HAL
open science

Computing modular Galois representations

Nicolas Mascot

To cite this version:

Nicolas Mascot. Computing modular Galois representations. Rendiconti del Circolo Matematico di Palermo, 2013, 62 (3), pp.451 - 476. 10.1007/s12215-013-0136-4 . hal-01110451

HAL Id: hal-01110451

https://hal.science/hal-01110451v1

Submitted on 28 Jan 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Computing modular Galois representations

Nicolas Mascot*

nmascot@math.u-bordeaux1.fr

October 2, 2013

Abstract

We present an algorithm to compute modular Galois representations attached to a newform f, and study the related problem of computing the coefficients of f modulo a small prime ℓ. To this end, we design a practical variant of the complex approximations method presented in [EC11]. Its efficiency stems from several new ingredients. For instance, we use fast exponentiation in the modular jacobian instead of analytic continuation, which greatly reduces the need to compute abelian integrals, since most of the computation handles divisors. Also, we introduce an efficient way to compute arithmetically well-behaved functions on jacobians, a method to expand cuspforms in quasi-linear time, and a trick making the computation of the image of a Frobenius element by a modular Galois representation more effective. We illustrate our method on the newforms Δ and $E_4 \cdot \Delta$, and manage to compute for the first time the associated faithful representations modulo ℓ and the values modulo ℓ of Ramanujan's τ function at huge primes for $\ell \in \{11, 13, 17, 19, 29\}$. In particular, we get rid of the sign ambiguity stemming from the use of a projective representation as in [Bos07]. As a consequence, we can compute the values of $\tau(p) \bmod 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 691 \approx 2.8 \cdot 10^{19}$ for huge primes p. The representations we computed lie in the jacobian of modular curves of genus up to 22.

*IMB, Université Bordeaux 1, UMR 5251, F-33400 Talence, France. CNRS, IMB, UMR 5251, F-33400 Talence, France. INRIA, project LFANT, F-33400 Talence, France.

Acknowledgements

I would like to heartily thank my advisor J.-M. Couveignes for offering me this beautiful subject to work on. More generally, I would like to thank people from the Bordeaux 1 university's IMB for their support, with special thoughts to B. Allombert, K. Belabas, H. Cohen and A. Enge, as well as the PlaFRIM team. Finally, I thank B. Edixhoven for his remarks on earlier versions of this article, A. Page for helping me to make explicit the similarity classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$, J. Klüners for his interest and assistance in formally proving that the polynomials I computed have the expected Galois group, and T. Selig for proofreading my English.

This research was supported by the French ANR-12-BS01-0010-01 through the project PEACE, and by the DGA maîtrise de l'information. Experiments presented in this paper were carried out using the PlaFRIM experimental testbed, being developed under the Inria PlaFRIM development action with support from LABRI and IMB and other entities: Conseil Régional d'Aquitaine, FeDER, Université de Bordeaux and CNRS (see https://plafrim.bordeaux.inria.fr/).

1 Introduction

Consider a non-CM newform $f = q + \sum_{n \geqslant 2} a_n q^n \in S_k\big(\Gamma_1(N)\big)$ of weight $k \in \mathbb{N}_{\geqslant 2}$, level $N \in \mathbb{N}^*$, and nebentypus ε. Denote by $K_f = \mathbb{Q}(a_n, n \geqslant 2)$ the number field spanned by its q-expansion coefficients. Let $\mathfrak{l}$ be one of its finite primes, lying over some rational prime $\ell \in \mathbb{N}$, let $K_{f,\mathfrak{l}}$ be the corresponding completion, and let $\mathbb{Z}_{K_{f,\mathfrak{l}}}$ be its ring of integers. Thanks to P. Deligne [Del71], we know that there exists a continuous ℓ-adic Galois representation

$$G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_{f,\mathfrak{l}}})$$

of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$, which is unramified outside ℓN, and such that for all rational primes $p \nmid \ell N$, the image of the Frobenius element corresponding to any prime lying above p has characteristic polynomial

