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

J.-M. Couveignes*

July 31, 2008

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

*Institut de Mathématiques de Toulouse, Université de Toulouse et CNRS, Département de Mathématiques et Informatique, Université Toulouse 2, 5 allées Antonio Machado, 31058 Toulouse cédex 9.

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 over $\mathbb{F}_q$ 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 that 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 monic 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 $(g_i)_{1\le i\le I}$ should induce a decomposition of $\mathcal{J}[\ell^k](\mathbb{F}_q)$ as a direct product $\prod_{1\le i\le I} < g_i >$ 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 3 we recall how to compute in the Picard group $\mathcal{J}(\mathbb{F}_q)$. Section 4 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 5. Section 6 is concerned with characteristic subspaces for the action of Frobenius inside the ℓ^∞-torsion of $\mathcal{J}(\bar{\mathbb{F}}_q)$. In section 7 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 8 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 9 and 10 are devoted to two families of modular curves. We give a nice plane model for such curves. The general algorithms presented in section 8 are then applied to these modular curves in section 11 in order to compute explicitly the modular representation modulo ℓ associated with the discriminant modular form (level 1 and weight 12). This modulo ℓ representation V_ℓ is seen as a subgroup of order ℓ^2 inside the ℓ-torsion of $J_1(\ell)/\mathbb{Q}$.

The idea is to compute the reduction modulo p of the group scheme V_ℓ as a subgroup of $J_1(\ell)/\mathbb{F}_p$, for many small primes p. One then lifts using the Chinese Remainder Theorem. This makes a connection with Edixhoven's program for computing coefficients of modular forms. My contribution to this program is sketched in section 2. See [10, 11]. The core of Edixhoven's program is that if one knows V_ℓ, one can efficiently compute the Ramanujan function $\tau(P)$ modulo ℓ for a large prime P. If we have enough primes ℓ, we can deduce the actual value of $\tau(P)$.

The last three sections present variants of the main algorithm and auxiliary results. Section 12 presents a simpler variant of the method of section 11, that is particularly useful when the action of the p-Frobenius on V_ℓ modulo p is semisimple non-scalar. In the non-semisimple case, this simpler method may only produce a non-trivial subspace inside V_ℓ modulo p. Section 14 proves that this semisimplicity condition holds quite often indeed, as expected. As a consequence, one may compute the representation V_ℓ associated with the discriminant form for at least half (say) the primes ℓ, using this simplified algorithm. This suffices for the purpose of computing the Ramanujan function $\tau(P)$ at a large prime P since we may afford to skip half the auxiliary primes ℓ. On the other hand, if one wishes to compute a representation modulo ℓ for a given ℓ, then one should be ready to face (at least theoretically) the case when no small prime p is semisimple for ℓ. In that situation, the simplified algorithm would only give a non-trivial subspace of V_ℓ modulo p for many primes p.

Section 13 addresses the problem of computing V_ℓ from all the knowledge we have collected concerning $V_\ell \bmod p$ for many small primes p. It requires a sort of interpolation theorem in the context of polynomials with integer coefficients. The goal is to recover a polynomial $P(X)$ once given a collection of non-trivial factors of $P(X) \bmod p$ for many primes p. This helps recovering $V_\ell/\mathbb{Q}$ once given a subspace in its reduction modulo p for enough small primes p.

Altogether, this proves that the simplified algorithm, despite the possibility of many non-semisimple primes p, suffices to compute $V_\ell/\mathbb{Q}$ for all ℓ.

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 occurrence by some large enough real number.*

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. One 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 Context: the inverse Jacobi problem

The initial motivation for this work is a discussion I had in 2000 with Bas Edixhoven about his program aiming at polynomial time computation of coefficients of modular forms.

He asked how one can compute (e.g.) the decomposition field of the dimension two modulo ℓ Galois representation V_ℓ associated to the discriminant modular form Δ. This amounts to computing the field of moduli of some very special ℓ-cyclic coverings of $X_1(\ell)$.

I had some experience in explicit computation of coverings using numerical techniques and got the impression that a purely algebraic approach would fail to solve such a problem. This is because V_ℓ, however small it is, is lost in the middle of the full ℓ-torsion of $J_1(\ell)$. And the latter is a huge dimension zero variety (its number of geometric points is exponential in ℓ).

The second time I discussed this question with Edixhoven, it became clear that we had two options. We might compute V_ℓ inside the complex torus of $J_1(\ell)$ and evaluate a theta function at some point x in V_ℓ. Edixhoven convinced me that this approach was unlikely to succeed since the number of terms to be considered in the expansion of the theta function would be exponential in ℓ, even for a poor accuracy. Another possibility was to solve the inverse Jacobi problem for x and find a divisor $D = P_1 + \cdots + P_g - gO$ in the class associated to x in the Picard group of $X_1(\ell)$. Then one would pick a function f on $X_1(\ell)$ and evaluate $F(x) = f(P_1) + \cdots + f(P_g)$ for example.

Solving the inverse Jacobi problem seemed easy. Indeed one could pick any divisor $D^0 = P_1^0 + \cdots + P_g^0 - gO$ of the above form on $X_1(\ell)$ and compute its image x^0 by the Jacobi map. Then one would move slowly from x^0 to x inside the complex torus $J_1(\ell)(\mathbb{C})$. At each step the corresponding divisor would be computed from the previous one using Newton's method.

Although the Jacobi map is birational, it is not quite an isomorphism however. It has a singular locus and it was not clear how one could avoid this obstacle in the journey from x^0 to x.

It was decided that I would think about how to solve this problem while Edixhoven would prove good bounds on the height of the algebraic number $F(x)$ coming out of the algorithm. Edixhoven first proved the analogous bound in the function field case. Then, Bas Edixhoven and Robin de Jong, using Arakelov theory and results by Merkl in [11] or J. Jorgenson and J. Kramer in [19], proved the bound for the height of $F(x)$.

On my side, I was trying to avoid the singular locus. I believe that in general, the problem of avoiding the singular locus might very well be NP-complete. Indeed, if the curve under consideration is very close to the boundary of the moduli space, the problem takes a discrete aspect: the curve has long tubes and sometimes one may have to decide to push one point through one tube or the other one. In case one makes the wrong decision, one may be lost for ever. The problem can be phrased in a more mathematical way: if the curve is (close to) a Mumford curve, solving the inverse Jacobi problem assumes one can solve the discrete counterpart for it: solving the Jacobi problem for a finite graph; namely the intersection graph of the curve. See [7] theorem Theorem 2.1 and the following remark for a statement of this problem, that I suspect is very hard when the genus of the graph tends to infinity.

Of course one may expect that $J_1(\ell)$ keeps far enough from the boundary of its moduli space when ℓ tends to infinity. However, I was not able to give a proof that the above ideas do succeed in solving the inverse Jacobi problem, even for these curves. I had to build on a rather different idea and proved in [8] that for $X_0(\ell)$ at least, solving the inverse Jacobi problem is deterministic polynomial time in ℓ and the required precision.

The first version of [8] was ready in January 2004. Extending this result to any modular curve is just a technical problem, but I confess I was tired with technicalities and I stopped there with the complex method.

Starting in August 2003 I decided to look for a p-adic analogue of this complex method: looking for a p-adic approximation instead of a complex one. After some hesitation I realized that computing modulo several small primes p and then lifting using the Chinese remainder would lead to a simpler algorithm. This text gathers the results of this research. The methods presented here are the discrete counterpart of the ones in [8]. The essence of theorem 2 is that the discrete method presented in this paper applies to modular curves $X_1(\ell)$. This is exactly what is needed for the purpose of computing the Ramanujan function.

The complex approach is more tedious but leads to deterministic algorithms. The main reason is that the set of complex points in the jacobian is a connected topological space. The modulo p approach that we present here seems intrinsically probabilistic, because one has to find generators of Picard groups of curves over finite fields.

I should also say that the complex approach was not abandoned since Johan Bosman started in June 2004 his PhD with Edixhoven on this topic and he succeeded in explicitly computing some V_ℓ using the complex method. See [3]. He built on the Newton approach to solving the inverse Jacobi problem, as sketched above. This shows that the singular locus of the Jacobi map is not so disturbing after all, at least in practice.

Several sections in this text have been included in Edixhoven's report [11]. Many thanks are due to Bas Edixhoven and Robin de Jong for useful discussions, suggestions, and comments.

Many thanks also to John Cremona and the anonymous referee for reading in detail this long manuscript and for their useful comments.

3 Basic algorithms for plane curves

We recall elementary results about computing in the Picard group of an algebraic curve over a finite field. See [16, 33].

3.1 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.

3.2 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 over $\mathbb{F}_q$ 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 curve C is assumed to be absolutely irreducible and reduced. By a *point* on C we mean a geometric point (an element of $C(\bar{\mathbb{F}}_q)$). Any $\bar{\mathbb{F}}_q$-point on C can be represented by its affine or projective coordinates.

Let $\mathcal{X}$ be a smooth model of C. There is a desingularization map $\mathcal{X} \to C$. If $P \in \mathcal{X}(\bar{\mathbb{F}}_q)$ is a geometric point on $\mathcal{X}$ above a singular point S on C, we say that P is a *singular branch*.

The *conductor* $\mathfrak{C}$ is an effective divisor on $\mathcal{X}$ with even coefficients. Some authors call it the adjunction divisor. Its support is made of all singular branches. The conductor expresses the local behaviour of the map $\mathcal{X} \to C$. See [29, IV.1], [15]. We have $\deg(\mathfrak{C}) = 2\delta$ where δ is the difference between the arithmetic genus $\frac{(d-1)(d-2)}{2}$ of C and the geometric genus g of $\mathcal{X}$. Since $\delta \leq \frac{(d-1)(d-2)}{2}$, the support of $\mathfrak{C}$ contains at most $\frac{(d-1)(d-2)}{2}$ geometric points in $\mathcal{X}(\bar{\mathbb{F}}_q)$. So the field of definition of any singular branch on $\mathcal{X}$ is an extension of $\mathbb{F}_q$ with degree $\leq \frac{(d-1)(d-2)}{2}$. A modern reference for singularities of plane curves is [5] and especially section 5.8.

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

More precisely, let $P \in \mathcal{X}(\bar{\mathbb{F}}_q)$ be a geometric point above a singular point S, and let v be the corresponding valuation. 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 even coefficients. The following algorithms still work if the conductor is replaced by any divisor $\mathfrak{D}$ that is greater than the conductor and has polynomial degree in d. Such a divisor can be found easily: the singular branches on $\mathcal{X}$ are supposed to be known already, and the multiplicities are bounded above by $\frac{(d-1)(d-2)}{2}$.

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 9 and 10 that this is also the case for two nice families of modular curves.

