Linearizing torsion classes in the Picard group of algebraic curves over finite fields

J.-M. Couveignes*

January 1, 1997

Abstract

We address the problem of computing in the group of ℓ^k-torsion rational points of the jacobian variety of algebraic curves over finite fields, with a view toward computing modular representations.

Contents

*Groupe de Recherche en Informatique et Mathématiques du Mirail, Université de Toulouse II, Le Mirail

1 Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic p and $\mathbb{A}^2 \subset \mathbb{P}^2$ the affine and projective planes over $\mathbb{F}_q$ and $C \subset \mathbb{P}^2$ a plane projective absolutely irreducible reduced curve and $\mathcal{X}$ its smooth projective model and $\mathcal{J}$ the jacobian variety of $\mathcal{X}$. Let g be the genus of $\mathcal{X}$ and d the degree of C.

We assume we are given the numerator of the zeta function of the function field $\mathbb{F}_q(\mathcal{X})$. So we know the characteristic polynomial of the Frobenius endomorphism F_q of $\mathcal{J}$. This is a unitary degree $2g$ polynomial $\chi(X)$ with integer coefficients.

Let $\ell \neq p$ be a prime integer and let $n = \ell^k$ be a power of ℓ. We look for a *nice generating set* for the group $\mathcal{J}[\ell^k](\mathbb{F}_q)$ of ℓ^k-torsion points in $\mathcal{J}(\mathbb{F}_q)$. By *nice* we mean that the generating set $(g_i)_{1 \leq i \leq I}$ should induce a decomposition of $\mathcal{J}[\ell^k](\mathbb{F}_q)$ as a direct product $\prod_{1 \leq i \leq I} < g_i >$ of cyclic subgroups with non-decreasing orders.

Given such a generating set and an $\mathbb{F}_q$-endomorphism of $\mathcal{J}$, we also want to describe the action of this endomorphism on $\mathcal{J}[\ell^k](\mathbb{F}_q)$ by an $I \times I$ integer matrix.

In section 2 we recall how to compute in the Picard group $\mathcal{J}(\mathbb{F}_q)$. Section 3 gives a naive algorithm for picking random elements in this group. Pairings are useful when looking for relations between divisor classes. So we recall how to compute pairings in section 4. Section 5 is concerned with characteristic subspaces for the action of Frobenius inside the ℓ^∞-torsion of $\mathcal{J}(\bar{\mathbb{F}}_q)$. In section 6 we look for a convenient surjection from $\mathcal{J}(\mathbb{F}_q)$ onto its ℓ^k-torsion subgroup. We use the Kummer exact sequence and the structure of the ring generated by the Frobenius endomorphism. In section 7 we give an algorithm that, on input a degree d plane projective curve over $\mathbb{F}_q$, plus some information on its singularities, and the zeta function of its function field, returns a nice generating set for the group of ℓ^k-torsion points inside $\mathcal{J}(\mathbb{F}_q)$ in probabilistic polynomial time in $\log q$, d and ℓ^k. Sections 8 and 9 are devoted to two families of modular curves. We give a nice plane model for such curves. The general algorithms presented in section 7 are then applied to these modular curves in section 10 in order to compute explicitely the modular representations associated with the discriminant modular form (level 1 and weight 12). This makes a connexion with the Edixhoven's program for computing coefficients of modular forms.

Important remark 1 *The symbol $\mathcal{O}$ in this article stands for a positive effective absolute constant. So any statement containing this symbol becomes true if the symbol is replaced in every occurence by some well chosen positive real number, that may be every time different.*

Important remark 2 *By an algorithm in this paper we usually mean a probabilistic (Las Vegas) algorithm. This is an algorithm that succeeds with probability $\geq \frac{1}{2}$. When it fails, it gives no answer. In some places we shall give deterministic algorithms or probabilistic (Monte-Carlo) algorithms, but this will be stated explicitly. A Monte-Carlo algorithm gives a correct answer with probability $\geq \frac{1}{2}$. But it may give an incorrect answer with probability $\leq \frac{1}{2}$. A*

Monte-Carlo algorithm can be turned into a Las Vegas one, provided we can efficiently check the correctness of the result. The reason for using probabilistic Turing machines is that in many places it will be necessary (or at least wiser) to decompose a divisor as a sum of places. This is the case in particular for the conductor of some plane curve. Another more intrinsically probabilistic algorithm in this paper is the one that searches for generators of the Picard group.

2 Basic algorithms for plane curves

We recall elementary results about computing in the Picard group of an algebraic curve over a finite field. See [9, 18].

2.1 Finite fields

We should first explain how finite fields are represented. The base field $\mathbb{F}_q$ is given by an irreducible polynomial $f(X)$ with degree a and coefficients in $\mathbb{F}_p$ where p is the characteristic and $q = p^a$. So $\mathbb{F}_q$ is $\mathbb{F}_p[X]/f(X)$. An extension of $\mathbb{F}_q$ is given similarly by an irreducible polynomial in $\mathbb{F}_q[X]$. Polynomial factoring in $\mathbb{F}_q[X]$ is probabilistic polynomial time in $\log q$ and the degree of the polynomial to be factored.

2.2 Plane projective curves and their smooth model

We now explain how curves are supposed to be represented in this paper.

To start with, a projective plane curve $C/\mathbb{F}_q$ is given by a degree d homogeneous polynomial $E(X, Y, Z)$ in the three variables X, Y and Z, with coefficients in $\mathbb{F}_q$.

The smooth model $\mathcal{X}$ of C is not given as a projective variety. Indeed, we shall only need a nice local description of $\mathcal{X}$ at every singularity of C. This means we need a list (a labelling) of all places above every singularity of C and a uniformizing parameter at every place. We also need the Laurent series expansions of affine plane coordinates in terms of all these uniformizing parameters.

More precisely, let P be a place above a singular point S and v the corresponding valuation. We say that P is a singular branch. The field of definition of P is an extension field $\mathbb{F}_P$ of $\mathbb{F}_q$ with degree $\leq \frac{(d-1)(d-2)}{2}$. Let x and y be affine coordinates that vanish at the singular point S on C. We need a local parameter t at P and expansions $x = \sum_{k \geq v(x)} a_k t^k$ and $y = \sum_{k \geq v(y)} b_k t^k$ with coefficients in $\mathbb{F}_P$.

Because these expansions are not finite, we just assume we are given an oracle that on input a positive integer n returns the first n terms in all these expansions.

This is what we mean when we say the smooth model $\mathcal{X}$ is given.

We may also assume that we are given the conductor $\mathfrak{C}$ of C as a combination of singular branches with integer coefficients. The degree $\deg(\mathfrak{C})$ is even and we have $\deg(\mathfrak{C}) = 2\delta$ where δ is the difference between the arithmetic genus $\frac{(d-1)(d-2)}{2}$ and the geometric genus g. In fact it suffices to have a divisor $\mathfrak{D}$ that

is greater than the conductor and has polynomial degree in d. Such a divisor can be computed from the equation of C in deterministic polynomial time in $\log q$ and d.

There are many families of curves for which such a smooth model can be given as a Turing machine that answers in probabilistic polynomial time in the size $\log q$ of the field and the degree d of C and the number n of requested significant terms in the parametrizations of singular branches. This is the case for curves with ordinary multiple points for example. We shall show in sections 8 and 9 that this is also the case for two nice families of modular curves.

2.3 Points, forms, and functions

Smooth points on C can be represented by their affine or projective coordinates. Labelling for the branches above singular points is given in the description of $\mathcal{X}$. So we know how to represent divisors on $\mathcal{X}$.

For any integer $h \geq 0$ and extension field K of $\mathbb{F}_q$, we set

$$\mathcal{S}_h/K = H^0(\mathbb{P}^2/K, \mathcal{O}_{\mathbb{P}^2/K}(h))$$

the K-linear space of degree h homogeneous polynomials in X, Y, and Z. It is a vector space of dimension $\frac{(h+1)(h+2)}{2}$ over K. A basis for it is made of all monomials of the form $X^aY^bZ^c$ with $a, b, c \in \mathbb{N}$ and $a+b+c = h$.

We denote by

$$\mathcal{H}^h/K = H^0(\mathcal{X}/K, \mathcal{O}_{\mathcal{X}/K}(h))$$

the space of forms of degree h on $\mathcal{X}/K$. Here $\mathcal{O}_{\mathcal{X}/K}(h)$ is the pullback of $\mathcal{O}_{\mathbb{P}^2/K}(h)$ to $\mathcal{X}$. Let W be a form on $\mathbb{P}^2$ having non-zero pull back $W_{\mathcal{X}}$ on $\mathcal{X}$. Let $H = (W_{\mathcal{X}})$ be the divisor of this retriction. The map $f \mapsto \frac{f}{W_{\mathcal{X}}}$ is a bijection from $H^0(\mathcal{X}/K, \mathcal{O}_{\mathcal{X}/K}(h))$ to the linear space $\mathcal{L}(H)$. If Δ is a divisor on $\mathcal{X}/K$ we note $\mathcal{H}^h(\Delta)/K$ the subspace of forms in $\mathcal{H}^h/K$ with divisor $\geq \Delta$. The dimension of $\mathcal{H}^h(\mathfrak{C})$ is at least $dh + 1 - g - \deg(\mathfrak{C})$ and is equal to this number when it exceeds $g-1$. This is the case if $h \geq d$. The dimension of $\mathcal{H}^h(\mathfrak{C})$ is greater than $2g$ if $h \geq 2d$.

The image of the restriction map $\rho : \mathcal{S}_h \to \mathcal{H}^h$ contains $\mathcal{H}^h(\mathfrak{C})$ according to Noether's residue theorem [8, Theorem 7].

We set $h_C = 2d$ and $S_C = \mathcal{S}_{h_C}$ and $\mathcal{H}_C = \mathcal{H}^{h_C}(\mathfrak{C})$, and $H_C = \rho^{-1}(\mathcal{H}_C) \subset S_C$ and $K_C = \mathrm{Ker}(\rho) \subset H_C$.

So we have $0 \to K_C \to H_C \to \mathcal{H}_C \to 0$.

To find linear equations for $H_C \subset S_C$ we consider a generic homogeneous form $F(X,Y,Z) = \sum_{a+b+c=h_C} \epsilon_{a,b,c} X^aY^bZ^c$ of degree h_C in X, Y and Z.

For every branch P above a singular point S with homogeneous coordinates $[X,Y,Z]$ (assuming for example that P has non-zero Z-coordinate) we replace in $F(\frac{X}{Z}, \frac{Y}{Z}, 1)$ the affine coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ by their expansions as series in the local parameter t at this branch.

We ask the resulting series in t to have valuation at least the multiplicity of P in the conductor $\mathfrak{C}$.

Every singular branch thus produces linear equations in the $\epsilon_{a,b,c}$. The collection of all such equations defines the subspace H_C.

A basis for the subspace $K_C \subset H_C \subset S_C$ consists of all $X^a Y^b Z^c E(X,Y,Z)$ with $a+b+c = h_C - d$. We fix a supplementary space M_C to K_C in H_C and assimilate $\mathcal{H}_C$ to it.

Given a homogeneous form in three variables one can compute its divisor using resultants and the given expansions of affine coordinates in terms of the local parameters at every singular branch.

A function is given as a quotient of two forms.

2.4 The Brill-Noether algorithm

Linear spaces of forms computed in the previous paragraph allow us to compute in the group $\mathcal{J}(\mathbb{F}_q)$ of $\mathbb{F}_q$-points in the jacobian of $\mathcal{X}$. We fix an effective $\mathbb{F}_q$-divisor ω with degree g on $\mathcal{X}$. A point $\alpha \in \mathcal{J}(\mathbb{F}_q)$ is represented by a divisor $A - \omega$ in the corresponding linear equivalence class, where A is an effective $\mathbb{F}_q$-divisor with degree g. Given another point $\beta \in \mathcal{J}(\mathbb{F}_q)$ by a similar divisor $B - \omega$, we can compute the space $\mathcal{H}^{h_C}(\mathfrak{C} + A + B)$ which is non-trivial and pick a non-zero form f_1 in it. The divisor of f_1 is $(f_1) = A + B + \mathfrak{C} + R$ where R is an effective divisor with degree $(2g-2)h_C - 2g - 2\delta$. The linear space $\mathcal{H}^{h_C}(\mathfrak{C} + R + \omega)$ has dimension at least 1. We pick a non-zero form f_2 in it. It has divisor $(f_2) = \mathfrak{C} + R + \omega + D$ where D is effective with degree g. And $D - \omega$ is linearly equivalent to $A - \omega + B - \omega$.

In order to invert the class α of $A - \omega$ we pick a non-zero form f_1 in $\mathcal{H}^{h_C}(\mathfrak{C} + 2\omega)$. The divisor of f_1 is $(f_1) = 2\omega + \mathfrak{C} + R$ where R is an effective divisor with degree $(2g-2)h_C - 2g - 2\delta$. The linear space $\mathcal{H}^{h_C}(\mathfrak{C} + R + A)$ has dimension at least 1. We pick a non-zero form f_2 in it. It has divisor $(f_2) = \mathfrak{C} + R + A + B$ where B is effective with degree g. And $B - \omega$ is linearly equivalent to $-(A - \omega)$.

This algorithm works just as well if we replace $\mathfrak{C}$ by some $\mathfrak{D} \geq \mathfrak{C}$ having polynomial degree in d.

Lemma 1 (Arithmetic operations in the jacobian) *Let $C/\mathbb{F}_q$ be a degree d plane projective absolutely irreducible reduced curve. Let g be the geometric genus of C. Assume we are given the smooth model $\mathcal{X}$ of C and a degree g origin $\mathbb{F}_q$-divisor ω on $\mathcal{X}$. Arithmetic operations in the Picard group $\mathrm{Pic}^0(\mathcal{X}/\mathbb{F}_q)$ can be performed in polynomial time in $\log q$ and d. This includes addition, substraction and comparison of divisor classes.*

We now recall the principle of the Brill-Noether algorithm for computing complete linear series. Functions in $\mathbb{F}_q(\mathcal{X})$ are represented as quotients of forms.

