

# Modular equations for hyperelliptic curves

P. Gaudry and É. Schost

LIX – GAGE

École polytechnique

91128 Palaiseau, France

{gaudry@lix, schost@gage}.polytechnique.fr

July 15, 2002

## Abstract

We define modular equations describing the  $\ell$ -torsion subgroups of the Jacobian of a hyperelliptic curve. Over a finite base field, we prove factorization properties that extend the well-known results used in Atkin's improvement of Schoof's genus 1 point counting algorithm.

2000 *Mathematics Subject Classification*: Primary 11Y40; Secondary 11G20, 11Y16.

## Introduction

Modular equations relating invariants of  $\ell$ -isogenous elliptic curves are a fundamental tool in computational arithmetic geometry. A great effort has been devoted to obtain equations sparser or with smaller coefficients than the classical polynomials  $\Phi_\ell$  [12], so nowadays these equations can be computed efficiently even for quite large  $\ell$ . One of their important applications is the determination of the cardinality of an elliptic curve defined over a finite field [23]: the best method to date, at least for prime finite fields, is the Schoof-Elkies-Atkin algorithm in which the  $\ell$ -torsion structure is widely used.

Nevertheless, very little is known about similar equations for higher genus curves. Since the hyperelliptic case is the best suited for computations, we restrict to this situation. Our goal in this article is then twofold:

- We define modular equations for hyperelliptic curves, without appealing to modular forms. In the particular case of genus 1, our equations coincide with those introduced by Charlap, Cooley and Robbins in [11].
- When the base field is finite, we prove that the well-known factorization properties of genus 1 modular equations extend to our higher genus construction. This makes them amenable for use in higher genus extensions of the Atkin improvement of Schoof's initial algorithm [26].

Here is a brief overview of our construction. Consider an hyperelliptic curve  $\mathcal{C}$  of genus  $g$ ,  $\mathbf{Jac}(\mathcal{C})$  its Jacobian, and  $\ell$  a prime. The quotient of the Jacobian by a subgroup of order  $\ell$  is an abelian variety  $\ell$ -isogenous to  $\mathbf{Jac}(\mathcal{C})$ , but in genus greater than 1, it is in general not the Jacobian of a curve. General abelian varieties are more intricate to handle than Jacobians of curves, for which invariants can be easily computed, so we rather study directly the  $\ell$ -torsion subgroup of the Jacobian. Our modular equations are thus defined using the group structure of the  $\ell$ -torsion subgroup.

More precisely, these equations are univariate polynomials whose roots are in correspondence with the cyclic subgroups of the  $\ell$ -torsion group. This definition avoids the use of modular forms, so it is valid over any perfect field. The construction is very similar to that of resolvents in Galois theory; as such, when the base field is finite, the factorization patterns of the modular equations are very specific, and carry enough information to be of use in higher genus Schoof point-counting algorithms. As an example, we have detailed the relationship between the 3-torsion modular equation of a genus 2 curve and the cardinality of its Jacobian modulo 3. These results are now used for point-counting within Magma's hyperelliptic curve package [1].

The paper is organized as follows. In Section 1, we precise the notations used in the sequel. The modular equations are defined in Section 2, where we also give their basic properties and detail the example of genus 1. In Section 3, we prove that the modular equations have the expected specialization properties. This is crucial for the computational point of view, which is studied in Section 4. In Section 5, we finally consider the finite field case, and show how the factorization patterns of our modular equations extend the well-known case of genus 1; we apply this for the point-counting problem.

**Acknowledgments.** We thank François Morain for his numerous comments and suggestions. We are grateful to John Boxall for giving us references about the Manin-Mumford conjecture. The heaviest computations were done on the machines of the CNRS – École polytechnique MEDICIS computation center [2], using the Magma computer algebra system [1]. The second author is a member of the TERA project [3].

## 1 Notations

Let  $k$  be a perfect field of characteristic different from 2 and  $\mathcal{C}$  a genus  $g$  hyperelliptic curve defined over  $k$ . We suppose that the affine part of  $\mathcal{C}$  is defined by the equation  $y^2 = f(x)$ , with  $f$  monic of degree  $2g + 1$  and for simplicity, we shall say that  $\mathcal{C}$  is the curve defined by  $y^2 = f(x)$ . The unique point at infinity on  $\mathcal{C}$  is denoted by  $\infty$ .

We also assume that the characteristic of  $k$  is different from  $2g + 1$ , so that we can transform  $f(x)$  into a polynomial whose coefficient in  $x^{2g}$  is zero. This simplification is similar to what is often done in genus 1 when taking an equation of the form  $y^2 = x^3 + Ax + B$ . In principle, our results also hold in characteristic  $2g + 1$ , but with different equations.

We denote the Jacobian of  $\mathcal{C}$  by  $\mathbf{Jac}(\mathcal{C})$ . This is a projective variety defined over  $k$ ; the canonical injection  $\mathcal{C} \rightarrow \mathbf{Jac}(\mathcal{C})$  associates to  $P \in \mathcal{C}$  the divisor class of  $P - \infty$ ; it is also defined over  $k$ .

If  $K$  is an extension field of  $k$ , we may distinguish the curves defined on  $k$  and  $K$  by  $y^2 = f(x)$ , by denoting them  $\mathcal{C}/k$  and  $\mathcal{C}/K$ . Then the injection  $\mathcal{C}/K \rightarrow \mathbf{Jac}(\mathcal{C}/K)$  extends the injection  $\mathcal{C}/k \rightarrow \mathbf{Jac}(\mathcal{C}/k)$ , and the group law on  $\mathbf{Jac}(\mathcal{C}/K)$  extends that of  $\mathbf{Jac}(\mathcal{C}/k)$ .

In particular, let  $\bar{k}$  be an algebraic closure of  $k$ . Then for a prime  $\ell$ , we will denote by  $\mathbf{Jac}[\ell]$  the subgroup of  $\ell$ -torsion elements of  $\mathbf{Jac}(\mathcal{C}/\bar{k})$ .

Let  $\tau$  be the hyperelliptic involution on  $\mathcal{C}/\bar{k}$ , and let  $\iota$  denote the injection  $\mathcal{C}/\bar{k} \rightarrow \mathbf{Jac}(\mathcal{C}/\bar{k})$ . As a consequence of the Riemann-Roch theorem, any element in  $\mathbf{Jac}(\mathcal{C}/\bar{k})$  can be uniquely represented by a divisor of the form  $D = \sum_{1 \leq j \leq r} \iota(P_j)$  with the following properties:

1. all  $P_j$  are points on the affine part of  $\mathcal{C}/\bar{k}$ ,
2.  $P_j \neq \tau(P_{j'})$  for all  $j \neq j'$ ,
3.  $r$  is at most  $g$ .

The integer  $r$  is called the *weight* of  $D$ .

Let  $D$  and  $\{P_j\}_{1 \leq j \leq r}$  be as above; since the points  $P_j$  are not at infinity, we may take  $P_j = (x_j, y_j, 1)$ . Then the *Mumford-Cantor* representation of  $D$  [24, 9] is defined by

$$D = \langle u(x), v(x) \rangle = \langle x^r + u_{r-1}x^{r-1} + \cdots + u_0, v_{r-1}x^{r-1} + \cdots + v_0 \rangle,$$

where  $u = \prod_{1 \leq j \leq r} (x - x_j)$  and  $v(x_j) = y_j$  holds with suitable multiplicities, so that  $u$  divides  $v^2 - f$ . Since  $k$  is perfect, the divisor  $D$  is defined over a field  $K$  containing  $k$  if and only if the polynomials  $u$  and  $v$  have coefficients in  $K$ .

For  $j$  in  $0, \dots, r-1$ , we will denote by  $u_j(D)$  (resp.  $v_j(D)$ ) the coefficient  $u_j$  (resp.  $v_j$ ) in this representation.

## 2 Modular equations

### 2.1 Definition

Let  $\ell$  be an odd prime different from the characteristic of  $k$ . In this paragraph, we define the  $\ell$ -th modular equation of a genus  $g$  hyperelliptic curve  $\mathcal{C}$  defined over  $k$ .

To this end, we consider the  $\ell$ -torsion divisors in  $\mathbf{Jac}(\mathcal{C}/\bar{k})$ . The assumption that  $\ell$  differs from the characteristic of  $k$  implies that the number of  $\ell$ -torsion divisors of non-zero weight is  $\ell^{2g} - 1$  [21]. From now on, we assume that all these divisors have weight exactly  $g$ ; see Subsection 2.3 for the relevance of this assumption.

**Genericity Assumption** *All non-zero  $\ell$ -torsion divisors in  $\mathbf{Jac}(\mathcal{C}/\bar{k})$  have weight  $g$ .*

Let  $D$  be an  $\ell$ -torsion divisor. The divisors

$$\langle D \rangle = \left\{ - \left[ \frac{\ell-1}{2} \right] D, \dots, -D, 0, D, \dots, \left[ \frac{\ell-1}{2} \right] D \right\}$$

form a cyclic subgroup of cardinality  $\ell$  in  $\mathbf{Jac}[\ell]$ . Our objective is to be able to “separate” these subgroups, using only algebraic constructions. To this effect we choose a function  $t_\ell(D)$  with values in  $\bar{k}$ , which takes a constant value on each of the subgroups  $\langle D \rangle$ . Our modular equations may then be thought as a minimal polynomial of  $t_\ell$ .

Precisely, we define  $t_\ell$  as the following sum:

$$t_\ell(D) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} u_{g-1}([i]D). \quad (1)$$

Our genericity assumption implies that this sum is well-defined for all non-zero  $\ell$ -torsion divisors  $D$ . Note that  $[-i]D$  and  $[i]D$  have the same  $u_{g-1}$ -coordinate, so even though we restrict the number of summands to  $(\ell-1)/2$ ,  $t_\ell(D)$  depends only on the subgroup generated by  $D$ , as requested.

We next define the polynomial  $\chi_\ell \in \bar{k}[T]$ , whose roots are the values taken by  $t_\ell$  on the non-zero  $\ell$ -torsion divisors:

$$\chi_\ell = \prod_{D \in \mathbf{Jac}[\ell] \setminus \{0\}} (T - t_\ell(D)).$$

The polynomial  $\chi_\ell$  is a  $(\ell-1)$ -th power in  $\bar{k}[T]$ . Indeed  $\mathbf{Jac}[\ell] \setminus \{0\}$  can be written as the disjoint union of the  $\frac{\ell^2 g - 1}{\ell - 1}$  sets  $\langle D \rangle \setminus \{0\}$ , and the function  $t_\ell(D)$  takes a constant value on each part of this partition.

We now show that  $\chi_\ell$  is actually in  $k[T]$ . Let  $\sigma$  be in  $\text{Gal}(\bar{k}/k)$ . If  $D$  is any divisor,  $\sigma(u_{g-1}(D)) = u_{g-1}(\sigma(D))$ . Also,  $\sigma$  commutes with the group law, whence  $\sigma([i]D) = [i]\sigma(D)$ , so  $\sigma$  induces a permutation among the non-zero  $\ell$ -torsion divisors. If  $D$  is such a divisor, then equality

$$\sigma(t_\ell(D)) = t_\ell(\sigma(D))$$

obviously holds. Since  $\sigma$  permutes the  $\ell$ -torsion divisors, this equality shows that  $\chi_\ell$  is left invariant by  $\sigma$ , so  $\chi_\ell$  is in  $k[T]$ . Since  $k$  is a perfect field, and  $\chi_\ell$  is a  $(\ell-1)$ -th power in  $\bar{k}[T]$ , there exists a polynomial  $\Xi_\ell$  with coefficients in  $k$  such that  $\chi_\ell = \Xi_\ell^{\ell-1}$ .

