.

Curves of genus 0 can be represented as a plane conic, i.e., in homogeneous coordinates on $\mathbb{P}^2$ as the zero locus of a quadratic form $f(x, y, z)$. Elliptic curves (curves of genus 1 *with a rational point*), have "Weierstrass models"

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

where the coefficients a_i are in k. But already for curves of genus 1 without a rational point, things can be very complicated: for each $N \geq 1$ there exists a genus 1 curve over $\mathbb{Q}$ which is not birational over $\mathbb{Q}$ to a plane curve of degree less than N.

In some ways, things are less terrible for curves of fixed genus $g \geq 2$, because in this case one always has a rational divisor of bounded positive degree, namely the canonical divisor, and it can be used to construct a projective model of reasonable degree. For example, if the characteristic of k is not 2, then every curve of genus 2 over k is birational to a curve of the form $y^2 = f(x)$ where $f(x) \in k[x]$ is a separable polynomial of degree 5 or 6. If $\deg f = 6$, then one can make a further change of variables over $\overline{k}$ in order to get a new model with $\deg f = 5$, but this is possible over k if and only if the curve has a rational Weierstrass point, i.e., if $f(x)$ has a zero in k. Models $y^2 = f(x)$ with $\deg f = 5$ or 6 have a singularity at infinity, but singularities are unavoidable if one wishes to remain in the plane, since the genus of a nonsingular plane curve of degree d is $(d-1)(d-2)/2 \neq 2$.

A curve X is *hyperelliptic* if it admits a 2-1 map to $\mathbb{P}^1$ *over* $\overline{k}$ and its genus is at least 2. The *hyperelliptic involution* on such a curve is the canonical map that interchanges the two points of each non-degenerate fiber. Every curve of genus 2 is hyperelliptic, but most curves of genus $g \geq 3$ are not. Again let us assume that the characteristic of k is not 2. If $f(x) \in k[x]$ is separable of degree $2g+1$ or $2g+2$, then $y^2 = f(x)$ is a model for a hyperelliptic curve g, with one singularity, at infinity.[1]

If $\deg f = 2g+1$, the singularity at infinity corresponds to a single point ∞ on the nonsingular model. If $\deg f = 2g+2$, it corresponds to a pair of points ∞^+ and ∞^- on the nonsingular model, and these can be distinguished by the value of the rational function y/x^{g+1}. Again, a model with $\deg f = 2g+2$ is birational over $\overline{k}$ to one with $\deg f = 2g+1$, but the rational map will be definable over k if and only if the original $f(x)$ had a zero in k. In some sense, hyperelliptic curves over $\mathbb{Q}$ of the form $y^2 = f(x)$ with $\deg f = 2g+1$ are rare compared to those with $\deg f = 2g+2$, just as polynomials in $\mathbb{Q}[x]$ of degree $2g+2$ having a rational zero are rare among the set of all polynomials in $\mathbb{Q}[x]$ of degree $2g+2$.

We have not yet addressed the question of how to *find* models of the form $y^2 = f(x)$ when they exist. One way of doing this will be sketched at the end of the next section.

3. The Riemann-Roch problem

Let X be a curve over k of genus g. As usual, if D is a k-rational divisor on X, $L(D)$ denotes the set of k-rational functions on X such that $D + \operatorname{div} f \geq 0$, $\ell(D)$ denotes the dimension of $L(D)$ over k, and K denotes a canonical divisor on X. The Riemann-Roch theorem states that

$$\ell(D) = \deg D + 1 - g + \ell(K - D).$$

The Riemann-Roch problem is to construct explicitly a basis for $L(D)$, given X and D. Coates [25] proved that for curves over algebraic number fields, bases over $\overline{\mathbb{Q}}$ could be effectively constructed. (He needed this for his work with Baker on effective bounds for integer points on elliptic curves [7].)

Much more recently, Huang and Ierardi [50] proved that the problem could be solved over the ground field k, and in polynomial time, for plane curves whose singularities are all defined over k. Finally, Volcheck in his thesis described an algorithm, based on some 19th-century methods of Brill and Noether, that solved the problem without assuming the rationality of the singularities. (See [114], [115].)

As alluded to at the end of the last section, a solution to the Riemann-Roch problem can be useful for finding low-degree models of curves. For instance, if one

[1] We should warn that not every hyperelliptic curve has a model of the form $y^2 = f(x)$ over k, because the quotient of the curve by its hyperelliptic involution might be a *twist* of $\mathbb{P}^1$; i.e., birational over k to a conic in $\mathbb{P}^2$ without a k-rational point. From the point of view of determining rational points on hyperelliptic curves, this is not a problem, because one can effectively determine whether the k-form of $\mathbb{P}^1$ has a k-rational point. If so (and in fact this always happens when g is even), then the hyperelliptic curve *does* have a model $y^2 = f(x)$ over k; if not, then the hyperelliptic curve cannot have any k-rational points either.

Another warning: there are rational points on the moduli space of genus 2 curves that do not come from any curve of genus 2 over $\mathbb{Q}$. In other words, there are genus 2 curves over $\overline{\mathbb{Q}}$ which are isomorphic to all of their Galois conjugates, but which are not isomorphic to curves defined by polynomial equations over $\mathbb{Q}$. See the end of [105], and also [82].

is handed a genus 1 curve and a rational point P, one can find a Weierstrass model simply by computing $L(2P)$ and $L(3P)$. If handed a genus 2 curve, compute any canonical divisor K, compute $L(K)$ to find an *effective* canonical divisor D, let x be a non-constant function in $L(D)$ and let y be a function in $L(3D)$ outside the span of $\{1, x, x^2, x^3\}$. This yields a model $y^2 = f(x)$ with $f(x)$ of degree 5 or 6.

In practice, ad hoc methods for finding nice models can be successful too! See [45] for an example.

4. Computing in the Jacobian of a curve

There are at least three different ways of doing computations in the Jacobian J of a curve X of genus $g \geq 2$. One way is to use the description of J as the group of divisors of degree zero on the curve, modulo linear equivalence. Fix a divisor D_0 of degree g on X. Then each effective divisor D of degree g gives rise to a point in $J(\overline{k})$, namely the divisor class of $D - D_0$, and the Riemann-Roch theorem shows that every point $P \in J(\overline{k})$ arises this way. In other words, we have a surjective map $X^g/S_g \to J$, and we can represent each $P \in J$ by some divisor D of degree g which maps to it. (Here X^g/S_g denotes the g-th symmetric power of X.)

There are several problems with this approach. The first problem is that the map $X^g/S_g \to J$ is only a birational morphism, so even though most $P \in J(\overline{k})$ (in the sense of Zariski topology) will be associated with a *unique* divisor D, some P will have infinitely many pre-images. This problem can sometimes be circumvented by adding additional conditions on D to make it unique. For example [16], if X is $y^2 = f(x)$ where f is a separable polynomial of degree $2g+1$, then every point on J is represented by a divisor of the form $P_1 + P_2 + \cdots + P_r - r \cdot \infty$ where P_i are affine points, $r \leq g$, and such that if $P_i = (a, b)$, then no P_j, $j \neq i$, equals $(a, -b)$.

A second problem is that in order to define the map $X^g/S_g \to J$ *over* k, one needs a k-rational divisor D_0 of degree g, and these do not always exist. A third problem (related to the first), is that even if D_0 can be found, a k-rational point on J might not be representable by a k-rational divisor. (The divisor *class* can be Galois-stable without having a rational divisor in it.) If X has a k-rational point P, however, then the second problem vanishes (let $D_0 = g \cdot P$), and so does the third problem [84, p. 168].

Adding points on the Jacobian, in this representation of the problem, amounts to finding an effective divisor D'' of degree g such that $D'' - D_0$ is linearly equivalent to $(D - D_0) + (D' - D_0)$, for given D and D'. This is an instance of the Riemann-Roch problem: we must find a nonzero function f in $L(D + D' - D_0)$. For generic D and D', this f will be unique up to scalar multiple, and otherwise we must make a choice (cf. the “first problem” with the approach, above).