Lemma 2 (Brill-Noether) *There exists an algorithm that on input a degree d plane projective absolutely irreducible reduced curve $C/\mathbb{F}_q$ and the smooth model $\mathcal{X}$ of C and two effective $\mathbb{F}_q$-divisors A and B on $\mathcal{X}$, computes a basis for $\mathcal{L}(A - B)$ in time polynomial in d and $\log q$ and the degrees of A and B.*

We assume $\deg(A) \geq \deg(B)$, otherwise $\mathcal{L}(A - B) = 0$. We let h be the smallest integer such that $h \geq h_C$ and $\dim(\mathcal{H}^h(\mathfrak{C} + A)) > 0$.

The space $\mathcal{H}^h(\mathfrak{C}+A)$ is non-zero and is contained in the image of the restriction map $\rho : \mathcal{S}_h \to \mathcal{H}^h$ so that we can represent it as a subspace of $\mathcal{S}_h$. We pick a non-zero form f in $\mathcal{H}^h(\mathfrak{C}+A)$ and compute its divisor $(f) = \mathfrak{C}+A+D$.

The space $\mathcal{H}^h(\mathfrak{C}+B+D)$ is contained in the image of the restriction map $\rho : \mathcal{S}_h \to \mathcal{H}^h$ so that we can represent it as a subspace of $\mathcal{S}_h$. We compute forms γ_1, γ_2, ..., γ_k in $\mathcal{S}_h$ such that their images by ρ provide a basis for $\mathcal{H}^h(\mathfrak{C}+B+D)$. A basis for $\mathcal{L}(A-B)$ is made of the functions $\frac{\gamma_1}{f}$, $\frac{\gamma_2}{f}$, ..., $\frac{\gamma_k}{f}$. Again this algorithm works just as well if we replace $\mathfrak{C}$ by some $\mathfrak{D} \geq \mathfrak{C}$ having polynomial degree in d. □

We deduce an explicit moving lemma for divisors.

Lemma 3 (Moving divisor lemma I) *There exists an algorithm that on input a degree d plane projective absolutely irreducible reduced curve $C/\mathbb{F}_q$ and the smooth model $\mathcal{X}$ of C and a degree zero $\mathbb{F}_q$-divisor $D = D^+ - D^-$ and an effective divisor A with degree $< q$ on $\mathcal{X}$ computes a divisor $E = E^+ - E^-$ linearly equivalent to D and disjoint to A in time polynomial in d and $\log q$ and the degrees of D^+, and A. Further the degree of E^+ and E^- can be taken to be $\leq 2gd$.*

Let O be an $\mathbb{F}_q$-rational divisor on $\mathcal{X}$ having degree $\leq d$ and disjoint to A. We may take O to be a well chosen fiber of some plane coordinate function on $\mathcal{X}$. We compute the linear space $\mathcal{L} = \mathcal{L}(D^+ - D^- + 2gO)$. The subset of functions f in $\mathcal{L}$ such that $(f)+D^+-D^-+2gO$ is not disjoint to A is contained in a union of at most $\deg(A) < q$ hyperplanes. We conclude invoking lemma 4 below. □

There remains to state and prove the

Lemma 4 (Solving inequalities) *Let q be a prime power, $d \geq 2$ and $n \geq 1$ two integers and let H_1, ..., H_n be hyperplanes inside $V = \mathbb{F}_q^d$, each given by a linear equation. Assume $n < q$. There exists a deterministic algorithm that finds a vector in $U = V - \bigcup_{1 \leq k \leq n} H_k$ in time polynomial in $\log q$, d and n.*

This is proven by lowering the dimension d. For $d = 2$ we pick any affine line L in V not containing the origin. We observe that there are at least $q - n$ points in $U \cap L = L - \bigcup_{1 \leq k \leq n} L \cap H_k$. We enumerate points in L until we find one which is not in any H_k. This requires at most $n + 1$ trials.

Assume now d is bigger than 2. Hyperplanes in V are parametrized by the projective space $\mathbb{P}(\hat{V})$ where $\hat{V}$ is the dual of V. We enumerate points in $\mathbb{P}(\hat{V})$ until we find a hyperplane K distinct from every H_k. We compute a basis for K and an equation for every $H_k \cap K$ in this basis. This way, we have lowered the dimension by 1. □

We can strengthen a bit the moving divisor algorithm by removing the condition that A has degree $< q$. Indeed, in case this condition is not met, we pick two distinct primes α and β such that $q^\alpha > \deg(A)$ and $q^\beta > \deg(A)$. We apply lemma 3 after base change to the field with q^α element and find a divisor E_α. We call e_α the norm of E_α from $\mathbb{F}_{q^\alpha}$ to $\mathbb{F}_q$. It is equivalent to αD. We similarly construct a divisor e_β that is equivalent to βD. Let u and v be positive

integers such that $\alpha u - \beta v = 1$. We return the divisor $E = ue_\alpha - ve_\beta = E^+ - E^-$. We observe that we can take $\alpha \leq 2 + 2\log_q \deg(A)$ and $\beta \leq 2\alpha$ and $u < \beta$ and $v < \alpha$ so the degree of E^+ is $\leq 12gd(\log_q(\deg(A)) + 1)$.

Lemma 5 (Moving divisor lemma II) *There exists an algorithm that on input a degree d plane projective absolutely irreducible curve $C/\mathbb{F}_q$ and the smooth model $\mathcal{X}$ of C and a degree zero $\mathbb{F}_q$-divisor $D = D^+ - D^-$ and an effective divisor A on $\mathcal{X}$ computes a divisor $E = E^+ - E^-$ linearly equivalent to D and disjoint to A in time polynomial in d and $\log q$ and the degrees of D^+, and A. Further the degree of E^+ and E^- can be taken to be $\leq 12gd(\log_q(\deg(A)) + 1)$.*

3 A first approach to picking random divisors

Given a finite field $\mathbb{F}_q$ and a plane projective absolutely irreducible reduced curve C over $\mathbb{F}_q$ with projective smooth model $\mathcal{X}$, we call $\mathcal{J}$ the jacobian of $\mathcal{X}$ and we consider the two related problems : picking a random element in $\mathcal{J}(\mathbb{F}_q)$ with (close to) uniform distribution and finding a generating set for (a large subgroup of) $\mathcal{J}(\mathbb{F}_q)$.

We will assume the size q of the field is greater than or equal to $4g^2$. This condition ensures the existence of a $\mathbb{F}_q$-rational point[1].

Picking efficiently and provably random elements in $\mathcal{J}(\mathbb{F}_q)$ with uniform distribution seems difficult to us. We first give here an algorithm for efficiently constructing random divisors with a distribution that is far from uniform but still sufficient to construct a generating set for a large subgroup of $\mathcal{J}(\mathbb{F}_q)$. Once given generators, picking random elements becomes much easier.

Let r be the smallest prime integer bigger than 30, $2g-2$ and d. We observe r is less than $\max(4g - 4, 2d, 60)$.

The set $\mathcal{P}(r, q)$ of $\mathbb{F}_q$-places with degree r on $\mathcal{X}$ has cardinality

$$\#\mathcal{P}(r,q) = \frac{\#\mathcal{X}(\mathbb{F}_{q^r}) - \#\mathcal{X}(\mathbb{F}_q)}{r}.$$

So

$$(1 - 10^{-2})\frac{q^r}{r} \leq \#\mathcal{P}(r,q) \leq (1 + 10^{-2})\frac{q^r}{r}.$$

Indeed, $|\#\mathcal{X}(\mathbb{F}_{q^r}) - q^r - 1| \leq 2gq^{\frac{r}{2}}$ and $|\#\mathcal{X}(\mathbb{F}_q) - q - 1| \leq 2gq^{\frac{1}{2}}$. So $\left|\#\mathcal{P}(r,q) - \frac{q^r}{r}\right| \leq \frac{4g+3}{r}q^{\frac{r}{2}} \leq 8q^{\frac{r}{2}}$ and $8rq^{\frac{-r}{2}} \leq r2^{3-\frac{r}{2}} \leq 10^{-2}$ since $r \geq 31$.

Since we are given a degree d plane model C for the curve $\mathcal{X}$, we have a degree d map $x : \mathcal{X} \to \mathbb{P}^1$. Since $d < r$, the function x maps $\mathcal{P}(r, q)$ to the set $\mathcal{U}(r, q)$ of unitary prime polynomials of degree r over $\mathbb{F}_q$. The cardinality of $\mathcal{U}(r, q)$ is $\frac{q^r - q}{r}$ so

[1] If we are given a curve over $\mathbb{F}_q$ with genus g such that $q < 4g^2$ then we find ourselves in a much better situation. By the Riemann hypothesis the Picard group is generated by the classes of prime divisors of degree $\leq d$ where d is the first integer bigger than or equal to $2\log_q(4g - 2)$. See [7]. The number of such divisors is then bounded by a polynomial in the genus. So the problems treated in that section become trivial in this special case.

$$(1-10^{-9})\frac{q^r}{r} \leq \#\mathcal{U}(r,q) \leq \frac{q^r}{r}.$$

The fibers of the map $x : \mathcal{P}(r,q) \to \mathcal{U}(r,q)$ have cardinality between 0 and d.

We can pick a random element in $\mathcal{U}(r,q)$ with uniform distribution in the following way : we pick a random unitary polynomial of degree r with coefficients in $\mathbb{F}_q$, with uniform distribution. We check whether it is irreducible. If it is, we output it. Otherwise we start again. This is polynomial time in r and $\log q$.

Given a random element in $\mathcal{U}(r,q)$ with uniform distribution, we can compute the fiber of x above it and, provided it is non-empty, pick a random element in it with uniform distribution. If the fiber is empty, we pick another element in $\mathcal{U}(r,q)$ until we find a non-empty fiber. At least one over $d \times (0.99)^{-1}$ fiber is non-empty. We thus define a distribution μ on $\mathcal{P}(r,q)$ and prove the following

Lemma 6 (A very rough measure) *There exists a probabilistic algorithm that picks a random element in $\mathcal{P}(r,q)$ with distribution μ in time polynomial in d and $\log q$. For every subset Z of $\mathcal{P}(r,q)$ the measure $\mu(Z)$ is related to the uniform measure $\frac{\#Z}{\#\mathcal{P}(r,q)}$ by*

$$\frac{\#Z}{d\#\mathcal{P}(r,q)} \leq \mu(Z) \leq \frac{d\#Z}{\#\mathcal{P}(r,q)}.$$

Now let $\mathcal{D}(r,q)$ be the set of effective $\mathbb{F}_q$-divisors with degree r on $\mathcal{X}$.

Since we have assumed $q \geq 4g^2$ we know that $\mathcal{X}$ has at least one $\mathbb{F}_q$-rational point.

Let Ω be a degree r effective divisor on $\mathcal{X}/\mathbb{F}_q$. Now we associate to every α in $\mathcal{D}(r,q)$ the class of $\alpha - \Omega$ in $\mathcal{J}(\mathbb{F}_q)$. This defines a surjection $\zeta : \mathcal{D}(r,q) \to \mathcal{J}(\mathbb{F}_q)$ with all its fibers having cardinality $\#\mathbb{P}^{r-g}(\mathbb{F}_q)$.

So the set $\mathcal{D}(r,q)$ has cardinality $\frac{q^{r-g+1}-1}{q-1}\#\mathcal{J}(\mathbb{F}_q)$.

So

$$\#\mathcal{P}(r,q) \leq \#\mathcal{D}(r,q) \leq q^{r-g}\frac{1-\frac{1}{q^{r-g+1}}}{1-\frac{1}{q}}q^g(1+\frac{1}{\sqrt{q}})^{2g}.$$

Since $q \geq 4g^2$ we have $\#\mathcal{D}(r,q) \leq 2eq^r$.

Assume G is a finite group and ψ an epimorphism of groups $\psi : \mathcal{J}(\mathbb{F}_q) \to G$. We look for some divisor $\Delta \in \mathcal{D}(r,q)$ such that $\psi(\zeta(\Delta)) \neq 0 \in G$. Since all the fibers of $\psi \circ \zeta$ have the same cardinality, the fiber above 0 has at most $\frac{2eq^r}{\#G}$ elements. So the number of prime divisors $\Delta \in \mathcal{P}(r,q)$ such that $\psi(\zeta(\Delta))$ is not 0 is at least $q^r(\frac{0.99}{r} - \frac{2e}{\#G})$. We assume $\#G$ is at least $12r$. Then at least half of the divisors in $\mathcal{P}(r,q)$ are not mapped onto 0 by $\psi \circ \zeta$. The μ-measure of the subset consisting of these elements is at least $\frac{1}{2d}$.

So if we pick a random Δ in $\mathcal{P}(r,q)$ with μ-measure as in lemma 6, the probability of success is at least $\frac{1}{2d}$.

Lemma 7 (Finding non-zero classes) *There exists a probabilistic (Monte-Carlo) algorithm that takes as input*

1. *a degree d and geometric genus g plane projective absolutely irreducible reduced curve C over $\mathbb{F}_q$, such that $q \geq 4g^2$,*

2. *the smooth model $\mathcal{X}$ of C,*

3. *a degree g effective divisor ω, as origin,*

4. *an epimorphism $\psi : \mathrm{Pic}^0(\mathcal{X}/\mathbb{F}_q) \to G$ (that need not be computable) such that the cardinality of G is at least $\max(48g, 24d, 720)$,*

and outputs a sequence of $2d$ elements in $\mathrm{Pic}^0(\mathcal{X}/\mathbb{F}_q)$ such that at least one of them is not in the kernel of ψ with probability $\geq \frac{1}{2}$. The algorithm is polynomial time in d and $\log q$.

As a special case we take $G = G_0 = \mathcal{J}(\mathbb{F}_q)$ and $\psi = \psi_0$ the identity. Applying lemma 7 we find a sequence of elements in $\mathcal{J}(\mathbb{F}_q)$ out of which one at least is non-zero. We take G_1 to be quotient of G by the subgroup generated by these elements and ψ_1 the quotient map. Applying the lemma again we construct another sequence of elements in $\mathcal{J}(\mathbb{F}_q)$ out of which one at least is not in G_0. We go on like that and produce a sequence of subgroups in $\mathcal{J}(\mathbb{F}_q)$ that increase with constant probability until the index in $\mathcal{J}(\mathbb{F}_q)$ becomes smaller than $\max(48g, 24d, 720)$.