3.3 Divisors, forms, and functions

Smooth $\bar{\mathbb{F}}_q$-points on C are 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 $h \geq 0$ we set

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

the $\mathbb{F}_q$-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 $\mathbb{F}_q$. 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

$$\mathcal{H}_h = H^0(\mathcal{X}/\mathbb{F}_q, \mathcal{O}_{\mathcal{X}/\mathbb{F}_q}(h))$$

the space of forms of degree h on $\mathcal{X}$. Here $\mathcal{O}_{\mathcal{X}/\mathbb{F}_q}(h)$ is the pullback of $\mathcal{O}_{\mathbb{P}^2/\mathbb{F}_q}(h)$ to $\mathcal{X}$.

Let W be a degree h form on $\mathbb{P}^2$ having non-zero pullback $W_{\mathcal{X}}$ on $\mathcal{X}$. Let $H = (W_{\mathcal{X}})$ be the divisor of this restriction. The map $f \mapsto \frac{f}{W_{\mathcal{X}}}$ is a bijection from $H^0(\mathcal{X}/\mathbb{F}_q, \mathcal{O}_{\mathcal{X}/\mathbb{F}_q}(h))$ to the linear space $\mathcal{L}(H)$.

If Δ is a divisor on $\mathcal{X}$ we note $\mathcal{H}_h(-\Delta)$ the subspace of forms in $\mathcal{H}_h$ 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 [15, Theorem 7].

We set $S_C = \mathcal{S}_{2d}$ and $\mathcal{H}_C = \mathcal{H}_{2d}(-\mathfrak{C})$, 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 $F(X, Y, Z) = \sum_{a+b+c=2d} \epsilon_{a,b,c} X^aY^bZ^c$ of degree $2d$ in X, Y and Z. For every branch P above a singular point $S \in C$ (assuming for example that S 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_P at this branch. We ask the resulting series in t_P 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 $X^aY^bZ^cE(X, Y, Z)$ with $a+b+c = d$. 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 on $\mathcal{X}$ 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.

3.4 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 $\mathcal{X}$. This ω will serve as an origin: 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 $\mathcal{H}_{2d}(-\mathfrak{C}-A-B)$ 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 $2d^2 - 2g - 2\delta$. The linear space $\mathcal{H}_{2d}(-\mathfrak{C} - R - \omega)$ 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 $\mathcal{H}_{2d}(-\mathfrak{C} - 2\omega)$. The divisor of f_1 is $(f_1) = 2\omega + \mathfrak{C} + R$ where R is an effective divisor with degree $2d^2 - 2g - 2\delta$. The linear space $\mathcal{H}_{2d}(-\mathfrak{C} - R - A)$ 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 $\mathbb{F}_q$-divisor with degree g on $\mathcal{X}$, denoted ω. We assume ω is given as a difference between two effective divisors with degrees bounded by a polynomial in d. This ω serves as an origin. Arithmetic operations in the Picard group $\mathrm{Pic}^0(\mathcal{X}/\mathbb{F}_q)$ can be performed in time polynomial in $\log q$ and d. This includes addition, substraction and comparison of divisor classes.*

If ω is not effective, we use lemma 2 below to compute a non-zero function f in $\mathcal{L}(\omega)$ and we write $\omega' = (f) + \omega$. This is an effective divisor with degree g. We replace ω by ω' and finish as in the paragraph before lemma 1 □

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 $\mathcal{L}(A - B) = 0$. Let a be the degree of A. We let h be the smallest integer such that $h \geq 2d$ and $hd + g + 1 > a + (d-1)(d-2)$.

So the space $\mathcal{H}_h(-\mathfrak{C} - A)$ is non-zero. It 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 $\mathcal{X}$ such that $1 \leq \deg(O) \leq d$ 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 proved 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 call α the smallest integer such that $q^\alpha > \deg(A)$ and we set $\beta = \alpha + 1$. We apply lemma 3 after base change to the field with q^α elements 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 $(\alpha + 1)D$. We return the divisor $E = e_\beta - e_\alpha$. We observe that we can take $\alpha \leq 1 + \log_q \deg(A)$ so the degree of the positive part E^+ of E is $\leq 6gd(\log_q(\deg(A)) + 1)$.

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 $\leq 6gd(\log_q(\deg(A)) + 1)$.*

4 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 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) $\mathcal{J}(\mathbb{F}_q)$. Let g be the genus of $\mathcal{X}$. We assume we are given a degree 1 divisor $O = O^+ - O^-$ where O^+ and O^- are effective, $\mathbb{F}_q$-rational and have degree bounded by an absolute constant times g.

We know from [26, Theorem 2] that the group $\mathrm{Pic}^0(\mathcal{X}/\mathbb{F}_q)$ is generated by the classes $[\mathfrak{p} - \deg(\mathfrak{p})O]$ where $\mathfrak{p}$ runs over the set of prime divisors of degree $\leq 1 + 2\log_q(4g-2)$. For the convenience of the reader we quote this result as a lemma.

Lemma 6 (Müller, Stein, Thiel) *Let K be an algebraic function field of one variable over $\mathbb{F}_q$. Let $N \geq 0$ be an integer. Let g be the genus of K. Let $\chi : \mathrm{Div}(K) \to \mathbb{C}^*$ be a character of finite order which is non-trivial when restricted to Div^0. Assume that $\chi(\mathfrak{B}) = 1$ for every prime divisor $\mathfrak{B}$ of degree $\leq N$. Then*

$$N < 2\log_q(4g-2).$$

If $q < 4g^2$, the number of prime divisors of degree $\leq 1 + 2\log_q(4g-2)$ is bounded by $\mathcal{O}g^{\mathcal{O}}$. So we can compute easily a small generating set for $\mathcal{J}(\mathbb{F}_q)$.

In the rest of this section, we will assume that 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.

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 monic prime polynomials of degree r over $\mathbb{F}_q$. The cardinality of $\mathcal{U}(r,q)$ is $\frac{q^r - q}{r}$ so

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

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 monic 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 $x : \mathcal{P}(r,q) \to \mathcal{U}(r,q)$ above it and, provided this fiber 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 in every $d \times (0.99)^{-1}$ fibers is non-empty. We thus define a distribution μ on $\mathcal{P}(r,q)$ and prove the following.

Lemma 7 (A very rough measure) *There is a unique measure μ on $\mathcal{P}(r,q)$ such that all non-empty fibers of the map $x : \mathcal{P}(r,q) \to \mathcal{U}(r,q)$ have the same measure, and all points in a given fiber have the same 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 $\mathcal{X}/\mathbb{F}_q$. 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 $J_r : \mathcal{D}(r,q) \to \mathcal{J}(\mathbb{F}_q)$ 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 $\psi(J_r(\Delta)) \neq 0 \in G$. Since all the fibers of $\psi \circ J_r$ 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 $\psi(J_r(\Delta))$ 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 $\psi \circ J_r$. 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 7, the probability of success is at least $\frac{1}{2d}$. If we make $2d$ trials, the probability of success is $\geq 1 - \exp(-1) \geq \frac{1}{2}$.

Lemma 8 (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 8 we find a sequence of elements in $\mathcal{J}(\mathbb{F}_q)$ out of which one at least is non-zero (with high probability). 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 (with high probability). 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 $\max(48g, 24d, 720)$. Note that every step in this method is probabilistic: it succeeds with some probability, that can be made very high (exponentially close to 1) while keeping a polynomial overall complexity.

Lemma 9 (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 $\log q$.

Note that we do not catch the whole group $\mathcal{J}(\mathbb{F}_q)$ of rational points but a subgroup $\mathcal{A}$ with index at most $\iota = \max(48g, 24d, 720)$. This is a small but annoying gap. In the sequel we shall try to compute the ℓ-torsion of the group $\mathcal{J}(\mathbb{F}_q)$ of rational points. Because of the small gap in the above lemma, we may miss some ℓ-torsion points if ℓ is smaller than ι. However, let k be an integer such that $\ell^k > \iota$. And let x be a point of order ℓ in $\mathcal{J}(\mathbb{F}_q)$. Assume there exists a point y in $\mathcal{J}(\mathbb{F}_q)$ such that $x = \ell^{k-1}y$. The group $< y >$ generated by y and the group $\mathcal{A}$ have non-trivial intersection because the product of their orders is bigger than the order of $\mathcal{J}(\mathbb{F}_q)$. Therefore x belongs to $\mathcal{A}$.

Our strategy for computing $\mathcal{J}(\mathbb{F}_q)[\ell]$ will be to find a minimal field extension $\mathbb{F}_Q$ of $\mathbb{F}_q$ such that all points in $\mathcal{J}(\mathbb{F}_q)[\ell]$ are divisible by ℓ^{k-1} in $\mathcal{J}(\mathbb{F}_Q)$. We then shall apply the above lemma to $\mathcal{J}(\mathbb{F}_Q)$. To finish with, we shall have to compute $\mathcal{J}(\mathbb{F}_q)$ as a subgroup of $\mathcal{J}(\mathbb{F}_Q)$. To this end, we shall use the Weil pairing.

5 Pairings

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

We first recall the definition of Weil pairing following [20]. Let k be an algebraically closed field with characteristic p. For every abelian variety A over k, 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 irreducible and reduced varieties over k, and let $\alpha : V \to A$ and $\beta : W \to B$ be the 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 $na = nb = 0$. The Weil pairing $e_{n,D}(a, b)$ is defined in [20, VI, §4, Theorem 10]. 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 irreducible and reduced curve over k and $A = B = \mathcal{J}$ is its jacobian and $\alpha = \beta = f : \mathcal{X} \to \mathcal{J}$ is the Jacobi map (once an origin on $\mathcal{X}$ has been chosen). 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.

The jacobian $\mathcal{J}$ is principally polarized. We have an isomorphism $\lambda : \mathcal{J} \to \hat{\mathcal{J}}$ between $\mathcal{J}$ and its dual $\hat{\mathcal{J}}$. If α is an endomorphism $\alpha : \mathcal{J} \to \mathcal{J}$, we denote by ${}^t\alpha$ its transpose ${}^t\alpha : \hat{\mathcal{J}} \to \hat{\mathcal{J}}$. If D is a divisor on $\mathcal{J}$ that is algebraically equivalent to zero, the image by ${}^t\alpha$ of the linear equivalence class of D is the linear equivalence class of the inverse image $\alpha^{-1}(D)$. See [20, V, §1]. The Rosati dual of α is defined to be $\alpha^* = \lambda^{-1} \circ {}^t\alpha \circ \lambda$. The map $\alpha \to \alpha^*$ is an involution, and α^* is the adjoint of α for the Weil pairing

$$e_{n,\mathcal{X}}(a, \alpha(b)) = e_{n,\mathcal{X}}(\alpha^*(a), b) \tag{1}$$

according to [20, VII, §2, Proposition 6].