Cantor [16] used this approach to give a very explicit algorithm for adding points on the Jacobian of curves of the form $y^2 = f(x)$ where $f(x)$ is a separable polynomial of degree $2g+1$ over a field of characteristic not 2. His algorithm requires only $O(g^2 \log g)$ field operations to add two points. In [17], he gives explicit closed form expressions for the multiplication-by-n map on the Jacobian of such a curve, and obtains recurrence relations for calculating the analogues of the division polynomials. Bertrand [8] incorporated Cantor's group law algorithm for hyperelliptic curves as part of an algorithm for evaluating hyperelliptic integrals, and this has been implemented as a part of the AXIOM computer algebra system.

Huang and Ierardi [50] used their solution to the Riemann-Roch problem to give a polynomial-time algorithm for adding two points in the Jacobian of any plane curve whose singularities were k-rational. Volcheck [114], [115] used his solution to the Riemann-Roch problem to give a polynomial-time algorithm which applies to all plane curves. He improved upon the running time as well: after a precomputation to deal with the singularities, his algorithm requires $O(M^7)$ operations in a field extension of k of bounded degree, where M is the maximum of the degree and genus of the curve. More recently, he has *implemented* an algorithm for computing multiples of a point in the Jacobian of a nonsingular plane curve over $\mathbb{Z}/N\mathbb{Z}$, in the hope that it can eventually be used to factor integers as in Lenstra's elliptic curve method.

A second way of dealing with the Jacobian J is to use the fact that J is itself an algebraic variety. Adopting this point of view also facilitates computations with the formal group. For curves of genus 2 over fields of characteristic not 2, explicit equations defining the Jacobian in projective space (of dimension 8 or 15), explicit equations for the morphism $J \times J \to J$ giving the group law in these coordinates, and the first few terms of the power series giving the formal group law in terms of two chosen local parameters at the origin on J, have all been given, for $y^2 =$ (quintic) by Grant [48] and for the general case $y^2 =$ (sextic) by Flynn [37], [40], where the quintic or sextic has indeterminate coefficients.[2] Flynn's formulas are available via anonymous ftp at `ftp.liv.ac.uk` in the directory `~ftp/pub/genus2`.

The main problem with this approach is the unwieldy size of the algebra. At present, dealing with Jacobians of curves of genus 3 or more in this way seems hopeless.

A third possible way to do computations in the Jacobian J of a curve, at least over fields of characteristic zero, would be to use the analytic description of J as $\mathbb{C}^g/\Lambda$ where Λ is the period lattice, a discrete $\mathbb{Z}$-module in $\mathbb{C}^g$ of rank $2g$. For elliptic curves, the period lattice can be computed using the arithmetic-geometric mean iteration, which amounts to iteratively replacing the curve by a 2-isogenous curve. A generalization to genus 2 was developed by Richelot in 1836. See [10] for a modern treatment. Analytic methods might prove useful in certain situations, for example determining the degrees of possible isogenies between Jacobians of genus 2 curves, but on the other hand, recovering provably correct algebraic results might not always be easy.

5. Counting points on curves and their Jacobians over finite fields

Let X be a smooth projective geometrically irreducible curve over $\mathbb{F}_q$ of genus g (presented, as usual, as a possibly singular plane model), and let J be its Jacobian. Let $P(t)$ denote the characteristic polynomial of the q-power Frobenius endomorphism on J, so that $P(t)$ is a monic polynomial of degree $2g$ with integer coefficients whose roots a_i all have absolute value $q^{1/2}$. We then have three problems.

[2] Actually this is not fully carried out in the sextic case: as Flynn states in [40], the biquadratic forms defining the group law are much too large to be written down in terms of indeterminate coefficients of the sextic, but bilinear forms giving the composition of $J \times J \to J$ with the projection to the Kummer surface $J/\{\pm 1\}$ are given explicitly in terms of indeterminate coefficients, and Flynn indicates how the biquadratic forms can be obtained from this for any particular specialization of the coefficients of the sextic to integers.

1. Compute $\#X(\mathbb{F}_q)$.
2. Compute $\#J(\mathbb{F}_q)$.
3. Compute $P(t)$.

As is well known, these problems are closely related. For example,

$$\#X(\mathbb{F}_{q^m}) = 1 - \sum_{i=1}^{2g} a_i^m + q^m$$

and

$$\#J(\mathbb{F}_{q^m}) = \prod_{i=1}^{2g}(1 - a_i^m),$$

both of which can be calculated in terms of the coefficients of $P(t)$. (See [83, §19] and [84, §11].) In the other direction, given $\#X(\mathbb{F}_{q^m})$ for $m = 1, 2, \ldots, g$, one can recover $\#J(\mathbb{F}_q)$ and $P(t)$. For example, if X is a curve of genus 2 over $\mathbb{F}_q$, then

$$\#J(\mathbb{F}_q) = \frac{1}{2}\#X(\mathbb{F}_{q^2}) + \frac{1}{2}\#X(\mathbb{F}_q)^2 - q.$$

If q is small, the number of points on a plane curve $f(x, y) = 0$ over $\mathbb{F}_q$ can be found simply: plug in all values of x and y and count those for which $f(x, y) = 0$. If moreover it is hyperelliptic and in the form $y^2 = f(x)$, then one need only go through the values of x and check whether $f(x)$ is a square in each case (and the list of all squares in $\mathbb{F}_q$ can be precomputed). Finally $\#X(\mathbb{F}_q)$ can be found by correcting for the singularities and the missing points at infinity. If q^g is reasonably small, one can also solve problems 2 and 3 above by computing $\#X(\mathbb{F}_{q^m})$ in this way for $1 \leq m \leq g$. We will refer to this as the naïve method.

But better techniques are available, at least in theory, if q is large compared to g. Schoof [103] gave a polynomial-time algorithm for computing $\#X(\mathbb{F}_q)$ where X is an elliptic curve given by a Weierstrass equation in characteristic not equal to 2 or 3. (As usual, polynomial time means polynomial in the length of the input in bits, which is $O(\log q)$ in this case; the naïve method, in contrast, requires time slightly worse than linear in q.) Subsequently, Atkin and Elkies introduced improvements that made the algorithm computationally viable, and Couveignes [28] developed a practical version for the case of small characterstic. Powerful implementations have been written by Lercier and Morain [66], [67]: they have computed the number of points on elliptic curves over fields of prime order $p = 10^{499} + 153$ and 2-power order $q = 2^{1301}$.

Pila [98] gave a theoretical generalization of Schoof's algorithm to curves of higher genus. He proved that for a curve X over $\mathbb{F}_q$ of any genus, all three problems above can be solved in time $O((\log q)^\Delta)$, where Δ and the implied constant depend only on the dimension N of the projective embedding of the Jacobian J, the number of equations defining J and the addition law, and their degrees. Huang and Ierardi [51] remarked that for a genus g curve described by an equation $f(x, y) = 0$ in the plane, Pila's Δ is at least doubly exponential in $\deg f$, and they gave a randomized algorithm in which the exponent Δ is at worst polynomial in $\deg f$, at least for the case in which the curve has only ordinary multiple points. Very recently Adleman and Huang [4] have given a *deterministic* algorithm in which Δ is polynomial in g and N. (But note that while g is at worst polynomial in $\deg f$, the dimension N of the projective space N in which the Jacobian is embedded could be exponential in g.) For hyperelliptic curves of genus g, they obtain a deterministic algorithm in which $\Delta = O(g^6)$, which is much better. Apparently no one has ever actually *implemented* an algorithm, even for genus 2, in which the running time (for fixed genus) is polynomial in $\log q$.

Katz and Sarnak recently asked whether one could compute the characteristic polynomial of Frobenius associated to curves X of large genus over very small finite fields. (They are hoping for numerical illustrations of their theorems on the local spacing distribution of the zeros of zeta functions of curves over finite fields.) For concreteness, suppose X is hyperelliptic of genus $g = 100$ over $\mathbb{F}_3$, given by an equation $y^2 = f(x)$ with $f(x) \in \mathbb{F}_3[x]$ of degree 202. It is known [5] that one can compute the number of $\mathbb{F}_3$-points on the Jacobians of such curves in subexponential time (and even determine the group structure, and solve the discrete logarithm problem), but computing the entire characteristic polynomial is apparently much more difficult. In fact, no one seems to be able to improve substantially upon the naïve method.