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{Z}_{K_{f,\mathfrak{l}}}[X].$$

Assume now that $\mathfrak{l}$ has inertia degree 1. By reducing modulo $\mathfrak{l}$, we get a mod ℓ representation

$$\rho_{f,\mathfrak{l}} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell).$$

By [Rib85, theorem 2.1] and [Swi72, lemma 2], for almost every $\mathfrak{l}$, the image of this representation contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, and in particular this representation is irreducible. In the rare case when the image of $\rho_{f,\mathfrak{l}}$ fails to contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, we say that the representation degenerates. We will exclude the finitely many $\mathfrak{l}$ for which $\rho_{f,\mathfrak{l}}$ degenerates from now on. For instance, if we choose $f = \Delta$, according to [Swi72, corollary to theorem 4] the values of ℓ we exclude are 2, 3, 5, 7, 23 and 691.

Further assume now that $\ell \geqslant k+1$ and that $\ell \nmid N$. In this case, this mod ℓ representation can be constructed in a more concrete way as follows. Being an eigenform, f has a system of Hecke eigenvalues $\lambda_f \colon \mathbb{T}_{k,N} \longrightarrow \mathbb{Z}_{K_f}$ such that

$$Tf = \lambda_f(T) f \qquad \forall\, T \in \mathbb{T}_{k,N},$$

where $\mathbb{T}_{k,N} = \mathbb{Z}[T_n,\, n \geqslant 2]$ denotes the Hecke algebra acting on cuspforms of weight k and level N, and where $\mathbb{Z}_{K_f}$ is the ring of integers of K_f. Reducing modulo $\mathfrak{l}$, we get a ring morphism $\lambda_{f,\mathfrak{l}} \colon \mathbb{T}_{k,N} \longrightarrow \mathbb{F}_\ell$. By a weight-lowering theorem (cf [Gro90, proposition 9.3 part 2]), there exists another ring morphism $\mu_{f,\mathfrak{l}} \colon \mathbb{T}_{2,\ell N} \longrightarrow \mathbb{F}_\ell$ such that $\lambda_{f,\mathfrak{l}}(T_p) = \mu_{f,\mathfrak{l}}(T_p) \in \mathbb{F}_\ell$ for all rational

primes p. This other Hecke algebra $\mathbb{T}_{2,\ell N}$ also acts on the jacobian $J_1(\ell N)$ of the modular curve $X_1(\ell N)$, so we can consider the subspace

$$V_{f,\mathfrak{l}} = \bigcap_{T \in \mathbb{T}_{2,\ell N}} \operatorname{Ker}\big(T - [\mu_{f,\mathfrak{l}}(T)]\big)\big|_{J_1(\ell N)[\ell]}$$

of the ℓ-torsion of $J_1(\ell N)$. By [DS05, section 7.9], this subspace $V_{f,\mathfrak{l}}$ is defined over $\mathbb{Q}$, and by [Edi92, theorem 9.2], it has dimension 2 as a vector space over $\mathbb{F}_\ell$, so that the action of $G_\mathbb{Q}$ on its points yields a Galois representation $\rho'_{f,\mathfrak{l}}$ into $\mathrm{GL}_2(\mathbb{F}_\ell)$ which cuts out the Galois number field $L = \overline{\mathbb{Q}}^{\operatorname{Ker}\rho'_{f,\mathfrak{l}}} = \mathbb{Q}(P,\ P \in V_{f,\mathfrak{l}})$, as shown below :

$$\begin{tikzcd}
G_\mathbb{Q} \arrow[r, "\rho'_{f,\mathfrak{l}}"] \arrow[d, two heads] & GL(V_{f,\mathfrak{l}}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell). \\
\mathrm{Gal}(L/\mathbb{Q}) \arrow[ur, hook] &
\end{tikzcd}$$

Of course, if we had $k = 2$ in the first place, there is no need to appeal to the weight-lowering theorem, and the subspace $V_{f,\mathfrak{l}}$ already exists in the ℓ-torsion of $J_1(N)$ instead of $J_1(\ell N)$.