If $\mathcal{Y}$ is another smooth projective irreducible and reduced curve over k 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-Rück pairing can be constructed from the Lichtenbaum version of Tate's pairing [22] as was shown in [14]. Let q be a power of p. Let again $n \geq 2$ be an integer prime to p 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-Rück 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 $[E] \bmod n$ 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, Vanstone, Frey and Rück. The Tate-Lichtenbaum-Frey-Rück pairing can be computed similarly.

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 [24] in the context of elliptic curves, and in [14] 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 $\leq 6gd(\log_q(\deg(\mathfrak{b})) + 1)$. 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 $\leq 6gd(\log_q(\deg(\mathfrak{b})) + 1)$. 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 $\Psi \prod_k \mu_k^{-\epsilon_k}$ has divisor $n\mathfrak{a}$ so is the ϕ we were looking for.

Lemma 10 (Computing the Weil pairing) *There exists an algorithm that on input an integer $n \geq 2$ prime to q and a degree d absolutely irreducible reduced plane projective curve C over $\mathbb{F}_q$ and its smooth model $\mathcal{X}$ and two $\mathbb{F}_q$-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 $\mathfrak{a}^+$, $\mathfrak{a}^-$, $\mathfrak{b}^+$, $\mathfrak{b}^-$, the positive and negative parts of $\mathfrak{a}$ and $\mathfrak{b}$.*

Lemma 11 (Computation of Tate-Lichtenbaum-Frey-Rück pairings) *There exists an algorithm that on input an integer $n \geq 2$ dividing $q-1$ and a degree d absolutely irreducible reduced plane projective curve C over $\mathbb{F}_q$ and its smooth model $\mathcal{X}$ and two $\mathbb{F}_q$-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-Rück pairing $\{\mathfrak{a}, \mathfrak{b}\}_n$ in time polynomial in d, $\log q$, $\log n$ and the degrees of $\mathfrak{a}^+$, $\mathfrak{a}^-$, $\mathfrak{b}^+$, $\mathfrak{b}^-$, the positive and negative parts of $\mathfrak{a}$ and $\mathfrak{b}$.*

6 Divisible groups

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 $\ell \neq p$ be a prime integer. We assume $g \geq 1$. Let $\mathcal{J}$ be the jacobian of $\mathcal{X}$ and let $\mathrm{End}(\mathcal{J}/\mathbb{F}_q)$ be the ring of endomorphisms of $\mathcal{J}$ over $\mathbb{F}_q$. Let F_q be the Frobenius endomorphism. In this section we study the action of F_q on ℓ^k-torsion points of $\mathcal{J}$. We first consider the whole ℓ^k-torsion group. We then restrict to some well chosen subgroups where this action is more amenable.

Let $\chi(X)$ be the characteristic polynomial of $F_q \in \mathrm{End}(\mathcal{J}/\mathbb{F}_q)$. 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 $\varphi_q = X \bmod \chi(X) \in \mathcal{O}$. Mapping φ_q onto F_q defines an epimorphism from the ring $\mathcal{O}$ onto $\mathbb{Z}[F_q]$. In order to control the degree of the field of definition of ℓ^k-torsion points we shall bound the order of φ_q in $(\mathcal{O}/\ell^k\mathcal{O})^*$.

We set $\mathcal{U}_1 = (\mathcal{O}/\ell\mathcal{O})^* = (\mathbb{F}_\ell[X]/\chi(X))^*$. 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 $\prod_i \ell^{(e_i-1)f_i}(\ell^{f_i}-1)$. 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 $M_1(X) \in \mathbb{Z}[X]$ 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 Ξ_i monic and $\deg(\Xi_i) = e_i f_i$, and the order of $\mathcal{U}_k$ is $\prod_i \ell^{f_i(ke_i-1)}(\ell^{f_i}-1)$. 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 $M_k(X) \in \mathbb{Z}[X]$ 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 the χ_i 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 12 (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 $\mathcal{J}/\mathbb{F}_q$. 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 $\mathcal{J}$ splits completely 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.*

In order to state sharper results 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 now see how to define such subgroups and control their rationality properties.

Lemma 13 (Divisible group) *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's theorem [30] Π is induced by some endomorphism in $\mathrm{End}(\mathcal{J}/\mathbb{F}_q) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ 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 $\mathbb{G}$.*

Remark 3 *The dual $\mathbb{G}^*$ does not only depend on $\mathbb{G}$. It may depend on Π also.*

Remark 4 *We may equivalently define Π^* as the dual of Π for the Weil pairing. See formula (1).*

We now give an example of divisible group. Let $F(X) = F_1(X)$ and $G(X) = G_1(X)$ be two monic 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 monic and $\chi(X) = F_k(X)G_k(X) \bmod \ell^k$ and $F_kH_k + G_kK_k = 1 \bmod \ell^k$ and $\deg(H_k) < \deg(G_1)$ and $\deg(K_k) < \deg(F_1)$ 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 F_q for X in F_0H_0 we obtain a map $\Pi_G : \mathcal{J}[\ell^\infty] \to \mathcal{J}[\ell^\infty]$ and similarly, if we substitute F_q for X in G_0K_0 we obtain 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.

Definition 1 (Characteristic subspaces) *For every non-trivial monic factor $F(X)$ 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 $F = (X-q)^e$ then we write similarly $\mathbb{G}_{(X-q)^e} = \mathbb{G}_q = \mathbb{G}_1^*$.*

We now compute fields of definitions for torsion points inside such divisible groups. 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 smaller ring $\mathcal{O}_\ell/(\ell^k, F_0(\varphi_q)) = \mathbb{Z}_\ell[X]/(\ell^k, F_0)$. We deduce the following.

Lemma 14 (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 monic 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 $\mathbb{G}_F$ splits completely 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 $M_k(X)$ modulo 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 can take $B(F)=1$ 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 split completely over small degree extensions of $\mathbb{F}_q$.

7 The Kummer map

Let $\mathcal{X}$ be a smooth projective absolutely 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 $R \in \mathcal{J}(\bar{\mathbb{F}}_q)$ 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

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

in

$$\mathrm{Hom}(\mathcal{J}[n](\mathbb{F}_q), H^1(\mu_n)) = \mathrm{Hom}(\mathcal{J}[n](\mathbb{F}_q), \mathrm{Hom}(\mathrm{Gal}(\mathbb{F}_q), \mu_n)).$$

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-Rück pairing is non-degenerate. We observe that $\mathrm{Hom}(\mathrm{Gal}(\mathbb{F}_q), \mu_n)$ is isomorphic to μ_n: giving an homomorphism from $\mathrm{Gal}(\mathbb{F}_q)$ to μ_n is equivalent to giving 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 $\mathcal{J}[n]$ splits completely 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*.

Definition 2 (The Kummer map) *Let $\mathcal{J}/\mathbb{F}_q$ be a jacobian and $n \geq 2$ an integer. Assume $\mathcal{J}[n]$ splits completely over $\mathbb{F}_q$. For P in $\mathcal{J}(\mathbb{F}_q)$ we choose any R in $\mathcal{J}(\bar{\mathbb{F}}_q)$ such that $nR = P$ and we set $K_{n,q}(P) = {}^{F_q}R - R$. This defines a bijection*

$$K_{n,q} : \mathcal{J}(\mathbb{F}_q)/n\mathcal{J}(\mathbb{F}_q) \to \mathcal{J}[n](\mathbb{F}_q) = \mathcal{J}[n].$$

We now assume that $n = \ell^k$ is a power of some prime integer $\ell \neq p$. We also make the (strong !) assumption that $\mathcal{J}[n]$ splits completely 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 $\mathbb{Z}[F_q] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[F_q]$ 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 be seen to be very useful but it requires that $\mathcal{J}[n]$ splits completely 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 12 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 15 (Computing the Kummer map) *Let $\mathcal{J}/\mathbb{F}_q$ be a jacobian. Let $g \geq 1$ be its dimension. Let $\ell \neq p$ be a prime integer and $n = \ell^k$ a power of ℓ. 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 $Q = q^{A_k}$ and observe that n divides $Q - 1$ because $\mathcal{J}[n]$ splits completely over $\mathbb{F}_Q$. 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 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, namely the n-torsion of a given divisible group.

So 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 $\mathbb{G}[n]$ splits completely over $\mathbb{F}_Q$. Let P be an $\mathbb{F}_Q$-rational point in $\mathbb{G}$. Let $R \in \mathbb{G}(\bar{\mathbb{F}}_q)$ 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 14 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 16 (The Kummer map for a divisible group) *Let $\mathcal{J}/\mathbb{F}_q$ be a jacobian. Let g be its dimension. 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 monic 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 14 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 $F(X)$ 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, $\log N$.*

8 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. We also assume we are given a degree 1 divisor $O = O^+ - O^-$ where O^+ and O^- are effective, $\mathbb{F}_q$-rational and have degree bounded by an absolute constant times g.

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, ..., 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 17 (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 $3I\#G$ 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_1x_1 that is equal to zero. This gives us the relation $r_1 = (e_1, 0, \dots, 0) \in \mathcal{R}$. 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_2x_2 that is in $L_1 = \{0, x_1, \dots, (e_1 - 1)x_1\}$. 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 $e_1e_2 \leq o$ comparisons.

We then compute successive multiples of x_3 until we find the first one e_3x_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 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 1 and lemma 16 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 1 and lemma 16 we obtain two surjective maps $\Pi_q : \mathcal{J}(\mathbb{F}_{Q_k})[\ell^\infty] \to \mathbb{G}_q(\mathbb{F}_{Q_k})$ and $K_{\mathbb{G}_q,\ell^k,Q_k} : \mathbb{G}_q(\mathbb{F}_{Q_k}) \to \mathbb{G}_q[\ell^k]$.

There exists a unit u in $\mathrm{End}(\mathcal{J}/\mathbb{F}_q) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ such that the Rosati dual Π_1^* of Π_1 is

$$\Pi_1^* = u\Pi_q.$$

Therefore $\mathbb{G}_q = \mathbb{G}_1^*$ and the restriction of the Weil pairing to $\mathbb{G}_1[\ell^k] \times \mathbb{G}_q[\ell^k]$ is non-degenerate.

If $Q_k \geq 4g^2$, we use lemma 9 to produce a sequence $\gamma_1, \ldots, \gamma_I$ of elements in $\mathcal{J}(\mathbb{F}_{Q_k})$ that generate (with high probability) a subgroup of index at most $\iota = \max(48g, 24d, 720)$. If $Q_k \leq 4g^2$ we use lemma 6 to produce a sequence $\gamma_1, \ldots, \gamma_I$ of elements in $\mathcal{J}(\mathbb{F}_{Q_k})$ that generate it.

Let N be the largest divisor of $\#\mathcal{J}(\mathbb{F}_{Q_k})$ which is prime to ℓ.