Lemma 8 (Finding an almost generating set) *There exists a probabilistic (Monte-Carlo) algorithm that takes as input*

1. *a degree d and geometric genus g plane projective absolutely irreducible reduced curve C over $\mathbb{F}_q$, such that $q \geq 4g^2$,*

2. *the smooth model $\mathcal{X}$ of C,*

3. *a degree g effective divisor ω, as origin,*

and outputs a sequence of elements in $\mathrm{Pic}^0(\mathcal{X}/\mathbb{F}_q)$ that generate a subgroup of index at most

$$\max(48g, 24d, 720)$$

with probability $\geq \frac{1}{2}$. The algorithm is polynomial time in d and $\log q$.

4 Pairings

Let m be a prime to p integer and $\mathcal{J}$ a jacobian variety over $\mathbb{F}_q$. The Weil pairing relates the full m-torsion subgroup $\mathcal{J}(\bar{\mathbb{F}}_q)[m]$ with itself. It can be defined using Kummer theory and is geometric in nature. The Tate-Lichtenbaum-Frey-Ruck pairing is more cohomological and relates the m-torsion $\mathcal{J}(\mathbb{F}_q)[m]$ in the group of $\mathbb{F}_q$-rational points and the quotient $\mathcal{J}(\mathbb{F}_q)/m\mathcal{J}(\mathbb{F}_q)$. In this section, we quickly review the definitions and algorithmic properties of these pairings, following work by Weil, Lang, Menezes, Okamoto, Vanstone, Frey and Ruck.

For every abelian variety A, we denote by $Z_0(A)_0$ the group of 0-cycles with degree 0 and by $S : Z_0(A)_0 \to A$ the summation map, that associates to every 0-cycle of degree 0 the corresponding sum in A.

Let V and W be two projective non-singular absolutely irreducible varieties over an algebraically closed field k with characteristic p, and let $\alpha : V \to A$ and $\beta : W \to B$ be canonical maps into their Albanese varieties. Let D be a correspondence on $V \times W$.

Let $n \geq 2$ be a prime to p integer. Let $\mathfrak{a}$ (resp. $\mathfrak{b}$) be a 0-cycle of degree 0 on V (resp. W) and let $a = S(\alpha(\mathfrak{a}))$ (resp. $b = S(\beta(\mathfrak{b}))$) be the associated point in A (resp. B). Assume $na = nb = 0$.

Following [11, VI, §4, Theorem 10] one can define the Weil pairing $e_{n,D}(a, b)$. It is an n-th root of unity in k. It depends linearly in a, b and D.

Assume $V = W = \mathcal{X}$ is a smooth projective absolutely irreducible reduced curve and $A = B = \mathcal{J}$ is its jacobian and $\alpha = \beta = f : \mathcal{X} \to \mathcal{J}$ is the Jacobi map (once chosen an origin on $\mathcal{X}$). If we take D to be the diagonal on $\mathcal{X} \times \mathcal{X}$ we define a pairing $e_{n,D}(a, b)$ that will be denoted $e_n(a, b)$ or $e_{n,\mathcal{X}}(a, b)$. It does not depend on the origin for the Jacobi map. It is non-degenerate.

If $\mathcal{Y}$ is another smooth projective absolutely irreducible reduced curve and $\mathcal{K}$ its jacobian and $\phi : \mathcal{X} \to \mathcal{Y}$ a non-constant map with degree d, and $\phi^* : \mathcal{K} \to \mathcal{J}$ the associated map between jacobians, then for a and b of order dividing n in $\mathcal{K}$ one has $e_{n,\mathcal{X}}(\phi^*(a), \phi^*(b)) = e_{n,\mathcal{Y}}(a, b)^d$.

The Frey-Ruck pairing can be constructed from the Lichtenbaum version of Tate pairing [12] as was shown in [6]. Let $\mathbb{F}_q$ be a finite field with characteristic p. Let again $n \geq 2$ be a prime to p integer and $\mathcal{X}$ a smooth projective absolutely irreducible reduced curve over $\mathbb{F}_q$. Let g be the genus of $\mathcal{X}$. We assume n divides $q - 1$. Let $\mathcal{J}$ be the jacobian of $\mathcal{X}$. The Frey-Ruck pairing $\{,\}_n : \mathcal{J}(\mathbb{F}_q)[n] \times \mathcal{J}(\mathbb{F}_q)/n\mathcal{J}(\mathbb{F}_q) \to {\mathbb{F}_q}^*/({\mathbb{F}_q}^*)^n$ is defined as follows. We take a class of order dividing n in $\mathcal{J}(\mathbb{F}_q)$. Such a class can be represented by an $\mathbb{F}_q$-divisor D with degree 0. We take a class in $\mathcal{J}(\mathbb{F}_q)$ and pick a degree zero $\mathbb{F}_q$-divisor E in this class, that we assume to be disjoint to D. The pairing evaluated at the classes $[D]$ and $[E]$ mod n is $\{[D], [E] \bmod n\}_n = f(E) \bmod ({\mathbb{F}_q}^*)^n$ where f is any function with divisor nD.

This is a non-degenerate pairing.

We now explain how one can compute the Weil pairing, following work by Menezes, Okamoto, Van Stone, Frey and Ruck. The Tate-Lichtenbaum-Frey-Ruck pairing can be computed similarly.

The Weil pairing is computed as follows. As usual, we assume we are given a degree d plane model C for $\mathcal{X}$. Assume $\mathfrak{a}$ and $\mathfrak{b}$ have disjoint support (otherwise we may replace $\mathfrak{a}$ by some linearly equivalent divisor using the explicit moving lemma 3.)

We compute a function ϕ with divisor $n\mathfrak{a}$. We similarly compute a function ψ with divisor $n\mathfrak{b}$. Then $e_n(a, b) = \frac{\psi(\mathfrak{a})}{\phi(\mathfrak{b})}$. This algorithm is polynomial in the degree d of C and the order n of the divisors, provided the initial divisors $\mathfrak{a}$ and $\mathfrak{b}$ are given as differences between effective divisors with polynomial degree in d.

Using an idea that appears in a paper by Menezes, Okamoto and Vanstone [14] in the context of elliptic curves, and in [6] for general curves, one can make

this algorithm polynomial in $\log n$ in the following way.

We write $\mathfrak{a} = \mathfrak{a}_0 = \mathfrak{a}_0^+ - \mathfrak{a}_0^-$ where $\mathfrak{a}_0^+$ and $\mathfrak{a}_0^-$ are effective divisors. Let ϕ be the function computed in the above simple minded algorithm. One has $(\phi) = n\mathfrak{a}_0^+ - n\mathfrak{a}_0^-$. We want to express ϕ as a product of small degree functions. We use a variant of fast exponentiation. Using lemma 3 we compute a divisor $\mathfrak{a}_1 = \mathfrak{a}_1^+ - \mathfrak{a}_1^-$ and a function ϕ_1 such that $\mathfrak{a}_1$ is disjoint to $\mathfrak{b}$ and $(\phi_1) = \mathfrak{a}_1 - 2\mathfrak{a}_0$ and such that the degrees of $\mathfrak{a}_1^+$ and $\mathfrak{a}_1^-$ are $\leq 12gd(\log_q(\deg(\mathfrak{b})) + 1)$. We go on and compute, for $k \geq 1$ an integer, a divisor $\mathfrak{a}_k = \mathfrak{a}_k^+ - \mathfrak{a}_k^-$ and a function ϕ_k such that $\mathfrak{a}_k$ is disjoint to $\mathfrak{b}$ and $(\phi_k) = \mathfrak{a}_k - 2\mathfrak{a}_{k-1}$ and such that the degrees of $\mathfrak{a}_k^+$ and $\mathfrak{a}_k^-$ are $\leq 12gd(\log_q(\deg(\mathfrak{b})) + 1)$.

We write the base 2 expansion of $n = \sum_i \epsilon_k 2^k$ with $\epsilon_k \in \{0, 1\}$. We compute the function Ψ with divisor $\sum_k \epsilon_k \mathfrak{a}_k$. We claim that the function ϕ can be written as a product of the ϕ_k, for $k \leq \log_2 n$, and Ψ with suitable integer exponents bounded by n in absolute value. Indeed we write $\mu_1 = \phi_1$, $\mu_2 = \phi_2\phi_1^2$, $\mu_3 = \phi_3\phi_2^2\phi_1^4$ and so on. We have $(\mu_k) = \mathfrak{a}_k - 2^k\mathfrak{a}$ and $\Phi\prod_k \mu_k^{-\epsilon_k}$ has divisor $n\mathfrak{a}$ so is the ϕ we were looking for.

Lemma 9 (Computing the Weil pairing) *There exists an algorithm that on input a prime to q integer $n \geq 2$ and a degree d absolutely irreducible reduced plane projective curve C over $\mathbb{F}_q$ and its smooth model $\mathcal{X}$ and two effective $\mathbb{F}_q$-divisors on $\mathcal{X}$, denoted $\mathfrak{a} = \mathfrak{a}^+ - \mathfrak{a}^-$ and $\mathfrak{b} = \mathfrak{b}^+ - \mathfrak{b}^-$, with degree 0, and order dividing n in the jacobian, computes the Weil pairing $e_n(\mathfrak{a}, \mathfrak{b})$ in time polynomial in d, $\log q$, $\log n$ and the degrees of $\mathfrak{a}^+$, $\mathfrak{a}^-$, $\mathfrak{b}^+$, $\mathfrak{b}^-$.*

Lemma 10 (Computation of Tate-Lichtenbaum-Frey-Ruck pairings) *There exists an algorithm that on input a prime to q integer $n \geq 2$ and a degree d absolutely irreducible reduced plane projective curve C over $\mathbb{F}_q$ and its smooth model $\mathcal{X}$ and two effective $\mathbb{F}_q$-divisors on $\mathcal{X}$, denoted $\mathfrak{a} = \mathfrak{a}^+ - \mathfrak{a}^-$ and $\mathfrak{b} = \mathfrak{b}^+ - \mathfrak{b}^-$, with degree 0, and such that the class of $\mathfrak{a}$ has order dividing $n \geq 2$ in the jacobian, computes the Tate-Lichtenbaum-Frey-Ruck pairing $\{\mathfrak{a}, \mathfrak{b}\}_n$ in time polynomial in d, $\log q$, $\log n$ and the degrees of $\mathfrak{a}^+$, $\mathfrak{a}^-$, $\mathfrak{b}^+$, $\mathfrak{b}^-$.*

5 Divisible groups

For ℓ a prime integer, it is convenient to introduce ℓ-divisible subgroups inside the ℓ^∞-torsion of a jacobian $\mathcal{J}$, that may or may not correspond to subvarieties. We see how to define such subgroups and control their rationality properties.

Definition 1 (Divisible group) *Let $\mathbb{F}_q$ be a finite field with characteristic p and let $\mathcal{X}$ be a projective smooth absolutely irreducible reduced algebraic curve over $\mathbb{F}_q$. Let g be the genus of $\mathcal{X}$ and let ℓ be a prime integer and $n = \ell^k$ a power of ℓ. We assume $g \geq 1$. Let $\mathcal{J}$ be the jacobian of $\mathcal{X}$ and let $\mathcal{E}nd(\mathcal{J}/\mathbb{F}_q)$ be the ring of endomorphisms of $\mathcal{J}$ over $\mathbb{F}_q$. Let $\Pi : J[\ell^\infty] \to J[\ell^\infty]$ be a group homomorphism whose restriction to its image $\mathbb{G}$ is a bijection. Multiplication by ℓ is then a surjection from $\mathbb{G}$ to itself. We denote by $\mathbb{G}[\ell^k]$ the ℓ^k-torsion in $\mathbb{G}$. There is an integer w such that $\mathbb{G}[\ell^k]$ is a free $\mathbb{Z}/\ell^k\mathbb{Z}$ module of rank w for every k. We assume that Π commutes with the Frobenius endomorphism F_q.*

We then say $\mathbb{G}$ *is the divisible group associated with* Π. *From Tate theorem [17]* Π *is induced by some endomorphism in* $\mathcal{E}nd(\mathcal{J}/\mathbb{F}_q)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell$ *and we can define* Π^* *the Rosati dual of* Π *and denote by* $\mathbb{G}^* = \mathrm{Im}(\Pi^*)$ *the associated divisible group, that we call the adjoint of* $\mathbb{G}$.

Let $\chi(X)$ be the characteristic polynomial of the Frobenius endomorphism $F_q \in \mathcal{E}nd(\mathcal{J}/\mathbb{F}_q)$. Let $F(X) = F_1(X)$ and $G(X) = G_1(X)$ be two unitary coprime polynomials in $\mathbb{F}_\ell[X]$ such that $\chi(X) = F_1(X)G_1(X) \bmod \ell$. From Bezout's theorem we have two polynomials $H_1(X)$ and $K_1(X)$ in $\mathbb{F}_\ell[X]$ such that $F_1H_1 + G_1K_1 = 1$ and $\deg(H_1) < \deg(G_1)$ and $\deg(K_1) < \deg(F_1)$. From Hensel's lemma, for every positive integer k there exist four polynomials $F_k(X)$, $G_k(X)$, $H_k(X)$ and $K_k(X)$ in $(\mathbb{Z}/\ell^k\mathbb{Z})[X]$ such that F_k and G_k are unitary an $\chi(X) = F_k(X)G_k(X) \bmod \ell^k$ and $F_kH_k + G_kK_k = 1 \bmod \ell^k$ and $\deg(H_k) < \deg(G_1)$ and $\deg(K_1) < \deg(F_1)$ and $F_1 = F_k \bmod \ell$, $G_1 = G_k \bmod \ell$, $H_1 = H_k \bmod \ell$, $K_1 = K_k \bmod \ell$. The sequences $(F_k)_k$, $(G_k)_k$, $(H_k)_k$, $(K_k)_k$ converge in $\mathbb{Z}_\ell[X]$ to F_0, G_0, H_0, K_0. If we substitute X by F_q in F_0H_0 we define a map $\Pi_G : \mathcal{J}[\ell^\infty] \to \mathcal{J}[\ell^\infty]$ and similarly, if we substitute X by F_q in G_0K_0 we define a map Π_F. It is clear that $\Pi_F^2 = \Pi_F$ and $\Pi_G^2 = \Pi_G$ and $\Pi_F + \Pi_G = 1$ and $\Pi_F\Pi_G = 0$. We call $\mathbb{G}_F = \mathrm{Im}(\Pi_F)$ and $\mathbb{G}_G = \mathrm{Im}(\Pi_G)$ the associated supplementary ℓ-divisible groups. The Rosati dual to F_q is q/F_q. Let $\mathcal{O} = \mathbb{Z}[X]/\chi(X)$ and $\mathcal{O}_\ell = \mathbb{Z}_\ell[X]/\chi(X)$. We set $\varphi_q = X \bmod \chi(X) \in \mathcal{O}$. Maping φ_q onto F_q defines an epimorphism from the ring $\mathcal{O}$ onto $\mathbb{Z}[F_q]$.