This representation $\rho'_{f,\mathfrak{l}}$ is unramified outside ℓN (cf [DS05, theorem 9.6.5]). Furthermore, it follows from the Eichler-Shimura relation (cf [DS05, theorem 8.7.2]) that for $p \nmid \ell N$, the image of any Frobenius element $\left(\frac{L/\mathbb{Q}}{p}\right)$ by $\rho'_{f,\mathfrak{l}}$ has characteristic polynomial

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{F}_\ell[X],$$

where a_p and $\varepsilon(p)$ have both been reduced modulo $\mathfrak{l}$. By the Brauer-Nesbitt theorem (cf [CR62, theorem 30.16]), $\rho_{f,\mathfrak{l}}$ is therefore isomorphic to the semisimplification of $\rho'_{f,\mathfrak{l}}$, so that $\rho'_{f,\mathfrak{l}}$ is actually irreducible and thus realises $\rho_{f,\mathfrak{l}}$ indeed.

It is interesting to compute explicitly these Galois representations $\rho_{f,\mathfrak{l}}$ for several reasons:

- First, simply for the sake of the Galois representation itself.
- Next, because the number field L is an explicit solution with controlled ramification to the inverse Galois problem for the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ made up of the matrices whose determinant is of the form $\varepsilon(n)n^{k-1}$, which often turns out to be the whole of $\mathrm{GL}_2(\mathbb{F}_\ell)$. It is for instance used as such by J. Bosman in [Bos07a] and [Bos11].
- The number field L is actually even a solution to the Gross problem, which asks to find a non-solvable Galois number field ramified at only one prime.
- Last but not least, because it gives a fast way of computing the q-expansion coefficients a_p of f modulo $\mathfrak{l}$. Letting $\mathfrak{l}$ vary and using Chinese remainders, we thus obtain a Schoof-like algorithm (cf [Sch95]) to compute q-expansions of newforms, as bounds on the coefficients a_p are well-known.

Computing these representations is the goal pursued by the book [EC11]. The idea is to approximate ℓ-torsion divisors representing the points of $V_{f,\mathfrak{l}}$. To compute these torsion divisors, the book [EC11] suggests two approaches: a probabilistic one [CouC13], which creates ℓ-torsion divisors by applying Hecke operators to random divisors on the modular curve over small finite fields, and a deterministic one [CouC12], which relies on fast exponentiation to create approximations of torsion divisors on the modular curve over $\mathbb{C}$. However, neither of these two methods is practical at all, although their theoretical complexities are polynomial in ℓ.

In [Bos07], J. Bosman presents a practical variant of the complex method. It uses an analytic continuation method (cf for instance [AG90]) instead of fast exponentiation. To deal with the Abel-Jacobi map

$$\jmath\colon \mathrm{Div}^0\big(X_1(\ell N)\big)(\mathbb{C}) \to J_1(\ell N)(\mathbb{C}),$$

J. Bosman has to compute a lot of abelian integrals. This leads to precision problems as this requires summing q-series very close to the edge of the convergence disk, and because of the singular locus of $\jmath$, of which little is known. J. Bosman still manages to compute representations up to level 23,

but he only gets projective Galois representations in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ instead of $\mathrm{GL}_2(\mathbb{F}_\ell)$, which means he gets the coefficients $a_p \bmod \mathfrak{l}$ up to a sign only (cf for instance the table on the very first page of [EC11]).

It seems that the implementation [Zen12] by J. Zeng of the probabilistic method suffers from the same limitations. J. Zeng computes polynomials defining projective representations, but seems not to compute actual coefficients.

In this paper, we present another improved, practical and deterministic version of the complex approximations approach, and we can prove this approach works since the singular locus of $\jmath$ is no longer a problem. It has far fewer precision issues, as it computes abelian integrals only along very short paths well inside the convergence disks, and uses K. Khuri-Makdisi's algorithms [KM04, KM07] for fast exponentiation in the jacobian. Consequently, we get approximations of torsion divisors fairly easily. This allows us to compute the full Galois representations for the prime levels $17 \leqslant \ell \leqslant 29$, which, to our knowledge, had never been done before. As a consequence, we can for instance find the signs which were missing in J. Bosman's results.