**Definition 1** *The unique monic polynomial  $\Xi_\ell$  such that  $\chi_\ell = \Xi_\ell^{\ell-1}$  is called the  $\ell$ -th modular equation of  $\mathcal{C}$ .*

The polynomial  $\Xi_\ell$  has degree  $\frac{\ell^2 g - 1}{\ell - 1}$ . To emphasize the dependence on the curve  $\mathcal{C}$ , it may also be denoted by  $\Xi_\ell(\mathcal{C})$ .

The rest of this article is devoted to describe the main properties of these equations, how to compute them and how to use them for cardinality computation, in the case when  $k$  is a finite field.

**Remark 1** Our choice of the function  $t_\ell$  is arbitrary. In Section 5, we show that the interesting case is when  $\Xi_\ell$  is squarefree, which happens when  $t_\ell$  takes distinct values on distinct cyclic subgroups. Unfortunately, this will not be the case for all curves; then, an alternative choice of  $t_\ell$  may solve the problem:

Instead of considering the sum of the  $u_{g-1}$ -coordinates of half of the divisors in the subgroup, we choose some integer  $k$  and form the sum of the  $k$ -th power of any linear combination of all the

coordinates  $(u, v)$ . Then, we might have to extend the summation in Equation (1) to all elements in the subgroup  $\langle D \rangle$ , since not all coordinates are negation-invariant. The subsequent results follow in a similar manner for such alternative constructions.

Yet in practice, choosing the coordinate  $u_{g-1}$  yields the polynomial with smallest coefficients when working over  $\mathbb{Q}$ , and in most of our experiments in genus 1 and 2, this polynomial turned out to be squarefree, as requested.

**Remark 2** In the sequel, we will often consider curves with generic coefficients. Thus we define for once the *generic curve of genus  $g$*  as the curve of equation

$$\mathcal{C}_g : y^2 = x^{2g+1} + F_{2g-1}x^{2g-1} + \cdots + F_0,$$

over the rational function field  $\mathbb{Q}(F_0, \dots, F_{2g-1})$ . In this case, the polynomial  $\Xi_\ell$  belongs to  $\mathbb{Q}(F_0, \dots, F_{2g-1})[T]$ , and satisfies the following homogeneity property.

**Theorem 1** *The  $\ell$ -th modular equation of the curve  $\mathcal{C}_g$  is weighted homogeneous, when giving weight 1 to  $T$  and weight  $2g + 1 - i$  to  $F_i$  for  $i = 0, \dots, 2g - 1$ .*

*Proof.* Let  $\lambda$  be a non-zero rational, and let  $\widetilde{\mathcal{C}}_g$  be the curve defined by

$$y^2 = x^{2g+1} + \widetilde{F_{2g-1}}x^{2g-1} + \cdots + \widetilde{F_0},$$

where  $\widetilde{F}_i = \lambda^{2g+1-i}F_i$ , for  $i = 1, \dots, 2g - 1$ . Then the map  $\varphi : \mathcal{C}_g \rightarrow \widetilde{\mathcal{C}}_g$  defined by  $\varphi(x, y) = (\lambda x, \lambda^{2g+1}y)$  is an isomorphism between  $\mathcal{C}_g$  and  $\widetilde{\mathcal{C}}_g$ . This isomorphism extends to an isomorphism between  $\mathbf{Jac}(\mathcal{C}_g)$  and  $\mathbf{Jac}(\widetilde{\mathcal{C}}_g)$ , which acts as follows in Mumford-Cantor's representation:

$$(u_0, \dots, u_{g-1}, v_0, \dots, v_{g-1}) \mapsto (\lambda^g u_0, \dots, \lambda u_{g-1}, \lambda^{2g+1} v_0, \dots, \lambda^{g+2} v_{g-1}).$$

Given an  $\ell$ -torsion divisor  $D$  on  $\mathbf{Jac}(\mathcal{C}_g)$ , the value  $t_\ell(D)$  is sent to  $\lambda t_\ell(D)$ . Thus

$$\Xi_\ell(F_0, \dots, F_{2g-1}, t_\ell) = 0 \iff \Xi_\ell(\lambda^{2g+1}F_0, \dots, \lambda^2F_{2g-1}, \lambda t_\ell) = 0.$$

This proves the theorem. □

The weighted homogeneity implies that not all monomials appear in the modular equation for the generic curve. As a consequence, our modular equations are somewhat sparse, and we shall see below that for elliptic curves they provide a much smaller alternative to the classical  $\Phi_\ell$  modular polynomials.

**Remark 3** In our formalism, the modular equation for 2-torsion  $\Xi_2$  is ill-defined in genus greater than 1. Indeed, the genericity assumption for 2-torsion is never satisfied, since the  $2g + 1$  roots of the defining polynomial  $f(x)$  give the abscissae of  $2g + 1$  weight 1 divisors of 2-torsion. In the particular case of elliptic curves, we can set  $\Xi_2 = f$ .

## 2.2 The elliptic case

We illustrate our definition on an elliptic curve  $\mathcal{E}$ , given by an equation  $y^2 = f(x)$ , with  $f$  monic of degree 3. In genus 1, the genericity assumption is always verified, since the only divisor whose weight is not maximal is zero.

If  $P = (x, y)$  is a point on  $\mathcal{E}$  and  $i$  a positive integer, the coordinates of  $[i]P$  are rational functions of  $P$ , see [29]:

$$[i]P = \left( \frac{\phi_i(P)}{\psi_i(P)^2}, \frac{\omega_i(P)}{\psi_i(P)^3} \right).$$

The polynomials  $\phi_i(P)$ ,  $\psi_i(P)^2$ , and also  $\psi_i(P)$  if  $i$  is odd, are polynomials in  $x$  only. To follow the notation of the previous subsection, we see them as polynomials in the variable  $T$ .

Given an odd prime  $\ell$ , the abscissae of the  $\ell$ -torsion points are the roots of  $\psi_\ell$ . Let  $P$  be such a point; for  $i$  in  $1, \dots, \frac{\ell-1}{2}$ , the denominator in the rational function

$$\left( \frac{\phi_i(P)}{\psi_i(P)^2} \right)$$

is coprime to  $\psi_\ell$ . The image of this rational function modulo  $\psi_\ell$  is a polynomial  $h_{i,\ell}$  in  $k[T]$  which gives the abscissa of  $[i]P$  in terms of the abscissa of  $P$ , for  $P$  of  $\ell$ -torsion. Then, for all  $\ell$ -torsion points  $P$ ,  $t_\ell(P)$  is given by the sum

$$t_\ell(P) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} h_{i,\ell}(x(P)).$$

The polynomial  $\chi_\ell$  is thus the characteristic polynomial of  $\sum_{1 \leq i \leq \frac{\ell-1}{2}} h_{i,\ell}$  modulo  $\psi_\ell$ , and the modular equation  $\Xi_\ell \in k[T]$  is the  $(\ell - 1)$ -th root of  $\chi_\ell$ .

Let us take  $f = x^3 + F_1x + F_0$ , defining what we called the generic curve of genus 1 over  $\mathbb{Q}(F_0, F_1)$ . Then the first values of  $\Xi_\ell$  are:

$$\Xi_3 = T^4 + 2F_1T^2 + 4F_0T - \frac{1}{3}F_1^2,$$

$$\Xi_5 = T^6 + 20F_1T^4 + 160F_0T^3 - 80F_1^2T^2 - 128F_1F_0T - 80F_0^2,$$

$$\Xi_7 = T^8 + 84F_1T^6 + 1512F_0T^5 - 1890F_1^2T^4 - 9072F_1F_0T^3 + (-21168F_0^2 + 644F_1^3)T^2 + 5832F_1^2F_0T - 567F_1^4,$$

$$\begin{aligned} \Xi_{11} = & T^{12} + 550F_1T^{10} + 27500F_0T^9 - 103125F_1^2T^8 - 1650000F_1F_0T^7 + (-13688400F_0^2 + \\ & 645700F_1^3)T^6 + 20625000F_1^2F_0T^5 + (35793120F_1F_0^2 - 11407385F_1^4)T^4 + \\ & (34041920F_0^3 - 58614160F_1^3F_0)T^3 + (-175832976F_1^2F_0^2 - 2177802F_1^5)T^2 + \\ & (-235016704F_1F_0^3 + 1351692F_1^4F_0)T - 110680064F_0^4 + 6297984F_1^3F_0^2 - 321651F_1^6. \end{aligned}$$

These polynomials were already considered by Charlap, Cooley and Robbins in [11], where the authors constructed them via modular forms. Our modular equations are a generalization to higher genus.

**Remark 4** Except for  $\Xi_3$  for which a factor  $\frac{1}{3}$  occurs, there are no denominators in the coefficients of the modular equations of the generic elliptic curve. This fact is proven in [11] using properties of modular forms. In higher genus we do not know a priori whether there are denominators in the modular equations of the generic curves. The computation in Section 4 shows that the modular equation  $\Xi_3$  of the genus 2 generic curve does not have any denominator, but we do not expect this to be true in general.

### 2.3 Relevance of the genericity assumption

As mentioned in the previous subsection, the genericity assumption is satisfied in genus 1 for all curves, for all torsion indices coprime to the characteristic of the base field.

This condition is also satisfied for all genus 2 curves for 3-torsion. To see this, consider a genus 2 curve  $\mathcal{C}$ . A divisor with non maximal weight is of the form  $P - \infty$  for some point  $P \in \mathcal{C}$ . Then the equality  $[3](P - \infty) = 0$  can be rewritten as  $[2](P - \infty) = -(P - \infty)$ , which implies that  $P = \infty$  by the Riemann-Roch theorem. Thus except zero, all 3-torsion divisors have weight 2.

More generally, the genericity assumption is closely related to the Manin-Mumford conjecture which states that the Jacobian of a curve over the complex field contains only finitely many torsion elements of weight 1. More generally, Lang's conjecture, which is now known to be true [17, p. 435], implies that the Jacobian of a given curve over the complex field contains only finitely many torsion elements of non-maximal weight, as soon as this Jacobian is simple. As a consequence, for a given curve with simple Jacobian, the number of primes  $\ell$  for which the genericity assumption does not hold is finite, hence the name.

Note finally that this condition is true for all  $\ell$  for the curve of genus 2 defined by  $y^2 = x^5 + 5x^3 + x$ , see [7]. Using the specialization theorem given in Section 3, we deduce that the genericity assumption is also true for all  $\ell$  for the generic curve of genus 2.

## 3 Specialization properties

In the elliptic curve point-counting methods, a widely used strategy is to compute modular equations over the rationals and then reduce them modulo the characteristic of the base field. In this section, we want to legitimate this approach for our modular equations. Our purpose is thus to prove the intuitive result that the reduction of the modular equations of a curve  $\mathcal{C}$  coincide with the modular equations of the reduction of  $\mathcal{C}$ .

We are interested in both specializing the coefficients of a curve defined over a rational function field, and also in reducing the coefficients of a curve defined over a number field. Thus we work in the setting of local and global fields, which will help encompass both notions. Throughout this section, *we assume once and for all that all the fields are perfect.*

We recall below the definition of reduction and good reduction of a curve defined on a local or a global field. Then Theorem 2 proves that if  $\mathcal{C}$  is a curve with good reduction, and if the reduced curve satisfies the genericity assumption for some prime  $\ell$ , then this is also the case for  $\mathcal{C}$  and its

$\ell$ -modular equation specializes as expected; the main ingredient of the proof is the injectivity of the reduction of the  $\ell$ -torsion, as proven for instance in [17]. We will use Theorem 2 for computational purposes in Section 4.

First, a few notations are necessary. If  $(K, v)$  is a non-Archimedean local field, we denote by

$$R_K = \{a \in K, v(a) \leq 1\}, \quad \mathfrak{m}_K = \{a \in K, v(a) < 1\}$$

respectively the ring of integers of  $K$  and its maximal ideal.