One application of the algorithms in this section is to bounding the size of the torsion subgroup of the Mordell-Weil group of Jacobians over number fields. Suppose J is the Jacobian of a curve X over a number field K, and X has good reduction at the prime $\mathfrak{p}$ of K lying above the rational prime p. Let $J_\mathfrak{p}$ denote the reduction of J at $\mathfrak{p}$, which is also the Jacobian of the reduced curve over the residue field $k_\mathfrak{p}$. Then the prime-to-p-part of the torsion subgroup of $J(K)$ maps injectively under reduction modulo $\mathfrak{p}$ into $J_\mathfrak{p}(k_\mathfrak{p})$. If the absolute ramification index of $\mathfrak{p}$ is less than $p-1$ (in particular if $K = \mathbb{Q}$ and $p > 2$), then the entire torsion subgroup injects. By calculating the size of $J_\mathfrak{p}(k_\mathfrak{p})$ for various $\mathfrak{p}$, one can get an upper bound on the size of the torsion subgroup of $J(K)$. (But see [53] for the limitations of this method.) In practice, there will usually be plenty of small primes of good reduction, so if the genus is reasonably small, the naïve method of computing points is sufficient.

Another application of the algorithms in this section is to the computation of endomorphism rings of Jacobians over number fields. The endomorphism ring maps injectively into the endomorphism ring of the Jacobian of the reduction of the curve at a prime of good reduction, and the latter endomorphism ring can be related to the characteristic polynomial of Frobenius. By comparing the results obtained this way for various primes, one can bound the rank of the endomorphism ring of the original Jacobian.[3] See [100, Appendix A] or [45] for an example. If the rank of the endomorphism ring is small, one can deduce that the Jacobian is not a quotient of a modular Jacobian $J_1(N)$, and so in particular the curve does not admit a dominant morphism from $X_1(N)$.[4] For example, if X is a genus 2 curve whose Jacobian has endomorphism ring $\mathbb{Z}$, then X is not modular.

6. The Mordell-Weil group of the Jacobian

If A is an abelian variety over a number field k, then the Mordell-Weil group $A(k)$ of k-rational points on A is finitely generated. In particular, if J is the Jacobian of a curve X over $\mathbb{Q}$ of genus $g \geq 1$, then the Mordell-Weil group $J(\mathbb{Q})$ is isomorphic

[3] There are other ways of computing the endomorphism ring for abelian varieties which are quotients of modular Jacobians. Mestre [80], for example, computed the endomorphism rings for all simple 2-dimensional factors of $J_0(p)$ for primes $p < 2000$.

[4] Even when the Jacobian of a curve *is* a quotient of $J_1(N)$, it is not necessarily the case that the curve admits a dominant morphism from $X_1(N)$. In general, one obtains only a correspondence.

as an abstract group to the direct sum of $\mathbb{Z}^r$ and a finite abelian group, the group of rational torsion points on J. In the case of elliptic curves, although at present no algorithm for computing generators of this group is known to succeed, there are several methods which work in practice for elliptic curves of reasonably small discriminant, and the effectiveness of some of these can be proved if one assumes certain standard conjectures, such as that the Shafarevich-Tate group is finite.

Here we will describe the generalization of one of these methods, 2-descent, to the case of hyperelliptic curves. Cassels outlined an approach for genus 2 curves in [20]. Gordon and Grant [47] carried this out for some curves, but their method worked only in the very special case where all six Weierstrass points were rational, and the method was quite involved in that it required explicit equations for homogeneous spaces of the Jacobian. Cassels' descent was made explicit and was generalized to hyperelliptic curves over $\mathbb{Q}$ of any genus by Schaefer [102] for the odd degree case, and recently by Flynn, Schaefer, and the author [45] for the general even degree case.

For concreteness, assume X is a curve $y^2 = f(x)$ where $\deg f(x) = 5$, and J is its Jacobian. Let $L = \mathbb{Q}[T]/(f(T))$, which is a product of number fields. What Cassels did in [20] was to define a injective homomorphism

$$J(\mathbb{Q})/2J(\mathbb{Q}) \overset{x-T}{\longrightarrow} \left(\ker : L^*/L^{*2} \overset{\mathrm{Norm}}{\to} \mathbb{Q}^*/\mathbb{Q}^{*2}\right).$$

Schaefer [102] proved that $\left(\ker : L^*/L^{*2} \overset{\mathrm{Norm}}{\to} \mathbb{Q}^*/\mathbb{Q}^{*2}\right)$ was isomorphic to the Galois cohomology group $H^1(G_{\mathbb{Q}}, J[2])$, and that under this identification the "$(x-T)$" map coincided with the usual coboundary map of Galois cohomology. Moreover he demonstrated how to compute the 2-Selmer group of J explicitly as a subgroup of L^*/L^{*2}, without having to write down homogeneous spaces. When the Shafarevich-Tate group has trivial 2-torsion, this method thus lets one compute the size of $J(\mathbb{Q})/2J(\mathbb{Q})$, from which one can readily compute the rank of $J(\mathbb{Q})$.

For $y^2 = f(x)$ with $\deg f(x) = 6$, Cassels described an $(x - T)$ map from $J(\mathbb{Q})/2J(\mathbb{Q})$ to the kernel of the norm map from $L^*/L^{*2}\mathbb{Q}^*$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. But the cohomological interpretation is not as neat in this case: this kernel is not isomorphic to $H^1(G_{\mathbb{Q}}, J[2])$, and the $(x - T)$ map could even fail to be injective. Schaefer and the author have recently discovered that the $(x-T)$ map can be related to the coboundary map of Galois cohomology for the 2-torsion of a generalized Jacobian.

As will be mentioned in Section 11, Smart [108] has an implementation of Schaefer's algorithm, but only for a very restricted class of genus 2 curves. Stoll also has implemented a 2-descent for most curves of the form $y^2 = x^5 + D$. The $\deg f = 6$ algorithm has been successfully used a few times (see [45] and [99]), but no one has automated it yet. Stoll also written a program that computes lower bounds on the rank of $J(\mathbb{Q})$ by attempting to find the exact rank of a subgroup generated by a given set of points by looking at the rank of the q-part of the image of the subgroup in finite products $\prod J_p(\mathbb{F}_p)$ for various primes q. In [110] he finds simple genus 2 Jacobians with Mordell-Weil rank at least 19; recently he has found one with rank at least 20.

When these methods succeed, they let one compute the rank of $J(\mathbb{Q})$. But there is still a significant amount of work to be done if one wants to list *generators* for $J(\mathbb{Q})$. One could in theory do an exhaustive search for rational points of small height, but the generators might have height very large compared to the coefficients of the original curve, so large that they could not be found by a naïve search.[5] And even if one does find enough independent points in $J(\mathbb{Q})$ to generate a subgroup of the correct rank, one still needs to use height functions in order to prove that the points are generators modulo torsion. An explicit theory of heights for genus 2 Jacobians has been worked out in [42], but so far it has proved useful in practice only for curves with very small coefficients. For example [45], the methods are not strong enough to decide whether the divisor class $[\infty^+ - \infty^-]$ generates the Mordell-Weil group of the rank 1 Jacobian of

$$y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Currently it seems that no explicit computations have been done with Selmer groups and Shafarevich-Tate groups of Jacobians of non-hyperelliptic curves, except for special curves whose Jacobians have a large endomorphism ring, such as Fermat quotients (see [74] and [55], for example) and modular curves (see [72], for example). For some computations of "analytic ranks" of certain quotients of $J_0(N)$, see Brumer [14]. Assuming the Birch and Swinnerton-Dyer conjecture, these should be the same as the "algebraic" Mordell-Weil ranks.

7. Provably finding all rational points on a curve

By Faltings' Theorem [36] (originally the Mordell Conjecture), if a curve over a number field k has genus at least 2, then it has only finitely many k-rational points. Unfortunately the proof is ineffective: it does not provide a bound for the heights of the rational points on any given curve. Nevertheless, it is sometimes possible in practice to list all the rational points on a curve by using an idea of Chabauty that predates Faltings' work by 40 years!