Definition 2 (Characteristic subspaces) *For every non-trivial unitary factor* F *of* $\chi(X) \bmod \ell$ *such that the cofactor* $G = \chi/F \bmod \ell$ *is prime to* F, *we write* $\chi = F_0G_0$ *the corresponding factorization in* $\mathbb{Z}_\ell[X]$. *The* ℓ*-divisible group* $\mathbb{G}_F$ *is called the* F_0*-torsion in* $\mathcal{J}[\ell^\infty]$ *and is denoted* $\mathcal{J}[\ell^\infty, F_0]$. *It is the characteristic subspace of* F_q *associated with the factor* F. *If* $F = (X-1)^e$ *is the largest power of* $X-1$ *dividing* $\chi(X) \bmod \ell$ *we abbreviate* $\mathbb{G}_{(X-1)^e} = \mathbb{G}_1$. *If* $\ell \neq p$ *and* $F = (X-q)^e$ *then we write similarly* $\mathbb{G}_{(X-q)^e} = \mathbb{G}_q = \mathbb{G}_1^*$.

We now compute fields of definitions for torsion points.

We assume ℓ is prime to q. The element φ_q belongs to the unit group $\mathcal{U}_1 = (\mathcal{O}/\ell\mathcal{O})^*$ of the quotient algebra $\mathcal{O}/\ell\mathcal{O} = \mathbb{F}_\ell[X]/\chi(X)$. Let the prime factorization of $\chi(X) \bmod \ell$ be $\prod_i \chi_i(X)^{e_i}$ with $\deg(\chi_i) = f_i$. The order of $\mathcal{U}_1$ is $\prod_i(\ell^{f_i}-1)\ell^{(e_i-1)f_i}$. Let γ be the smallest integer such that ℓ^γ is bigger than or equal to $2g$. Then the exponent of the group $\mathcal{U}_1$ divides $A_1 = \ell^\gamma \prod_i(\ell^{f_i}-1)$. We set $B_1 = \prod_i(\ell^{f_i}-1)$ and $C_1 = \ell^\gamma$. There is a unique polynomial $M_1(X)$ with degree $< 2g$ such that $\frac{\varphi_q^{A_1}-1}{\ell} = M_1(\varphi_q) \in \mathcal{O}$.

Now for every positive integer k, the element φ_q belongs to the unit group $\mathcal{U}_k = (\mathcal{O}/\ell^k\mathcal{O})^*$ of the quotient algebra $\mathcal{O}/\ell^k\mathcal{O} = \mathbb{Z}[X]/(\ell^k, \chi(X))$. The prime factorization of $\chi(X) \bmod \ell$ is lifted modulo ℓ^k as $\prod_i \Xi_i(X)$ with $\deg(\Xi_i) = e_if_i$ and the order of $\mathcal{U}_k$ is $\prod_i(\ell^{f_i}-1)\ell^{f_i(ke_i-1)}$. The exponent of the latter group divides $A_k = A_1\ell^{k-1}$. So we set $B_k = B_1 = \prod_i(\ell^{f_i}-1)$ and $C_k = C_1\ell^{k-1} = \ell^{k-1+\gamma}$. There is a unique polynomial $M_k(X)$ with degree $< \deg(\chi)$ such that $\frac{\varphi_q^{A_k}-1}{\ell^k} = M_k(\varphi_q) \in \mathcal{O}$. For every integer $N \geq 2$ we can compute $M_k(X) \bmod N$ from $\chi(X)$ in probabilistic polynomial time in $\log q$, $\log \ell$, $\log N$, k, g : we first

factor $\chi(X) \bmod \ell$ then compute χ and the e_i and f_i. We compute X^{A_k} modulo $(\chi(X), \ell^k N)$ using fast exponentiation. We remove 1 and divide by ℓ^k.

Lemma 11 (Frobenius and ℓ-torsion) *Let k be a positive integer and $\ell \neq p$ a prime. Let $\chi(X)$ be the characteristic polynomial of the Frobenius F_q of $\mathcal{J}$. Let e_i and f_i be the multiplicities and inertiae in the prime decomposition of $\chi(X) \bmod \ell$. Let γ be the smallest integer such that ℓ^γ is bigger than or equal to $2g$. Let $B = \prod_i (\ell^{f_i} - 1)$. Let $C_k = \ell^{k-1+\gamma}$ and $A_k = BC_k$. The ℓ^k-torsion in $\mathcal{J}$ decomposes over the degree A_k extension of $\mathbb{F}_q$. There is a degree $< 2g$ polynomial $M_k(X) \in \mathbb{Z}[X]$ such that $F_q^{A_k} = 1 + \ell^k M_k(F_q)$. For every integer N one can compute such a $M_k(X) \bmod N$ from $\chi(X)$ in probabilistic polynomial time in $\log q$, $\log \ell$, $\log N$, k, g.*

We obtain sharper rationality results if we restrict to ℓ-divisible groups. So let $\chi = FG \bmod \ell$ with F and G unitary coprime and let $\chi = F_0 G_0$ be the corresponding factorization in $\mathbb{Z}_\ell[X]$. The action of F_q on the ℓ^k-torsion $\mathbb{G}_F[\ell^k] = \mathcal{J}[\ell^k, F_0]$ inside $\mathbb{G}_F$ factors through the ring $\mathcal{O}_\ell/(\ell^k, F_0) = \mathbb{Z}_\ell[X]/(\ell^k, F_0)$. We deduce the

Lemma 12 (Frobenius and F_0-torsion) *Let k be a positive integer and $\ell \neq p$ a prime. Let $\chi(X)$ be the characteristic polynomial of the Frobenius F_q of $\mathcal{J}$. Let $\chi = FG \bmod \ell$ with F and G unitary coprime. Let e_i and f_i be the multiplicities and inertiae in the prime decomposition of $F(X) \bmod \ell$. Let γ be the smallest integer such that ℓ^γ is bigger than or equal to $2g$. Let $B(F) = \prod_i (\ell^{f_i} - 1)$. Let $C_k(F) = \ell^{k-1+\gamma}$ and $A_k(F) = B(F)C_k(F)$. The ℓ^k-torsion in $\mathbb{G}_F$ decomposes over the degree $A_k(F)$ extension of $\mathbb{F}_q$. There is a degree $< \deg(F)$ polynomial $M_k(X) \in \mathbb{Z}_\ell[X]$ such that $\Pi_F F_q^{A_k(F)} = \Pi_F + \ell^k \Pi_F M_k(F_q)$. For every power N of ℓ, one can compute such an $M_k(X) \bmod N$ from $\chi(X)$ and $F(X)$ in probabilistic polynomial time in $\log q$, $\log \ell$, $\log N$, k, g.*

If we take for F the largest power of $X-1$ dividing $\chi(X) \bmod \ell$ in the above lemma, we have $B(F) = 1$ so $A_k(F)$ is an ℓ power $\leq 2g\ell^k$.

If we take for F the largest power of $X-q$ dividing $\chi(X) \bmod \ell$ in the above lemma, we have $B(F) = \ell - 1$ so $A_k(F)$ is $\leq 2g(\ell-1)\ell^k$.

So the characteristic spaces associated with the eigenvalues 1 and q decompose over small degree extensions of $\mathbb{F}_q$.

6 The Kummer map

Let $\mathcal{X}$ be a smooth projective algebraically irreducible reduced curve over $\mathbb{F}_q$ of genus g and $\mathcal{J}$ the jacobian of $\mathcal{X}$. Let $n \geq 2$ be an integer dividing $q-1$. We assume $g \geq 1$. In this section, we construct a convenient surjection from $\mathcal{J}(\mathbb{F}_q)$ to $\mathcal{J}(\mathbb{F}_q)[n]$.

If P is in $\mathcal{J}(\mathbb{F}_q)$ we take some R such that $nR = P$ and form the 1-cocycle $({}^\sigma R - R)_\sigma$ in $H^1(\mathbb{F}_q, \mathcal{J}[n])$. Using the Weil pairing we deduce an element

$$\square \mapsto (e_n({}^\sigma R - R, \square))_\sigma$$

of $\mathrm{Hom}(\mathcal{J}[n](\mathbb{F}_q),H^1(\mu_n))=\mathrm{Hom}(\mathcal{J}[n](\mathbb{F}_q),\mathrm{Hom}(\mathrm{Gal}(\mathbb{F}_q),\mu_n))=\mathrm{Hom}(\mathcal{J}[n](\mathbb{F}_q),{\mathbb{F}_q}^*/({\mathbb{F}_q}^*)^n)$. The map that sends $P \bmod n\mathcal{J}(\mathbb{F}_q)$ to $\square \mapsto (e_n({}^{\sigma}R - R, \square))_\sigma$ is injective because the Frey-Ruck pairing is non-degenerate. We observe that $\mathrm{Hom}(\mathrm{Gal}(\mathbb{F}_q), \mu_n)$ is isomorphic to μ_n since an homomorphism from $\mathrm{Gal}(\mathbb{F}_q)$ to μ_n is characterized by the image of the Frobenius generator F_q. We obtain a bijection $T_{n,q}$ from $\mathcal{J}(\mathbb{F}_q)/n\mathcal{J}(\mathbb{F}_q)$ to the dual $\mathrm{Hom}(\mathcal{J}[n](\mathbb{F}_q), \mu_n)$ of $\mathcal{J}[n](\mathbb{F}_q)$ that we call the *Tate map*. It maps P onto $\square \mapsto e_n({}^{F_q}R - R, \square)$. If $\mathcal{J}[n]$ decomposes over $\mathbb{F}_q$ we set $K_{n,q}(P) = {}^{F_q}R - R$ and define a bijection $K_{n,q} : \mathcal{J}(\mathbb{F}_q)/n\mathcal{J}(\mathbb{F}_q) \to \mathcal{J}[n](\mathbb{F}_q) = \mathcal{J}[n]$ that we call the *Kummer map*.

We now assume that $n = \ell^k$ is a power of some prime integer $\ell \neq p$. We also make the (strong !) assumption that $\mathcal{J}[n]$ decomposes over $\mathbb{F}_q$. We want to compute the Kummer map $K_{n,q}$ explicitly. Let P be an $\mathbb{F}_q$-rational point in $\mathcal{J}$. Let R be such that $nR = P$. Since $F_q - 1$ kills $\mathcal{J}[n]$, there is an $\mathbb{F}_q$-endomorphism κ of $\mathcal{J}$ such that $F_q - 1 = n\kappa$. We note that κ belongs to $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[F_q]$ and therefore commutes with F_q. We have $\kappa(P) = (F_q - 1)(R) = K_{n,q}(P)$ and $\kappa(P)$ is $\mathbb{F}_q$-rational.

Computing the Kummer map will show very usefull but it requires that $\mathcal{J}[n]$ decomposes over $\mathbb{F}_q$. In general, we shall have to base change to some extension of $\mathbb{F}_q$.

Let $\chi(X)$ be the characteristic polynomial of F_q and let $B = \prod_i(\ell^{f_i} - 1)$ where the f_i are the degrees of prime divisors of $\chi(X) \pmod{\ell}$. Let ℓ^γ be the smallest power of ℓ that is bigger than or equal to $2g$. Let $C_k = \ell^{\gamma+k-1}$ and $A_k = BC_k$. Set $Q = q^{A_k}$. From lemma 11 there is a polynomial $M_k(X)$ such that $F_Q = 1 + \ell^k M_k(F_q)$. So, for P an $\mathbb{F}_Q$-rational point in $\mathcal{J}$ and R such that $nR = P$ the Kummer map $K_{n,Q}$ applied to P is $M_k(F_q)(P) = (F_Q - 1)(R) = K_{n,Q}(P)$ and this is an $\mathbb{F}_Q$-rational point.

Lemma 13 (The Kummer map) *Let $\mathbb{F}_q$ be a finite field and let $\mathcal{X}$ be a projective smooth absolutely irreducible reduced algebraic curve over $\mathbb{F}_q$. Let g be the genus of $\mathcal{X}$ and let $\ell \neq p$ be a prime integer and $n = \ell^k$ a power of ℓ. We assume $g \geq 1$. Let $\chi(X)$ be the characteristic polynomial of F_q and let $B = (\ell - 1)\prod_i(\ell^{f_i} - 1)$ where the f_i are the degrees of prime divisors of $\chi(X) \pmod{\ell}$. Let ℓ^γ be the smallest power of ℓ that is bigger than or equal to $2g$. Let $C_k = \ell^{\gamma+k-1}$ and $A_k = BC_k$. Set $Q = q^{A_k}$ and observe that n divides $Q - 1$. There exists an endomorphism $\kappa \in \mathbb{Z}[F_q]$ of $\mathcal{J}$ such that $n\kappa = F_Q - 1$ and for every $\mathbb{F}_Q$-rational point P and any R with $nR = P$ one has $\kappa(P) = (F_Q - 1)(R) = K_{n,Q}(P)$. This endomorphism κ induces a bijection between $\mathcal{J}(\mathbb{F}_Q)/n\mathcal{J}(\mathbb{F}_Q)$ and $\mathcal{J}[n](\mathbb{F}_Q) = \mathcal{J}[n]$. Given $\chi(X)$ and a positive integer N one can compute $\kappa \bmod N$ as a polynomial in F_q with coefficients in $\mathbb{Z}/N\mathbb{Z}$ in probabilistic polynomial time in g, $\log \ell$, $\log q$, k, $\log N$.*

This lemma is not of much use in practice because the the field $\mathbb{F}_Q$ is too big. On the other hand, we may not be interested in the whole n-torsion in $\mathcal{J}$ but just a small piece in it, that may or may not correspond to a subvariety.