Like J. Bosman, we limit ourselves to prime levels ℓ for commodity, although our algorithm could easily be extended to general levels N. This implies that we can only use our algorithm to compute Galois representations attached to newforms of weight 2 and level ℓ, or to newforms of arbitrary even weight but of level 1. Typically, we use it on the newform Δ, which is of weight 12 and level 1. As the genus of $X_1(\ell)$ is 0 for $\ell \leqslant 7$, we will assume $\ell \geqslant 11$ throughout this paper. The genus of $X_1(\ell)$ is then $g = \frac{(\ell-5)(\ell-7)}{24}$.

We should however stress the fact that the results we get in practice are not yet rigourously proved. Indeed, our method relies on numerical computations in $\mathbb{C}$, so that we need a bound on the height of the result to prove it. Unfortunately, the best bounds we know (cf [EdJC11, section 11.7]) are impractical, whereas the results we have obtained let us think that these bounds are really not sharp. As a consequence, when we run our computations we use much less precision in $\mathbb{C}$ than required by these bounds, so as to still get interesting results, although not rigouroulsy proved.

Nevertheless, there are some easy tests which we performed so as to convince ourselves that our results are correct without any reasonable doubt. Namely, we checked that the discriminant of the polynomial $F(X)$ defining the representation (see the next section) is of the form $(-1)^{\ell(\ell-1)/2}\ell^v M^2$ for

some large $v \in \mathbb{N}$ and some $M \in \mathbb{Q}^*$ coprime to ℓ, which is what we expect since the representation is supposed to be odd and the number field L it cuts out is supposed to ramify only at ℓ. Also, the fact that the resolvents $\Gamma_C(X)$ we compute (see next section) have rational coefficients with the expected form (we explain in section 3.7 that their denominators should all divide some known bound) hints that $\mathrm{Gal}(L/\mathbb{Q})$ indeed is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Finally, we checked for a few small primes p that the values $a_p \bmod \mathfrak{l}$ which we obtain are correct, by computing a_p by "classical" methods (e.g. using modular symbols, cf [Ste07]) and reducing it modulo $\mathfrak{l}$.

In order to prove our results rigourously, we can appeal to Serre's conjecture [Ser87], which is now a theorem thanks to [KW09]. It would be enough to first prove that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ so that we are sure we are really dealing with a representation, then to make sure that this representation is odd so that Serre's conjecture applies, next to check that it has the correct level and weight, and finally that it corresponds to the right newform f. This is the approach followed by J. Bosman in [Bos07]. We have not succeeded in using it to prove our results yet, but we are working on it. We were for instance able to prove the correctness of the *projective* version of the representation $\rho_{\Delta,29}$ of level 29 attached to the newform $f = \Delta$ which we computed (cf our results section): J. Klüners helped us to formally prove that we have the correct Galois group, we checked that the representation was odd, and that the subfield of $\overline{\mathbb{Q}}$ fixed by the stabiliser of a line in $V_{\Delta,29}$ has discriminant 29^{39}. By the results of [Bos07], this is enough to conclude.

In the next section, we present a quick review of our algorithm. Then, in section 3, we give a detailed description of the key steps. Finally, in the last section, we present actual computations of Galois representations and of coefficients of newforms, and we give complexity estimates.

2 Outline of the algorithm

Our first task consists in computing the period lattice Λ of $X_1(\ell)$, which we do by integrating cuspforms along modular symbols. Using our knowledge of the action of the Hecke algebra on modular symbols, we then deduce an analytic representation of the ℓ-torsion subspace $V_{f,\mathfrak{l}} \subset J_1(\ell)(\mathbb{C}) = \mathbb{C}^g/\Lambda$. Next, we find a way to invert the Abel-Jacobi map $\jmath$, so that we may, for each $x \in J_1(\ell)(\mathbb{C})$, find a null-degree divisor D_x on $X_1(\ell)$ such that $\jmath(D_x) = x$, and especially so for two ℓ-torsion divisor classes x_1 and x_2 forming a basis of the two-dimensional $\mathbb{F}_\ell$-subspace $V_{f,\mathfrak{l}}$. This is done as follows.