Chabauty [23] proved that if the Mordell-Weil rank of a curve over a number field k is less than the genus, then the curve has finitely many k-rational points. In order to sketch his idea, let us restrict to the case of a genus 2 curve X over $\mathbb{Q}$ whose Jacobian J has Mordell-Weil rank 1. Fix a non-constant map $X \to J$ over $\mathbb{Q}$ and a prime p of good reduction for J. Inside the 2-dimensional p-adic Lie group $J(\mathbb{Q}_p)$, we have two analytic 1–dimensional subvarieties: $X(\mathbb{Q}_p)$ and the closure of $J(\mathbb{Q})$. Their intersection is 0-dimensional and in fact finite, and $X(\mathbb{Q})$ maps into this finite set. (This can also be rephrased in terms of the formal group or in terms of p-adic integration.) Coleman [26] was the first to realize that one could give effective bounds for the size of this finite intersection. Using this idea, he was able to show, for example, that if X is a genus g curve over $\mathbb{Q}$ with good reduction at a prime $p > 2g$, and if the Mordell-Weil rank of X is less than g, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2$. Coleman himself did not give explicit examples where $X(\mathbb{Q})$ was computed using this bound, presumably because of the difficulty of bounding the Mordell-Weil rank; the first non-trivial example was given by Grant [49].

In some cases, it is actually possible to compute the size of the intersection exactly, and this leads to an improved upper bound for $\#X(\mathbb{Q})$. With luck, one

---

[5] This actually happens in genus 1: for instance, for the rank 1 elliptic curve $1063y^2 = x^3 - x$ of [33], the x-coordinate of a generator of the Mordell-Weil group modulo torsion is $X^2/1063$ where

$$X = \frac{11091863741829769675047021635712281767382339667434645}{317342657544772180735207977320900012522807936777887}.$$

Elkies suggests that similar examples might be found in some Jacobians of curves of the form $Dy^2 = x^5 - x$ with $D \in \mathbb{Q}^*$.

will actually be able to exhibit this many rational points on X, and then one will know that all rational points have been found. (See [44], [45] and [99] for examples in which this refinement of the method has had success.)

McCallum [75] has used this "method of Chabauty and Coleman" to prove the second case of Fermat's Last Theorem for regular primes. Although this particular application is superseded by the work of Wiles [116] and Taylor-Wiles [111], and preceded by the work of Kummer, who proved Fermat's Last Theorem in its entirety for regular primes, McCallum's work still serves as evidence of the power of the method.

When the method of Chabauty and Coleman fails to resolve the rational points (for example, if the Mordell-Weil rank is not less than the genus, or if the bound obtained for the number of rational points appears not to be sharp), there are a few other methods that sometime work in practice, for somewhat limited classes of curves. For example, if X is a genus 2 curve that admits a non-constant morphism to an elliptic curve over $\mathbb{Q}$, so that the Jacobian of X splits up to isogeny as a product of two elliptic curves, then if one of those elliptic curves has rank 0, the rational points of X can be found in the (finite) pre-image of the rational points on that elliptic curve. This is a trivial instance of a general method of Dem'janenko [32], further generalized by Manin [71][6]: if X is a curve over a number field k, if A is a k-simple abelian variety such that A^m occurs in the decomposition of the Jacobian of X up to isogeny over k, and if

$$m > \frac{\operatorname{rank} A(k)}{\operatorname{rank} \operatorname{End}_k A},$$

then $X(k)$ is finite. This can be made effective. See [106] for some explicit applications of this method.

One can also attempt to use unramified covers of X: if Y is an unramified cover of X, then according to a theorem of Chevalley and Weil [24], there is a certain extension field k' such that the pre-images of the rational points on X are contained in $Y(k')$. Although Y will have higher genus than X if the genus of X is at least 2 (and if the cover is non-trivial), one can hope to compute $Y(k')$ by finding a map from Y to a curve of smaller genus (for example, an elliptic curve over k' of rank 0). Some examples of this are given in [27].

If one suspects that there may be no rational points on a curve X, one can of course try to prove this by determining whether X has points over all completions of $\mathbb{Q}$. But just as in genus 1, the "Hasse principle" can fail: existence of local points over all completions is not enough to guarantee the existence of a rational point. See [85] for a few examples of genus 2 curves for which the Hasse principle fails.

Some computations have been done with rational points on quartic curves given in homogeneous coordinates by an equation

$$F(x^2, y^2, z^2) = 0$$

where $F(X, Y, Z)$ is a nonsingular quadratic form. What facilitates the study here is the fact that these curves admit three maps to genus 1 curves. In particular, their Jacobians split completely into elliptic curves. See [13], [21], [11], and [12], for example. Bremner has studied similar examples of families of curves up to genus 5 whose Jacobians split completely into elliptic curves.

[6] In fact, what we are stating here is only a special case of Manin's result, which applies also to smooth projective varieties of higher dimension whose Néron-Severi group has rank 1.

Finally, if one wants only to find the *integer* points on a hyperelliptic curve, one can attempt to use a diophantine approximation method made explicit by de Weger [31].

8. Curves with many rational points

In light of Faltings' Theorem, it is natural to ask whether the number of k-rational points on a genus g curve over a number field k can be bounded solely in terms of k and g. Caporaso, Harris, and Mazur [18] have shown that this would follow from some very general conjectures of Lang on rational points on varieties of general type. Abramovich [2] showed more: that the bound could be made uniform for curves of fixed genus over all quadratic or cubic extensions k of a fixed number field. Finally Pacelli [96], still assuming Lang's conjectures, generalized this to prove that the number of k-rational points on a curve of genus g could be bounded by a quantity depending only on $[k : \mathbb{Q}]$ and g.

In the other direction, several people have been finding curves having many rational points; here we give some current records. There is a genus 2 curve over $\mathbb{Q}$ with at least 588 rational points (Keller and Kulesz [54]), a genus 3 curve with at least 176 rational points ([54] again), *infinitely many* genus 4 curves with at least 126 rational points (Elkies), and a genus 5 curve with at least 120 rational points (Kulesz). In general, Mestre has proved that there exists a genus g hyperelliptic curve having at least $8g + 16$ rational points.

Most of these curves were found by a search within a family of curves having a large automorphism group. On the other hand, Stahlke [109] has found a genus 2 curve with at least 336 rational points having minimal automorphism group, $\mathbb{Z}/2\mathbb{Z}$ (nothing but the identity and the hyperelliptic involution).

Not surprisingly, another feature of these curves is that their Jacobians tend to have large Mordell-Weil rank. Elkies showed that the Keller-Kulesz genus 2 curve with at least 588 rational points has Jacobian isogenous to the square of an elliptic curve of rank at least 12.

9. Curves whose Jacobians have rational torsion points of large order

Mazur [72] proved that if E is an elliptic curve over $\mathbb{Q}$, the group of rational torsion points on E is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ with $N \leq 10$ or $N = 12$, or isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ with $N \leq 4$. The uniform boundedness of the torsion has been generalized to number fields by work of Manin [71], Kamienny and Mazur [52], Abramovich [1], and finally Merel [76].

It is not known whether there is a uniform bound on the size of the torsion subgroup of an abelian variety of fixed dimension $g \geq 2$ over a fixed number field In fact, there is no bound known even for 2-dimensional abelian varieties, even if one restricts to Jacobians of genus 2 curves over $\mathbb{Q}$. There is not even a single integer ℓ for which it is known that there is no genus 2 Jacobian with a rational point of order ℓ. Working with the full moduli spaces (the higher dimensional analogues of $X_1(N)$) seems forbidding from a computational point of view.

On the other hand, Flynn ([38], [39]) has exhibited hyperelliptic curves and families of hyperelliptic curves over $\mathbb{Q}$ whose Jacobians have rational torsion points of fairly large order. His method for constructing such curves is elementary: he writes down a specific equation $y^2 = f(x)$, carefully choosing $f(x)$ so that the divisors of certain rational functions are combinations of a few explicitly given points on the curve. Each such rational function gives rise to a relation in the Jacobian, and with enough relations, one can hope to deduce that the differences of the points involved represent torsion points on the Jacobian. For example, the divisor of the rational function $y - x^g$ on the curve

$$y^2 + y = x^{2g+1} + x^{2g} + x^g$$

is $(2g+1)D$ where $D = (1,0) - \infty$, and one can check that D represents a torsion point on the Jacobian of order $2g+1$. (See [39].)