Let $\ell \neq p$ be a prime integer and $\mathbb{G}$ an ℓ-divisible group in $\mathcal{J}[\ell^\infty]$ and $\Pi = \Pi^2 : \mathcal{J}[\ell^\infty] \to \mathbb{G}$ a projection onto it. Let $n = \ell^k$ and let Q be a power of q such that $\mathbb{G}[n]$ decomposes over $\mathbb{F}_Q$. Let P be an $\mathbb{F}_Q$-rational point in $\mathbb{G}$.

Let $R \in \mathbb{G}$ be such that $nR = P$. We set $K_{\mathbb{G},n,Q}(P) = {}^{F_Q}R - R$ and define an isomorphism $K_{\mathbb{G},n,Q} : \mathbb{G}(\mathbb{F}_Q)/n\mathbb{G}(\mathbb{F}_Q) \to \mathbb{G}(\mathbb{F}_Q)[n] = \mathbb{G}[n]$.

In order to make this construction explicit, we now assume that there exists some $\kappa \in \mathbb{Z}_\ell[F_q]$ such that $\Pi(F_Q - 1 - n\kappa) = 0$.

Lemma 12 provides us with such a Q and such a κ when $\mathbb{G} = \mathcal{J}[\ell^\infty, F_0]$ is some characteristic subspace.

We now can compute this new Kummer map $K_{\mathbb{G},n,Q}$. Let P be an $\mathbb{F}_Q$-rational point in $\mathbb{G}$. Let $R \in \mathbb{G}$ be such that $nR = P$. From $(F_Q - 1 - n\kappa)\Pi(R) = 0 = (F_Q - 1 - n\kappa)(R)$ we deduce that $K_{\mathbb{G},n,Q}(P) = \kappa(P)$. Hence the

Lemma 14 (The Kummer map) *Let $\mathbb{F}_q$ be a finite field and let $\mathcal{X}$ be a projective smooth absolutely irreducible reduced algebraic curve over $\mathbb{F}_q$. Let g be the genus of $\mathcal{X}$ and let $\ell \neq p$ be a prime integer and $n = \ell^k$ a power of ℓ. We assume $g \geq 1$. Let $\chi(X)$ be the characteristic polynomial of F_q. Assume $\chi(X) = F(X)G(X) \bmod \ell$ with F and G unitary coprime polynomials in $\mathbb{F}_\ell[X]$ and let $\mathbb{G}_F$ be the associated ℓ-divisible group. Let $B = (\ell - 1)\prod_i (\ell^{f_i} - 1)$ where the f_i are the degrees of prime divisors of $F(X) \pmod \ell$. Let ℓ^γ be the smallest power of ℓ that is bigger than or equal to $2g$. Let $C_k = \ell^{k-1+\gamma}$ and $A_k = BC_k$. Set $Q = q^{A_k}$. From lemma 12 there exists an endomorphism $\kappa \in \mathbb{Z}_\ell[F_q]$ such that $\Pi_F(n\kappa - F_Q + 1) = 0$ and for every $\mathbb{F}_Q$-rational point $P \in \mathbb{G}_F$ and any $R \in \mathbb{G}_F$ with $nR = P$ one has $\kappa(P) = (F_Q - 1)(R) = K_{\mathbb{G},n,Q}(P)$. This endomorphism κ induces a bijection between $\mathbb{G}_F(\mathbb{F}_Q)/n\mathbb{G}_F(\mathbb{F}_Q)$ and $\mathbb{G}_F[n](\mathbb{F}_Q) = \mathbb{G}_F[n]$. Given $\chi(X)$ and F and a power N of ℓ, one can compute $\kappa \bmod N$ as a polynomial in F_q with coefficients in $\mathbb{Z}/N\mathbb{Z}$ in probabilistic polynomial time in g, $\log \ell$, $\log q$, k, $\log N$.*

7 Linearization of torsion classes

Let C be a degree d plane projective absolutely irreducible reduced curve C over $\mathbb{F}_q$ with geometric genus $g \geq 1$, and assume we are given the smooth model $\mathcal{X}$ of C. Let $\mathcal{J}$ be the jacobian of $\mathcal{X}$. We assume $\ell \neq p$ is a prime integer that divides $\#\mathcal{J}(\mathbb{F}_q)$. Let $n = \ell^k$ be a power of ℓ. We want to describe $\mathcal{J}(\mathbb{F}_q)[\ell^k]$ by generators and relations.

If $x_1, x_2, \ldots, x_I$ are elements in a finite commutative group G we let $\mathcal{R}$ be the kernel of the map $\xi : \mathbb{Z}^I \to G$ defined by $\xi(a_1, \cdots, a_I) = \sum_i a_i x_i$. We call $\mathcal{R}$ the lattice of relations between the x_i.

We first give a very general and rough algorithm for computing relations in any finite commutative group.

Lemma 15 (Finding relations in blackbox groups) *Let G be a finite and commutative group and let x_1, x_2, ..., x_I be elements in G. A basis for the lattice of relations between the x_i can be computed at the expense of $3I(\#G)^2$ operations (or comparisons) in G.*

We first compute and store all the multiples of x_1. So we list 0, x_1, $2x_1$, ... until we find the first multiple $e_1 x_1$ that is equal to zero. This gives us

the relation $r_1 = (e_1, 0, \ldots, 0) \in \mathcal{R}$. This first step requires at most $o = \#G$ operations in G and o comparisons.

We then compute successive multiples of x_2 until we find the first one $e_2 x_2$ that is in $L_1 = \{0, x_1, \ldots, (e_1 - 1)x_1\}$. This gives us a second relation r_2. The couple (r_1, r_2) is a basis for the lattice of relations between x_1 and x_2. Using this lattice, we compute the list L_2 of elements in the group generated by x_1 and x_2. This second step requires at most $2o$ operations and o^2 comparisons.

We then compute successive multiples of x_3 until we find the first one $e_3 x_3$ that is in L_2. This gives us a third relation r_3. The triple (r_1, r_2, r_3) is a basis for the lattice of relations between x_1, x_2 and x_3. Using this lattice, we compute the list L_3 of elements in the group generated by x_1, x_2 and x_3. This third step requires at most $2o$ operations and o^2 comparisons. And we go on like this. □

This is far from efficient unless the group is very small.

We come back to the computation of generators and relations for $\mathcal{J}(\mathbb{F}_q)[\ell^k]$.

Let $B = \ell - 1$. Let ℓ^γ be the smallest power of ℓ that is bigger than or equal to $2g$ and let $A_k = B\ell^{\gamma+k-1}$. We set $Q_k = q^{A_k}$.

If we take for F a power of $X - 1$ in definition 2 and lemma 14 we obtain two surjective maps $\Pi_1 : \mathcal{J}(\mathbb{F}_{Q_k})[\ell^\infty] \to \mathbb{G}_1(\mathbb{F}_{Q_k})$ and $K_{\mathbb{G}_1,\ell^k,Q_k} : \mathbb{G}_1(\mathbb{F}_{Q_k}) \to \mathbb{G}_1[\ell^k]$.

If we now take for F a power of $X - q$ in definition 2 and lemma 14 we obtain two surjective maps $\Pi_q : \mathcal{J}(\mathbb{F}_{Q_k})[\ell^\infty] \to \mathbb{G}_q(\mathbb{F}_{Q_k})$ and $K_{\mathbb{G}_q,\ell^k,Q_k} : \mathbb{G}_q(\mathbb{F}_{Q_k}) \to \mathbb{G}_q[\ell^k]$.

We observe that Π_1 and Π_q are Rosati dual to each other (as elements in $\mathcal{E}nd(\mathcal{J}/\mathbb{F}_q) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$), and adjoint for the Weil pairing.

Using lemma 8 we produce a sequence $\gamma_1, \ldots, \gamma_I$ of elements in $\mathcal{J}(\mathbb{F}_{Q_k})$ that generate a subgroup of index at most $\iota = \max(48g, 24d, 720)$. Let N be the largest prime to ℓ divisor of $\#\mathcal{J}(\mathbb{F}_{Q_k})$. We set $\alpha_i = K_{\mathbb{G}_1,\ell^k,Q_k}(\Pi_1(N\gamma_i))$ and $\beta_i = K_{\mathbb{G}_q,\ell^k,Q_k}(\Pi_q(N\gamma_i))$.

The group $\mathcal{A}_k$ generated by the α_i has index at most ι in $\mathbb{G}_1[\ell^k]$. The group $\mathcal{B}_k$ generated by the β_i has index at most ι in $\mathbb{G}_q[\ell^k]$.

Let ℓ^δ be smallest power of ℓ that is bigger than ι and assume $k > \delta$. Then $\mathcal{A}_k$ contains $\mathbb{G}_1[\ell^{k-\delta}]$.

We now explain how to compute the lattice of relations between given elements $\rho_1, \ldots, \rho_J$ in $\mathbb{G}_1[\ell^k]$. We denote by $\mathcal{R}$ this lattice. We notice that the restriction of the Weil pairing to $\mathbb{G}_1[\ell^k] \times \mathbb{G}_q[\ell^k]$ is non-degenerate. We fix an isomorphism between the group $\mu_{\ell^k}(\bar{\mathbb{F}}_q)$ of ℓ^k-th roots and $\mathbb{Z}/\ell^k\mathbb{Z}$. We regard the matrix $(e_{\ell^k}(\beta_i, \rho_j))$ as a matrix with I lines, J columns and coefficients in $\mathbb{Z}/\ell^k\mathbb{Z}$. This matrix defines a morphism from $\mathbb{Z}^J$ to $(\mathbb{Z}/\ell^k\mathbb{Z})^I$ whose kernel is a lattice $\mathcal{R}'$ that contains $\mathcal{R}$. The index of $\mathcal{R}$ in $\mathcal{R}'$ is at most ι. Indeed $\mathcal{R}'/\mathcal{R}$ is isomorphic to the orthogonal of $\mathcal{B}_k$ in $< \rho_1, \ldots, \rho_J > \subset \mathbb{G}_1[\ell^k]$ and the latter group has order $\leq \iota$. Once given a basis of $\mathcal{R}'$, the sublattice $\mathcal{R}$ can be computed using lemma 15 at the expense of $\leq 3J\iota^2$ operations.

Assume k is bigger than δ. We apply this method to the generators $(\alpha_i)_i$ of $\mathcal{A}_k$. Once given the lattice $\mathcal{R}$ of relations between the α_i it is a matter of linear algebra to find a basis $(b_1, \ldots, b_w)$ for $\mathcal{A}_k[\ell^{k-\delta}] = \mathbb{G}_1[\ell^{k-\delta}]$. The latter group is a rank w free module over $\mathbb{Z}/\ell^{k-\delta}\mathbb{Z}$ and is acted on by the q-Frobenius F_q.

For every b_j we can compute the lattice of relations between $F_q(b_j)$, b_1, b_2, ..., b_w and deduce the matrix of F_q in the basis $(b_1, \ldots, b_w)$. From this matrix we deduce a nice generating set for the kernel of $F_q - 1$ in $\mathbb{G}_1[\ell^{k-\delta}]$. This kernel is $\mathcal{J}[\ell^{k-\delta}](\mathbb{F}_q)$. We deduce the

Theorem 1 *There is a probabilistic Monte-Carlo algorithm that on input*

1. *a degree d and geometric genus g plane projective absolutely irreducible reduced curve C over $\mathbb{F}_q$,*
2. *the smooth model $\mathcal{X}$ of C,*
3. *a degree 1 divisor $O = O^+ - O^-$ where O^+ and O^- are effective, $\mathbb{F}_q$-rational and have degree bounded by a constant times g,*
4. *a prime ℓ different from the characteristic p of $\mathbb{F}_q$ and a power $n = \ell^k$ of ℓ,*
5. *the zeta function of $\mathcal{X}$;*

outputs a set g_1, ..., g_W of divisor classes in the Picard group of $\mathcal{X}/\mathbb{F}_q$, such that the ℓ^k torsion $\mathrm{Pic}(\mathcal{X}/\mathbb{F}_q)[\ell^k]$ is the direct product of the $< g_i >$, and the orders of the g_i form a non-decreasing sequence. Every class g_i is given by a divisor $G_i - gO$ in it, where G_i is a degree g effective $\mathbb{F}_q$-divisor on $\mathcal{X}$.

The algorithm runs in probabilistic polynomial time in d, g, $\log q$ and ℓ^k. It outputs the correct answer with probability $\geq \frac{1}{2}$. Otherwise, it may return either nothing or a strict subgroup of $\mathrm{Pic}(\mathcal{X}/\mathbb{F}_q)[\ell^k]$.

If one is given a degree zero $\mathbb{F}_q$-divisor $D = D^+ - D^-$ of order dividing ℓ^k, one can compute the coordinates of the class of D in the basis $(g_i)_{1 \leq i \leq W}$ in polynomial time in d, $\log q$, ℓ^k and the degree of D^+. These coordinates are integers x_i such that $\sum_{1 \leq i \leq W} x_i g_i = [D]$.

8 An example : modular curves

In this section we consider a family of modular curves for which we can easily provide and study a plane model. Let $\ell \geq 5$ be a prime. We set $d_\ell = \frac{\ell^2-1}{4}$ and $m_\ell = \frac{\ell-1}{2}$. We denote by $\mathcal{X}_\ell = X(2)_1(\ell)$ the moduli of elliptic curves with full 2-torsion plus one non-trivial ℓ-torsion point. We first describe a homogeneous singular plane model C_ℓ for this curve. We enumerate the places of $\mathcal{X}_\ell$ above every singularity of C_ℓ and compute the adjoint divisor $\mathfrak{C}_\ell$ using the Tate elliptic curve.

Let λ be an indeterminate and form the Legendre elliptic curve with equation $y^2 = x(x-1)(x-\lambda)$. Call $\mathcal{T}_\ell(\lambda, x)$ the ℓ-division polynomial of this curve. It is a polynomial in $\mathbb{Q}[\lambda][x]$ with degree $2d_\ell = \frac{\ell^2-1}{2}$ in x.

As a polynomial in x we have

$$\mathcal{T}_\ell(\lambda, x) = \sum_{0 \leq k \leq 2d_\ell} a_{2d_\ell - k}(\lambda) x^k$$

where $a_0(\lambda)$ has degree 0 in λ so that we normalise by setting $a_0(\lambda) = \ell$.