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. Recall the restriction of the Weil pairing to $\mathbb{G}_1[\ell^k] \times \mathbb{G}_q[\ell^k]$ is a non-degenerate pairing

$$e_{\ell^k} : \mathbb{G}_1[\ell^k] \times \mathbb{G}_q[\ell^k] \rightarrow \mu_{\ell^k}.$$

We fix an isomorphism between the group $\mu_{\ell^k}(\bar{\mathbb{F}}_q) = \mu_{\ell^k}(\mathbb{F}_{Q_k})$ of ℓ^k-th roots of unity and $\mathbb{Z}/\ell^k\mathbb{Z}$. Having chosen the preimage of $1 \bmod \ell^k$, computing this isomorphism is a problem called *discrete logarithm*. We can compute this discrete logarithm by exhaustive search at the expense of $O(\ell^k)$ operations in $\mathbb{F}_{Q_k}$. There exist more efficient algorithms, but we don't need them for our complexity estimates.

We regard the matrix $(e_{\ell^k}(\beta_i, \rho_j))$ as a matrix with I rows, 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 complement of $\mathcal{B}_k$ in $< \rho_1, \ldots, \rho_J > \subset \mathbb{G}_1[\ell^k]$. So it has order $\leq \iota$. We then compute a basis of $\mathcal{R}'$. This boils down to computing the kernel of an $I \times (J + I)$ integer matrix with entries bounded by ℓ^k. This can be done by putting this matrix in Hermite normal form (see [6, 2.4.3]). The complexity is polynomial in I, J and $k \log \ell$. See [17], [6, 2.4.3] and [31].

Once given a basis of $\mathcal{R}'$, the sublattice $\mathcal{R}$ can be computed using lemma 17 at the expense of $\leq 3J\iota$ operations.

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 $F_q(b_j), b_1, b_2, \ldots, b_w$ and deduce the matrix of F_q with respect to 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 following.

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 $g_1, \dots, g_W$ 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 the class, 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 $\sum_{1 \leq i \leq W} x_i g_i = [D]$.

9 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 geometric points on $\mathcal{X}_\ell$ above every singularity of C_ℓ and compute the conductor $\mathfrak{C}_\ell$ 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 $a_0(\lambda) = \ell$.

Let $\mathcal{F}$ be a splitting field of $\mathcal{T}_\ell(\lambda, x)$ over $\mathbb{Q}(\lambda)$. A suitable twist of the Legendre curve has a point of order ℓ defined over $\mathcal{F}$ (and the full two torsion also). This proves that $\mathcal{F}$ contains the function field $\mathbb{Q}(\mathcal{X}_\ell)$. Comparison of the degrees of $\mathcal{F}/\mathbb{Q}(\lambda)$ and $\mathbb{Q}(\mathcal{X}_\ell)/\mathbb{Q}(\lambda)$ shows that the two fields $\mathcal{F}$ and $\mathbb{Q}(\mathcal{X}_\ell)$ are equal and the polynomial $\mathcal{T}_\ell$ is irreducible in $\bar{\mathbb{Q}}(\lambda)[x]$.

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 that $j^{-1} = 2^{-8}(\lambda^{-2} + \lambda^{-3} - 2\lambda^{-4} - 5\lambda^{-5} + \cdots)$.

We introduce Tate's q-parameter, defined implicitly by

$$j = \frac{1}{q} + 744 + 196884q + \cdots$$

so that

$$\begin{aligned} q &= j^{-1} + 744j^{-2} + 750420j^{-3} + \cdots \\ &= \frac{1}{256}\lambda^{-2} + \frac{1}{256}\lambda^{-3} + \frac{29}{8192}\lambda^{-4} + \frac{13}{4096}\lambda^{-5} + \cdots \end{aligned}$$

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 similarly

$$E_6 \left(\frac{dq}{q}\right)^3 = \frac{4(\lambda - 2)(\lambda + 1)(2\lambda - 1)(d\lambda)^3}{\lambda^3(1 - \lambda)^3}.$$

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 $1 \leq a \leq \frac{\ell-1}{2}$ or $1 \leq b \leq \frac{\ell-1}{2}$ and $0 \leq a \leq \ell - 1$ we set $w = \zeta_\ell^a q^{\frac{b}{\ell}}$ in the expansion

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

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 $1 \leq k \leq \frac{\ell-1}{2}$ 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 $\leq d_\ell$.

The coefficients in all the series expansions above are in $\mathbb{Z}[\frac{1}{6\ell}, \zeta_\ell, 2^{\frac{1}{\ell}}]$. The coefficients of $\mathcal{T}_\ell(\lambda, x)$ 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 $\mathcal{C}_\ell$. Let $C_\ell \subset \mathbb{P}^2$ be the projective plane curve made of the zeroes of the homogeneous polynomial $\mathcal{T}_\ell(\frac{\Lambda}{Y}, \frac{X}{Y})Y^{2d_\ell}$.

For every geometric point 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 geometric point on $\mathcal{X}_\ell$ 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

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

We call $\Sigma_\infty = [1, 0, 0]$ the unique singular point at infinity and for every $1 \leq b \leq \frac{\ell-1}{2}$ 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 local monodromy 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 $1 \leq \alpha_b \leq \ell - 1$ and $1 \leq \beta_b \leq \ell - 1$. 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 point $\sigma_{\infty,b}$) 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 [15, 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. The degree $\deg(\mathfrak{C}_\ell)$ of $\mathfrak{C}_\ell$ is $2m_\ell(2m_\ell^3 + 4m_\ell^2 - 2m_\ell - 1)$. So we set $\delta = m_\ell(2m_\ell^3 + 4m_\ell^2 - 2m_\ell - 1)$ and we check that $g_a = g_\ell + \delta$.

Now let $p \notin \{2, 3, \ell\}$ be a prime. Let $\mathbb{C}_p$ be the (complete, algebraically closed) 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 $\mathbb{Z}[\frac{1}{6\ell}, \zeta_\ell, 2^{\frac{1}{\ell}}]$. More precisely, the curves C_ℓ and $\mathcal{X}_\ell$ are defined over $\mathbb{Z}[\frac{1}{6\ell}]$. We write $C_\ell \bmod p = C_\ell/\mathbb{F}_p = C_\ell \otimes_{\mathbb{Z}[\frac{1}{6\ell}]} \mathbb{F}_p$ for the reduction of C_ℓ modulo p, and define similarly $\mathcal{X}_\ell \bmod p$. We write similarly $\sigma_{\infty,b} \bmod p$ and $\mu_{\infty,a} \bmod p$.

We deduce the following.

Lemma 18 (Computing C_ℓ and resolving its singularities) *There exists a deterministic algorithm that given a prime $\ell \ge 5$ 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.*

10 Another family 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. The genus of $\mathcal{X}_\ell$ is $g_\ell = \ell^2 - 4\ell + 4$. We first describe a homogeneous singular plane model C_ℓ for this curve. We then enumerate the geometric points on $\mathcal{X}_\ell$ above every singularity of C_ℓ and provide series expansions for affine coordinates at every such branch. Finally, for $p \notin \{2, 3, 5, \ell\}$ a prime integer, we recall how to compute the zeta function of the function field $\mathbb{F}_p(\mathcal{X}_\ell)$. All this will be useful in section 11 where we apply theorem 1 to the curve $\mathcal{X}_\ell$.

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 function on x-coordinates: $x \mapsto \frac{\mathcal{N}(x)}{\mathcal{M}(x)}$ where $\mathcal{N}(x)$ is a monic degree ℓ^2 polynomial in $\mathbb{Q}(b)[x]$. Recursion formulae for division polynomial (see [12] 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 $x - b$, accordingly. This is a monic polynomial in $\mathbb{Z}[b][x]$ with degree $\ell^2 - 1$ in x. As a polynomial in x we have

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

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

As in the previous section, we check that $\mathcal{T}_\ell$ is irreducible in $\bar{\mathbb{Q}}(b)[x]$ and $\mathbb{Q}(\mathcal{X}_\ell)$ is the splitting field of $\mathcal{T}_\ell$ over $\mathbb{Q}(b)$. Let $C_\ell \subset \mathbb{P}^2$ be the projective curve made of the zeroes of the homogeneous polynomial $\mathcal{T}_\ell(\frac{B}{Y}, \frac{X}{Y})Y^d$.

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 forgetful map $X_1(5\ell) \to X_1(5)$ is unramified except at $b \in \{0, \infty, s, \bar{s}\}$. For every point 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 points on $\mathcal{X}_\ell$ above points in $C_\ell - \mathcal{U}$ are cusps in the modular sense (i.e. the modular invariant at these points is infinite).

In order to desingularize C_ℓ at a given cusp, we shall construct an isomorphism between the Tate q-curve and the completion 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

$$\begin{aligned} q &= j^{-1} + 744j^{-2} + 750420j^{-3} + \cdots \\ &= b^{-5} + 25b^{-6} + \cdots \end{aligned}$$

and we fix an embedding of the local field at A_∞ inside the field of Puiseux series $\mathbb{C}\{\{q\}\}$ 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 [18, Theorem 10.1.6].

From the classical (see [28, Proposition 7.1]) identities

$$\left(\frac{qdj}{dq}\right)^2 = j(j-1728)E_4$$

$$\left(\frac{qdj}{dq}\right)^3 = -j^2(j-1728)E_6$$

we deduce

$$\left(\frac{qdb}{dq}\right)^2 = \frac{b^2(b^2 - 11b - 1)^2 E_4}{25(b^4 - 12b^3 + 14b^2 + 12b + 1)}$$

and

$$\left(\frac{qdb}{dq}\right)^3 = -\frac{b^3(b^2 - 11b - 1)^3 E_6}{125(b^2+1)(b^4 - 18b^3 + 74b^2 + 18b + 1)}.$$

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

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

we deduce that $w(P) = q^{\pm\frac{2}{5}} \mathrm{mod} < q >$. We may take either sign in the exponent because we may choose any of the two isomorphisms corresponding to either possible values for γ. We decide that $w(P) = q^{\frac{2}{5}} \mathrm{mod} < q >$. 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 (2) 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 local monodromy 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 the local monodromy group. 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 points on $\mathcal{X}_\ell$ above A_∞ and $\ell-1$ ramified points with ramification index ℓ.

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

Lemma 19 (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.*

In appendix A we give a few lines of GP-PARI code (see [1]) that compute these expansions.

We now study the singular points 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 (2) 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 proved the following.

Lemma 20 (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.*

In order to apply theorem 1 to the curve $\mathcal{X}_\ell$, we shall also need the following result due to Manin, Shokurov, Merel and Cremona [23, 25, 9, 13].