Leprévost ([59], [60], [61], [62], [63], [64], [65]) and Ogawa [91] have used similar methods to find many other possibilities for the orders of rational torsion points on Jacobians. Here are samples of what is now known:

Theorem 1. *For $\ell \leq 30$, $\ell \neq 28$, there exists a genus 2 curve over $\mathbb{Q}$ whose Jacobian has a rational torsion point of exact order ℓ.*[7] *For $\ell \leq 23$ or $\ell = 26$ or $\ell = 30$, there exists a non-constant genus 2 curve over $\mathbb{Q}(t)$ whose Jacobian has a rational torsion point of exact order ℓ. There exists a non-constant genus 2 curve over $\mathbb{Q}(t)$ whose Jacobian has a subgroup of rational points isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.*

Theorem 2. *If $\ell \leq 3g$ then there is at least one genus g curve over $\mathbb{Q}$ whose Jacobian has a rational torsion point of exact order ℓ. The same is true if g is even and $g^2+2g+1 \leq \ell \leq g^2+3g+1$. If $1 \leq \ell \leq 2g+1$ or $\ell = 2g^2+2g+1, 2g^2+3g+1, 2g^2+4g+1, 2g(2g+1)$, then there exists a non-constant genus g curve over $\mathbb{Q}(t)$ whose Jacobian has a rational torsion point of exact order ℓ. The same is true for $2g+2 \leq \ell \leq 3g$ if ℓ is even.*

Note that from each non-constant curve over $\mathbb{Q}(t)$ with a rational torsion point of a certain order, one can obtain infintely many pairwise non-$\overline{\mathbb{Q}}$-isomorphic curves over $\mathbb{Q}$ whose Jacobian has a torsion point of the same order by specializing t.

10. Computing the special fiber of a genus 2 curve

There is a well-known classification of the fibers of minimal proper regular models of elliptic curves, and an algorithm of Tate which lets one compute the type of this fiber given a Weierstrass equation for the elliptic curve, and this has been implemented in various elliptic curve packages. (See [107, Chapter IV] for an exposition of this theory.) For the case of genus 2 curves, a similar classification has been given by [93] and completed by Namikawa and Ueno [90]. There are well over 100 different types of fibers! Liu [68] gave an algorithm for explicitly computing the special fiber of the minimal model in terms of the coefficients of a genus 2 curve for residue characteristic not equal to 2, and he (with help from Henri Cohen) has implemented this algorithm over $\mathbb{Z}$ for computing the special fiber of a genus 2 curve at any prime $p \neq 2$. The program, which is available via anonymous ftp at `megrez.math.u-bordeaux.fr` in the directory `/pub/liu`, also computes the odd

[7] The existence for $\ell = 19$ and $\ell = 21$ was in fact demonstrated over 20 years ago by Ogg [94]: the 2-dimensional modular Jacobians $J_1(13)$ and $J_1(18)$ have torsion subgroups isomorphic to $\mathbb{Z}/19\mathbb{Z}$ and $\mathbb{Z}/21\mathbb{Z}$, respectively. The only other $J_1(N)$ of dimension 2 is $J_1(16)$, whose torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Ironically it is the existence of the rational 19-torsion points on $J_1(13)$ which was used by Mazur and Tate [73] to prove the non-existence of rational points of order 13 on elliptic curves over $\mathbb{Q}$.

part of the conductor. It is to be hoped that algorithms will soon be available for residue characteristic 2 as well. Some work towards this goal is described in [70].

11. Curves of genus 2 with good reduction outside 2

Shafarevich proved that for each number field K and finite set of places S, there are only finitely many K-isomorphism classes of elliptic curves over K with good reduction outside S. (See [104].) Ogg [92] determined explicitly all elliptic curves over $\mathbb{Q}$ up to isomorphism with good reduction outside 2, and various other authors have produced lists for various other K and S. (See for instance, [58].)

Shafarevich also conjectured a generalization to higher genus, namely, that for each number field K, finite set of places S, and positive integer g, there are only finitely many K-isomorphism classes of curves of genus g over K with good reduction outside S. This was proved by Faltings [36], but the hyperelliptic case had already been resolved by several authors: [97], [95], [77].

Smart [108] has recently produced the complete list of genus 2 curves over $\mathbb{Q}$ with good reduction outside 2, up to isomorphism over $\mathbb{Q}$. (There are 428 of them!) This completes the earlier work on this problem in [77], [112], and [78]. The method for producing this list is to reduce to the problem of enumerating equivalence classes of binary forms whose discriminant is an S-unit (where $S = \{2\}$). Birch and Merriman [9] proved that there were only finitely many such equivalence classes, and Evertse and Győry [35] gave an effective proof, which then had to be made explicit for the case at hand.

Smart also in [108] heuristically divides his list of genus 2 curves according to the isogeny class of the Jacobian over $\mathbb{Q}$. If two Jacobians are isogenous over $\mathbb{Q}$, then for each p of good reduction, their traces of Frobenius will coincide. Conversely, by Faltings [36], if the traces of Frobenius coincide for all such p, then the Jacobians are isogenous, and in principle one need only check primes p up to an effective bound, but in practice this bound is usually too large for computation. Smart checks the Jacobians of his genus 2 curves for p up to 541, which is almost certainly sufficient, but not completely proven to separate the curves according to isogeny class. The 428 curves fall into 165 putative isogeny classes.

Finally Smart has implemented Schaefer's algorithm for calculating the Mordell-Weil rank for genus 2 curves $y^2 = f(x)$ over $\mathbb{Q}$ in the special case where the degree of f is 5, the curve has good reduction outside 2, and the irreducible factors of $f(x)$ define number fields of class number one.[8] He uses this to calculate the rank of some of the curves in his list, and is able to deduce the ranks of many more under the assumptions that the order of the 2-torsion in the Shafarevich-Tate group is a square, and that curves in his putative isogeny classes actually have isogenous Jacobians.

All this data can be obtained on the World Wide Web: the URL is `http://www.ukc.ac.uk/IMS/maths/people/N.P.Smart/curves.html`.

12. Miscellaneous examples of genus 2 curves

The genus 2 curve

$$y^2 = 278271081x^2(x^2-9)^2 - 229833600(x^2-1)^2$$

[8] As it turns out, the last of the three conditions is automatically true for genus 2 curves with good reduction outside 2.

(with automorphism group of order 12) has at least 588 rational points [54]. The genus 2 curve

$$y^2 = 1306881x^6 + 18610236x^5 - 46135758x^4 - 1536521592x^3 - 2095359287x^2 + 32447351356x + 89852477764$$

has no automorphisms other than the identity and the hyperelliptic involution, but still has at least 336 rational points [109].

Leprévost [63] showed that the divisor $(0,2) - \infty^+$ on the genus 2 curve

$$y^2 = (2x-1)(2x^5 - x^4 - 4x^2 + 8x - 4)$$

represents a 29-torsion point on the Jacobian.

Elkies showed that the curve

$$y^2 = 4x^6 + 12x^5 + 29x^4 + 38x^3 + 29x^2 + 12x + 4$$

is the only genus 2 curve with 12 automorphisms and six rational points whose differences generate a torsion subgroup isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$ in the Jacobian. (The rational points are at $x = 0, -1, \infty$.) The Jacobian splits up to isogeny over $\mathbb{Q}$ as the product of the two elliptic curves

$$y^2 + xy + y = x^3 + x^2 - 3x + 1, \qquad y^2 + xy + y = x^3 + x^2 + 22x - 9,$$

(50B1(A) and 50B2(B) in [29]), and these are the only two elliptic curves over $\mathbb{Q}$ having both a rational 5-torsion point and a rational 3-isogeny (to each other).

Let X be the curve

$$y^2 = x(x-1)(x-2)(x-5)(x-6)$$

and let J be its Jacobian. According to [47], the Mordell-Weil group $J(\mathbb{Q})$ is isomorphic to $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^4$. In particular, its rank is less than the genus, and Coleman's effective Chabauty bound for $p = 7$ applies to show that $\#X(\mathbb{Q}) \le 10$, and in fact there do exist 10 points:

$$X(\mathbb{Q}) = \{\infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3,\pm 6), (10, \pm 120)\}.$$

This is the first curve for which the method of Chabauty and Coleman was used to find all the rational points. See [49].