We can compute the $2d_\ell$ roots of $\mathcal{T}_\ell(\lambda, x)$ in the field $\bar{\mathbb{Q}}\{\{\lambda^{-1}\}\}$ of Puiseux series in λ^{-1}. We set $j = j(\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} = 2^8\lambda^2(1-\lambda^{-1}+3\lambda^{-2}+3\lambda^{-4}+\cdots)$ so $j^{-1} = 2^{-8}(\lambda^{-2}+\lambda^{-3}-2\lambda^{-4}-5\lambda^{-5}+\cdots)$.

We introduce Tate's q-parameter, defined implicitly by $j = \frac{1}{q} + 744 + 196884q + \cdots$ so $q = j^{-1} + 744j^{-2} + 750420j^{-3} + \cdots = \frac{1}{256}\lambda^{-2} + \frac{1}{256}\lambda^{-3} + \frac{29}{8192}\lambda^{-4} + \frac{13}{4096}\lambda^{-5} + \cdots$.

We set $x = x' + \frac{1+\lambda}{3}$ and $y' = y$ and find the reduced Weierstrass equation for the Legendre curve $y'^2 = x'^3 - \frac{\lambda^2-\lambda+1}{3}x' - \frac{(\lambda-2)(\lambda+1)(2\lambda-1)}{27}$.

We want to compare the latter curve and the Tate curve with equation $y''^2 = x''^3 - \frac{E_4(q)}{48}x'' + \frac{E_6(q)}{864}$ where $E_4(q) = 1 + 240q + \cdots$ and $E_6(q) = 1 - 504q + \cdots$.

The quotient $\frac{E_4(q)(dq)^2}{(\lambda^2-\lambda+1)q^2}$ is a quadratic differential on the curve $X(2)$ with divisor $-2(0) - 2(1)$ in the λ coordinate. Examination of the leading terms of its expansion shows that $E_4\left(\frac{dq}{q}\right)^2 = \frac{4(\lambda^2-\lambda+1)(d\lambda)^2}{\lambda^2(1-\lambda)^2}$ and simimarly $E_6\left(\frac{dq}{q}\right)^3 = \frac{4(\lambda-2)(\lambda+1)(2\lambda-1)(d\lambda)^3}{\lambda^3(1-\lambda)^3}$.

We deduce the isomorphism $x' = \gamma^2 x''$ and $y' = \gamma^3 y''$ with $\gamma^2 = 2\lambda(\lambda-1)\left(\frac{dq}{qd\lambda}\right) = -4\lambda + 2 + \frac{3}{8}\lambda^{-1} + \frac{3}{16}\lambda^{-2} + \cdots$.

Set $\zeta_\ell = \exp(\frac{2i\pi}{\ell})$. For a and b integers such that either $b = 0$ and $1 \le a \le \frac{\ell-1}{2}$ or $1 \le b \le \frac{\ell-1}{2}$ and $0 \le a \le \ell - 1$ we set $w = \zeta_\ell^a q^{\frac{b}{\ell}}$ in the expansion

$$x''(w,q) = \frac{1}{12} + \sum_{n\in\mathbb{Z}} \frac{wq^n}{(1-wq^n)^2} - 2\sum_{n\ge 1}\frac{nq^n}{1-q^n}$$

and find

$$x''_{a,b} = \frac{1}{12} + \zeta_\ell^a q^{\frac{b}{\ell}} + O(q^{\frac{b+1}{\ell}})$$

if $b \neq 0$ and $x''_{a,0} = \frac{1}{12} + \frac{\zeta_\ell^a}{(1-\zeta_\ell^a)^2} + O(q)$.

So

$$x_{a,b} = \gamma^2 x'' + \frac{1+\lambda}{3} = -4\zeta_\ell^a 2^{\frac{-8b}{\ell}}\lambda^{1-\frac{2b}{\ell}} + O(\lambda^{1-\frac{2b+1}{\ell}})$$

if $b \neq 0$ and $x_{a,0} = \frac{-4\zeta_\ell^a}{(1-\zeta_\ell^a)^2}\lambda + O(1)$.

The $x_{a,b}$ are the roots of $\mathcal{T}_\ell(\lambda, x)$ in the field $\bar{\mathbb{Q}}\{\{\lambda^{-1}\}\}$ of Puiseux series.

We deduce that for $1 \le k \le \frac{\ell-1}{2}$ the polynomial $a_k(\lambda)$ has degree at most k. Further $a_{\frac{\ell-1}{2}}(\lambda) = 2^{\ell-1}(-\lambda)^{\frac{\ell-1}{2}} + O(\lambda^{\frac{\ell-3}{2}})$. For $k > \frac{\ell-1}{2}$ the polynomial $a_k(\lambda)$ has degree $< k$ and $\le d_\ell$.

The coefficients in all the series expansions above are in $\bar{\mathbb{Z}}[\frac{1}{6\ell}]$. The coefficients in $\mathcal{T}_\ell(\lambda, x)$ are in $\mathbb{Z}[\frac{1}{6\ell}]$. In fact $\mathcal{T}_\ell(\lambda, x)$ is in $\mathbb{Z}[\lambda, x]$ but this is not needed here.

Since $\mathcal{T}_\ell \in \mathbb{Q}[\lambda, x]$ is absolutely irreducible, the equation $\mathcal{T}_\ell(\lambda, x) = 0$ defines a plane absolutely irreducible affine curve $\mathcal{C}_\ell$.

We denote by $T_\ell(\Lambda, X, Y) = \mathcal{T}_\ell(\frac{\Lambda}{Y}, \frac{X}{Y})Y^{2d_\ell}$ the associated homogeneous polynomial and call $C_\ell \subset \mathbb{P}^2$ the corresponding projective curve.

For every place P on $\mathcal{X}_\ell$ such that $\lambda(P) \notin \{0,1,\infty\}$, the function $\lambda - \lambda(P)$ is a uniformizing parameter at P. Further $x(P)$ is finite and P is the only place of $\mathcal{X}_\ell$ above the point $(\lambda(P), x(P))$ of $\mathcal{C}_\ell$. So the only possible singularities of C_ℓ lie on one of the three lines with equations $\Lambda = 0$, $Y = 0$ and $\Lambda - Y = 0$.

The points at infinity are given by the degree $2d_\ell$ form

$$2^{\ell-1}(-1)^{\frac{\ell-1}{2}}\Lambda^{\frac{\ell-1}{2}}X^{\frac{\ell^2-\ell}{2}} + \cdots + \ell X^{\frac{\ell^2-1}{2}} = X^{\frac{\ell^2-\ell}{2}} \prod_{0 \le a \le \frac{\ell-1}{2}} (-4\Lambda - (\zeta_\ell^a + \zeta_\ell^{-a} - 2)X).$$

We call $\Sigma_\infty = [1,0,0]$ the unique singular point at infinity and for every $1 \le b \le \frac{\ell-1}{2}$ we call $\sigma_{\infty,b}$ the point above Σ_∞ on $\mathcal{X}_\ell$ associated with the orbit $\{x_{0,b}, x_{1,b}, \cdots, x_{\ell-1,b}\}$ for the inertia group. We call $\mu_{\infty,a}$ the point on $\mathcal{X}_\ell$ corresponding to the expansion $x_{a,0}$. The ramification index of the covering map $\lambda : \mathcal{X}_\ell \to X(2)$ is ℓ at $\sigma_{\infty,b}$ and 1 at $\mu_{\infty,a}$. Since $\ell - 2b$ and ℓ are coprime, there exist two integers α_b and β_b such that $\alpha_b(\ell - 2b) - \beta_b\ell = 1$ and $1 \le \alpha_b \le \ell - 1$ and $1 \le \beta_b \le \ell - 1$. The monomial $x^{\alpha_b}\lambda^{-\beta_b} \in \bar{\mathbb{Q}}(\mathcal{X}_\ell)$ is a local parameter at $\sigma_{\infty,b}$. Of course, $\lambda^{-\frac{1}{\ell}}$ is also a local parameter at this point, and it is much more convenient, although it is not in $\bar{\mathbb{Q}}(\mathcal{X}_\ell)$.

The morphism $\phi : \mathcal{X}_\ell \to X_1(\ell)$ corresponding to forgetting the 2-torsion structure is Galois with group $\mathcal{S}_3$ generated by the two transpositions $\tau_{(0,\infty)}$ and $\tau_{(0,1)}$ defined in homogeneous coordinates by $\tau_{(0,\infty)} : [\Lambda, X, Y] \to [Y, X, \Lambda]$ and $\tau_{(0,1)} : [\Lambda, X, Y] \to [Y - \Lambda, Y - X, Y]$. We observe that these act on $\mathcal{X}_\ell$, $\mathbb{P}^2$ and C_ℓ in a way compatible with the maps $\mathcal{X}_\ell \to C_\ell$ and $C_\ell \subset \mathbb{P}^2$.

We set $\Sigma_0 = \tau_{(0,\infty)}(\Sigma_\infty) = [0,0,1]$ and $\Sigma_1 = \tau_{(0,1)}(\Sigma_0) = [1,1,1]$. We set $\sigma_{0,b} = \tau_{(0,\infty)}(\sigma_{\infty,b})$ and $\sigma_{1,b} = \tau_{(0,1)}(\sigma_{0,b})$, $\mu_{0,a} = \tau_{(0,\infty)}(\mu_{\infty,a})$ and $\mu_{1,a} = \tau_{(0,1)}(\mu_{0,a})$.

The genus of $\mathcal{X}_\ell$ is $g_\ell = \frac{(\ell-3)^2}{4} = (m_\ell - 1)^2$. The arithmetic genus of C_ℓ is $g_a = (m_\ell^2 + m_\ell - 1)(2m_\ell^2 + 2m_\ell - 1)$. We now compute the conductor of C_ℓ. Locally at Σ_∞ the curve C_ℓ consists of m_ℓ branches (one for each place $\sigma_{\infty,b}$) that are cusps with equations $\left(\frac{X}{\Lambda}\right)^\ell = -2^{2\ell-8b}\left(\frac{Y}{\Lambda}\right)^{2b} + \cdots$. The conductor of this latter cusp is $\sigma_{\infty,b}$ times $(\ell-1)(2b-1)$ which is the next integer to the last gap of the additive semigroup generated by ℓ and $2b$. The conductor of the full singularity Σ_∞ is now given by Gorenstein's formula [8, Theorem 2] and is

$$\sum_{1 \le b \le m_\ell} \{b(4m_\ell^2 + 4m_\ell - 1) - 2m_\ell - (2m_\ell + 1)b^2\} \cdot \sigma_{\infty,b}.$$

The full conductor $\mathfrak{C}_\ell$ is the sum of this plus the two corresponding terms to the isomorphic singularities Σ_0 and Σ_1. Some authors call it the adjunction divisor.

The degree $\deg(\mathfrak{C}_\ell)$ of $\mathfrak{C}_\ell$ is $2m_\ell(2m_\ell^3 + 4m_\ell^2 - 2m_\ell - 1)$. So we have $\delta(\mathfrak{C}_\ell) = m_\ell(2m_\ell^3 + 4m_\ell^2 - 2m_\ell - 1)$ and we check that $g_a = g_\ell + \delta(\mathfrak{C}_\ell)$.

Now let $p \notin \{2,3,\ell\}$ be a prime. Let $\mathbb{C}_p$ be the field of p-adics and $\bar{\mathbb{F}}_p$ its residue field. We embed $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$ and also in $\mathbb{C}$. In particular $\zeta_\ell = \exp(\frac{2i\pi}{\ell})$ and $2^{\frac{1}{\ell}}$ are well defined as p-adic numbers.

We observe that in the calculations above, all coefficients belong to $\bar{\mathbb{Z}}[\frac{1}{6\ell}]$.

More precisely, the curves C_ℓ and $\mathcal{X}_\ell$ are defined over $\mathbb{Z}[\frac{1}{6\ell}]$. We note $C_\ell \bmod p = C_\ell/\mathbb{F}_p = C_\ell \otimes_{\mathbb{Z}[\frac{1}{6\ell}]} \mathbb{F}_p$ the reduction of C_ℓ modulo p and define similarly $\mathcal{X}_\ell \bmod p$. The points $\sigma_{\infty,b} \in \mathcal{X}_\ell$ are defined over $\mathbb{Z}[\frac{1}{6\ell}]$ and their reductions $\sigma_{\infty,b} \bmod p = \sigma_{\infty,b} \otimes_{\mathbb{Z}[\frac{1}{6\ell}]} \mathbb{F}_p$ are defined over $\mathbb{F}_p$.

The points $\mu_{\infty,a} \in \mathcal{X}_\ell$ are defined over $\mathbb{Z}[\zeta_\ell, \frac{1}{6\ell}]$ and their reductions $\mu_{\infty,a} \bmod p = \mu_{\infty,a} \otimes_{\mathbb{Z}[\zeta_\ell, \frac{1}{6\ell}]} \mathbb{F}_p(\zeta_\ell)$ are defined over $\mathbb{F}_p(\zeta_\ell)$.

We deduce the

Lemma 16 (Computing C_ℓ and resolving its singularities) *There exists a deterministic algorithm that given a prime $\ell \geq 5$ and a prime $p \notin \{2, 3, \ell\}$ and a finite field $\mathbb{F}_q$ with characteristic p such that $\zeta_\ell \bmod p$ and $2^{\frac{1}{\ell}} \bmod p$ belong to $\mathbb{F}_q$, computes the equation $\mathcal{T}_\ell(\lambda, x)$ modulo p and the expansions of all $x_{a,b}$ as series in $\lambda^{\frac{-1}{\ell}}$ with coefficients in $\mathbb{F}_q$, in time polynomial in ℓ, $\log q$ and the required $\lambda^{\frac{-1}{\ell}}$-adic accuracy.*

9 Another example of modular curves

In this section we consider another family of modular curves for which we can easily provide and study a plane model. This family will be useful in the calculation of modular representations as sketched in the next section. Let $\ell > 5$ be a prime. This time we set $\mathcal{X}_\ell = X_1(5\ell)$ the moduli of elliptic curves with one point of order 5ℓ. We first describe a homogeneous singular plane model C_ℓ for this curve. We enumerate the places of $\mathcal{X}_\ell$ above every singularity of C_ℓ and provide series expansions for affine coordinates at every such place.