Lemma 21 (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 deterministic polynomial time 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 the Eichler-Shimura identity $T_p = F_p + p < p > /F_p$ we deduce the characteristic polynomial of the Frobenius F_p. □

In appendix B we give a few lines of Magma code (see [2]) that compute the zeta function of $X_1(5\ell)/\mathbb{F}_p$.

11 Computing the Ramanujan subspace over $\mathbb{F}_p$

This section explains the connection between the methods given here and Edixhoven's 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 $\mathbb{T} \subset \mathrm{End}(J_1(\ell)/\mathbb{Q})$ the algebra of endomorphisms of $J_1(\ell)$ generated by the Hecke operators T_n for all integers $n \geq 2$. Following Edixhoven [11, Definition 10.9] we state the

Definition 3 (The Ramanujan ideal) *Assume $\ell \geq 13$ is a prime. We denote by $\mathfrak{m}$ the maximal ideal in $\mathbb{T}$ 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 at ℓ and denoted V_ℓ.*

This V_ℓ is a 2-dimensional vector space over $\mathbb{F}_\ell$ and for $p \neq \ell$ 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 address the problem of computing $\mathfrak{m}$-torsion divisors on modular curves over some extension field $\mathbb{F}_q$ of $\mathbb{F}_p$ for $p \neq \ell$. 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 10 we have defined the modular curve $\mathcal{X}_\ell = X_1(5\ell)$ and the degree 24 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 5-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 the composite map $\phi_* \circ \phi^*$ is multiplication by 24 in $J_1(\ell)$. We write $\phi_* \circ \phi^* = [24]$. Thus the curve $\mathcal{X}_\ell$ provides a convenient computational model for the group of $\mathbb{F}_q$-points of the jacobian of $X_1(\ell)$.

We denote by $\mathcal{A}_\ell \subset \mathcal{J}_\ell$ the image of $\nu = \phi^* \circ \phi_*$. This is a subvariety of $\mathcal{J}_\ell$ isogenous to $J_1(\ell)$. The restriction of ν to $\mathcal{A}_\ell$ is multiplication by 24. 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 integer N which is prime to 6.

We call $W_\ell \subset \mathcal{A}_\ell \subset \mathcal{J}_\ell$ the image of the Ramanujan subspace by ϕ^*. We choose an integer k such that $24k$ is congruent to 1 modulo ℓ, and set $\hat{T}_n = [k] \circ \phi^* \circ T_n \circ \phi_*$, for every n. We 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 $J_1(\ell)[\ell]$ 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 at ℓ 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 following.

Lemma 22 (Computing the Hecke action) *Let ℓ and p be primes such that $p \notin \{2, 3, 5, \ell\}$. Let $n \geq 2$ be an integer. Let q be a power of p and let D be an effective $\mathbb{F}_q$-divisor of degree $\deg(D)$ on $\mathcal{X}_\ell \pmod p$. The divisors $\phi^* \circ \phi_*(D)$ and $\phi^* \circ T_n \circ \phi_*(D)$ can be computed in polynomial time in ℓ, $\deg(D)$, n and $\log q$.*

If n is prime to ℓ, we define the Hecke operator $T(n, n)$ as an element in the ring of correspondences on $X_1(\ell)$ tensored by $\mathbb{Q}$. See [21, VII, §2]. From [21, VII, §2, Theorem 2.1] we have $T_{\ell^i} = (T_\ell)^i$ and $T_{n^i} = T_{n^{i-1}} T_n - n T_{n^{i-2}} T(n, n)$ if n is prime and $n \neq \ell$. And of course $T_{n_1} T_{n_2} = T_{n_1 n_2}$ if n_1 and n_2 are coprime. So it suffices to explain how to compute T_ℓ and also T_n and $T(n, n)$ for n prime and $n \neq \ell$.

Let $x = (E, u)$ be a point on $Y_1(\ell) \subset X_1(\ell)$ representing an 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 $(E_I, I(u))$, where $I : E \to E_I$ runs over the set of all isogenies of degree n from E such that $I(u)$ still has order ℓ. If n is prime to ℓ, the Hecke operator $T(n, n)$ maps x onto $\frac{1}{n^2}$ times

(E, nu). So we can compute the action of these Hecke correspondences on points $x = (E, u)$ using Vélu's formulae [32].

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 $\mu_{\infty,\tilde{\alpha}}$. To every cusp one can associate a set of Tate curves with ℓ-torsion point (one Tate curve for every branch at this cusp).

For example the Tate curves at $\sigma_{\tilde{\beta}}$ are the Tate curves $\mathbb{C}^*/q$ with ℓ-torsion point $w = \zeta_\ell^* q^{\frac{\tilde{\beta}}{\ell}}$ where the star runs over the set of all residues modulo ℓ. There are ℓ branches at each such cusp.

Similarly, the Tate curves at $\mu_{\tilde{\alpha}}$ are the Tate curves $\mathbb{C}^*/q$ with ℓ-torsion point $w = \zeta_\ell^{\tilde{\alpha}}$. One single branch here: no ramification.

For n prime and $n \neq \ell$ 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 a class in $(\mathbb{Z}/\ell\mathbb{Z})^*/\{1, -1\}$.

Similarly

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

and

$$T_\ell(\mu_{\tilde{\alpha}}) = \ell\mu_{\tilde{\alpha}}.$$

And of course, if n is prime to ℓ, then $T(n, n)(\sigma_{\tilde{\beta}}) = \frac{1}{n^2}\sigma_{n\tilde{\beta}}$ and $T(n, n)(\mu_{\tilde{\alpha}}) = \frac{1}{n^2}\mu_{n\tilde{\alpha}}$.

All together, one can compute the effect of T_n on cusps for all n. For the sake of completeness, we also give the action of the diamond operator $<n>$ on cusps. If n is prime to ℓ then $<n>\ (\sigma_{\tilde{\beta}}) = \sigma_{n\tilde{\beta}}$ and $<n>\ (\mu_{\tilde{\alpha}}) = \mu_{n\tilde{\alpha}}$.

$\square$

We can now state the following.

Theorem 2 *There is a probabilistic (Las Vegas) algorithm that on input a prime $\ell \geq 13$ and a prime $p \geq 7$ such that $\ell \neq p$, 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 being the origin ω. The algorithm runs in probabilistic polynomial time in p and ℓ.*

Lemma 20 gives us a plane model for $\mathcal{X}_\ell \pmod{p}$ and a resolution of its singularities. From lemma 21 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. □

Remark 5 *In the above theorem, one may impose an origin ω rather than letting the algorithm choose it. For example, following work by Edixhoven in [11, Section 12], one may choose as origin a well designed linear combination of the cusps. Such an adapted choice of the origin may ensure that the ℓ^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.*

12 The semisimple non-scalar case

In this section we present a simplified algorithm for computing the Ramanujan subspace V_ℓ modulo p, that applies when the Frobenius action on it is semisimple and non-scalar or equivalently when $\tau(p)^2 - 4p^{11}$ is not divisible by ℓ. The main idea is to associate a divisible group with V_ℓ.

For every integer $n \geq 2$ we call $A_n(X) \in \mathbb{Z}[X]$ the characteristic polynomial of T_n acting on weight 2 modular forms for $\Gamma_1(\ell)$. We factor

$$A_n(X) = B_n(X)(X - \tau(n))^{e_n}$$

in $\mathbb{F}_\ell[X]$ with $B_n(X)$ monic and $B_n(\tau(n)) \neq 0 \in \mathbb{F}_\ell$. For every integer $k \geq 1$ this polynomial factorization lifts modulo ℓ^k as

$$A_n(X) = B_{n,k}(X)C_{n,k}(X) \pmod{\ell^k}.$$

We call $\Pi_k : J_1(\ell)[\ell^k] \to J_1(\ell)[\ell^k]$ the composite map of all $B_{n,k}(T_n)$ for all integers n such that $2 \leq n < \ell^2$. We observe that Π_{k+1} coincides with Π_k on $J_1(\ell)[\ell^k]$. So we have defined a map $\Pi : J_1(\ell)[\ell^\infty] \to J_1(\ell)[\ell^\infty]$.

We have the following.

Lemma 23 (The Ramanujan modules) *For $k \geq 1$ an integer, we denote by $\mathbb{G}_k$ the subgroup of $J_1(\ell)[\ell^k]$ consisting of elements killed by some power of $\mathfrak{m}$. Let $\mathbb{G}$ be the union of all $\mathbb{G}_k$. The group $\mathbb{G}_k$ is the image $\Pi_k(J_1(\ell)[\ell^k])$ of the ℓ^k-torsion by Π_k. It is killed by $\mathfrak{m}^{2kg(X_1(\ell))}$ and the restriction of Π_k to $\mathbb{G}_k$ is a bijection. Further $\mathbb{G}_{k+1}[\ell^k] = \mathbb{G}_k = \ell\mathbb{G}_{k+1}$. The $(\mathbb{Z}/\ell^k\mathbb{Z})$-module $\mathbb{G}_k$ is free. We call it the Ramanujan module.*

We show that for every integer $n \geq 2$, the restriction of $B_{n,k}(T_n)$ to $\mathbb{G}_k$ is a bijection. It suffices to show injectivity. Assume $B_{n,k}(T_n)$ restricted to $\mathbb{G}_k$ is not injective. There is a non-zero ℓ-torsion element P in its kernel. This P is killed by $(T_n - \tau(n))^m \pmod{\ell}$ for some integer m. It is also killed by $B_n(T_n) \pmod{\ell}$. Since these two polynomials are coprime, P is zero, contradiction.

So Π_k is an automorphism of $\mathbb{G}_k$. In particular $\mathbb{G}_k \subset \Pi_k(J_1(\ell)[\ell^k])$. We set $\mathbb{I}_k = \Pi_k(J_1(\ell)[\ell^k])$ and we prove the converse inclusion $\mathbb{I}_k \subset \mathbb{G}_k$. For every integer n between 2 and ℓ^2, the restriction of T_n to $\mathbb{I}_1$ is killed by $(X - \tau(n))^{e_n}$. Since the Hecke algebra is generated by these T_n and is commutative, its image in $\mathrm{End}(\mathbb{I}_1)$ is triangulisable [1] and consists of matrices with a single eigenvalue. We deduce that for every integer n the restriction of T_n to $\mathbb{I}_1$ has a single eigenvalue (namely $\tau(n) \pmod{\ell}$). Because the dimension of $\mathbb{I}_1$ as a $\mathbb{F}_\ell$-vector space is $\leq 2g(X_1(\ell))$ we deduce that $\mathbb{I}_1$ is killed by $\mathfrak{m}^{2g(X_1(\ell))}$. So $\mathbb{I}_1 = \mathbb{G}_1$ is killed by $\mathfrak{m}^{2g(X_1(\ell))}$.