The curve that classifies quadratic polynomials $f(x)$ (up to conjugation by linear polynomials) together with a point t which upon iteration of f enters a 3-cycle after two steps is birational to the genus 2 curve

$$X : y^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

Its Jacobian J is an absolutely simple abelian surface of prime conductor 743, but it is not modular, since its endomorphism ring over $\overline{\mathbb{Q}}$ is only $\mathbb{Z}$. Its Mordell-Weil group is isomorphic to $\mathbb{Z}$, and is probably generated by the divisor class $[\infty^+ - \infty^-]$. The method of Chabauty and Coleman shows that there are eight points on X:

$$X(\mathbb{Q}) = \{(-1, \pm 1), (0, \pm 1), (1, \pm 3), \infty^+, \infty^-\}.$$

(See [99].)

The method of Chabauty and Coleman does not apply to the genus 2 curve

$$X : y^2 = x^5 + 4x^3 + x$$

since its Mordell-Weil rank is 2: its Jacobian is isogenous over $\mathbb{Q}$ to the product of two elliptic curves

$$w^2 = v^3 + 4v^2 + 6v, \qquad w^2 = v^3 - 4v^2 + 6v,$$

both of which have rank 1. Nevertheless, using an unramified cover on X, Coombes and Grant [27] were able to prove that $X(\mathbb{Q}) = \{\infty, (0,0)\}$.

Mestre [80],[81] reinterpreted a geometric result of Humbert to write down the following two-parameter family of hyperelliptic curves whose Jacobians have real multiplication by $\mathbb{Z}[(1+\sqrt{5})/2]$:

$$y^2 = ux^5 - (u+t-3)x^4 + (u^2 - 3u + 5 - 2t)x^3 - tx^2 + (u-3)x - 1.$$

He noted that his family is strictly contained in the following family of such curves given by Brumer in a 1988 letter to Serre (the equation for the family is reproduced in [14]):[9]

$$y^2 + (x^3 + x + 1 + c(x^2 + x))y = b + (1+3b)x + (1 - bd + 3b)x^2 + (b - 2bd - d)x^3 - bdx^4.$$

Brumer is currently preparing a paper on curves with real multiplication [15]; presumably it will explain further how to come up with such examples. Mestre used a generalization of his construction to prove the existence of a two-parameter family of genus 19 hyperelliptic curves whose Jacobians split completely into elliptic curves.

Rodriguez-Villegas [101] shows how to exhibit all curves of genus 2 whose unpolarized Jacobians are isomorphic to the product of two elliptic curves with complex multiplication by a specified order $\mathcal{O}$ in an imaginary quadratic field. For the case $\mathcal{O} = \mathbb{Z}[(1+\sqrt{-163})/2]$, one of the seven such curves (up to isomorphism over $\mathbb{C}$) is

$$y^2 = 6^{-3} h(x) h^{\iota}(x),$$

where

$$\begin{aligned} h(x) = (-151790 + 7144\sqrt{-163})x^3 + (1752597 + 129789\sqrt{-163})x^2 \\ + (510153 - 47481\sqrt{-163})x + (-37250 - 1596\sqrt{-163}), \end{aligned}$$

and

$$h^{\iota}(x) = \overline{x^3 h(-1/x)}.$$

(bar denoting complex conjugation of coefficients). This curve is isomorphic to its conjugate, so its field of moduli is $\mathbb{Q}$, but it has no model over $\mathbb{Q}$. The same is true for all seven of the curves, except for one which is actually definable over $\mathbb{Q}$.

The equation

$$u^2 - (t^3 + t - 1)u = t^3 + t^2 - t$$

is a model for the genus 2 modular curve $X^*(191)$. The rational point $(t,u) = (\infty,\infty)$ is the cusp, the points $(0,-1), (0,0), (\infty,-1), (2,-1)$ are CM-points of conductor $7, 11, 19$, and 28, respectively, and $(2,10)$ is a non-CM point corresponding to a 191-isogeny between two elliptic curves conjugate over $\mathbb{Q}(\sqrt{2036079533})$ with additive reduction at a prime above 191 and good reduction elsewhere [34]. A model for $X^*(191)$ was independently obtained by Murabayashi [89], who also computed explicit models for some other modular curves of prime level.

[9] Although Brumer's family appears to have three independent parameters, Elkies points out that the moduli space of curves whose Jacobians have real multiplication by $\mathbb{Z}[(1+\sqrt{5})/2]$ is only 2-dimensional, so many of the curves in the family must be isomorphic at least over $\overline{\mathbb{Q}}$.

13. Reasonable projects for the near future?

Below are what might be considered "next steps" in the development of algorithms for curves of genus 2 or more. The author conjectures that these particular problems, with the exception of the third, are accessible enough that many of them will be solved within the next few years.

- Implement a polynomial time algorithm for counting points on genus 2 curves over $\mathbb{F}_p$.
- Generalize the algorithm in [5] to show (modulo heuristic assumptions) that one can find the group structure of the Jacobian and solve the discrete logarithm problem for an *arbitrary* curve of large genus over a small finite field, in subexponential time.
- Find an algorithm for computing the characteristic polynomial of Frobenius for a hyperelliptic curve of large genus over a small finite field, in subexponential time.
- Devise and implement an algorithm for calculating the endomorphism ring over $\overline{\mathbb{Q}}$ of the Jacobian of a genus 2 curve over $\mathbb{Q}$, or at least an algorithm for determining if such a Jacobian is simple (over $\mathbb{Q}$ or over $\overline{\mathbb{Q}}$).
- Devise and implement an algorithm for calculating the size of the torsion subgroup of the Jacobian of a genus 2 curve over $\mathbb{Q}$.
- Automate the $(x - T)$-descent completely. (Write a program that takes as input the coefficients of a sextic $f(x) \in \mathbb{Q}[x]$, and spits out an upper bound for the rank of the Jacobian of $y^2 = f(x)$.)
- Improve upon Flynn's theory of heights so that one can provably find generators of Mordell-Weil groups of genus 2 curves with coefficients of moderate size.
- Automate the method of Chabauty and Coleman. (Let X be the curve $y^2 = f(x)$ with $f(x) \in \mathbb{Q}[x]$ sextic. Write a program that takes as input $f(x)$, an odd prime p not dividing the discriminant of $f(x)$, and a non-torsion point P in $J(\mathbb{Q})$, and returns the size of the intersection of the closure of $\mathbb{Z} \cdot P$ in $J(\mathbb{Q}_p)$ with the image of $X(\mathbb{Q}_p)$ in $J(\mathbb{Q}_p)$ under one of the embeddings of X into J.)
- Extend the minimal model program of Liu so that it is able to compute the fiber type and conductor exponent at $p = 2$.
- List all genus 2 curves over $\mathbb{Q}$ whose *Jacobians* have good reduction outside 2, up to isomorphism over $\mathbb{Q}$.[10]
- Verify that the genus 2 curves in Smart's putative isogeny classes [108] are actually isogenous. More generally, devise and implement an algorithm for determining with proof whether the Jacobians of two given genus 2 curves are isogenous over $\mathbb{Q}$. Better still, given a genus 2 curve over $\mathbb{Q}$, list all others which have an isogenous Jacobian.
- Assemble a list of genus 2 curves over $\mathbb{Q}$ of small conductor, analogous to the lists for elliptic curves in [6] and [29].[11]

---

[10] If a curve has good reduction outside 2, then so does its Jacobian. Thus the list in question should at least contain the 428 curves in [108].

[11] Mestre [79] proves that the conductor N of an g-dimensional abelian variety satisfies $N > (10.32)^g$, assuming standard conjectures about the L-series. Thus one expects the minimal conductor for genus 2 curves to be somewhat larger than in the genus 1 case.

It is the author's hope that this survey will entice the reader into working on some of these projects.

Acknowledgements

An enormous number of people have helped me gather an enormous number of references! But I thank especially Noam Elkies, for many insightful comments on an earlier draft of this survey.

References

[1] Abramovich, D., Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: "Rational torsion of prime order in elliptic curves over number fields," [Astérisque No. 228 (1995), 3, 81–100] by S. Kamienny and B. Mazur, Columbia University Number Theory Seminar (New York, 1992), *Astérisque* No. 228 (1995), 3, 5–17.

[2] Abramovich, D., Uniformité des points rationnels des courbes algébriques sur les extensions quadratiques et cubiques, *C. R. Acad. Sci. Paris Sér. I Math.* **321** (1995), no. 6, 755–758.