Let b be an indeterminate and form the elliptic curve E_b in Tate normal form with equation $y^2 + (1-b)xy - by = x^3 - bx^2$. The point $P = (0, 0)$ has order 5 and its multiples are $2P = (b, b^2)$, $3P = (b, 0)$, $4P = (0, b)$. The multiplication by ℓ isogeny induces a degree ℓ^2 rational fraction on x-coordinates : $x \mapsto \frac{\mathcal{N}(x)}{\mathcal{M}(x)}$ where $\mathcal{N}(x)$ is a unitary degree ℓ^2 polynomial in $\mathbb{Q}(b)[x]$. Recursion formulae for division polynomial (see [4] section 3.6) provide a quick algorithm for computing this polynomial, and also show that the coefficients actually lie in $\mathbb{Z}[b]$. If ℓ is congruent to ± 1 modulo 5 then $\ell P = \pm P$ and x divides $\mathcal{N}(x)$. Otherwise $\mathcal{N}(x)$ is divisible by $x - b$.

Call $\mathcal{T}_\ell(b, x)$ the quotient of $\mathcal{N}(x)$ by x or $x - b$. This is a unitary polynomial in $\mathbb{Z}[b][x]$ with degree $\ell^2 - 1$ in x.

As a polynomial in x we have

$$\mathcal{T}_\ell(b, x) = \sum_{0 \leq k \leq \ell^2 - 1} a_{\ell^2 - 1 - k}(b) x^k$$

where $a_0(\lambda) = 1$. Let d be the total degree of $\mathcal{T}_\ell$.

We denote by $T_\ell(B, X, Y) = \mathcal{T}_\ell(\frac{B}{Y}, \frac{X}{Y}) Y^d$ the associated homogeneous polynomial and call $C_\ell \subset \mathbb{P}^2$ the corresponding projective curve.

We set

$$j = j(b) = \frac{(b^4 - 12b^3 + 14b^2 + 12b + 1)^3}{b^5(b^2 - 11b - 1)}.$$

Let $\sqrt{5} \in \mathbb{C}$ be the positive square root of 5 and let $\zeta_5 = \exp(\frac{2i\pi}{5})$. Let $s = \frac{11+5\sqrt{5}}{2}$ and $\bar{s}$ be the two roots of $b^2 - 11b - 1$.

The forgetting map $X_1(5\ell) \to X_1(5)$ is unramified except at $b \in \{0, \infty, s, \bar{s}\}$. For every place P on $\mathcal{X}_\ell$ such that $b(P) \notin \{0, s, \bar{s}, \infty\}$, the function $b - b(P)$ is a uniformizing parameter at P.

Let $\mathcal{U}$ be the affine open set with equation $YB(B^2-11BY+Y^2) \neq 0$. Every point on $C_\ell \cap \mathcal{U}$ is smooth and all places of $\mathcal{X}_\ell$ above points in $C_\ell - \mathcal{U}$ are cusps in the modular sense (i.e. the modular invariant at these places is infinite).

In order to desingularize C_ℓ at a given cusp, we shall construct an isomorphism between the Tate q-curve and the localization of E_b at this cusp.

We call A_∞, A_0, A_s, $A_{\bar{s}}$ the points on $X_1(5)$ corresponding to the values ∞, 0, s and $\bar{s}$ of b.

We first study the situation locally at A_∞. A local parameter is b^{-1} and $j^{-1} = b^{-5} + 25b^{-6} + \cdots$.

We introduce Tate's q-parameter, defined implicitly by $j = \frac{1}{q} + 744 + 196884q + \cdots$ so $q = j^{-1} + 744j^{-2} + 750420j^{-3} + \cdots = b^{-5} + 25b^{-6} + \cdots$ and we fix an embedding of the local field at A_∞ inside $\mathbb{C}\{\{q\}\}$ by setting $b^{-1} = q^{\frac{1}{5}} - 5q^{\frac{2}{5}} + \cdots$.

We set $x' = 36x + 3(b^2 - 6b + 1)$ and $y' = 108(2y + (1-b)x - b)$ and find the reduced Weierstrass equation

$$y'^2 = x'^3 - 27(b^4 - 12b^3 + 14b^2 + 12b + 1)x' + 54(b^2+1)(b^4 - 18b^3 + 74b^2 + 18b + 1).$$

We want to compare the latter curve and the Tate curve with equation

$$y''^2 = x''^3 - \frac{E_4(q)}{48}x'' + \frac{E_6(q)}{864}$$

where $E_4(q) = 1 + 240q + \cdots$ and $E_6(q) = 1 - 504q + \cdots$. See [10, Theorem 10.1.6].

From the (classical see [16, Proposition 7.1]) identities $\left(\frac{qdj}{dq}\right)^2 = j(j - 1728)E_4$ and $\left(\frac{qdj}{dq}\right)^3 = -j^2(j-1728)E_6$ we deduce $\left(\frac{qdb}{dq}\right)^2 = \frac{b^2(b^2-11b-1)^2E_4}{25(b^4-12b^3+14b^2+12b+1)}$ and $\left(\frac{qdb}{dq}\right)^3 = -\frac{b^3(b^2-11b-1)^3E_6}{125(b^2+1)(b^4-18b^3+74b^2+18b+1)}$.

We deduce the isomorphism $x' = \gamma^2 x''$ and $y' = \gamma^3 y''$ with

$$\gamma^2 = -\frac{36b(b^2 - 11b - 1)dq}{5qdb}.$$

The point P has (x, y) coordinates equal to $(0, 0)$. So $x''(P) = 3(b^2 - 6b + 1)/\gamma^2 = \frac{1}{12} + b^{-2} + 11b^{-3} + \cdots = \frac{1}{12} + q^{\frac{2}{5}} + O(q^{\frac{3}{5}})$.

Since on the Tate curve we have

$$x''(w, q) = \frac{1}{12} + \sum_{n \in \mathbb{Z}} \frac{wq^n}{(1 - wq^n)^2} - 2\sum_{n \geq 1} \frac{nq^n}{1 - q^n} \tag{1}$$

we deduce that $w(P) = q^{\pm\frac{2}{5}} \bmod < q >$. We may decide for the sign in the exponent because we may choose any of the two isomorphisms corresponding to either possible values for γ. We decide that $w(P) = q^{\frac{2}{5}} \bmod < q >$.

Set $\zeta_\ell = \exp(\frac{2i\pi}{\ell})$. For α and β integers such that $0 \leq \alpha, \beta \leq \ell - 1$ we set $w = \zeta_\ell^\alpha q^{\frac{\beta}{\ell}} q^{\frac{2}{5\ell}}$ in the expansion 1 and find

$$x''_{\alpha,\beta} = \frac{1}{12} + \zeta_\ell^\alpha q^{\frac{\beta}{\ell}} q^{\frac{2}{5\ell}}(1 + O(q^{\frac{1}{5\ell}}))$$

if $0 \leq \beta \leq \frac{\ell-1}{2}$ and

$$x''_{\alpha,\beta} = \frac{1}{12} + \zeta_\ell^{-\alpha} q^{\frac{\ell-\beta}{\ell} - \frac{2}{5\ell}}(1 + O(q^{\frac{1}{5\ell}}))$$

if $\frac{\ell+1}{2} \leq \beta \leq \ell - 1$.

Since

$$x_{\alpha,\beta} = (\gamma^2 x''_{\alpha,\beta} - 3(b^2 - 6b + 1))/36$$

and $\gamma^2 = 36b^2 - 216b - 396 + O(b^{-1}) = 36q^{\frac{-2}{5}} + 144q^{\frac{-1}{5}} + 144 + \cdots$ we deduce that

$$x_{\alpha,\beta} + 1 = \zeta_\ell^\alpha q^{\frac{\beta}{\ell} + \frac{2}{5\ell} - \frac{2}{5}}(1 + O(q^{\frac{1}{5\ell}}))$$

if $0 \leq \beta \leq \frac{\ell-1}{2}$ and

$$x_{\alpha,\beta} + 1 = \zeta_\ell^{-\alpha} q^{\frac{\ell-\beta}{\ell} - \frac{2}{5\ell} - \frac{2}{5}}(1 + O(q^{\frac{1}{5\ell}}))$$

if $\frac{\ell+1}{2} \leq \beta \leq \ell - 1$.

In particular, the degree of $\mathcal{T}_\ell(b, x)$ in b is $\leq 2(\ell^2 - 1)$.

For $0 \leq \alpha < \ell$ and $0 \leq \beta < \ell$ we set $\tilde{\alpha} = 5\alpha \bmod \ell$ and $\tilde{\beta} = 5\beta + 2 \bmod \ell$.

If $\tilde{\beta}$ is non-zero, the inertia group permutes cyclically the ℓ roots $x_{\alpha,\beta}$ for $0 \leq \alpha < \ell$. We call $\sigma_{\infty,\tilde{\beta}}$ the corresponding branch on $\mathcal{X}_\ell$. On the other hand, if $\beta = \frac{-2}{5} \bmod \ell$ then $\tilde{\beta} = 0 \bmod \ell$ and every $x_{\alpha, \frac{-2}{5} \bmod \ell}$ is fixed by inertia. We observe that $x_{0, \frac{-2}{5} \bmod \ell}$ is either b or 0 and is not a root of $\mathcal{T}_\ell(b, x)$. For $\tilde{\alpha}$ a non-zero residue modulo ℓ, we denote by $\mu_{\infty,\tilde{\alpha}}$ the branch on $\mathcal{X}_\ell$ corresponding to $x_{\alpha, \frac{-2}{5} \bmod \ell}$.

So we have $\ell - 1$ unramified places on $\mathcal{X}_\ell$ above A_∞ and $\ell - 1$ ramified places with ramification index ℓ.

The coefficients in all the series expansions above are in $\mathbb{Z}[\frac{1}{30}, \zeta_\ell]$. The coefficients in $\mathcal{T}_\ell(b, x)$ are in $\mathbb{Z}$.

From the discussion above we deduce the

Lemma 17 (Computing C_ℓ and resolving its singularities, I) *There exists a deterministic algorithm that given a prime $\ell \geq 7$ and a prime $p \notin \{2, 3, 5, \ell\}$ and a finite field $\mathbb{F}_q$ with characteristic p such that $\zeta_\ell \bmod p$ belongs to $\mathbb{F}_q$, computes the equation $\mathcal{T}_\ell(b, x)$ modulo p and the expansions of all $x_{\alpha,\beta}$ as series in $b^{-\frac{1}{\ell}}$ with coefficients in $\mathbb{F}_q$, in time polynomial in ℓ, $\log q$ and the required $b^{\frac{-1}{\ell}}$-adic accuracy.*

The equation is computed using recursion formulae for division polynomials. The q-series for the modular function j is given by $j(q) = 1728E_4^3(q)(E_4^3(q) -$

$E_6^2(q))^{-1}$ where $E_4(q) = 1 + 240\sum_{n\geq 1}\frac{n^3q^n}{1-q^n}$ and $E_6(q) = 1 - 504\sum_{n\geq 1}\frac{n^5q^n}{1-q^n}$. The expansions for the $x_{\alpha,\beta}$ are then obtained through standard operations on series like product, sum, reversion, composition. And this is done in polynomial time in the absolute accuracy. □

Here are a few lines of GP-PARI code:

```
{ser(aa,bb,prec,ell,p,z,b,jc,E4,E6,D,jq,qc,gc,w,x)=if(1,
ell=7;
p=953;
z=Mod(431,p);
b=1/c;
jc=(b^4-12*b^3+14*b^2+12*b+1)^3/b^5/(b^2-11*b-1);
E4=sum(n=1,prec, n^3*q^n/(1-q^n))*240+1+O(q^prec);
E6=sum(n=1,prec, -n^5*q^n/(1-q^n))*504+1+O(q^prec);
D=(E4^3-E6^2)/1728;
jq=E4^3/D;
qc=subst(serreverse(1/jq),q,1/jc+O(c^prec));
gc= -36*b*(b^2-11*b-1)*deriv(qc)*(-c^2)/5/qc;
w=z^aa*Q^(2+5*bb);
xabs=Mod(1,p)*(1/12
+sum(n=1,prec,w*Q^(5*ell*n)/(1-w*Q^(5*ell*n))^2+O(Q^(5*ell*prec)))
+w/(1-w)^2
+sum(n=1,prec,Q^(5*ell*n)/w/(1-(w)^(-1)*Q^(5*ell*n))^2+O(Q^(5*ell*prec)))
-2*sum(n=1,prec,n*Q^(5*ell*n)/(1-Q^(5*ell*n))+O(Q^(5*ell*prec )) ));
cQ=subst(serreverse((qc/c^5)^(1/5)*c),c,Q^ell);
bQ=1/cQ;
gQ=subst(gc,c,cQ);
XabQ=(gQ*xabs-3*(bQ^2-6*bQ+1) )/36;
QC=subst(serreverse(1/((bQ*Q^ell)^(1/ell)/Q)),Q,C);
XabC=subst(XabQ,Q,QC);
,)}
```

The same holds for singular places above A_0. A local parameter at A_0 is b and $j^{-1} = -b^5 + 25b^6 + \dots$ so $q = -b^5 + 25b^6 + \dots$ and we fix an embedding of the local field at A_0 inside $\mathbb{C}\{\{q\}\}$ by setting $b = -q^{\frac{1}{5}} + 5q^{\frac{2}{5}} + \dots$. From $\gamma^2 = 36 - 216q^{\frac{1}{5}} + \dots$ we deduce that the coordinate $x''(P)$ of the 5-torsion point P is $x''(P) = \frac{1}{12} + q^{\frac{1}{5}} + O(q^{\frac{2}{5}})$ so the parameter w at P can be taken to be $w(P) = q^{\frac{1}{5}} \bmod < q >$ this time. For α and β integers such that $0 \leq \alpha, \beta \leq \ell - 1$ we set $w = \zeta_\ell^\alpha q^{\frac{\beta}{\ell}} q^{\frac{1}{5\ell}}$ in the expansion 1 and we finish as above.