For every integer n between 2 and ℓ^2, the restriction of T_n to $\mathbb{I}_k[\ell]$ is killed by $C_{n,k}(X)$ which is congruent to $(X - \tau(n))^{e_n}$ modulo ℓ. So $\mathbb{I}_k[\ell]$ is killed by $(T_n - \tau(n))^{e_n}$ and by $\mathfrak{m}^{2g(X_1(\ell))}$. So any morphism in $\mathfrak{m}^{2kg(X_1(\ell))}$ kills $\mathbb{I}_k[\ell^k] = \mathbb{I}_k$. So $\mathbb{I}_k$ is killed by $\mathfrak{m}^{2kg(X_1(\ell))}$ and $\mathbb{I}_k = \mathbb{G}_k$.

It is clear that $\ell\mathbb{G}_{k+1} \subset \mathbb{G}_k$. Conversely if $P = \Pi_k(Q)$ and Q is ℓ^k-torsion then let R such that $\ell R = Q$ and $S = \Pi_{k+1}(R)$. Then S is in $\mathbb{I}_{k+1} = \mathbb{G}_{k+1}$ and $\ell S = \Pi_{k+1}(Q) = \Pi_k(Q) = P$. So $\ell\mathbb{G}_{k+1} = \mathbb{G}_k$. From $\mathbb{G}_{k+1}[\ell^k] = \ell\mathbb{G}_{k+1}$ we deduce that $\mathbb{G}_{k+1}$ is a free $(\mathbb{Z}/\ell^{k+1}\mathbb{Z})$-module. □

We now study the Galois action on this divisible group. Let $p \neq \ell$ be a prime. We regard $J_1(\ell)$ as a variety over the finite field $\mathbb{F}_p$. The Ramanujan module $\mathbb{G} = J_1(\ell)[\mathfrak{m}^\infty]$ is then an ℓ-divisible group inside $J_1(\ell)[\ell^\infty]$ in the sense of definition 13. According to the Eichler-Shimura identity $F_p^2 - T_pF_p + p < p >= 0$. The diamond operator $<p>\in \mathbb{T}$ has a unique eigenvalue on $\mathbb{G}_1$, namely $p^{10} \pmod{\ell}$. Since F_p commutes with $\mathbb{T}$, the algebra generated by $\mathbb{T}$ and F_p is triangulisable[1] in $\mathrm{GL}(\mathbb{G}_1 \otimes_{\mathbb{F}_\ell} \bar{\mathbb{F}}_\ell)$. So any eigenvalue of F_p on $\mathbb{G}_1$ is killed by $X^2 - \tau(p)X + p^{11} \pmod{\ell}$. Let η be an integer that kills the roots of the polynomial $X^2 - \tau(p)X + p^{11} \pmod{\ell}$ in $\bar{\mathbb{F}}_\ell^*$. For example one may take $\eta = \ell^2 - 1$. As an endomorphism of $\mathbb{G}_1$ one has $F_p^\eta = \mathrm{Id} + n$ where n is nilpotent. Since the dimension of $\mathbb{G}_1$ is $\leq 2g(X_1(\ell)) \leq \ell^2$ one has $n^{\ell^2} = 0$ and $F_p^{\eta\ell^2} = \mathrm{Id}$. So $\mathbb{G}_1$ splits completely over $\mathbb{F}_{p^{\ell^2(\ell^2-1)}}$. As a consequence, $\mathbb{G}_k$ splits completely over the extension of degree $(\ell^2 - 1)\ell^{k+1}$ of $\mathbb{F}_p$.

Lemma 24 (Galois action on the Ramanujan module) *If $p \neq \ell$ is a prime, then the Ramanujan module $\mathbb{G} = J_1(\ell)[\mathfrak{m}^\infty]$ is a divisible group inside $J_1(\ell)[\ell^\infty](\bar{\mathbb{F}}_p)$. Let η be an integer that kills the roots of $X^2 - \tau(p)X + p^{11}$ in $\bar{\mathbb{F}}_\ell^*$. For example $\eta = \ell^2 - 1$. The ℓ^k-torsion $\mathbb{G}_k = \mathbb{G}[\ell^k]$ inside $\mathbb{G}$ splits completely over the extension of degree $\eta\ell^{k+1}$ of $\mathbb{F}_p$.*

For computational convenience we may prefer $\mathcal{X}_\ell = X_1(5\ell)$ to $X_1(\ell)$. If this is the case, we embed $\mathbb{G}$ inside the jacobian $\mathcal{J}_\ell$ of $\mathcal{X}_\ell$ using the map ϕ^*. For the sake of simplicity we present the calculations below in the context of $J_1(\ell)$ although they take place inside $\mathcal{J}_\ell$.

The knowledge of a non-zero element in $\mathbb{G}_k$ sometimes suffices to construct a basis of $V_\ell(\bar{\mathbb{F}}_p)$:

Lemma 25 (The inert case) *Assume $X^2 - \tau(p)X + p^{11} \pmod{\ell}$ is irreducible. Let $k \geq 1$ be an integer and $q = p^d$ a power of p. Given a non zero element in $\mathbb{G}_k(\mathbb{F}_q)$, one can compute a basis of $V_\ell(\bar{\mathbb{F}}_p)$ in polynomial time in $\log q$, ℓ and k.*

Indeed, let $P \in \mathbb{G}_k(\mathbb{F}_q)$ be non-zero. We replace P by ℓP until we find a non-zero element in $\mathbb{G}_1(\mathbb{F}_q)$. Given such a P we can test whether it belongs to V_ℓ by computing $(T_n - \tau(n))x$ for all $2 \leq n \leq \ell^2$. If we only obtain zeroes this shows P is in V_ℓ. Otherwise we replace P by

[1] If K is a field and V a K-vector space, we write $\mathcal{L}(V)$ for the algebra of linear maps from V to itself. Let A be a subset of $\mathcal{L}(V)$. We say that A is triangulisable if there exists a basis $\mathcal{B}$ of V such that the matrix of every element in A with respect to $\mathcal{B}$ is upper triangular.

some non-zero $(T_n - \tau(n))P$ and test again. This process stops after $2g(X_1(\ell))$ steps at most, and produces a non-zero element P in $V_\ell(\mathbb{F}_q)$. Since F_p has no eigenvector in $V_\ell(\bar{\mathbb{F}}_p)$, the couple $(P, F_p(P))$ is a basis of $V_\ell(\bar{\mathbb{F}}_p)$. $\square$

So assuming that $\tau(p)^2 - 4p^{11}$ is not a square modulo ℓ, we have a simpler method to construct a basis for the Ramanujan module V_ℓ modulo p:

We set $q = p^{(\ell^2-1)\ell^3}$. We have $\mathbb{G}(\mathbb{F}_q) \supset \mathbb{G}_2 = \mathbb{G}_2(\mathbb{F}_q)$. Set $N_q = \#J_1(\ell)(\mathbb{F}_q) = M_q L_q$ where M_q is prime to ℓ. This N_q can be computed using Manin symbols as in lemma 21. Let $L_q = \ell^w$. The image of $J_1(\ell)(\mathbb{F}_q)$ by the morphism $\psi = \Pi_w \circ [M_q]$ contains $\mathbb{G}_2(\mathbb{F}_q)$ and is in fact equal to $\mathbb{G}(\mathbb{F}_q)$. We check $\#\mathbb{G}(\mathbb{F}_q) \geq \#\mathbb{G}_2 \geq \ell^4$. So at least one of the elements in $J_1(\ell)(\mathbb{F}_q)$ given by lemma 9 has a non-zero image by ψ for ℓ large enough. We apply lemma 25 to this element and find a basis for the Ramanujan module at ℓ.

We now assume the polynomial $X^2 - \tau(p)X + p^{11} \bmod \ell$ has two distinct roots $a \bmod \ell$ and $b \bmod \ell$. So $(F_p - a)^{2g(X_1(\ell))}(F_p - b)^{2g(X_1(\ell))}$ kills $\mathbb{G}_1$. Since $\mathbb{G}_1 = \mathbb{G}_k[\ell]$ we deduce that $(F_p - a)^{2kg(X_1(\ell))}(F_p - b)^{2kg(X_1(\ell))}$ kills $\mathbb{G}_k$.

This leads us to the following definition.

Definition 4 (Split Ramanujan modules) *Assume $X^2 - \tau(p)X + p^{11} \bmod \ell$ has two distinct roots $a \bmod \ell$ and $b \bmod \ell$ where a and b are integers. Let $\mathfrak{m}_a$ be the ideal in $\mathbb{T}[F_p]$ generated by ℓ, all $T_n - \tau(n)$ and $F_p - a$. Let $V_{\ell,a} = J_1(\ell)[\mathfrak{m}_a] \subset V_\ell$ be the eigenspace associated with a. For $k \geq 1$ an integer, we denote by $\mathbb{G}_{k,a}$ the subgroup of $J_1(\ell)[\ell^k]$ consisting of elements killed by some power of $\mathfrak{m}_a$. Let $\Pi_{k,a}$ the composition of Π_k and $(F_p - b)^{2kg(X_1(\ell))}$. We denote by $\mathbb{G}_a$ the union of all $\mathbb{G}_{k,a}$.*

We have the following.

Lemma 26 (Properties of split Ramanujan modules) *For every integer $k \geq 1$, the group $\mathbb{G}_{k,a}$ is the image $\Pi_{k,a}(J_1(\ell)[\ell^k])$ of the ℓ^k-torsion by $\Pi_{k,a}$. It is killed by $\mathfrak{m}_a^{2kg(X_1(\ell))}$ and the restriction of $\Pi_{k,a}$ to $\mathbb{G}_{k,a}$ is a bijection. So $\mathbb{G}_a = J_1(\ell)[\mathfrak{m}_a^\infty] \subset \mathbb{G}$ is a divisible group. Let η be an integer that kills a in $\mathbb{F}_\ell^*$ (e.g. $\eta = \ell - 1$). Then $\mathbb{G}_{k,a}$ splits over $\mathbb{F}_{p^{\eta\ell^{k+1}}}$.*

The lemma below is the counterpart to lemma 25 in the split non-scalar case.