With these notations, let  $\mathcal{C} : y^2 = f(x)$  be a hyperelliptic curve defined over  $K$ , such that  $f$  has its coefficients in  $R_K$ . We say that  $\mathcal{C}$  has *good reduction* if  $2\text{disc}(f)$  is not in  $\mathfrak{m}_K$ . In this case, the curve defined by the reduction of  $y^2 = f(x)$  modulo  $\mathfrak{m}_K$  has the same genus as  $\mathcal{C}$ . This curve is called the reduction of  $\mathcal{C}$ ; its Jacobian is the reduction of the Jacobian of  $\mathcal{C}$  modulo  $\mathfrak{m}_K$ , see [22].

If now  $\mathcal{K}$  is a global field and  $v$  a non-Archimedean valuation of  $\mathcal{K}$ , the completion  $K$  of  $\mathcal{K}$  at  $v$  is a local field. Thus the above discussion enables us to define the notion of good reduction at  $v$  of a curve  $\mathcal{C}$  defined over  $\mathcal{K}$ : if  $\mathcal{C}$  is defined by an equation with coefficients in  $\mathcal{K} \cap R_K$ ,  $\mathcal{C}$  has good reduction at  $v$  if  $\mathcal{C}/K$  has good reduction. Then the specialization properties are stated as follows.

**Theorem 2** *Let  $\mathcal{K}$  be a global field, and  $v$  a non-Archimedean valuation of  $\mathcal{K}$ . Let  $K$  be the completion of  $\mathcal{K}$  at  $v$ ,  $R_K$  its ring of integers,  $\mathfrak{m}_K$  its maximal ideal and  $k$  the residual field  $R_K/\mathfrak{m}_K$ . Let  $\mathcal{C}$  be a genus  $g$  hyperelliptic curve defined over  $\mathcal{K}$ , and  $\ell$  an odd prime different from the characteristic of  $k$ .*

*Assume that  $\mathcal{C}$  is defined by an equation with coefficients in  $\mathcal{K} \cap R_K$ , that  $\mathcal{C}$  has good reduction at  $v$ , and that the reduced curve  $\overline{\mathcal{C}}$  satisfies the genericity assumption for the prime  $\ell$ . Then  $\mathcal{C}$  satisfies the genericity assumption for  $\ell$ , all coefficients of  $\Xi_\ell(\mathcal{C})$  are in  $\mathcal{K} \cap R_K$  and  $\Xi_\ell(\overline{\mathcal{C}}) = \Xi_\ell(\mathcal{C})$  modulo  $\mathfrak{m}_K$ .*

Before proving the theorem, a few comments are in order. Theorem 2 applies to specializations at non-Archimedean places of number fields, so for instance it allows for the reduction modulo prime numbers of modular equations with rational coefficients. The second obvious application is the specialization of modular equations with coefficients in *univariate* function fields defined over a perfect field.

We considered in Section 2 the case of the *generic curve of genus  $g$* , which is defined over the rational function field  $\mathbb{Q}(F_0, \dots, F_{2g-1})$  by the equation

$$y^2 = x^{2g+1} + F_{2g-1}x^{2g-1} + \dots + F_0.$$

Its modular equations have coefficients in  $\mathbb{Q}(F_0, \dots, F_{2g-1})$ . For  $g > 1$ , the fraction field of  $\mathbb{Q}[[F_0, \dots, F_{2g-1}]]$  is not a local field, so Theorem 2 does not apply directly, i.e. it does not allow to specialize  $F_0, \dots, F_{2g-1}$  at once. Yet we may circumvent this difficulty. Consider the isomorphism  $\mathbb{Q}(F_0, \dots, F_{2g-1}) \simeq \mathbb{Q}(F_0, \dots, F_{2g-2})(F_{2g-1})$ . The right-hand side is a univariate function field over  $\mathbb{Q}(F_0, \dots, F_{2g-2})$ , for which Theorem 2 applies; i.e. specializing  $F_{2g-1}$  is allowed. Iterating this process allows to successively specialize  $F_{2g-2}, \dots, F_0$ , as requested.

*Proof of Theorem 2.* Since  $K$  is an extension field of  $\mathcal{K}$ , the modular equations  $\Xi_\ell(\mathcal{C}/\mathcal{K})$  and  $\Xi_\ell(\mathcal{C}/K)$  coincide. Thus it is enough to prove the result for the curve  $\mathcal{C}/K$ , defined over the local field  $K$ .



Let  $\mathfrak{K}$  be an algebraic closure of  $K$ , let  $\mathbf{Jac}[\ell]$  be the  $\ell$ -torsion divisors on  $\mathbf{Jac}(\mathcal{C}/\mathfrak{K})$  and let  $\mathfrak{J}$  be the canonical injection  $\mathcal{C}/\mathfrak{K} \rightarrow \mathbf{Jac}(\mathcal{C}/\mathfrak{K})$ . Each divisor  $D \neq 0$  in  $\mathbf{Jac}[\ell]$  can be uniquely written  $D = \sum_{1 \leq j \leq r(D)} \mathfrak{J}(P_j^D)$ , where  $P_1^D, \dots, P_{r(D)}^D$  are points in  $\mathcal{C}/\mathfrak{K}$ , not at infinity and not pairwise conjugate, and where  $r(D)$  is at most  $g$ .

We let  $L$  be a finite extension of  $K$ , such that all  $\ell$ -torsion divisors  $D$  and all points  $P_1^D, \dots, P_{r(D)}^D$  are  $L$ -rational. Then  $L$  is a non-Archimedean local field, for a valuation that extends that of  $K$ , and that is still denoted by  $v$ . We denote by  $R_L$  and  $\mathfrak{m}_L$  the ring of integers of  $L$  and its maximal ideal, and the reduction modulo  $\mathfrak{m}_L$  is denoted by a bar. We still denote by  $\mathfrak{J}$  the canonical injection  $\mathcal{C}/L \rightarrow \mathbf{Jac}(\mathcal{C}/L)$ .

The curve  $\mathcal{C}/L$  has good reduction; the reduced curve, defined over the residual field of  $L$ , is still denoted by  $\overline{\mathcal{C}}$ ; the canonical injection  $\overline{\mathcal{C}} \rightarrow \mathbf{Jac}(\overline{\mathcal{C}})$  is denoted by  $\iota$ . Note that the residual fields of  $K$  and  $L$  have the same characteristic.

Let  $D$  be a  $\ell$ -torsion divisor on  $\mathbf{Jac}(\mathcal{C}/L)$ . We simplify the notation  $D = \sum_{1 \leq j \leq r(D)} \mathfrak{J}(P_j^D)$ , writing  $D = \sum_{1 \leq j \leq r} \mathfrak{J}(P_j)$  instead. Then, due to the good reduction of  $\mathcal{C}$ , the following holds:

$$\overline{D} = \overline{\sum_{1 \leq j \leq r} \mathfrak{J}(P_j)} = \sum_{1 \leq j \leq r} \overline{\mathfrak{J}(P_j)} = \sum_{1 \leq j \leq r} \iota(\overline{P_j}).$$

Moreover,  $\overline{D}$  is a  $\ell$ -torsion divisor on  $\mathbf{Jac}(\overline{\mathcal{C}})$ . Since the characteristic of  $k$  is different from  $\ell$ , Theorem C.2.6 in [17] shows that  $\overline{D}$  is not zero. Using the genericity assumption on  $\overline{\mathcal{C}}$ , this shows that  $\overline{D}$  has weight  $g$ , which implies that  $r = g$ , so  $\mathcal{C}$  satisfies the genericity assumption too. This also implies that all points  $\overline{P_j}$  are on the affine part of  $\overline{\mathcal{C}}$ .

Let us write  $P_j = (x_j, y_j, z_j)$ , with all coordinates in the ring of integers  $R_L$ , and at least one of them not in  $\mathfrak{m}_L$ . By the above remark,  $z_j$  does not reduce to zero modulo  $\mathfrak{m}_L$ , so  $v(z_j) = 1$ . Dividing by  $z_j$ , we write  $P_j$  as  $(X_j, Y_j, 1)$ , with coordinates in  $R_L$ ; then  $\overline{P_j}$  is given by  $(\overline{X_j}, \overline{Y_j}, 1)$ . Taking all points  $P_j$  into account, this shows that  $u_{g-1}(D)$  is in  $R_L$ , and a short calculation also gives that  $u_{g-1}(\overline{D}) = \overline{u_{g-1}(D)}$ . Recall now that the function  $t_\ell(D)$  is defined as

$$t_\ell(D) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} u_{g-1}([i]D),$$

so that  $t_\ell(D)$  is in  $R_L$ . Since  $\overline{[i]D} = [i]\overline{D}$ , we finally conclude that  $\overline{t_\ell(D)} = t_\ell(\overline{D})$ .

The set of non-zero  $\ell$ -torsion divisors on  $\mathcal{C}$  reduces to the set of non-zero  $\ell$ -torsion divisors on  $\overline{\mathcal{C}}$ , so  $\chi_\ell(\mathcal{C}) = \prod_{D \in \mathbf{Jac}[\ell] \setminus \{0\}} (T - t_\ell(D))$  is in  $R_L[T]$ , and  $(\chi_\ell(\mathcal{C}) \bmod \mathfrak{m}_L) = \chi_\ell(\overline{\mathcal{C}})$ . Since  $\mathcal{C}$  is defined over  $K$ ,  $\chi_\ell(\mathcal{C})$  is actually in  $R_K[T]$ , and  $(\chi_\ell(\mathcal{C}) \bmod \mathfrak{m}_K) = \chi_\ell(\overline{\mathcal{C}})$ .

From the definition  $\chi_\ell(\mathcal{C}) = \Xi_\ell(\mathcal{C})^{\ell-1}$ , we see that  $\Xi_\ell(\mathcal{C})$  is also in  $R_K[T]$  by Gauss' lemma. The above reduction can then be written  $(\Xi_\ell(\mathcal{C})^{\ell-1} \bmod \mathfrak{m}_K) = \Xi_\ell(\overline{\mathcal{C}})^{\ell-1}$ . Since both polynomials are monic,  $(\Xi_\ell(\mathcal{C}) \bmod \mathfrak{m}_K) = \Xi_\ell(\overline{\mathcal{C}})$ .  $\square$

## 4 Algorithms

We consider now the question of computing the modular equations, with an emphasis on the genus 2 case. In the first subsection, we show how Cantor's division polynomials [10] can be used to give a description of the  $\ell$ -torsion subgroup of a hyperelliptic Jacobian in genus 2, from which its  $\ell$ -th modular equation can be deduced; we illustrate this with examples for 3 and 5-torsion. We also present a solution by specialization techniques for 3-torsion in genus 2. The arbitrary genus case is finally addressed, using Adleman and Huang's algorithm for computing the  $\ell$ -torsion points on a hyperelliptic Jacobian [4].

### 4.1 Computing $\Xi_\ell$ in genus 2

Computing  $\Xi_\ell$  is a two-stage process: first compute a representation of the  $\ell$ -torsion divisors, then compute the modular equation using this information. This strategy was already hinted at in Subsection 2.2, where we addressed the elliptic case. In genus 1, the  $\ell$ -torsion divisors are the roots of the elliptic division polynomials, and the modular equations come from characteristic polynomial computations modulo these division polynomials. In genus 2, the torsion divisors can be characterized using Cantor's division polynomials [10]; the subsequent characteristic polynomial computations are analogous to the elliptic case.

The solution we present here demands further conditions on the  $\ell$ -torsion divisors, which are generically satisfied. In Subsection 4.2, we will present a more intricate solution, but which is valid in all cases. In this subsection,  $\mathcal{C}$  is a genus 2 curve defined over a field  $k$  by the equation  $y^2 = f(x)$ , with  $f$  of degree 5.