[3] Adleman, L. and Huang, M.-D., *Primality testing and abelian varieties over finite fields*, *Lecture Notes in Math.* **1512**, Springer-Verlag, Berlin, 1992.

[4] Adleman, L. and Huang, M.-D., Counting rational points on curves and abelian varieties over finite fields (extended abstract), in this volume.

[5] Adleman, L., DeMarrais, J. and Huang, M.-D., A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, *Algorithmic number theory (Ithaca, NY, 1994)*, 28–40, *Lecture Notes in Comput. Sci.* **877**, Springer, Berlin, 1994.

[6] Birch, B. and Kuyk, W. (eds.), Modular functions of one variable IV, *Lecture Notes in Math.* **476**, Springer-Verlag, 1975.

[7] Baker, A. and Coates, J., Integer points on curves of genus 1, *Proc. Cambridge Philos. Soc.* **67** (1970), 595–602.

[8] Bertrand, L., Computing a hyperelliptic integral using arithmetic in the Jacobian of the curve, *Appl. Algebra Engrg. Comm. Comput.* **6** (1995), no. 4-5, 275–298.

[9] Birch, B. and Merriman, J. R., Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* (3) **24** (1972), 385–394.

[10] Bost, J.-B. and Mestre, J.-F., Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2, *Gaz. Math.*, No. 38 (1988), 36–64.

[11] Bremner, A., Some quartic curves with no points in any cubic field, *Proc. London Math. Soc. (3)* **52** (1986), no. 2, 193–214.

[12] Bremner, A. and Jones, J., On the equation $x^4 + mx^2y^2 + y^4 = z^2$, *J. Number Theory* **50** (1995), no. 2, 286–298.

[13] Bremner, A., Lewis, D. J., and Morton, P., Some varieties with points only in a field extension, *Arch. Math. (Basel)* **43** (1984), no. 4, 344–350.

[14] Brumer, A., The rank of $J_0(N)$, Columbia University Number Theory Seminar (New York, 1992), *Astérisque* No. 228 (1995), 3, 41–68.

[15] Brumer, A., Curves with real multiplications, in preparation.

[16] Cantor, D. G., Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), 95–101.

[17] Cantor, D. G., On the analogue of the division polynomials for hyperelliptic curves, *J. Reine Angew. Math.* **447** (1994), 91–145.

[18] Caporaso, L., Harris, J. and Mazur, B., Uniformity of rational points, to appear in *J. Amer. Math. Soc.*

[19] Caporaso, L., Harris, J. and Mazur, B., How many rational points can a curve have?, *The moduli space of curves (Texel Island, 1994)*, 13–31, *Progr. Math.* **129**, Birkhäuser, Boston, 1995.

[20] Cassels, J. W. S., The Mordell-Weil group of curves of genus 2., in: M. Artin, J. Tate (eds.), *Arithmetic and Geometry I*, Birkhäuser, Boston, (1983), 27–60.

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

[22] CASSELS, J. W. S. AND FLYNN, E. V., *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc., Lecture Notes, Cambridge Univ. Press, 1996.

[23] CHABAUTY, C., Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris* **212** (1941), 882–885.

[24] CHEVALLEY, C. AND WEIL, A., Un théorème d'arithmétiques sur les courbes algébriques, *Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris* **195** (1930), 570–572.

[25] COATES, J., Construction of rational functions on a curve, *Proc. Cambridge Philos. Soc.* **68** (1970), 105–123.

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

[27] COOMBES, K. R. AND GRANT, D. R., On heterogeneous spaces, *J. London Math. Soc. (2)* **40** (1989), no. 3, 385–397.

[28] COUVEIGNES, J.-M., *Quelques calcules en théorie des nombres*, Thèse, Université de Bordeaux I, 1994.

[29] CREMONA, J., *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992.

[30] DAVENPORT, J. H., On the integration of algebraic functions, *Lecture Notes in Computer Science* **102**, Springer-Verlag, 1981.

[31] DE WEGER, B. M. M., A hyperelliptic Diophantine equation related to imaginary quadratic number fields with class number 2, *J. Reine Angew. Math.* **427** (1992), 137–156. Correction: *J. Reine Angew. Math.* **441** (1993), 217–218.

[32] DEM'JANENKO, V., Rational points on a class of algebraic curves, *Amer. Math. Soc. Transl.* **66** (1968), 246–272.

[33] ELKIES, N. D., Heegner point computations, *Algorithmic number theory (Ithaca, NY, 1994)*, 122–133, *Lecture Notes in Comput. Sci.* **877**, Springer, Berlin, 1994.

[34] ELKIES, N. D., Remarks on elliptic K-curves, preprint, 1993.

[35] EVERTSE, J.-H. AND GYŐRY, K., Effective finiteness results for binary forms with given discriminant, *Compositio Math.* **79** (1991), no. 2, 169–204.

[36] FALTINGS, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366. Erratum: *Invent. Math.* **75** (1984), 381.

[37] 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.

[38] FLYNN, E. V., Large rational torsion on abelian varieties, *J. Number Theory* **36** (1990), 257–265.

[39] FLYNN, E. V., Sequences of rational torsions on abelian varieties, *Invent. Math.* **106** (1991), 433–442.

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

[41] FLYNN, E. V., Descent via isogeny in dimension 2, *Acta Arith.* **66** (1994), 23–43.

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

[43] FLYNN, E. V., On a theorem of Coleman, *Manuscr. Math.* **88** (1995), 447–456.

[44] FLYNN, E. V., A flexible method for applying Chabauty's Theorem, to appear in *Compositio Math.*

[45] FLYNN, E. V., POONEN, B., AND SCHAEFER, E., Cycles of quadratic polynomials and rational points on a genus 2 curve, preprint, 1995.

[46] GOPPA, V. D., *Geometry and codes*, volume 24 of *Mathematics and its applications (Soviet series)*, Kluwer Acad. Publ., 1988.

[47] GORDON, D. AND GRANT, D., Computing the Mordell-Weil rank of Jacobians of curves of genus two, *Trans. Amer. Math. Soc.* **337** (1993), 807–824.

[48] GRANT, D., Formal groups in genus 2, *J. Reine Angew. Math.* **411** (1990), 96–121.

[49] GRANT, D., A curve for which Coleman's effective Chabauty bound is sharp, *Proc. Amer. Math. Soc.* **122** (1994), 317–319.

[50] HUANG, M.-D. AND IERARDI, D., Efficient algorithms for the effective Riemann-Roch problem and for addition in the Jacobian of a curve, *J. Symbolic Comput.* **18** (1994), 519–539.

[51] HUANG, M.-D. AND IERARDI, D., Counting rational points on curves over finite fields, IEEE Symposium on the Foundations of Computer Science, Palo Alto, CA, November 1993.

[52] KAMIENNY, S. AND MAZUR, B., Rational torsion of prime order in elliptic curves over number fields, Columbia University Number Theory Seminar (New York, 1992), *Astérisque* No. 228 (1995), 3, 81–100.