Now, a local parameter at A_s is $b-s$ and $j^{-1} = (\frac{1}{2} - \frac{11\sqrt{5}}{50})(b-s) + O((b-s)^2)$ so $q = (\frac{1}{2} - \frac{11\sqrt{5}}{50})(b-s) + O((b-s)^2)$ and we fix an embedding of the local field at A_s inside $\mathbb{C}\{\{q\}\}$ by setting $b - s = \frac{125+55\sqrt{5}}{2}q + O(q^2)$. We deduce that the coordinate $x''(P)$ of the 5-torsion point P is $x''(P) = \frac{1}{12} + \frac{w}{(1-w)^2} + O(q)$ where $w = \exp(\frac{4i\pi}{5}) = \zeta_5^2$ so the parameter w at P can be taken to be $w(P) = \zeta_5^2 \bmod < q >$ this time.

Altogether we have proven the

Lemma 18 (Computing C_ℓ and resolving its singularities, II) *There exists a deterministic algorithm that given a prime $\ell \geq 7$ and a prime $p \notin \{2, 3, 5, \ell\}$ and a finite field $\mathbb{F}_q$ with characteristic p such that $\zeta_\ell \bmod p$ and $\zeta_5 \bmod p$ belong to $\mathbb{F}_q$, computes the equation $\mathcal{T}_\ell(b, x)$ modulo p and expansions (with coefficients in $\mathbb{F}_q$) at every singular branch of C_ℓ in time polynomial in ℓ, $\log q$ and the required number of significant terms in the expansions.*

We also need the following result due to Manin, Shokurov, Merel and Cremona [13, 15, 2, 5].

Lemma 19 (Manin, Shokurov, Merel, Cremona) *For ℓ a prime and $p \notin \{5, \ell\}$ another prime, the zeta function of $\mathcal{X}_\ell \pmod p$ can be computed in time polynomial in ℓ and p.*

We first compute the action of the Hecke operator T_p on the space of Manin symbols for the congruence group $\Gamma_1(5\ell)$ associated with $\mathcal{X}_\ell$. Then, from Eichler-Shimura identity $T_p = F_p + p < p > /F_p$ we deduce the characteristic polynomial of the Frobenius F_p. □

The lines below are written in the Magma language.

```
ZZ:=IntegerRing();
l:=11;
N:=5*11;
QN:=CyclotomicField(EulerPhi(N));
R1<T>:=PolynomialRing(QN,1);
R2<T,U>:=PolynomialRing(QN,2);
G := DirichletGroup(N,QN);
chars := Elements(G);
gen4:=chars[2];
gen10:=chars[5];
Genus(Gamma1(N));
charsmc:=[gen4,gen4^2,gen4^4, gen4*gen10,gen4^2*gen10,gen10,
gen4*gen10^2,gen4^2*gen10^2,gen10^2 , gen4*gen10^5,gen4^2*gen10^5,gen10^5];
p:=101;
PT:= R2 ! 1;
W:=1;
g:=1;

for eps in charsmc do

M := ModularForms([eps],2);
P:= R2 ! Evaluate(HeckePolynomial(CuspidalSubspace(M),p), T);
g:=Degree(P,T);
W :=   Evaluate(P,[ T+Evaluate(eps,p)*p/T,  1])*T^g;
PT:=PT*W;

end for;
```

```
PT := R2 ! PT;

k:=2;
PTk:= Resultant(PT, T^k-U,T);
```

10 Computing the Ramanujan subspace

This section explains the connexion between the methods given here and the Edixhoven program for computing coefficients of modular forms. Recall the definition of the Ramanujan arithmetic τ function, related to the sum expansion of the discriminant form : $\Delta(q) = q\prod_{k\geq 1}(1-q^k)^{24} = \sum_{k\geq 1}\tau(k)q^k$.

We call $\mathbb{E} \subset \mathcal{E}nd(J_1(\ell)/\mathbb{Q})$ the algebra of endomorphisms of $J_1(\ell)$ generated by the Hecke operators T_n for all integers $n \geq 2$. Following Edixhoven [3] we state the

Definition 3 (The Ramanujan ideal) *We denote by $\mathfrak{m}$ the maximal ideal in $\mathbb{E}$ generated by ℓ and the $T_n - \tau(n)$. The subspace $J_1(\ell)[\mathfrak{m}]$ of the ℓ-torsion of $J_1(\ell)$ cut out by all $T_n - \tau(n)$ is called the Ramanujan subspace and denoted V_ℓ.*

This V_ℓ is a 2-dimensional vector space over $\mathbb{F}_\ell$ and the characteristic polynomial of the Frobenius endomorphism F_p on it is $X^2 - \tau(p)X + p^{11} \bmod \ell$.

In this section, we adress the problem of computing $\mathfrak{m}$-torsion divisors on modular curves over some extension field $\mathbb{F}_q$ of $\mathbb{F}_p$. The definition field $\mathbb{F}_q$ for such divisors can be predicted from the characteristic polynomial of F_p on V_ℓ. So the strategy is to pick random $\mathbb{F}_q$-points in the ℓ-torsion of the jacobian $J_1(\ell)$ and to project them onto V_ℓ using Hecke operators.

In section 9 we have defined the modular curve $\mathcal{X}_\ell = X_1(5\ell)$ and the degree 12 covering $\phi : \mathcal{X}_\ell \to X_1(\ell)$ of $X_1(\ell)$. We prefer $\mathcal{X}_\ell$ to $X_1(\ell)$ because we are able to construct a natural and convenient plane model for it. The covering map $\phi : \mathcal{X}_\ell \to X_1(\ell)$ corresponds to forgetting the 2-torsion structure. It induces two morphisms $\phi^* : J_1(\ell) \to \mathcal{J}_\ell$ and $\phi_* : \mathcal{J}_\ell \to J_1(\ell)$ such that $\phi_* \circ \phi^* = [12]$ on $J_1(\ell)$.

The curve $\mathcal{X}_\ell$ provides a convenient computational model for the group of $\mathbb{F}_q$-points of the jacobian of $X_1(\ell)$. Indeed, the jacobian $J_1(\ell)$ of $X_1(\ell)$ and the jacobian $\mathcal{J}_\ell$ of $\mathcal{X}_\ell$ are related by the natural map $\phi^* : J_1(\ell) \to \mathcal{J}_\ell$ induced by ϕ.

We denote by $\mathcal{A}_\ell \subset J_\ell$ the image of $\nu = \phi^* \circ \phi_*$. This is a subvariety of J_ℓ isogenous to $J_1(\ell)$. The restriction of ν to $\mathcal{A}_\ell$ is multiplication by 12.

The maps ϕ^* and ϕ_* induce Galois equivariant bijections between the N-torsion subgroups $J_1(\ell)[N]$ and $\mathcal{A}_\ell[N]$ for every prime to 6 integer N.

We call $W_\ell \subset \mathcal{A}_\ell \subset \mathcal{J}_\ell$ the image of the Ramanujan subspace by ϕ^*. We choose an integer $\widehat{12}$ such that $12 \times \widehat{12}$ is congruent to 1 modulo ℓ. We set $\hat{T}_n = [\widehat{12}] \circ \phi^* \circ T_n \circ \phi_*$ and notice that $\hat{T}_n \circ \phi^* = \phi^* \circ T_n$ on $J_1(\ell)[\ell]$. This way, the map $\phi^* : J_1(\ell) \to \mathcal{J}_\ell$ induces a Galois equivariant bijection of Hecke modules between the $J_1(\ell)[\ell]$ and $\mathcal{A}_\ell[\ell]$ and $W_\ell = \phi^*(V_\ell)$ is the subspace in $\mathcal{A}_\ell[\ell]$

cut out by all $\hat{T}_n - \tau(n)$. So W_ℓ will also be called the Ramanujan subspace whenever there is no risk of confusion.

We notice that ϕ^*, ϕ_*, T_n, and $\hat{T}_n$ can be seen as correspondences as well as morphisms between jacobians, and we state the

Lemma 20 (Computing the Hecke action) *Let ℓ, p, n be primes such that $p \neq \ell$ and ℓ^2 does not divide n. Let q be a power of p and let D be an effective $\mathbb{F}_q$-divisor of degree d on $\mathcal{X}_\ell \pmod p$. The divisors $\phi^* \circ \phi_*(D)$ and $\phi^* \circ T_n \circ \phi_*(D)$ can be computed in deterministic polynomial time in ℓ, d, n and $\log q$.*

Let $x = (E, u)$ be a point on $X_1(\ell)$ representing and elliptic curve E with one ℓ-torsion point u. Let n be an integer. The Hecke operator T_n maps x onto the sum of all $(E_\phi, \phi(u))$, where $\phi : E \to E_\phi$ runs over the set of all isogenies of degree n from E such that $\phi(u)$ still has order ℓ. So we can compute the action of Hecke correspondences on points $x = (E, u)$ using Vélu's formulae.

There remains to treat the case of cusps.

We call $\sigma_{\tilde{\beta}}$ for $1 \leq \tilde{\beta} \leq \frac{\ell-1}{2}$ and $\mu_{\tilde{\alpha}}$ for $1 \leq \tilde{\alpha} \leq \frac{\ell-1}{2}$ the cusps on $X_1(\ell)$ images by ϕ of the $\sigma_{\infty,\tilde{\beta}}$ and $\mu_{\infty,\tilde{\alpha}}$.

For n prime to ℓ we have $T_n(\sigma_{\tilde{\beta}}) = \sigma_{\tilde{\beta}} + n\sigma_{n\tilde{\beta}}$ and $T_n(\mu_{\tilde{\alpha}}) = n\mu_{\tilde{\alpha}} + \mu_{n\tilde{\alpha}}$, where $n\tilde{\alpha}$ in $\mu_{n\tilde{\alpha}}$ (resp. $n\tilde{\beta}$ in $\sigma_{n\tilde{\beta}}$) should be understood as the class of this integer in $(\mathbb{Z}/\ell\mathbb{Z})^*/\{1, -1\}$.

Similarly $T_\ell(\sigma_{\tilde{\beta}}) = \sigma_{\tilde{\beta}} + 2\sum_{1 \leq \tilde{\alpha} \leq \frac{\ell-1}{2}} \mu_{\tilde{\alpha}}$ and $T_\ell(\mu_{\tilde{\alpha}}) = \ell\mu_{\tilde{\alpha}}$. □

We can now state the

Theorem 2 *There is a probabilistic (Las Vegas) algorithm that on input a prime ℓ and a prime $p \geq 7$ such that ℓ is prime to p, computes the Ramanujan subspace $W_\ell = \phi^*(V_\ell)$ inside the ℓ-torsion of the jacobian of $\mathcal{X}_\ell/\mathbb{F}_p$. The answer is given as a list of ℓ^2 degree g_ℓ effective divisors on $\mathcal{X}_\ell$, the first one beeing the origin ω. The algorithm runs in probabilistic polynomial time in p and ℓ.*

Lemma 18 gives us a plane model for $\mathcal{X}_\ell \pmod p$ and a resolution of its singularities. From lemma 19 we obtain the zeta function of $\mathcal{X}_\ell \pmod p$. The characteristic polynomial of F_p on the Ramanujan space V_ℓ is $X^2 - \tau(p)X + p^{11} \bmod \ell$. So we compute $\tau(p) \pmod \ell$ using the expansion of the discriminant form. We deduce some small enough field of decomposition $\mathbb{F}_q$ for $V_\ell \pmod p$. We then apply theorem 1 and obtain a basis for the ℓ-torsion in the Picard group of $\mathcal{X}_\ell/\mathbb{F}_q$. The same theorem allows us to compute the matrix of the endomorphism $\nu = \phi^* \circ \phi_*$ in this basis. We deduce a basis for the image $\mathcal{A}[\ell](\mathbb{F}_q)$ of ν. Using theorem 1 again, we now write down the matrices of the Hecke operators $\hat{T}_n$ in this basis for all $n < \ell^2$. It is then a matter of linear algebra to compute a basis for the intersection of the kernels of all $\hat{T}_n - \tau(n)$ in $\mathcal{A}[\ell](\mathbb{F}_q)$. The algorithm is Las Vegas rather than Monte-Carlo because we can check the result, the group W_ℓ having known cardinality ℓ^2. □

Important remark 3 *In the above theorem, one may impose an origin ω rather than letting the algorithm choose it. For example, following work by Edixhoven, one may choose as origin a well designed linear combination of the*

cusps. Such an adapted choice of the origin may insure that the $\ell^2 - 1$ divisors representing the non-zero classes in W_ℓ are unique in characteristic zero and thus remain unique modulo p for all but finitely many primes p.

References

[1] H. Cohen. *A course in computational algebraic number theory*. Springer, 1993.

[2] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1997.

[3] Sebastiaan Edixhoven. On computing coefficients of modular forms. *Talk at MSRI*, http://www.math.leidenuniv.nl/∼edix/public_html_rennes/talks/msridec2000.html , 2000.

[4] Andreas Enge. *Elliptic curves and their applications to cryptography, an introduction*. Kluwer Academic Publishers, 1999. — **N° 844**.

[5] Gerhard Frey and Michael Müller. Arithmetic of modular curves and applications. In *On Artin's conjecture for odd 2-dimensional representations*, number 1585 in Lecture Notes in Math. Springer, 1994.

[6] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of computation*, 62(206):865–874, 1994.

[7] S.D. Galbraith, S. Paulus, and N.P. Smart. Arithmetic of superelliptic curves. *Mathematics of computation*, 71(237):393–405, 2002.

[8] D. Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc.*, 72:414–436, 1952.

[9] Gaétan Haché. Computation in algebraic function fields for effective construction of algebraic-geometric codes. In *Proceedings of the 11th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 262–278. 1995.

[10] Dale Husemoller. *Elliptic curves*. Springer, 1987.

[11] Serge Lang. *Abelian varieties*, volume 7 of *Interscience Tracts in Pure and Applied Mathematics*. Interscience Publishers, 1959. — **N° 751**.

[12] S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent. Math.*, 7:120–136, 1969.

[13] Yuri Manin. Parabolic points and zeta function of modular curves. *Math. USSR Izvestija*, 6(1):19–64, 1972.

[14] A. Menezes, S. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inf. Theory*, IT-39(5):1639–1646, 1993.

[15] Loïc Merel. Universal Fourier expansions of modular forms. In *On Artin's conjecture for odd 2-dimensional representations*, number 1585 in Lecture Notes in Math. Springer, 1994.

[16] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7:219–254, 1995.

[17] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[18] Emil J. Volcheck. Computing in the jacobian of a plane algebraic curve. In *Algorithmic number theory, ANTS I*, number 877 in lecture notes in computer science, pages 221–233. Springer, 1994.