**First step: computing the torsion divisors.** We use the strategy from [13]. For a weight 2 divisor  $D = P_1 + P_2 - 2\infty$ , the condition  $[\ell]D = 0$  can be restated as

$$[\ell](P_1 - \infty) = -[\ell](P_2 - \infty).$$

Let  $x_1, x_2, y_1, y_2$  be new variables, and take  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$ . Then the Mumford-Cantor coordinates of  $[\ell](P_1 - \infty)$  and  $-[\ell](P_2 - \infty)$  are rational functions of  $x_1, x_2, y_1, y_2$  with coefficients in  $k$ . These rational functions can be derived efficiently by recursive formulae given in [10]:

$$[\ell]P_1 = \left\langle x^2 + \frac{d_1^{(\ell)}(x_1)}{d_0^{(\ell)}(x_1)}x + \frac{d_2^{(\ell)}(x_1)}{d_0^{(\ell)}(x_1)}, \frac{y_1 e_1^{(\ell)}(x_1)}{e_0^{(\ell)}(x_1)}x + \frac{y_1 e_2^{(\ell)}(x_1)}{e_0^{(\ell)}(x_1)} \right\rangle,$$

where  $d_0^{(\ell)}, d_1^{(\ell)}, d_2^{(\ell)}, e_0^{(\ell)}, e_1^{(\ell)}, e_2^{(\ell)}$  are univariate polynomials of degrees respectively  $2\ell^2 - 1, 2\ell^2 - 2, 2\ell^2 - 3, 3\ell^2 - 2, 3\ell^2 - 2, 3\ell^2 - 3$ . From now on we assume that  $\ell$  is fixed, and drop the superscript  $(\ell)$  for simplicity.

The genericity assumption on  $\mathcal{C}$  can then be made explicit: in [10] it is shown that a weight 1 divisor  $D = (x_1, y_1) - \infty$  is a  $\ell$ -torsion divisor if and only if  $d_1(x_1) = d_0(x_1) = 0$ . Hence the genericity assumption is valid on  $\mathcal{C}$  if and only if  $d_1$  and  $d_0$  are coprime polynomials.

If this is the case, we form the equations in  $x_1, x_2, y_1, y_2$  expressing that  $[\ell](P_1 - \infty) = -[\ell](P_2 - \infty)$ :

$$\begin{aligned}\frac{d_1(x_1)}{d_0(x_1)} &= \frac{d_1(x_2)}{d_0(x_2)}, \\ \frac{d_2(x_1)}{d_0(x_1)} &= \frac{d_2(x_2)}{d_0(x_2)}, \\ \frac{y_1 e_1(x_1)}{e_0(x_1)} &= -\frac{y_2 e_1(x_2)}{e_0(x_2)}, \\ \frac{y_1 e_2(x_1)}{e_0(x_1)} &= -\frac{y_2 e_2(x_2)}{e_0(x_2)}.\end{aligned}$$

Further equations and inequalities must be added to this system:

$$\begin{aligned}y_1^2 &= f(x_1), & y_2^2 &= f(x_2), \\ x_1 &\neq x_2, & d_0(x_1)e_0(x_1) &\neq 0.\end{aligned}$$

The equations specify that  $P_1$  and  $P_2$  are indeed points on the curve. The first inequality is necessary to discard the obvious solutions  $P_1 = -P_2$ , but may also eliminate points  $P_1$  such that  $[\ell](P_1 - \infty)$  is of 2-torsion. The second inequality allows to clean the denominators, and is equivalent to the assumption that  $[\ell](P_1 - \infty)$  has weight 2.

Due to the symmetry in  $(P_1, P_2)$ , for a general curve, this system has  $2(\ell^{2g} - 1)$  solutions, but this number may drop if  $[\ell](P_1 - \infty)$  is of 2-torsion or has weight 1, for some  $\ell$ -torsion divisor of the form  $D = P_1 + P_2 - 2\infty$ . Letting  $I_\ell \subset k[x_1, x_2, y_1, y_2]$  be the ideal defining the solutions of the above system, we thus have to check that  $I_\ell$  has the maximal number of solutions, i.e.  $2(\ell^{2g} - 1)$ . To this effect, we can use standard effective elimination algorithms such as Gröbner bases [8] or geometric resolution procedures [14, 15]. We refer to [13] for a faster solution based on resultant computations, which relies on the very specific shape of the system to solve.

Whatever routine we choose, we consider from now on that we are in the favorable case of an ideal  $I_\ell$  having  $2(\ell^{2g} - 1)$  solutions, and that, as an outcome of the elimination procedure, we can compute effectively modulo  $I_\ell$ .

**Second step: deducing  $\Xi_\ell$ .** In genus 2, the function  $t_\ell(D)$  defined in Section 2 becomes

$$t_\ell(D) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} u_1([i]D).$$

Roughly speaking, we want to compute  $t_\ell$  modulo  $I_\ell$ . To this effect, for  $i = 1, \dots, (\ell - 1)/2$ , we let  $h_{i,\ell}$  be the polynomial in  $k[x_1, x_2, y_1, y_2]$  which takes the value  $u_1([i]D)$  when evaluated on an  $\ell$ -torsion divisor  $D$ . The reader may refer to Subsection 2.2 where similar polynomials are derived in genus 1.

To obtain  $h_{i,\ell}$ , we compute the Mumford-Cantor coordinates of  $[i](P_1 - \infty) + [i](P_2 - \infty)$ , where  $P_1$  (resp.  $P_2$ ) is the point of coordinates  $(x_1, y_1)$ , resp.  $(x_2, y_2)$ , all computations being done modulo  $I_\ell$ . These computations can be done using Cantor's division polynomials and Cantor's addition algorithm [9]. As such, they involve divisions modulo  $I_\ell$ , which are possible in general, but may fail in unlucky cases.

We assume from now on that all these divisions can be done. In this lucky case, the polynomial  $\chi_\ell$  defined in Section 2 is the characteristic polynomial of  $\sum_{1 \leq i \leq \frac{\ell-1}{2}} h_{i,\ell}$  modulo  $I_\ell$ ; so it can be computed using linear algebra in the quotient  $k[x_1, x_2, y_1, y_2]/I_\ell$ . Knowing  $\chi_\ell$ , we then deduce the modular equation  $\Xi_\ell$  using the squarefree factorization of  $\chi_\ell$ . If we write

$$\chi_\ell = p_1^{M_1} \cdots p_s^{M_s},$$

with all  $p_i$  pairwise coprime squarefree polynomials in  $k[T]$ , then all  $M_i$  are multiples of  $\ell - 1$ , and

$$\Xi_\ell = p_1^{m_1} \cdots p_s^{m_s},$$

with  $M_i = (\ell - 1)m_i$  for all  $i$ . Since the base field is perfect, the squarefree factorization of  $\chi_\ell$  can be computed using for instance Yun's algorithm [30].

**First example: 3-torsion.** For the particular case of the 3-torsion in genus 2, we already noted that the genericity assumption is always satisfied. Further simplifications arise in this case.

Consider again the equations in  $x_1, x_2, y_1, y_2$  expressing that  $[3](P_1 - \infty) = -[3](P_2 - \infty)$ . The computation shows that all denominators in these equations are powers of  $f(x_1)$  and  $f(x_2)$ ; the Riemann-Roch theorem shows that these are non-zero quantities if  $P_1 + P_2 - 2\infty$  is of 3-torsion. In other words, the ideal  $I_3$  described above always has the maximal number of solutions, i.e.  $2 \times (3^4 - 1) = 160$ .

Cantor's division polynomials  $d_0, d_1, d_2, e_0, e_1, e_2$  for 3-torsion have degrees 17, 16, 15, 25, 25, 24. We define the ideal  $I_3 \subset k[x_1, x_2, y_1, y_2]$  using these polynomials; then the definitions in Section 2 show that for 3-torsion,  $t_3(D)$  coincides with  $u_1(D)$ , so  $\chi_3$  is the characteristic polynomial of  $x_1 + x_2$  modulo  $I_3$ , and  $\Xi_3$  is the square-root of  $\chi_3$ .

As an example, if  $\mathcal{C}$  is the genus 2 curve defined over  $\mathbb{F}_p$  with  $p = 101009$  by the equation

$$y^2 = x^5 + x^3 - 2233x^2 + 1944x + 21551,$$

then its modular equation for 3-torsion is

$$\begin{aligned} \Xi_3(T) = & T^{40} + 312T^{38} + 74066T^{37} + 21549T^{36} + 98476T^{35} + 77413T^{34} + 11876T^{33} + \\ & 87429T^{32} + 62497T^{31} + 26387T^{30} + 53806T^{29} + 55344T^{28} + 3150T^{27} + \\ & 85491T^{26} + 39525T^{25} + 66578T^{24} + 43546T^{23} + 37423T^{22} + \\ & 17475T^{21} + 96511T^{20} + 45626T^{19} + 38344T^{18} + 36106T^{17} + 88202T^{16} + \\ & 80287T^{15} + 16826T^{14} + 27075T^{13} + 64347T^{12} + 84421T^{11} + \\ & 99539T^{10} + 78579T^9 + 29813T^8 + 30858T^7 + 58361T^6 + 37204T^5 + \\ & 39712T^4 + 98618T^3 + 92702T^2 + 47474T + 57754. \end{aligned}$$

**Second example: 5-torsion.** We illustrate the case of 5-torsion with the same curve. The ideal  $I_5 \subset \mathbb{F}_p[x_1, x_2, y_1, y_2]$  is generated using the univariate polynomials  $d_0, d_1, d_2, e_0, e_1, e_2$  for 5-torsion, of respective degrees 49, 48, 47, 73, 73, 72. As indicated above, we apply the resolution techniques of [13], so as to obtain a basis of  $\mathbb{F}_p[x_1, x_2, y_1, y_2]/I_5$ .

For 5-torsion in genus 2,  $t_5(D)$  equals  $u_1(D) + u_1([2]D)$ . Taking  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$  and  $D = P_1 + P_2 - 2\infty$ , we compute the Mumford-Cantor coordinates of  $[2]D$  modulo  $I_5$ , from which we deduce  $t_5$  as a function defined modulo  $I_5$ , its characteristic polynomial  $\chi_5$ , and finally  $\Xi_5$ :