We first compute a high-precision floating point approximation of the period lattice Λ by computing a $\mathbb{Z}$-basis of the homology $H_1\big(X_1(\ell)(\mathbb{C}), \mathbb{Z}\big)$ made up of modular symbols (cf [Ste07] or [Cre97]), along which we integrate term-by-term the q-expansions of a basis $(\omega_i)_{1\leqslant i\leqslant g}$ of cuspforms of weight 2 In order to get a very accurate result, this requires q-expanding the ω_i to high precision, which we show how to do quickly below. Then, by computing the Hecke action on $J_1(\ell)[\ell]$, we can express our two divisor classes x_1 and x_2 as points of $\frac{1}{\ell}\Lambda/\Lambda \subset \mathbb{C}^g/\Lambda$.

Let $\widetilde{x_1}$ be a lift of x_1 to $\mathbb{C}^g$. We next pick g points $(P_j)_{1\leqslant j\leqslant g}$ on $X_1(\ell)$, and, using Newton iteration, we compute another g points $(P'_j)_{1\leqslant j\leqslant g}$ with P'_j close to P_j such that

$$\sum_{j=1}^{g}\left(\int_{P_j}^{P'_j}\omega_i(\tau)d\tau\right)_{1\leqslant j\leqslant g} = \frac{\widetilde{x_1}}{2^m},$$

where $m \in \mathbb{N}$ is large enough for Newton iteration to converge, and the integrals are taken along the short paths joining P_j to P'_j. Thus, we get the divisor

$$D_1^{(m)} = \sum_{j=1}^{g}(P'_j - P_j)$$

which satisfies $2^m\big[D_1^{(m)}\big] = x_1$. Then, using K. Khuri-Makdisi's algorithms [KM04, KM07] to compute in the jacobian $J_1(\ell)$, we double m times the divisor class of $D_1^{(m)}$, which yields an ℓ-torsion divisor D_1 representing x_1. We apply the same process to get another ℓ-torsion divisor D_2 representing x_2.

This way, we find ℓ-torsion divisors using only integrals along short paths which are well inside the convergence disks. Consequently we have far fewer precision problems than with J. Bosman's method [Bos07].

We thus now have two ℓ-torsion divisors D_1 and D_2 whose images by the Abel-Jacobi map form a basis of the ℓ-torsion subspace $V_{f,\mathfrak{l}}$. We then compute all the reduced divisors

$$D_{a,b} \sim aD_1 + bD_2, \quad a, b \in \mathbb{F}_\ell,$$

yielding a collection of ℓ^2 reduced divisors corresponding to the ℓ^2 points of $V_{f,\mathfrak{l}}$, and evaluate a well-chosen Galois-equivariant map $\alpha\colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$ in these points. The polynomial

$$F(X) = \prod_{\substack{a,b\in\mathbb{F}_\ell \\ (a,b)\neq(0,0)}} \big(X - \alpha(D_{a,b})\big)$$

then lies in $\mathbb{Q}[X]$; we can recognise its coefficients using continued fractions. This polynomial encodes the Galois representation we are attempting to compute, in that its splitting field L over $\mathbb{Q}$ is the number field cut out by the representation $\rho_{f,\mathfrak{l}}$, and $\mathrm{Gal}(L/\mathbb{Q})$ acts on its roots $\varphi(D_{a,b})$ just like $GL_2(\mathbb{F}_\ell)$ acts on $(a, b) \in \mathbb{F}_\ell^2$.