Lemma 27 (The split non-scalar case) *Assume $X^2 - \tau(p)X + p^{11} \pmod{\ell}$ has two distinct roots $a \pmod{\ell}$ and $b \pmod{\ell}$. Let $k \geq 1$ be an integer and $q = p^d$ a power of p. Given a non zero element in $\mathbb{G}_{k,a}(\mathbb{F}_q)$, one can compute a generator of $V_{\ell,a}$ in polynomial time in $\log q$, ℓ and k.*

So if $\tau(p)^2 - 4p^{11}$ is a non-zero square modulo ℓ we also have a simple method to construct a basis for the Ramanujan module V_ℓ modulo p:

We let $a \pmod{\ell}$ and $b \pmod{\ell}$ be the two roots of $X^2 - \tau(p)X + p^{11} \pmod{\ell}$. Take $q = p^{(\ell-1)\ell^4}$. We have $\mathbb{G}_a(\mathbb{F}_q) \supset \mathbb{G}_{3,a} = \mathbb{G}_{3,a}(\mathbb{F}_q)$ we set $N_q = \#J_1(\ell)(\mathbb{F}_q) = M_q L_q$ with M_q prime to ℓ. Let $L_q = \ell^w$ and $\psi = \Pi_{w,a} \circ [M_q]$. The image of $J_1(\ell)(\mathbb{F}_q)$ by ψ contains $\mathbb{G}_{3,a}(\mathbb{F}_q)$ and is in fact equal to $\mathbb{G}_a(\mathbb{F}_q)$. We check $\#\mathbb{G}_a(\mathbb{F}_q) \geq \#\mathbb{G}_{3,a} \geq \ell^3$. So at least one of the elements in $J_1(\ell)(\mathbb{F}_q)$ given by lemma 9 has a non-zero image by ψ for ℓ large enough. We apply lemma 27 to this element and find a generator of $V_{\ell,a}$. A similar calculation produces a generator of $V_{\ell,b}$. These two eigenvectors form a basis of V_ℓ modulo p.

All this is enough to compute the Ramanujan ideal when the Frobenius action on it is semisimple non-scalar i.e when ℓ is prime to $\tau(p)^2 - 4p^{11}$.

Remark 6 *The main simplification in this variant is that we do not need to compute pairings. In practice, one would just take a random degree zero $\mathbb{F}_q$-divisor on $X_1(\ell)$, multiply it by the prime to ℓ part of $\#J_1(\ell)(\mathbb{F}_q)$ and apply a few $B_{n,k}(T_n)$ to it. This should usually suffice.*

Remark 7 *If ℓ divides $\tau(p)^2 - 4p^{11}$, the method described in this section is no longer sufficient but one can easily show that it provides at least one non-zero element in V_ℓ modulo p.*

13 Computing the Ramanujan subspace over $\mathbb{Q}$

Once one has computed the Ramanujan space V_ℓ inside $J_1(\ell)$ (or rather W_ℓ inside $\mathcal{J}_\ell$ the jacobian of $\mathcal{X}_\ell$) modulo p for many small primes p, one can try to compute this space over the rationals. This calculation is described in detail in [11, Section 13]. In this section we sketch a variant of the method presented in [11, Section 13]. We then explain how this method should be modified to fit with the simplified method presented in section 12. This leads us to a sort of generalization of the Chinese Remainder Theorem that is more adapted to the context of polynomials with integer coefficients.

The complexity analysis of the methods presented in this section rely on results in Arakelov theory that have been proven by Bas Edixhoven and Robin de Jong, using results by Merkl in [11] or J. Jorgenson and J. Kramer in [19]. In fact, the complexity analysis of the variant described here requires a bit more than what has been already given in [11]. The necessary bounds to the proof of this variant will appear in Peter Bruin's PhD thesis [4].

We use the model over $\mathbb{Z}[\frac{1}{30\ell}]$ for $\mathcal{X}_\ell = X_1(5\ell)$ that is described in section 10. We start by fixing a $\mathbb{Q}$-rational cusp O on $\mathcal{X}_\ell$. This will be the origin of the Jacobi map.

Let x be a point in $\mathcal{J}_\ell(\bar{\mathbb{Q}})$. We denote by $\theta(x)$ the smallest integer k such that there exists an effective divisor D of degree k such that $D - kO$ belongs to the class represented by x in the Picard group. We call $\theta(x)$ the *stability* of x. For all but finitely many primes p and for any place $\mathfrak{p}$ of $\mathbb{Q}(x)$ above p, one can define $\theta_{\mathfrak{p}}(x)$ the stability of x modulo $\mathfrak{p}$: the smallest integer k such that there exists an effective divisor D of degree k such that $D - kO$ belongs to the class represented by $x \bmod \mathfrak{p}$ in the Picard group of $\mathcal{X}_\ell \bmod p$. We define $\theta_p(x)$ to be the minimum of all $\theta_{\mathfrak{p}}(x)$ for all places $\mathfrak{p}$ above p. We note that $\theta_p(x) \le \theta_{\mathfrak{p}}(x) \le \theta(x)$ whenever $\theta_p(x)$ is defined. Clearly $\theta_p(x)$ is defined and equal to $\theta(x)$ for all large enough primes.

A consequence of the results by Bas Edixhoven and Robin de Jong, extended by Peter Bruin in his forthcoming PhD thesis, see [11, 4], is that, for at least half the primes smaller than $\ell^{\mathcal{O}}$, the following holds: $\theta_p(x)$ is defined and equal to $\theta(x)$ for all x in W_ℓ. Notice that $\theta(x) = \theta(y)$ if x and y are Galois conjugate.

Now let x be a non-zero point in W_ℓ. We can compute x modulo places $\mathfrak{p}$ above p, for many small (e.g. polynomial in ℓ) primes p such that $\theta_p(x) = \theta(x)$. We only use primes such that $\theta_p(x) = \theta(x)$ for every x in W_ℓ.

There is a unique effective divisor $D = P_1 + \cdots + P_{\theta(x)}$ such that $D - \theta(x)O$ is mapped onto x by the Jacobi map. This divisor remains unique modulo all the places $\mathfrak{p}$ in question. Further, no P_i specializes to O modulo any such $\mathfrak{p}$. So we choose a function f on $\mathcal{X}_\ell$ having no pole except at O. We define e.g. $F(x) = f(P_1) + \cdots + f(P_{\theta(x)})$.

We form the polynomial

$$P_k(X) = \prod_{y \in W_\ell \text{ with } \theta(y)=k} (X - F(y)).$$

This polynomial has coefficients in $\mathbb{Q}$. For the above primes p we have

$$P_k(X) \bmod p = \prod_{y \in W_\ell \bmod p \text{ with } \theta_p(y)=k} (X - F(y)).$$

We set $P(X) = \prod_{k>0} P_k(X)$. If the Galois action on $W_\ell - \{0\}$ is transitive then $P(X)$ is likely to be irreducible and equal to the unique non-trivial $P_k(X)$. To be quite rigorous one should say some more about the choice of f. See [11, Section 22].

If a reasonable f (e.g. the divisor of f is $n(O - O')$ where O' is another rational cusp and n is the order of $O - O'$ in the jacobian) is chosen then Peter Bruin, improving on Edixhoven, de Jong, and Merkl, proves in [4] that the logarithmic height of $P(X)$ is bounded by a polynomial in ℓ.

If we know W_ℓ modulo p then we can compute $P(X)$ modulo p and, provided we have taken enough such primes p, we deduce $P(X)$ using Chinese remainder theorem and the bounds proved by Edixhoven, de Jong, Merkl and Bruin.

However, if we use the simplified algorithm presented in section 12 we shall only obtain $P(X)$ modulo p for those p such that ℓ does not divide $\tau(p)^2 - 4p^{11}$. If ℓ divides $\tau(p)^2 - 4p^{11}$ then we may only obtain a non-trivial factor of $P(X) \bmod p$. This factor has degree $\ell - 1$ in fact.

This leads us to the following problem:

Let $P(X)$ be a degree $d \geq 2$ *irreducible*[2] polynomial with integer coefficients.

Let H be an upper bound for the *naive height* of $P(X)$: any coefficient of P lies in $[-H, H]$.

Let I be a positive integer and for every integer i from 1 to I assume we are given an integer $N_i \geq 2$ and a degree a_i *monic* polynomial $A_i(X)$ in $\mathbb{Z}[X]$ where $1 \leq a_i \leq d$. Assume the N_i are pairwise coprime.

Question: assuming $P(X) \bmod N_i$ is a multiple of $A_i(X) \bmod N_i$ for every i, can we recover $P(X)$, and is $P(X)$ the unique polynomial fulfilling all these conditions ?

We start with the following.

Lemma 28 (Resultant and intersections) *Let P and Q be two non-constant polynomials with integer coefficients and trivial gcd*[3]*. Let $N \geq 2$ be an integer. If $P \bmod N$ and $Q \bmod N$ are*

[2] irreducible means here irreducible in the ring $\mathbb{Z}[X]$.

[3] the gcd here is the gcd in the ring $\mathbb{Z}[X]$.

both multiples of the same degree $d \geq 1$ monic polynomial $A \bmod N$, then the resultant of P and Q is divisible by N^d.

This easily follows from the resultant being given as a determinant. $\square$

Let $\mathcal{P}_d$ be the additive group of integer coefficient polynomials with degree $\leq d$. Let $\rho_i : \mathcal{P}_d \to \mathbb{Z}[X]/(A_i, N_i)$ be the reduction map modulo the ideal (A_i, N_i).

The product map

$$\rho = \prod_{1\leq i\leq I} \rho_i : \mathcal{P}_d \to \prod_{1\leq i\leq I} \mathbb{Z}[X]/(A_i, N_i)$$

is surjective (Chinese remainder). Its kernel is therefore a lattice $\mathcal{R}$ with index $\Theta = \prod_{1\leq i\leq I} N_i^{a_i}$ in $\mathcal{P}_d = \mathbb{Z}^{d+1}$.

If P_1 and P_2 are two coprime non-constant polynomials with degree $\leq d$ and respective naive heights K_1 and K_2, then their resultant is bounded above by $(2d)!K_1^dK_2^d$. If further $P_1, P_2 \in \mathcal{R}$ then, according to lemma 28, $\Theta = \prod_{1\leq i\leq I} N_i^{a_i}$ divides the resultant of P_1 and P_2.

Lemma 29 (Heights and intersections) *Let $(N_i)_{1\leq i\leq I}$ be pairwise coprime integers. Let P be an irreducible polynomial with integer coefficients and degree $d \geq 2$ and naive height bounded by H. Let Q be a polynomial with integer coefficients and degree $\leq d$ and naive height bounded by K. Assume that for every i from 1 to N the polynomials $P \bmod N_i$ and $Q \bmod N_i$ are multiples of the same monic polynomial $A_i(X) \bmod N_i$ with degree a_i where $1 \leq a_i \leq d$. Assume further that*

$$\prod_{1\leq i\leq I} N_i^{a_i} > (2d)!H^dK^d.$$

Then Q is a multiple of P.

We observe that the L^2 norm of P is $\leq H\sqrt{d+1}$. Also, if Q has L^2 norm $\leq H\sqrt{d+1}$ then its coefficients are $\leq H\sqrt{d+1}$. Therefore if

$$\Theta = \prod_{1\leq i\leq I} N_i^{a_i} > (2d)!(d+1)^{\frac{d}{2}}H^{2d}$$

the polynomial P is the shortest vector in the lattice $\mathcal{R}$ for the L^2 norm.