$$\begin{aligned} \Xi_5(T) = & T^{156} + 100894T^{155} + 45811T^{154} + 44233T^{153} + 39740T^{152} + 95818T^{151} + 4458T^{150} + 93570T^{149} \\ & + 28550T^{148} + 1113T^{147} + 63748T^{146} + 65156T^{145} + 19143T^{144} + 19730T^{143} + 33367T^{142} + \\ & 20907T^{141} + 63820T^{140} + 51940T^{139} + 42326T^{138} + 29817T^{137} + 75942T^{136} + 59745T^{135} + \\ & 97234T^{134} + 85218T^{133} + 24915T^{132} + 16689T^{131} + 93260T^{130} + 46818T^{129} + 27999T^{128} + \\ & 93775T^{127} + 2219T^{126} + 19973T^{125} + 1129T^{124} + 52225T^{123} + 6886T^{122} + 85816T^{121} + \\ & 77152T^{120} + 12511T^{119} + 64657T^{118} + 14966T^{117} + 42288T^{116} + 90382T^{115} + 60923T^{114} + \\ & 40482T^{113} + 43464T^{112} + 61885T^{111} + 2196T^{110} + 60160T^{109} + 78999T^{108} + 88624T^{107} + \\ & 86206T^{106} + 1602T^{105} + 73726T^{104} + 27596T^{103} + 4276T^{102} + 93140T^{101} + 58403T^{100} + \\ & 1234T^{99} + 88895T^{98} + 59594T^{97} + 13604T^{96} + 6248T^{95} + 30964T^{94} + 40104T^{93} + 58036T^{92} + \\ & 38120T^{91} + 69691T^{90} + 75816T^{89} + 22051T^{88} + 36408T^{87} + 59984T^{86} + 96659T^{85} + 35117T^{84} + \\ & 96676T^{83} + 62595T^{82} + 51710T^{81} + 38161T^{80} + 68329T^{79} + 99009T^{78} + 10635T^{77} + 97403T^{76} + \\ & 58767T^{75} + 74987T^{74} + 26947T^{73} + 100504T^{72} + 6849T^{71} + 50414T^{70} + 38143T^{69} + 82683T^{68} + \\ & 24600T^{67} + 83911T^{66} + 80258T^{65} + 98589T^{64} + 76450T^{63} + 89676T^{62} + 9956T^{61} + 58260T^{60} + \\ & 92379T^{59} + 57187T^{58} + 40082T^{57} + 33146T^{56} + 20951T^{55} + 77435T^{54} + 3376T^{53} + 67384T^{52} + \\ & 96487T^{51} + 74090T^{50} + 65498T^{49} + 61846T^{48} + 62046T^{47} + 30397T^{46} + 18364T^{45} + 55016T^{44} + \\ & 32487T^{43} + 94900T^{42} + 33300T^{41} + 25231T^{40} + 71704T^{39} + 59710T^{38} + 44750T^{37} + 31125T^{36} + \\ & 10050T^{35} + 7371T^{34} + 29794T^{33} + 72166T^{32} + 14168T^{31} + 53045T^{30} + 80342T^{29} + 20690T^{28} + \\ & 79145T^{27} + 74121T^{26} + 1983T^{25} + 37232T^{24} + 76446T^{23} + 6132T^{22} + 98206T^{21} + 94392T^{20} + \\ & 81694T^{19} + 43792T^{18} + 60209T^{17} + 98392T^{16} + 60483T^{15} + 71502T^{14} + 94495T^{13} + 77466T^{12} + \\ & 61989T^{11} + 51160T^{10} + 65902T^9 + 28152T^8 + 70740T^7 + 94924T^6 + 4993T^5 + 30256T^4 + \\ & 62697T^3 + 27820T^2 + 55949T + 63692. \end{aligned}$$

**The particular case of the generic curve.** We have a special interest for the generic curve of genus 2 defined over  $\mathbb{Q}(F_0, F_1, F_2, F_3)$  by the equation

$$\mathcal{C}_2 : y^2 = x^5 + F_3x^3 + F_2x^2 + F_1x + F_0,$$

and its modular equations in  $\mathbb{Q}(F_0, F_1, F_2, F_3)[T]$ . Computing these polynomials is a one-time job, which becomes useful in conjunction with the specialization Theorem of Section 3, as illustrated below.

The first case of interest is for 3-torsion. To compute  $\Xi_3(\mathcal{C}_2)$ , the elimination techniques mentioned above become cumbersome: the base field is now a rational function field, and we have no control on the degrees in  $(F_0, F_1, F_2, F_3)$  of the intermediate expressions we have to handle. Thus we used alternative resolution techniques, based on the work of the TERA group [3]: the algorithm we used is based on a symbolic Newton operator, which enables to compute successive approximations of  $\Xi_3(\mathcal{C}_2)$ , with increasing precisions in  $(F_0, F_1, F_2, F_3)$ , starting from the data of  $\Xi_3$  for a curve with rational coefficients.

Using these techniques, computing  $\Xi_3(\mathcal{C}_2)$  requires approximately 4 hours of CPU time using Magma, on a 4 GB, 500 MHz Compac DS20 processor. We mention that a direct approach based on a Gröbner basis computation fails, by lack of memory. For more details, we refer to [28].

The resulting polynomial  $\Xi_3(\mathcal{C}_2)$  can be downloaded from the web-page of the second author <http://www.medicis.polytechnique.fr/~schost/>. It has 1747 monomials with non-zero coefficients, belongs to  $\mathbb{Z}[F_0, F_1, F_2, F_3][T]$ , and is monic in  $T$ . To have an estimate of its size, here

are its first coefficients:

$$\begin{aligned}\Xi_3 = & T^{40} + 312F_3T^{38} - 7904F_2T^{37} + (-16344F_3^2 + 183488F_1)T^{36} + \\ & (337536F_3F_2 - 4179456F_0)T^{35} + (345456F_3^3 + 464064F_3F_1 - 2381088F_2^2)T^{34} + \\ & (-6044256F_3^2F_2 - 196322688F_3F_0 + 33608832F_2F_1)T^{33} + \dots\end{aligned}$$

The largest coefficient in absolute value is 304960695828480.

Let now  $p$  be a prime greater than 3 and  $\mathcal{C}$  a genus 2 curve defined over  $\mathbb{Z}/p\mathbb{Z}$  by the equation

$$\mathcal{C} : y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

Theorem 2 shows that the polynomial  $\Xi_3(\mathcal{C}) \in \mathbb{Z}/p\mathbb{Z}[T]$  is obtained by substituting the values  $f_i$  for the indeterminates  $F_i$  in  $\Xi_3(\mathcal{C}_2)$  after reducing its coefficient modulo  $p$ . We note that this solution is used within Magma's hyperelliptic curve package [1].

Until now, we always excluded the case  $\ell = p$ . To get a hint about the problems that can arise, we can reduce all the coefficients of  $\Xi_3(\mathcal{C}_2)$  modulo 3, expecting some degeneracy similar to the Kronecker relations for the elliptic modular polynomials  $\Phi_\ell$ . We obtain

$$\begin{aligned}\Xi_3(\mathcal{C}_2) & \equiv (T^4 + f_1T - f_2) \left( T^{12} + f_1T^9 - f_0f_2T^6 + (f_0^3f_1 - f_0f_1f_2 - f_1^3)T^3 + \right. \\ & \left. f_0^3f_1^2 - f_0^2f_2^2 - f_0f_1^2f_2 - f_0^4f_2 - f_1^4 - f_2^3 \right) \pmod{3} \\ & \equiv (T^4 + f_1T - f_2) \left( T^4 + \sqrt[3]{f_1}T^3 - \sqrt[3]{f_0f_2}T^2 + \sqrt[3]{f_0^3f_1 - f_0f_1f_2 - f_1^3}T + \right. \\ & \left. \sqrt[3]{f_0^3f_1^2 - f_0^2f_2^2 - f_0f_1^2f_2 - f_0^4f_2 - f_1^4 - f_2^3} \right) \pmod{3}\end{aligned}$$

In characteristic 3, the Jacobian of a curve of genus 2 has at most 9 points of 3-torsion. Therefore there are at most 4 distinct values for the  $u_1$ -coordinate of 3-torsion elements, whereas  $\Xi_3$  modulo 3 has 8 roots. We deduce that Theorem 2 cannot be generalized easily to the case  $p = \ell$ .

The next interesting case is that of  $\Xi_5(\mathcal{C}_2)$  for 5-torsion. We estimate that this polynomial has several million monomials, so new techniques will be needed to store it, relying on the evaluation philosophy of [16].

## 4.2 Computing the modular equation: the general case

The solution of Subsection 4.1 is specific to genus 2, and requires additional non-vanishing assumptions. We turn here to the general case of a genus  $g$  hyperelliptic curve  $\mathcal{C}$  defined over a field  $k$ , and indicate how to compute its  $\ell$ -th modular equation. This process is very similar to the one described above: first compute a representation of the  $\ell$ -torsion divisors on  $\mathbf{Jac}(\mathcal{C})$ , then compute the modular equation. The previous additional assumptions are ruled out now, at the cost notably of a more delicate pre-computation.

As in the genus 2 case, the Mumford-Cantor coordinates of the  $\ell$ -torsion divisors are algebraic over  $k$ . For the general case, Adleman and Huang propose in [4] an algorithm that computes a representation of these numbers by the following objects, whose existence is guaranteed if  $\mathcal{C}$  satisfies the genericity assumption for  $\ell$ :

1. A function  $q$  in  $k[u_0, \dots, u_{g-1}, v_0, \dots, v_{g-1}]$ , for instance a linear form. The function  $q$  must take  $\ell^{2g} - 1$  distinct values on  $\mathbf{Jac}[\ell] \setminus \{0\}$ , i.e.  $q$  must separate the points of  $\mathbf{Jac}[\ell] \setminus \{0\}$ .

2. The squarefree polynomial  $Q = \prod_{D \in \text{Jac}[\ell] \setminus \{0\}} (S - q(D))$  in  $k[S]$ .
3. The interpolating polynomials  $U_0, \dots, U_{g-1}, V_0, \dots, V_{g-1}$  in  $k[S]$  of degree less than  $\ell^{2g} - 1$  such that for all  $\ell$ -torsion divisors  $D$ ,  $U_i$  (resp.  $V_i$ ) takes the value  $u_i(D)$  (resp.  $v_i(D)$ ) when evaluated at  $q(D)$ .

Adleman and Huang's algorithm works in a complex setting of semi-algebraic maps, which reflects the fact that in the general case, the multiplication by  $\ell$ -map cannot be represented by a single rational function in Mumford-Cantor's coordinates.

Once the above objects are known, they enable to compute the polynomial  $\chi_\ell$ ; then the modular equation  $\Xi_\ell$  is deduced just as in Subsection 4.1. The computation of  $\chi_\ell$  follows the same inspiration as in the previous subsection. Again, recall that the function  $t_\ell(D)$  is defined as:

$$t_\ell(D) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} u_{g-1}([i]D).$$

For simplicity, assume first that the polynomial  $Q$  is irreducible, so  $A := k[S]/(Q)$  is a field, and let  $s$  be the image of  $S$  in  $A$ . Since  $A$  is a field, for any  $i$ , we can apply Cantor's algorithm [9] of multiplication by  $i$  in  $A[x]$ , on the divisor

$$D(s) = \langle x^g + U_{g-1}(s)x^{g-1} + \dots + U_0(s), V_{g-1}(s)x^{g-1} + \dots + V_0(s) \rangle.$$

Let  $h_{i,\ell} \in A$  be the  $u_{g-1}$ -coordinate of  $[i]D(s)$ . If we consider  $h_{i,\ell}$  in  $k[S]$ , then  $u_{g-1}([i]D) = h_{i,\ell}(q(D))$  holds for all  $\ell$ -torsion divisors  $D$ . This implies that

$$t_\ell(D) = \sum_{1 \leq i \leq \frac{\ell-1}{2}} h_{i,\ell}(q(D))$$

also holds for all  $\ell$ -torsion divisors  $D$ . Thus the polynomial  $\chi_\ell$  is the characteristic polynomial of  $\sum_{1 \leq i \leq \frac{\ell-1}{2}} h_{i,\ell}$  modulo  $Q$ .

In the general case, the polynomial  $Q$  is squarefree but not irreducible; then  $A$  is not a field, but a product of fields:  $A \simeq \prod A_j$ . This might make it impossible to apply the multiplication by  $i$  algorithm on the divisor  $D(s)$ , since this algorithm requires divisions in  $A$ . A first solution to obtain  $\chi_\ell$  consists in factorizing  $Q$ : applying the process described above in each field  $A_j$  yields a polynomial  $\chi_{\ell,j}$ , and the product of all  $\chi_{\ell,j}$  is  $\chi_\ell$ .

Of course, we want to avoid the factorization. Then a better solution is dynamic evaluation techniques [19]: the iterates of  $D(s)$  are computed as if  $A = k[S]/(Q)$  were a field. The divisions in  $A$  are performed using Extended GCD computations. When a division occurs where the dividend is not invertible in  $A$ , we have found a new factor of  $Q$ . Then we pursue the computations modulo each factor and finally multiply all results, as above. Thus the factorization of  $Q$  is not required; only the necessary factors come out the Extended GCD computations.