Our final task is to describe the image of Frobenius elements by this representation. For this, we adapt T. and V. Dokchitser's work [Dok10] to get resolvents

$$\Gamma_C(X) \in \mathbb{Q}[X], \quad C \text{ similarity class of } \mathrm{GL}_2(\mathbb{F}_\ell)$$

such that for almost all rational primes p,

$$\rho_{f,\mathfrak{l}}\,(\mathrm{Frob}_p) \in C \iff \Gamma_C\big(\mathrm{Tr}_{A_p/\mathbb{F}_p}\, a^p\, h(a)\big) = 0 \bmod p,$$

where Frob_p denotes any Frobenius element of L at p, $A_p = \mathbb{F}_p[X]/\big(F(X)\big)$, a denotes the class of X in A_p, and h is a polynomial (cf [Dok10] or section 3.7). We furthermore present a trick to reduce the amount of computations at this step.

Finally, we can use this to compute the coefficients a_p of the q-expansion of f modulo $\mathfrak{l}$:

$$a_p \bmod \mathfrak{l} = \mathrm{Tr}\,\rho_{f,\mathfrak{l}}\,(\mathrm{Frob}_p)\,.$$

3 Detailed description of the steps

We first show in subsection 3.1 how to quickly compute a huge number of terms of the q-expansion at infinity of the cuspforms of weight 2 and level ℓ, and next, in 3.2, how to efficiently compute the period lattice of $X_1(\ell)$ to high precision using these q-expansions. Then, we explain in 3.3 how to use K. Khuri-Makdisi's algorithms [KM04, KM07] on $X_1(\ell)$. Our method requires a careful choice of two Eisenstein series, as explained in 3.4. After this, we show in 3.5 how to compute an ℓ-torsion divisor. Finally, we explain in 3.6 how to construct a well-behaved function on the jacobian $J_1(\ell)$ and how to evaluate it at the ℓ-torsion divisors, and we conclude by describing in 3.7 an efficient way of computing the image of the Frobenius elements by the Galois representation.

3.1 Expanding the cuspforms of weight 2 to high precision

We will need to know the q-expansion of the newforms of weight 2 in order to compute the period lattice of the modular curve. Classical methods based on modular symbols (cf for instance [Ste07, chapter 3]) allow us to compute a moderate number of terms of these q-expansions. However, we will need to know the periods with very high accuracy, which requires computing a very large number of coefficients in these q-expansions. Consequently, as using classical methods for this, though possible, would be too slow, we present a new method to quickly compute a huge number of such coefficients. It proceeds roughly as follows :

- First, compute a moderate number of coefficients of the q-expansion of each cuspform ω.
- Then, use these coefficients to find a polynomial equation relating a modular function depending on ω to the modular invariant j, or some other modular function whose q-expansion is very easy to compute.
- Finally, use Newton iteration on this equation between q-series to compute a huge number of coefficients of the modular function depending on ω, and deduce those of ω.

Moreover, all this is done modulo some prime p so as to accelerate the computation by avoiding intermediate coefficient growth.

More precisely, to compute these q-expansions to the precision $O(q^B)$, we first compute a generator of the Hecke algebra $\mathbb{T}_{2,\ell} \otimes_{\mathbb{Z}} \mathbb{Q}$, by picking a Hecke operator and testing whether it is a $\mathbb{Q}$-algebra generator. This is easy as it amounts to check if its eigenvalues on $S_2\big(\Gamma_1(\ell)\big)$ are all distinct. One can for instance proceed as follows : starting with $n = 2$, first check whether T_n is a generator, if not then pick small integers λ_m and check whether $T_n + \sum_{m=2}^{n-1} \lambda_m T_m$ is a generator, and if still not increase n by 1 and start again. In an overwhelming majority of cases, it appears that at least one of T_2 and T_3 is a $\mathbb{Q}$-algebra generator.