Applying the LLL algorithm to the lattice $\mathcal{R}$ we find ([6, Theorem 2.6.2]) a vector in it with L^2 norm $\leq 2^{\frac{d}{4}}\Theta^{\frac{1}{d+1}}$. Taking this latter value for K we see that if

$$\prod_i N_i^{a_i} > (2d)!^{d+1}H^{d(d+1)}2^{\frac{d^2(d+1)}{4}}$$

then the vector output by the LLL algorithm is a multiple of P.

Lemma 30 (Interpolation and lattices) *Let $d \geq 2$ be an integer. Let I be a positive integer and for every i from 1 to I let $N_i \geq 2$ be an integer and $A_i(X)$ a monic polynomial with integer* *coefficients and degree a_i where $1 \leq a_i \leq d$. We assume the coefficients in $A_i(X)$ lie in the interval $[0, N_i[$.*

We assume there exists an irreducible polynomial $P(X)$ with degree d and integer coefficients and naive height $\leq H$ such that $P(X) \bmod N_i$ is a multiple of $A_i(X) \bmod N_i$ for all i.

We assume the N_i are pairwise coprime and

$$\prod_{1\leq i\leq I} N_i^{a_i} > (2d)!^{d+1} H^{d(d+1)} 2^{\frac{d^2(d+1)}{4}}.$$

Then $P(X)$ is the unique polynomial fulfilling all these conditions and it can be computed from the $(N_i, A_i(X))$ by a deterministic Turing machine in time polynomial in d, $\log H$ and I, and the $\log N_i$.

Note that the dependency on I and $\log N_i$ is harmless because one may remove some information if there is too much of it. We can always do with some I and $\log N_i$ that are polynomial in d and $\log H$.

This lemma shows that we can compute (lift) the Ramanujan module W_ℓ using the simplified algorithm of section 12, even if the action of the Frobenius at p on W_ℓ is not semisimple for any auxiliary prime p.

14 Are there many semi simple pairs (ℓ, p) ?

We have seen in section 12 that the computation of V_ℓ modulo p becomes simpler whenever the two primes p and ℓ satisfy the condition that ℓ is prime to $\tau(p)^2 - 4p^{11}$. If this is the case, we say that the pair (ℓ, p) is good (otherwise it is bad).

In the situation of section 13 we are given a fixed prime ℓ and we look for primes p such that (ℓ, p) is good. We need these primes p to be bounded by a polynomial in ℓ. And there should be enough of them that we can find them by random search.

This leads us to the following definition.

Definition 5 (What bad and good means in this section) *We say that a pair (ℓ, p) of prime integers is bad if ℓ divides $\tau(p)^2 - 4p^{11}$. Otherwise it is good. Let $c > 1$ be a real. We say that a given prime ℓ is c-bad if (ℓ, p) is bad for at least half the primes $p \leq \ell^c$. Otherwise it is c-good.*

In this section we give an elementary unconditional proof that there are enough good primes ℓ. Let α, β, γ and δ be four positive constants such that for every integer $k \geq 2$ the k-th prime p_k satisfies $\alpha k \log k \leq p_k \leq \beta k \log k$ and for every real $x \geq 2$ the arithmetic function $\pi(x)$ giving the number of primes $\leq x$ satisfies $\gamma x(\log x)^{-1} \leq \pi(x) \leq \delta x(\log x)^{-1}$.

Work by Tchebitchef allows $\gamma = \frac{1}{3}$ and $\delta = \frac{5}{4}$. Work by Rosser [27] shows that $\alpha = 1$ is fine. Rosser also proved that $p_k \leq k(\log k + \log\log k)$ for $k \geq 6$. So we can take $\beta = 2.17$ for example. I thank Guillaume Hanrot for pointing out these references to me.

Let $X \geq 3$ be an integer. Let L be the X-th prime integer. Let $\mathcal{X}(c, X)$ be the set of pairs of primes (ℓ, p) with $\ell \leq L$ and $p \leq \ell^c$. We set $\ell_1 = p_1 = 2$, $\ell_2 = p_2 = 3$, ... the successive prime integers. Let P be the largest prime $\leq L^c$ and let Y be the integer such that $P = p_Y$. One has $L \leq \beta X \log X$ and $P \leq \beta^c X^c (\log X)^c$ and $Y \leq P$.

Since $\tau(p)^2 - 4p^{11}$ has at most $\log_2(4p^{11})$ prime divisors, there are at most $Y(2 + 11\log_2 P)$ bad pairs and this is $\leq 51c\beta^c X^c (\log X)^{c+1}$ provided $X \geq \beta$. We want to bound from above the number of bad $\ell \leq L$. The worst case is when the smallest ℓ are bad. Assume all primes $\ell \leq \ell_x$ are bad. The number of bad pairs is then at least

$$\frac{1}{2}\sum_{1\leq k\leq x} \pi(\ell_k^c) \geq \frac{\gamma\alpha^c}{2} \sum_{\frac{3}{\alpha}\leq k\leq x} \frac{k^c(\log k)^c}{c\log\alpha + c\log k + c\log\log k} \geq \frac{\gamma\alpha^c}{4c} \sum_{\frac{3}{\alpha}\leq k\leq x} k^c(\log k)^{c-1}$$

and this is at least

$$\frac{\gamma\alpha^c}{4c(c+1)}\left(x^{c+1} - \left(\frac{3}{\alpha}\right)^{c+1}\right) \geq \frac{\gamma\alpha^c}{8c(c+1)} x^{c+1}$$

provided $x \geq 6/\alpha$. Assume at least half of the primes $\ell \leq L$ are bad. Then the number of bad pairs is at least $\frac{\gamma\alpha^c}{8c(c+1)}(X/2)^{c+1}$ provided $X \geq 12/\alpha$. So

$$\frac{\gamma\alpha^c}{8c(c+1)}(X/2)^{c+1} \leq 51c\beta^c X^c (\log X)^{c+1}$$

so

$$\frac{X}{(\log X)^{c+1}} \leq 816\left(\frac{2\beta}{\alpha}\right)^c c^2(c+1)\gamma^{-1}.$$

We call a the right-hand side in the above inequality. We set $Z = X^{\frac{1}{c+1}}$ and we have $\frac{Z}{\log Z} \leq (c+1)a^{\frac{1}{c+1}}$. Since $\log Z \leq \sqrt{Z}$ we have $Z \leq (c+1)^2 a^{\frac{2}{c+1}}$ and $X \leq (c+1)^{2(c+1)}a^2$.

Lemma 31 *Let α, β, γ and δ be the four constants introduced before definition 5 above. Let $c > 1$ be a real number. Assume X is an integer bigger than $816^2 c^4 (c+1)^{2(c+2)} \left(\frac{2\beta}{\alpha}\right)^{2c} \gamma^{-2}$. Then at least half among the X first primes are c-good.*

Lemma 32 (Effective bound for the density of good primes ℓ) *Let $c > 1$ be a real number. Assume X is an integer bigger than $2^{23+5c}c^4(c+1)^{2(c+2)}$. Then at least half among the X first primes are c-good.*

A A GP-PARI code for Puiseux expansions at singular branches of modular curves

Below are a few lines of GP-PARI code (see [1]) that compute the expansions of $x_{\alpha,\beta}$ as series in $b^{-\frac{1}{\ell}}$ with coefficients in a finite field containing a primitive ℓ-th root of unity. We use the methods and notation given in section 10, before the statement of lemma 19.

Our code computes the q-series for the modular function j as

$$j(q) = 1728 E_4^3(q)(E_4^3(q) - E_6^2(q))^{-1}$$

where

$$E_4(q) = 1 + 240 \sum_{n \geq 1} \frac{n^3 q^n}{1 - q^n}$$

and

$$E_6(q) = 1 - 504 \sum_{n \geq 1} \frac{n^5 q^n}{1 - q^n}.$$

The expansions for the $x_{\alpha,\beta}$ are then obtained through standard operations on series like product, sum, reversion, composition.

```
{ser(aa,bb,prec,ell,p,z,b,jc,E4,E6,D,jq,qc,gc,w,x)=
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);
}
```

B A Magma code that computes the zeta function of modular curves

Below are a few lines written in the Magma language (see [2]). They compute the characteristic polynomial of the Frobenius of $X_1(5\ell)/\mathbb{F}_p$ using the methods given in the proof of lemma 21.

```
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);
```

References

[1] Christian Batut, Karim Belabas, Dominique Bernardi, Henri Cohen, and Michel Olivier. *User's guide to PARI/GP (version 2.3.1)*. http://pari.math.u-bordeaux.fr.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[3] Johan Bosman. On the computation of Galois representations associated to level one modular forms. *arXiv:0710.1237v1*, 2007.

[4] Peter Bruin. *Doctoral dissertation*. University of Leiden, in preparation.

[5] Eduardo Casas-Alvero. *Singularities of plane curves*. Number 276 in London Mathematical Society Lecture Note Series. Cambridge University Press, 2000.

[6] Henri Cohen. *A course in computational algebraic number theory, 3rd printing*. Number 138 in Graduate Texts in Mathematics. Springer, 1996.

[7] Jean-Marc Couveignes. Boundary of Hurwitz spaces and explicit patching. *J. of Symbolic Computation*, 30:739–759, 2000.

[8] Jean-Marc Couveignes. Jacobien, jacobiennes et stabilité numérique. *Séminaire et Congrès*, 13:91–125, 2006.

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

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

[11] Sebastiaan Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, and Johan Bosman. On the computation of coefficients of a modular form. *arXiv:math/0605244v1*, 2006.

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

[13] 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.

[14] 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.

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

[16] 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.

[17] G. Havas, B.S. Majewski, and K.R. Matthews. Extended gcd and Hermite normal form algorithms via lattice basis reduction. *Experimental Mathematics*, 7:125–136, 1998.

[18] Dale Husemoller. *Elliptic Curves*. Springer, 1987.

[19] J. Jorgenson and J. Kramer. Bounds on canonical Green's functions. *Compos. Math.*, 142(3):679–700, 2006.

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

[21] Serge Lang. *Introduction to modular forms*. Springer-Verlag, 1976.

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

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

[24] 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.

[25] 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.

[26] V. Müller, A. Stein, and C. Thiel. Computing discrete logarithms in real quadratic function fields of large genus. *Math. Comp.*, 68:807–822, 1999.

[27] J. Barkley Rosser. The n-th prime is greater than $n \log n$. *Proc. London Math. Soc.*, 45:21–44, 1939.

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

[29] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Hermann, 1959.

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

[31] Wilberd van der Kallen. Complexity of the Havas, Majewski, Matthews LLL Hermite normal form algorithm. *arXiv:math/9812130v1*, 2008.

[32] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie de Sciences de Paris, Série A*, 273:238–241, 1971.

[33] 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.