## 5 Factorization patterns of $\Xi_\ell$ over a finite field

Let  $\mathcal{C}$  be a hyperelliptic curve of genus  $g$  over a finite field  $\mathbb{F}_q$ . Let  $\ell$  be a prime coprime to  $q$  and let us assume that the genericity assumption holds for the  $\ell$ -torsion on  $\mathcal{C}$ . The polynomial  $\Xi_\ell$  can

be factored over  $\mathbb{F}_q$ . Due to the galoisian properties of the polynomial, the possible patterns of factorization are very specific. The general result is stated in the first subsection; then we give the explicit examples of genus 1 and genus 2, and the application to point-counting in the last subsection.

## 5.1 Link with the Frobenius action

Let  $\pi : x \mapsto x^q$  denote the  $q$ -th power Frobenius action on  $\overline{\mathbb{F}_q}$ , extended to  $\mathcal{C}$  and to  $\mathbf{Jac}(\mathcal{C})$ . The  $\ell$ -torsion subgroup  $\mathbf{Jac}[\ell]$  can be viewed as an  $\mathbb{F}_\ell$ -vector space of dimension  $2g$  on which  $\pi$  acts as an endomorphism. The following result is a general statement on the relation between  $\pi$  and the factorization patterns of the modular equations; the precise form is given in Lemma 2 below.

**Theorem 3** *Assume that  $\Xi_\ell$  is squarefree. Then the endomorphism  $\pi$  of the  $\mathbb{F}_\ell$ -vector space  $\mathbf{Jac}[\ell]$  determines the factorization pattern of  $\Xi_\ell$ .*

The proof of Theorem 3 is derived from the following lemmata.

**Lemma 1** *Assume that  $\Xi_\ell$  is squarefree and let  $D$  and  $E$  be non-zero  $\ell$ -torsion divisors. Then*

$$t_\ell(D) = t_\ell(E) \iff E \in \langle D \rangle.$$

*Proof.* The direction  $\Leftarrow$  follows from the definition of  $t_\ell$ . For the converse implication, since  $\Xi_\ell$  is squarefree, the number of values taken by  $t_\ell$  is maximal, therefore two distinct subgroups cannot give the same value.  $\square$

We define the *modified order* of a polynomial  $P$  with coefficient in a finite field as

$$\text{ord}^*(P) = \min\{k \in \mathbb{N}^*, \deg(X^k \bmod P(X)) = 0\}.$$

This notation is used in this section and in the Appendix.

**Lemma 2** *Let  $D$  be a non-zero  $\ell$ -torsion divisor of  $\mathbf{Jac}[\ell]$ . Let  $V_D$  be the  $\mathbb{F}_\ell$ -vector space generated by the galoisian conjugates of  $D$ :*

$$V_D = \text{Span}_{\mathbb{F}_\ell}\{\pi^n(D), n \in \mathbb{N}\}.$$

*Let  $P$  be the characteristic polynomial of  $\pi$  restricted to  $V_D$ . If  $\Xi_\ell$  is squarefree, then the degree of the extension of  $\mathbb{F}_q$  where  $t_\ell(D)$  is defined is  $\text{ord}^*(P)$ .*

*Proof.* Let  $k$  be the smallest positive integer such that  $\pi^k(D) \in \langle D \rangle$ . Since  $\pi$  fixes  $\mathbb{F}_q$ , we check as in Section 2 that  $\pi(t_\ell(D)) = t_\ell(\pi(D))$ , and so for all  $i \geq 0$ ,  $\pi^i(t_\ell(D)) = t_\ell(\pi^i(D))$ . By definition of  $k$ , for  $i < k$ ,  $\pi^i(D)$  is not in  $\langle D \rangle$ , so  $t_\ell(\pi^i(D)) \neq t_\ell(D)$  by the previous lemma, i.e.  $\pi^i(t_\ell(D)) \neq t_\ell(D)$ . Since  $t_\ell(\pi^k(D)) = t_\ell(D)$ , we have proven that  $k$  is the degree of the extension of  $\mathbb{F}_q$  where  $t_\ell(D)$  is defined.

We now consider the characteristic polynomial  $P$  of  $\pi$  restricted to the space  $V_D$  generated by the conjugates of  $D$ . Due to the definition of  $V_D$ ,  $P$  is the minimal polynomial of  $\pi$  restricted to  $V_D$ .



Denoting  $\lambda$  the element of  $\mathbb{F}_\ell^*$  such that  $\pi^k(D) = \lambda D$ , the endomorphism  $\pi^k - \lambda \text{Id}$  is trivial on  $D$  and on all its conjugates, therefore it is trivial on the whole of  $V_D$ . Hence we have

$$X^k - \lambda \equiv 0 \pmod{P(X)}.$$

Conversely, let  $k'$  and  $\mu$  be such that  $X^{k'} - \mu \equiv 0 \pmod{P(X)}$ , then  $\pi^{k'}$  is equal to  $\mu \text{Id}$  on  $V_D$  and in particular on  $D$ : therefore  $k'$  must be larger than or equal to  $k$ . The integer  $k$  is then the minimal having this property, as announced.  $\square$

*Proof of Theorem 3:* Let  $M$  be the matrix of the action of  $\pi$  on a basis  $\mathcal{B}$  of  $\mathbf{Jac}[\ell]$ . For all  $D$  in  $\mathbf{Jac}[\ell]$  expressed as a vector according to the same basis, finding  $V_D$  and the associated polynomial  $P(X)$  is a matter of elementary linear algebra. The extension where the root of  $\Xi_\ell$  associated to  $D$  is defined follows easily. Hence knowing the matrix  $M$  gives all the extensions where the roots of  $\Xi_\ell$  are defined, which gives the factorization pattern, because the field of definition is finite.  $\square$

## 5.2 Genus 1

The factorization patterns of the modular polynomial of an elliptic curve are well known [6, p. 119]. We restate them here for completeness; this gives a flavor of the genus 2 case that follows. Note that this result is usually given for the classical modular equations  $\Phi_\ell$  relating the  $j$ -invariants of  $\ell$ -isogenous elliptic curves; they have the same factorization patterns as ours.

In the sequel, notations such as

$$(n_1)^{\alpha_1} \cdots (n_k)^{\alpha_k} \quad \text{or} \quad (\underbrace{n_1, \dots, n_1}_{\beta_1}, \dots, \underbrace{n_k, \dots, n_k}_{\beta_k})$$

stand for a squarefree polynomial having  $\alpha_i$  irreducible factors of degree  $n_i$ , for  $i$  in  $1, \dots, k$ ; then  $\beta_i = n_i \alpha_i$ .

**Theorem 4** *Let  $E$  be an elliptic curve over  $\mathbb{F}_q$  and  $\ell$  coprime to  $q$ . Let  $X^2 - cX + q$  be the characteristic polynomial of the Frobenius endomorphism  $\pi$ . Assume that the modular polynomial  $\Xi_\ell$  is squarefree, then the set of degrees of its irreducible factors is one of the following, where  $r$  is an integer greater than 1:*

1.  $(1, \ell)$  or  $(1, 1, \dots, 1)$  if  $c^2 - 4q \equiv 0 \pmod{\ell}$ .
2.  $(1, 1, r, r, \dots, r)$  if  $c^2 - 4q$  is a non-zero square modulo  $\ell$ .
3.  $(r, r, \dots, r)$  if  $c^2 - 4q$  is not a square modulo  $\ell$ .

Case 1 corresponds to a Frobenius endomorphism having a double eigenvalue. According to the presence of one or two blocks in the Jordan decomposition we get one or the other subcase. Case 2 is the case where there are two distinct eigenvalues. Case 3 is the non-diagonalizable case.

### 5.3 Genus 2

In genus 2, we study all possible reductions of the matrix of the Frobenius endomorphism and get the corresponding factorization patterns for  $\Xi_\ell$ . The classification is done according to the possible factorization patterns of the minimal and characteristic polynomials of the Frobenius endomorphism  $\pi$ , from which we deduce a block-reduction of the matrix of  $\pi$ ; the factorization pattern of the modular equation is then deduced from Lemma 2. The two lemmata below reduce the number of cases to consider.

**Lemma 3** *If the characteristic polynomial of the Frobenius endomorphism has a triple root modulo  $\ell$  then the multiplicity is actually 4.*

*Proof.* Let  $(X - a)^3(X - b)$  be the characteristic polynomial of  $\pi$  modulo  $\ell$ . By Weil's theorem, all the roots have absolute value  $\sqrt{q}$ . Therefore we have  $a^2 \equiv q \pmod{\ell}$  and  $ab \equiv q \pmod{\ell}$ . But  $q$  is non-zero modulo  $\ell$ , so that  $a \equiv b \pmod{\ell}$ .  $\square$

**Lemma 4** *Let  $D$  be such that  $V_D = \text{Span}_{\mathbb{F}_\ell}\{\pi^n(D), n \in \mathbb{N}\}$  has dimension 3. Then  $V_D$  is a non-trivial direct sum of  $\pi$ -stable sub-spaces.*

*Proof.* Let  $(D_1 = D, D_2 = \pi(D), D_3 = \pi^2(D))$  be a basis of  $V_D$  and  $D_4$  be a supplementary vector of  $\pi$ . We write  $\pi(D_3) = XD_1 + YD_2 + ZD_3$ ; then  $\pi$  being invertible implies  $X \neq 0$ . Let  $e_\ell(\cdot, \cdot)$  denote the Weil pairing on  $\mathbf{Jac}[\ell]$ . Recall that this is an alternate non-degenerate bilinear form with values in the  $\ell$ -th roots of unity in an algebraic closure of  $\mathbb{F}_q$  and such that  $e_\ell(\pi(\Delta), \pi(\Delta')) = (e_\ell(\Delta, \Delta'))^q$  for all  $\ell$ -torsion divisors  $\Delta, \Delta'$ .

Let  $\alpha$  be  $e_\ell(D_1, D_2)$ . Then iterated applications of the Frobenius endomorphism yield

$$e_\ell(D_2, D_3) = \alpha^q, \quad e_\ell(D_1, D_3) = \alpha^{-\frac{q(q+Y)}{X}},$$

and impose that

$$\alpha^{q^3 + q^2Y - X^2 + qZX} = 1.$$

If  $\alpha$  were equal to 1, then  $e_\ell$  would be trivial on a space of dimension 3, which contradicts its non-degeneracy. Consequently, we have  $\alpha \neq 1$ . Thus

$$q^3 + q^2Y - X^2 + qZX = 0 \text{ in } \mathbb{F}_\ell.$$

Let  $A$  be such that  $\pi(D_4) = AD_4 + E$ , with  $E$  in  $V_D$ . Weil's theorem implies that  $A^2 = q$  and  $\det(\pi) = XA = q^2$ . We deduce that  $X, Y, q$  can be written

$$X = A^3, \quad Y = -AZ, \quad q = A^2.$$

Then the characteristic polynomial of the restriction of  $\pi$  to  $\langle D_1, D_2, D_3 \rangle$  is

$$(T - A)(T^2 + (A - Z)T + A^2).$$

Suppose that  $A$  is a root of the right-hand factor. Then  $Z = 3A$  and the vector  $\Delta = A^2D_1 - 2AD_2 + D_3$  is such that  $e_\ell(\Delta, \Delta') = 0$  for all  $\Delta'$  in  $\mathbf{Jac}[\ell]$ , a contradiction. Hence the characteristic polynomial is the product of two coprime non-trivial factors and  $V_D$  splits non-trivially in two  $\pi$ -stable sub-spaces.  $\square$

Using Lemmata 3 and 4, we now proceed to enumerate all admissible reduction patterns of  $\pi$  and apply Lemma 2 to get the corresponding factorization pattern of  $\Xi_\ell$ . We give below all details for one case and leave the others to the reader. The results are collected in Appendix.