We can find a basis $\mathcal{B} = \bigsqcup_\varepsilon \mathcal{B}_\varepsilon$ of

$$S_2\big(\Gamma_1(\ell)\big) = \bigoplus_{\varepsilon \text{ even character mod } \ell} S_2(\varepsilon),$$

where $\mathcal{B}_\varepsilon$ is a basis of $S_2(\varepsilon)$ consisting in forms which are not necessarily eigenforms[1], but which are normalised, and whose q-expansion coefficients lie among the integers $\mathbb{Z}_K$ of the common cyclotomic field $K = \mathbb{Q}\left(\zeta_{(\ell-1)/2}\right)$. To make it easier to reduce mod p and lift back to K, we want p to split completely in K. Also, p should be chosen large enough for reduction mod p of the coefficients to be faithful. Deligne's bounds state that if $q + \sum_{n \geqslant 2} a_n q^n$ is a newform of weight 2, then for all $n \in \mathbb{N}$, we have $|a_n|_\sigma \leqslant d(n)\sqrt{n}$ for every complex embedding σ, where $d(n)$ denotes the number of positive divisors of n. These bounds may not apply to the forms in the bases $\mathcal{B}_\varepsilon$ as they are not eigenforms, but using our knowledge of a generator of the Hecke algebra, we can compute for each ε a change of basis matrix from the basis $\mathcal{B}_\varepsilon$ to a basis of eigenforms, then deduce from Deligne's bound a bound on the complex embeddings of the B first coefficients of the forms of $\mathcal{B}_\varepsilon$, and finally, compute a bound on the coefficients of these coefficients seen as polynomials in $\zeta_{(\ell-1)/2}$. We choose $p \neq \ell$ to be the smallest rational prime greater than twice this bound and such that $p \equiv 1 \bmod (\ell-1)/2$. Then the $(\ell-1)/2$-th cyclotomic polynomial splits completely over $\mathbb{F}_p$. Letting a_i denote lifts to $\mathbb{Z}$ of its roots in $\mathbb{F}_p$, and $\mathfrak{p}_i = \big(p, \zeta_{(\ell-1)/2} - a_i\big)$, the prime p splits completely as $\prod_i \mathfrak{p}_i$ in K.

[1] If we used a basis of eigenforms, the common number field containing the Fourier coefficients of all these forms could be much larger.

Next, we compute the forms

$$E_4 = 1 + 240 \sum_{n=1}^{+\infty} \sigma_3(n) q^n, \ E_6 = 1 - 540 \sum_{n=1}^{+\infty} \sigma_5(n) q^n, \text{ and } u = \frac{1}{j} = \frac{E_4^3 - E_6^2}{1728 E_6^2}$$

in $\mathbb{F}_p[[q]]$, as well as dj in $q^{-2}\mathbb{F}_p[[q]]dq$, to precision $O(q^B)$.

We then can compute the q-expansions of the forms ω with trivial nebentypus $\varepsilon = \mathbb{1}$ in $\mathcal{B}_{\mathbb{1}}$ as follows. Note that such a form ω has q-coefficients in $\mathbb{Z}$. Consider the form $v = \frac{\omega dq}{q dj} \in \mathbb{Z}[[q]]$. It has weight 0, so it is a rational function on $X_1(\ell)$, which actually descends to a rational function on $X_0(\ell)$ because $\varepsilon = \mathbb{1}$. Its degree there is at most $2g_0 + \ell + 1$, where g_0 denotes the genus of $X_0(\ell)$. Indeed, its degree is at most the number of zeroes of the 1-form $\omega \frac{dq}{q}$ plus the number of poles of the 1-form dj. On the one hand, $\omega \frac{dq}{q}$ has exactly $2g_0 - 2$ zeroes as it is regular. On the other hand, as dj has a double pole at the cusp on $X(1)$, it has a pole of order $e_c + 1$ at each cusp c of $X_0(\ell)$, where e_c is the ramification index of c. Summing over the two cusps of $X_0(\ell)$, we thus see that dj has $\ell + 3$ poles on $X_0(\ell)$, hence the announced bound on the degree of v. Besides, u has degree exactly $\ell + 1$ on $X_0(\ell)$. Consequently, there exists an irreducible polynomial $\Phi(U, V) \in \mathbb{F}_p[U, V]$ of degree at most $2g_0 + \ell + 1$ in U and exactly $\ell + 1$ in V such that $\Phi(u, v) \equiv 0 \bmod p$. We compute this polynomial by linear algebra over $\mathbb{F}_p$ in $\mathbb{F}_p[[q]]$, using a moderately precise q-expansion of ω computed by classical algorithms. Then, by Newton iteration, we can compute $v \bmod p$, and hence $\omega \bmod p$, to the precision $O(q^B)$, and finally lift the coefficients of ω back to $\mathbb{Z}$.