[53] Katz, N., Galois properties of torsion points on abelian varieties, *Invent. Math.* **62** (1981), no. 3, 481–502.
[54] Keller, W. and Kulesz, L., Courbes algébriques de genre 2 et 3 possedant de nombreux points rationnels, *C. R. Acad. Sci. Paris Sér. I Math.* **321** (1995), no. 11, 1469–1472.
[55] Klassen, M. and Schaefer, E., Arithmetic and geometry of the curve $y^3 + 1 = x^4$, to appear in *Acta Arith.*
[56] Koblitz, N., Hyperelliptic cryptosystems, *J. Cryptology* **1** (1989), no. 3, 139–150.
[57] Kulesz, L., Courbes algébriques de genre 2 possedant de nombreux points rationnels, *C. R. Acad. Sci. Paris Sér. I Math.* **321** (1995), no. 1, 91–94.
[58] Laska, M., *Elliptic curves over number fields with prescribed reduction type*, Aspects of Mathematics, E4. Friedr. Vieweg & Sohn, Braunschweig; distributed by Heyden & Son, Inc., Philadelphia, Pa., 1983.
[59] Leprévost, F., Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13, *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), 451–454.
[60] Leprévost, F., Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21, *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), 771–774.
[61] Leprévost, F., Torsion sur des familles de courbes de genre g, *Manuscripta Math.* **75** (1992), 303–326.
[62] Leprévost, F., Famille de courbes hyperelliptiques de genre g munies d'une classe de diviseurs rationnels d'ordre $2g^2+4g+1$, *Seminaire de Théorie des Nombres, 1991–92*, 107–119, Progr. Math. 116, Birkhäuser, 1993.
[63] Leprévost, F., Points rationnels de torsion de jacobiennes de certaines courbes de genre 2, *C. R. Acad. Sci. Paris Sér. I Math.* **316** (1993), 819–821.
[64] Leprévost, F., Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes, to appear in *J. Reine Angew. Math.*
[65] Leprévost, F., Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genres $g \geq 1$, preprint, 1996.
[66] Lercier, R. and Morain, F., Counting the number of points on elliptic curves over finite fields: strategies and performances, *Advances in cryptology—EUROCRYPT '95 (Saint-Malo, 1995)*, 79–94, *Lecture Notes in Comput. Sci.* **921**, Springer, Berlin, 1995.
[67] Lercier, R. and Morain, F., Counting points on elliptic curves over $\mathbb{F}_{p^n}$ using Couveignes's algorithm, preprint, 1995.
[68] Liu, Q., Modèles minimaux des courbes de genre deux, *J. Reine Angew. Math.* **453** (1994), 137–164.
[69] Liu, Q., Conducteur et discriminant minimal de courbes de genre 2, *Compositio Math.* **94** (1994), no. 1, 51–79.
[70] Liu, Q., Modèles entiers d'une courbe hyperelliptique sur un corps de valuation discrete, to appear in *Trans. Amer. Math. Soc.*
[71] Manin, J., The p-torsion of elliptic curves is uniformly bounded, *Isv. Akad. Nauk. SSSR Ser. Mat.* **33** (1969); *Amer. Math. Soc. Transl.*, 433–438.
[72] Mazur, B., Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186 (1978).
[73] Mazur, B. and Tate, J., Points of order 13 on elliptic curves, *Invent. Math.* **22** (1973/74), 41–49.
[74] McCallum, W., On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve, *Invent. Math.* **93** (1988), no. 3, 637–666.
[75] McCallum, W., On the method of Coleman and Chabauty, *Math. Ann.* **299** (1994), no. 3, 565–596.
[76] Merel, L., Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1996), no. 1-3, 437–449.
[77] Merriman, J. R., *Binary forms and the reduction of curves*, D. Phil. thesis, Oxford Univ., 1970.
[78] Merriman, J. R. and Smart, N. P., Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point, *Math. Proc. Camb. Phil. Soc.* **114** (1993), 203–214. Corrigenda: *Math. Proc. Camb. Phil. Soc.* **118** (1995), 189.
[79] Mestre, J.-F., Formules explicites et minorations de conducteurs de variétés algébriques, *Compositio Math.* **58** (1986), no. 2, 209–232.

[80] MESTRE, J.-F., Courbes hyperelliptiques à multiplications réelles, *Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988)*, Exp. No. 34, 6 pp., *Univ. Bordeaux I, Talence.*

[81] MESTRE, J.-F., Courbes hyperelliptiques à multiplications réelles, *C. R. Acad. Sci. Paris Sér. I Math.* **307** (1988), no. 13, 721–724.

[82] MESTRE, J.-F., Construction de courbes de genre 2 a partir de leurs modules, *Effective methods in algebraic geometry (Castiglioncello, 1990)*, 313–334, *Progr. Math.* **94**, Birkhäuser Boston, Boston, MA, 1991.

[83] MILNE, J. S., Abelian Varieties, in: Cornell, G., Silverman, J.H. (eds.), *Arithmetic geometry*, 103–150, Springer-Verlag, New York, 1986.

[84] MILNE, J. S., Jacobian Varieties, in: Cornell, G., Silverman, J.H. (eds.), *Arithmetic geometry*, 167–212, Springer-Verlag, New York, 1986.

[85] MORDELL, L. J., On some sextic diophantine equations of genus 2, *Proc. Amer. Math. Soc.* **21** (1969), 347–350.

[86] MUMFORD, D., On the equations defining abelian varieties I, *Invent. Math.* **1** (1966), 287–354.

[87] MUMFORD, D., On the equations defining abelian varieties II, *Invent. Math.* **3** (1966), 75–135.

[88] MUMFORD, D., On the equations defining abelian varieties III, *Invent. Math.* **3** (1966), 215–244.

[89] MURABAYASHI, N., On normal forms of modular curves of genus 2, *Osaka J. Math* **29** (1992), 405–418.

[90] NAMIKAWA, Y. AND UENO, K., The complete classification of fibres in pencils of curves of genus two, *Manuscripta Math.* **9** (1973), 143–186.

[91] OGAWA, H., Curves of genus 2 with a rational torsion divisor of order 23, *Proc. Japan Acad. Ser. A Math. Sci.* **70** (1994), 295–298.

[92] OGG, A., Abelian curves of 2-power conductor, *Math. Proc. Camb. Phil. Soc.* **62** (1966), 143–148.

[93] OGG, A., On pencils of curves of genus two, *Topology* **5** (1966), 355–362.

[94] OGG, A., Rational points on certain elliptic modular curves, *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pp. 221–231, *Amer. Math. Soc., Providence, R.I.*, 1973.

[95] OORT, F., Hyperelliptic curves over number fields, in H. Popp (ed.), *Classification of algebraic varieties and compact complex manifolds*, Springer-Verlag, 1974, 211–218.

[96] PACELLI, P., Uniform boundedness for rational points, preprint, 1996.

[97] PARSHIN, A. N., Minimal models of curves of genus 2, and homomorphisms of abelian varieties defined over a field of finite characteristic, *Math. of USSR. Izvestija* **6** (1972), 65–108.

[98] PILA, J., Frobenius maps of abelian varieties and finding roots of unity in finite fields, *Math. Comp.* **55** (1990), no. 192, 745–763.

[99] POONEN, B., The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$, preprint, 1996.

[100] PYLE, E., *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$*, Ph. D. thesis, Univ. of Calif. at Berkeley, 1995.

[101] RODRIGUEZ-VILLEGAS, F., Arithmetic intersection in a Siegel threefold, in preparation.

[102] SCHAEFER, E. F., 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995) 219–232.

[103] SCHOOF, R., Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), no. 170, 483–494.

[104] SHAFAREVICH, I., Algebraic number fields, *Proc. Internat. Congr. Math., Stockholm 1962*, Institute Mittag-Leffler, Djursholm, 1963, 163–176. English translation: *Amer. Math. Soc. Transl.* (2) **31** (1963), 25–39.

[105] SHIMURA, G., On the field of rationality for an abelian variety, *Nagoya Math. J.* **45** (1972), 167–178.

[106] SILVERMAN, J., Rational points on certain families of curves of genus at least 2, *Proc. London Math. Soc. (3)* **55** (1987), no. 3, 465–481.

[107] SILVERMAN, J., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

[108] SMART, N. P., S-unit equations, binary forms and curves of genus 2, preprint, 1996.

[109] STAHLKE, C., Algebraic curves over $\mathbb{Q}$ with many rational points and minimal automorphism group, preprint, 1996.

[110] Stoll, M., Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil group of rank at least 19, *C. R. Acad. Sci. Paris Sér. I Math.* **321** (1995), 1341–1345.

[111] Taylor, R. and Wiles, A., Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141** (1995), no. 3, 553–572.

[112] Top, J., *Hecke L-series related with algebraic cycles or with Siegel modular forms*, Ph. D. thesis, Utrecht, 1989.

[113] Tsfasman, M. A. and Vladut, S. G., *Algebraic geometric codes*, volume 58 of *Mathematics and its applications (Soviet series)*, Kluwer Acad. Publ., 1991.

[114] Volcheck, E., Computing in the Jacobian of a plane algebraic curve, *Algorithmic number theory (Ithaca, NY, 1994)*, 221–233, *Lecture Notes in Comput. Sci.* **877**, Springer, Berlin, 1994.

[115] Volcheck, E., Addition in the Jacobian of a curve over a finite field, preprint, 1995.

[116] Wiles, A., Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

Department of Mathematics, Princeton University, Princeton, NJ 08544-1000, USA
E-mail address: `poonen@math.princeton.edu`