**A complete example.** Assume that the minimal (resp. characteristic) polynomial of  $\pi$  can be written  $PQ$  (resp.  $PQ^2$ ), with  $P$  irreducible of degree 2 and  $Q$  of degree 1. Then there exists a basis  $(D_1, D_2, D_3, D_4)$  of  $\mathbf{Jac}[\ell]$  in which the matrix of  $\pi$  has the form

$$M = \begin{array}{|c|c|} \hline A_2 & 0 \\ \hline 0 & \begin{array}{|c|c|} \hline b & 0 \\ \hline 0 & b \\ \hline \end{array} \\ \hline \end{array},$$

where  $A_2$  is a  $2 \times 2$  matrix whose characteristic polynomial is irreducible modulo  $\ell$  and  $b$  is a scalar.

For all  $0 \neq D \in \langle D_3, D_4 \rangle$ , we have  $\pi(D) = bD$ , and by Lemma 2, the subgroups of order  $\ell$  inside  $\langle D_3, D_4 \rangle$  correspond to roots of  $\Xi_\ell$  defined over  $\mathbb{F}_\ell$ . There are as many roots as lines in  $\langle D_3, D_4 \rangle$ , i.e.  $\frac{\ell^2-1}{\ell-1} = \ell + 1$ .

For all  $0 \neq D \in \langle D_1, D_2 \rangle$ , the vector space generated by the conjugates of  $D$  is  $V_D = \langle D_1, D_2 \rangle$  and the characteristic polynomial of  $\pi$  restricted to  $V_D$  is the characteristic polynomial of the matrix  $A_2$ . By Lemma 2, the root of  $\Xi_\ell$  associated to the the subgroup generated by  $D$  is therefore in an extension of degree  $\text{ord}^*(\text{Characteristic polynomial of } A_2)$ , that we denote by  $\text{ord}(A_2)$ . Again there are  $\ell + 1$  roots, thus  $\text{ord}(A_2)$  divides  $\ell + 1$ . Finally, we have  $(\ell + 1)/\text{ord}(A_2)$  factors of degree  $\text{ord}(A_2)$  in  $\Xi_\ell$ .

For all  $D = E + F$  where  $0 \neq E \in \langle D_1, D_2 \rangle$  and  $0 \neq F \in \langle D_3, D_4 \rangle$ , the vector space generated by the conjugates of  $D$  is  $V_D = \langle D_1, D_2, F \rangle$  and the characteristic polynomial of  $\pi$  on  $V_D$  is equal to the characteristic polynomial of  $A_2$  multiplied by  $(X - b)$ . We denote by  $\text{ord}(A_2b)$  the value of  $\text{ord}^*$  for this polynomial; this is the degree of the extension where we find the roots. The number of lines generated by such  $D$ 's is  $(\ell - 1)(\ell + 1)^2$ .

To summarize,  $\Xi_\ell$  contains

- $\ell + 1$  linear factors,
- $(\ell + 1)/\text{ord}(A_2)$  factors of degree  $\text{ord}(A_2)$ ,
- $(\ell - 1)(\ell + 1)^2/\text{ord}(A_2b)$  factors of degree  $\text{ord}(A_2b)$ .

## 5.4 Application to point-counting

Let  $\mathcal{C}$  be a hyperelliptic curve of genus  $g$  over a finite field  $\mathbb{F}_q$  for which we want to compute the cardinality of the Jacobian. The characteristic polynomial of the Frobenius endomorphism is denoted by  $\mathcal{F}$ ; then  $\#\mathbf{Jac}(\mathcal{C}) = \mathcal{F}(1)$ .

The principle of the high genus variants of Schoof's algorithm [25, 20, 18] is to compute  $\mathcal{F}(1)$  modulo several small primes  $\ell$  using the restriction of  $\pi$  to  $\mathbf{Jac}[\ell]$ . When this is done for sufficiently many primes  $\ell$ ,  $\mathcal{F}(1)$  can be deduced using the Chinese Remainder Theorem.

In the 80's, Atkin [5] proposed a modification of Schoof's algorithm for elliptic curves: for each  $\ell$ , he only computes the factorization pattern of the modular polynomial and reduces the number of candidates for  $\mathcal{F}(1)$  modulo  $\ell$ . It then requires more primes  $\ell$  before having enough information to conclude. This method has exponential complexity but with further improvements by Elkies led to the so-called Schoof–Elkies–Atkin algorithm [27], which is the fastest method to date for large prime  $q$ .

Our modular equations can be used in the same manner for a curve  $\mathcal{C}$  of genus  $g$ . Let  $\ell$  be a small prime coprime to  $q$ . Assume that we have computed  $\Xi_\ell$  for this curve and that it is squarefree. Then a partial factorization can be computed in order to find its factorization pattern. Following the method developed in the previous section, it is possible to find all characteristic polynomials  $\mathcal{F}$  that could yield this pattern. Then computing the group order modulo  $\ell$  for each of these cases gives a list of candidates among which the actual one lies.

This yields the following algorithm “à la Atkin”:

1. While we do not have enough information, do
  - (a) Choose a new small prime  $\ell$  coprime to  $2q$ ;
  - (b) Compute the factorization pattern of  $\Xi_\ell$ ;
  - (c) Compute the values of  $\chi(1) \bmod \ell$  compatible with this pattern;
2. Determine the only value of  $\chi(1)$  compatible with all the modular informations.

To illustrate this approach, we give a table of the possible patterns for  $\ell = 3$  in genus 2 and the corresponding candidates for the cardinality of the Jacobian modulo 3. Recall that all genus 2 curves satisfy the genericity assumption for 3-torsion.

**Theorem 5** *Let  $\mathcal{C}$  be a curve of genus 2 over a finite field  $\mathbb{F}_q$  of characteristic different from 2 and 3. Assume that  $\Xi_3(\mathcal{C})$  is squarefree. Then the factorization pattern of  $\Xi_3(\mathcal{C})$  imply the values of  $\#\mathbf{Jac}(\mathcal{C}) \bmod 3$  according to the following table:*

$q \equiv 2 \pmod 3$		$q \equiv 1 \pmod 3$	
pattern	$\#\mathbf{Jac}(\mathcal{C}) \bmod 3$	pattern	$\#\mathbf{Jac}(\mathcal{C}) \bmod 3$
$(10)^4$	2	$(5)^8$	1, 2
$(2)^2(6)^6$	1	$(1)(2)^2(3)(4)^2(12)^2$	0, 2
$(4)(12)^3$	1	$(1)^4(2)^2(4)^8$	0, 2
$(2)^{20}$	1	$(1)(3)^4(9)^3$	0, 1
$(1)^2(2)(4)(8)^4$	0	$(1)^4(3)^{12}$	0, 1
$(1)^2(2)(3)^2(6)^5$	0	$(1)^{40}$	0, 1
$(1)^8(2)^{16}$	0	$(4)^{10}$	2
$(1)^5(2)^4(3)(6)^4$	0	$(2)^2(6)^6$	1
$(4)^{10}$	1, 2	$(2)^{20}$	1
		$(1)^2(2)(3)^2(6)^5$	0
		$(1)^5(2)^4(3)(6)^4$	0
		$(1)^8(2)^{16}$	0

As an example, consider again the curve  $\mathcal{C}$  defined in Section 4.1 over the field  $\mathbb{F}_q$  with  $q = 101009 \equiv 2 \pmod{3}$ . Then the factorization pattern of  $\Xi_3(\mathcal{C})$  is  $(1)^2(2)(4)(8)^4$  which implies that  $\#\mathbf{Jac}(\mathcal{C}) \equiv 0 \pmod{3}$ .

Similarly, the factorization pattern of  $\Xi_5(\mathcal{C})$  is  $(3)^{52}$ . Referring to the table given in the Appendix, we deduce that only the first four cases of that table are to be considered. An exhaustive enumeration of all possible characteristic polynomials in these four cases reveals that this polynomial is either  $(T^2 + 2T + 4)^2$  or  $(T^2 + 3T + 4)^2$ ; they both give the same number of points  $\#\mathbf{Jac}(\mathcal{C}) \equiv 4 \pmod{5}$ .

**Complexity considerations.** In the usual implementations of elliptic curve point counting algorithms, the generic modular equations are precomputed and stored. However, for genus 2 and higher, the generic equations are too large to be stored, even if we manage to precompute them. Therefore we have to recompute them on the fly for each instance of a curve. Let  $q$  be the size of the base field, and  $\ell$  be the prime under consideration. Computing  $\Xi_\ell$  for a given curve involves a number of operations in the base field which is polynomial in  $\ell$ . Then the factorization phase costs  $O(\log q)$  operations with polynomials of degree  $O(\ell^3)$ . On the other hand, the plain Schoof-like algorithm would require to deal with the whole torsion whose degree is in  $O(\ell^4)$ . Computing the action of the Frobenius endomorphism will then require  $O(\log q)$  operations with polynomials of degree  $O(\ell^4)$ . Therefore, for a fixed  $\ell$  and when  $q$  tends to infinity, the cost of computing  $\Xi_\ell$  and its factorization pattern is smaller than the cost of the plain Schoof algorithm. Still, in a complete point-counting algorithm, we need to take primes  $\ell$  up to  $\log q$ , and more efficient algorithms for computing  $\Xi_\ell$  of a given curve together with more precise analysis will be needed to conclude about the feasibility of this kind of approach.

## Appendix: Factorization patterns of $\Xi_\ell$ in genus 2

The lines in the following table are indexed by the possible decompositions of the Frobenius endomorphism  $\pi$  on  $\mathbf{Jac}[\ell]$ . These are given in the second column. The first column gives the corresponding factorization pattern of the characteristic polynomial of  $\pi$ , and the last gives the factorization pattern of the modular equation  $\Xi_\ell$ .

The notation for the factorization patterns is defined in Section 5. Notations such as  $A_i$  or  $B_i$  denote  $i \times i$  matrices with irreducible characteristic polynomials; the notation  $*$  denotes any non-zero matrix. Lower case letters stand for scalars, which may be thought as  $1 \times 1$  matrix.

The modified order  $\text{ord}^*(P)$  of a polynomial  $P$  is defined in Section 5. Given two matrices  $A_i, B_j$ , the notation  $\text{ord}(A_i B_j)$  is defined as the modified order of the product of their characteristic polynomials. This notation extends to three or four blocks.

The characteristic polynomial of  $\pi$  is not necessarily squarefree, so we adopt another notation for its factorization pattern:

$$[n_1]^{\alpha_1} \cdots [n_k]^{\alpha_k}$$

stands for a product  $P_1^{\alpha_1} \cdots P_k^{\alpha_k}$  where the  $P_i$  are distinct irreducible polynomials of degree  $n_i$ , for  $i = 1, \dots, k$ .

bl.	Matrix	Pattern of modular polynomial
One factor of degree 4		
	$A_4$	$(\underbrace{\text{ord}(A_4), \dots, \text{ord}(A_4)}_{\ell^3 + \ell^2 + \ell + 1})$
Two factors of degree 2		
	$\begin{array}{ c c } \hline A_2 & 0 \\ \hline 0 & A_2 \\ \hline \end{array}$	$(\underbrace{\text{ord}(A_2), \dots, \text{ord}(A_2)}_{\ell^3 + \ell^2 + \ell + 1})$ <span style="float: right;">22</span>
	$\begin{array}{ c c } \hline A_2 & * \\ \hline 0 & A_2 \\ \hline \end{array}$	$(\underbrace{\text{ord}(A_2), \dots, \text{ord}(A_2)}_{\ell + 1}, \underbrace{\text{ord}(A_2^2), \dots, \text{ord}(A_2^2)}_{\ell^2(\ell + 1)})$
	$\begin{array}{ c c } \hline A_2 & 0 \\ \hline 0 & B_2 \\ \hline \end{array}$	$(\underbrace{\text{ord}(A_2), \dots, \text{ord}(A_2)}_{\ell + 1}, \underbrace{\text{ord}(B_2), \dots, \text{ord}(B_2)}_{\ell^2(\ell + 1)}, \underbrace{\text{ord}(A_2 B_2), \dots, \text{ord}(A_2 B_2)}_{\ell^2(\ell + 1)})$

Char. pol.	Matrix	Pattern of modular polynomial											
Four factors of degree 1													
$[1]^4$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td><math>0</math></td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>a</math></td></tr> </table>	$a$	$0$	$0$	$0$	$a$	$0$	$a$	$0$		$0$	$a$	$(\underbrace{1, \dots, 1}_{\ell^3 + \ell^2 + \ell + 1})$
$a$	$0$	$0$											
$0$	$a$												
$0$	$a$	$0$											
	$0$	$a$											
$[1]^4$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td>*</td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>a</math></td></tr> </table>	$a$	*	$0$	$0$	$a$	$0$	$a$	$0$		$0$	$a$	$(\underbrace{1, \dots, 1}_{\ell^2 + \ell + 1}, \underbrace{\ell, \dots, \ell}_{\ell^2})$
$a$	*	$0$											
$0$	$a$												
$0$	$a$	$0$											
	$0$	$a$											
$[1]^4$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td>*</td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td><td>*</td></tr> <tr><td></td><td><math>0</math></td><td><math>a</math></td></tr> </table>	$a$	*	$0$	$0$	$a$	$0$	$a$	*		$0$	$a$	$(\underbrace{1, \dots, 1}_{\ell + 1}, \underbrace{\ell, \dots, \ell}_{\ell^2 + \ell})$
$a$	*	$0$											
$0$	$a$												
$0$	$a$	*											
	$0$	$a$											
$[1]^4$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td>*</td><td rowspan="2">*</td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td><td>*</td></tr> <tr><td></td><td><math>0</math></td><td><math>a</math></td></tr> </table>	$a$	*	*	$0$	$a$	$0$	$a$	*		$0$	$a$	$(1, \ell, \underbrace{\text{ord}(a^3), \dots, \text{ord}(a^3)}_{\ell^2}, \underbrace{\text{ord}(a^4), \dots, \text{ord}(a^4)}_{\ell^3})$
$a$	*	*											
$0$	$a$												
$0$	$a$	*											
	$0$	$a$											
$[1]^2[1]^2$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td><math>0</math></td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>b</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>b</math></td></tr> </table>	$a$	$0$	$0$	$0$	$a$	$0$	$b$	$0$		$0$	$b$	$(\underbrace{1, \dots, 1}_{2\ell + 2}, \underbrace{\text{ord}(ab), \dots, \text{ord}(ab)}_{(\ell - 1)(\ell + 1)^2})$
$a$	$0$	$0$											
$0$	$a$												
$0$	$b$	$0$											
	$0$	$b$											
$[1]^2[1]^2$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td>*</td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>b</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>b</math></td></tr> </table>	$a$	*	$0$	$0$	$a$	$0$	$b$	$0$		$0$	$b$	$(\underbrace{1, \dots, 1}_{\ell + 2}, \underbrace{\ell, \text{ord}(ab), \dots, \text{ord}(ab)}_{(\ell - 1)(\ell + 1)}, \underbrace{\text{ord}(a^2b), \dots, \text{ord}(a^2b)}_{\ell(\ell - 1)(\ell + 1)})$
$a$	*	$0$											
$0$	$a$												
$0$	$b$	$0$											
	$0$	$b$											
$[1]^2[1]^2$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td>*</td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>b</math></td><td>*</td></tr> <tr><td></td><td><math>0</math></td><td><math>b</math></td></tr> </table>	$a$	*	$0$	$0$	$a$	$0$	$b$	*		$0$	$b$	$(1, 1, \ell, \ell, \underbrace{r, \dots, r}_{\ell - 1}, \underbrace{s_1, \dots, s_1}_{\ell(\ell - 1)}, \underbrace{s_2, \dots, s_2}_{\ell(\ell - 1)}, \underbrace{t, \dots, t}_{\ell^2(\ell - 1)})$ where $r = \text{ord}(ab)$ , $s_1 = \text{ord}(ab^2)$ , $s_2 = \text{ord}(a^2b)$ , $t = \text{ord}(a^2b^2)$
$a$	*	$0$											
$0$	$a$												
$0$	$b$	*											
	$0$	$b$											
$[1]^2[1][1]$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td><math>0</math></td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>b</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>c</math></td></tr> </table>	$a$	$0$	$0$	$0$	$a$	$0$	$b$	$0$		$0$	$c$	$(\underbrace{1, \dots, 1}_{\ell + 3}, \underbrace{r, \dots, r}_{\ell - 1}, \underbrace{s_1, \dots, s_1}_{\ell^2 - 1}, \underbrace{s_2, \dots, s_2}_{\ell^2 - 1}, \underbrace{t, \dots, t}_{(\ell^2 - 1)(\ell - 1)})$ where $r = \text{ord}(bc)$ , $s_1 = \text{ord}(ab)$ , $s_2 = \text{ord}(ac)$ , $t = \text{ord}(abc)$
$a$	$0$	$0$											
$0$	$a$												
$0$	$b$	$0$											
	$0$	$c$											
$[1]^2[1][1]$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td>*</td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>a</math></td></tr> <tr><td><math>0</math></td><td><math>b</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>c</math></td></tr> </table>	$a$	*	$0$	$0$	$a$	$0$	$b$	$0$		$0$	$c$	$(1, 1, 1, \ell, \underbrace{r_1, \dots, r_1}_{\ell - 1}, \dots, \underbrace{r_3, \dots, r_3}_{\ell - 1}, \underbrace{s_1, \dots, s_1}_{\ell(\ell - 1)}, \underbrace{s_2, \dots, s_2}_{\ell(\ell - 1)}, \underbrace{t, \dots, t}_{(\ell - 1)^2}, \underbrace{u, \dots, u}_{\ell(\ell - 1)^2})$ where $r_1 = \text{ord}(bc)$ , $r_2 = \text{ord}(ab)$ , $r_3 = \text{ord}(ac)$ , $s_1 = \text{ord}(a^2b)$ , $s_2 = \text{ord}(a^2c)$ , $t = \text{ord}(abc)$ , $u = \text{ord}(a^2bc)$
$a$	*	$0$											
$0$	$a$												
$0$	$b$	$0$											
	$0$	$c$											
$[1][1][1][1]$	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td><math>a</math></td><td><math>0</math></td><td rowspan="2"><math>0</math></td></tr> <tr><td><math>0</math></td><td><math>b</math></td></tr> <tr><td><math>0</math></td><td><math>c</math></td><td><math>0</math></td></tr> <tr><td></td><td><math>0</math></td><td><math>d</math></td></tr> </table>	$a$	$0$	$0$	$0$	$b$	$0$	$c$	$0$		$0$	$d$	$(1, 1, 1, 1, \underbrace{r_1, \dots, r_1}_{\ell - 1}, \dots, \underbrace{r_6, \dots, r_6}_{\ell - 1}, \underbrace{s_1, \dots, s_1}_{(\ell - 1)^2}, \dots, \underbrace{s_4, \dots, s_4}_{(\ell - 1)^2}, \underbrace{t, \dots, t}_{(\ell - 1)^3})$ where $r_1 = \text{ord}(ab)$ , $r_2 = \text{ord}(ac)$ , $r_3 = \text{ord}(ad)$ , $r_4 = \text{ord}(bc)$ , $r_5 = \text{ord}(bd)$ , $r_6 = \text{ord}(cd)$ , $s_1 = \text{ord}(abc)$ , $s_2 = \text{ord}(abd)$ , $s_3 = \text{ord}(acd)$ , $s_4 = \text{ord}(bcd)$ , $t = \text{ord}(abcd)$
$a$	$0$	$0$											
$0$	$b$												
$0$	$c$	$0$											
	$0$	$d$											

## References

- [1] *Magma*, <http://www.maths.usyd.edu.au:8000/u/magma/>.
- [2] *Medicis*, <http://www.medicis.polytechnique.fr/>.
- [3] *Tera*, <http://tera.medicis.polytechnique.fr/>.
- [4] L. Adleman and M.-D. Huang, *Counting points on curves and abelian varieties over finite fields*, J. Symbolic Comput. **32** (2001), 171–189.
- [5] A. O. L. Atkin, *The number of points on an elliptic curve modulo a prime*, Series of e-mails to the NMBRTHRY mailing list, 1992.
- [6] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, London Math. Soc. Lecture Note Ser., vol. 265, Cambridge University Press, 1999.
- [7] J. Boxall and D. Grant, *Examples of torsion points on genus two curves*, Trans. Amer. Math. Soc. **352** (2000), no. 10, 4533–4555.
- [8] B. Buchberger, *Gröbner bases: An algorithmic method in polynomial ideal theory*, Multidimensional System Theory, Reidel, Dordrecht, 1985, pp. 374–383.
- [9] D. G. Cantor, *Computing in the Jacobian of an hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101.
- [10] ———, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145.
- [11] L. S. Charlap, R. Coley, and D. P. Robbins, *Enumeration of rational points on elliptic curves over finite fields*, Draft, 1991.
- [12] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational Perspectives on Number Theory (D.A. Buell and J.T. Teitelbaum, eds.), AMS/International Press, 1998, Proceedings of a Conference in Honor of A.O.L. Atkin, pp. 21–76.
- [13] P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, ANTS-IV (W. Bosma, ed.), Lecture Notes in Comput. Sci., vol. 1838, Springer–Verlag, 2000, pp. 313–332.
- [14] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo, *Straight-line programs in geometric elimination theory*, J. of Pure and App. Algebra **124** (1998), 101–146.
- [15] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211.
- [16] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein, *Deformation techniques for efficient polynomial equation solving*, J. Complexity **16** (2000), 70–109.



- [17] M. Hindry and J. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics, vol. 201, Springer–Verlag, 2000.
- [18] M.-D. Huang and D. Ierardi, *Counting points on curves over finite fields*, J. Symbolic Comput. **25** (1998), 1–21.
- [19] C. Dicrescenzo J. Della Dora and D. Duval, *About a new method for computing in algebraic number fields*, Proceedings Eurocal '85 Vol. 2, Lecture Notes in Comput. Sci., vol. 204, 1985, pp. 289–290.
- [20] W. Kampkötter, *Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven*, Ph.D. thesis, Universität Gesamthochschule Essen, August 1991.
- [21] J. S. Milne, *Abelian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer–Verlag, 1986, pp. 103–150.
- [22] ———, *Jacobian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer–Verlag, 1986, pp. 167–212.
- [23] F. Morain, *Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques*, J. Théor. Nombres Bordeaux **7** (1995), 255–282.
- [24] D. Mumford, *Tata lectures on theta I*, Progr. Math., vol. 28, Birkhauser, 1983.
- [25] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763.
- [26] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod  $p$* , Math. Comp. **44** (1985), 483–494.
- [27] ———, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), 219–254.
- [28] É. Schost, *Degree bounds and lifting techniques for triangular sets*, Proceedings of the 2002 Symposium on Symbolic and Algebraic Computation, ACM Press, 2002.
- [29] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer–Verlag, 1986.
- [30] D. Y. Y. Yun, *On square-free decompositions algorithms*, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, ACM Press, 1976, pp. 26–35.