Once this is done, we can compute the q-expansions of the forms ω with nontrivial nebentypus ε as follows. Let $\omega_0 \in \mathcal{B}_{\mathbb{1}}$ be one of the g_0 forms[2] with trivial nebentypus whose q-expansion we have just computed. Then $\frac{\omega}{\omega_0}$ is a rational function on $X_1(\ell)$ with nebentypus ε. We could thus proceed to find an equation Φ as previously by reasoning on $X_1(\ell)$ instead of $X_0(\ell)$, but this would lead to very high degrees and hence would be too slow. Instead, notice that if r denotes the order of ε, then $v = \left(\frac{\omega}{\omega_0}\right)^r$ has trivial nebentypus, so descends to a function on $X_0(\ell)$, of degree at most $\frac{(2g_1-2)r}{(\ell-1)/2}$, where $g_1 = g$

[2]Here, the method breaks down for $\ell = 13$. Indeed, this is the only case in which $g_0 = 0$ (remember we supposed $\ell \geqslant 11$), so that there is no such form in this case. So, in this special case $\ell = 13$, classical methods to expand the forms should be used instead. This is not a big problem, as this is a "small" case (g is only 2), so little accuracy is needed and the whole Galois representation computation is quite fast anyway.

denotes the genus of $X_1(\ell)$, because it has degree at most $(2g_1-2)r$ over $X_1(\ell)$. We can thus compute as previously for each $\mathfrak{p}_i$ an irreducible polynomial $\Phi(U,V) \in \mathbb{F}_p[U,V]$ of degree at most $\frac{(2g-2)r}{(\ell-1)/2}$ in U and exactly $\ell+1$ in V such that $\Phi(u,v) \equiv 0 \bmod \mathfrak{p}_\mathfrak{i}$. Next, we use Newton iteration as before to compute $v \bmod \mathfrak{p}_\mathfrak{i}$, then take the rth root to recover $\omega \bmod \mathfrak{p}_\mathfrak{i}$, and finally lift back to K by Chinese remainders.

Finally, we apply to the q-expansions of the forms we have just computed the change of basis matrices from $\mathcal{B}_\varepsilon$ to the basis of eigenforms which we computed in the beginning, so as to get the q-expansions of the newforms.

This method is faster than the classical one for large B.

Theorem 1. *For fixed prime level ℓ, the number of bit operations required to compute the q-expansion of the newforms in $S_2\big(\Gamma_1(\ell)\big)$ to precision $O(q^B)$ with the algorithm described above is quasi-linear in B.*

In comparison, the bit complexity of the classical algorithm based on modular symbols is at least quadratic in B, cf [Ste07, remark 8.3.3].

Proof. First notice that for fixed level ℓ, the change of basis matrices from the bases $\mathcal{B}_\varepsilon$ to eigenforms are fixed, and so is the common field $K = \mathbb{Q}\left(\zeta_{(\ell-1)/2}\right)$. Consequently, there exists some $C > 0$ not depending on B such that the coefficients of $\zeta_{(\ell-1)/2}$ in the coefficients up to q^B of the forms in the bases $\mathcal{B}_\varepsilon$ are bounded by $M = C \sup_{n<B} d(n)\sqrt{n}$. We have $M = O(B)$, because $d(n) = O(n^\delta)$ for every $\delta > 0$, cf for instance [HW08, theorem 315]. If B is large enough, then M will be large too, so that by the prime number theorem for arithmetic progressions (cf for instance [Sop10]), there exists a prime number $p \equiv 1 \bmod (\ell-1)/2$ lying between $2M$ and, say, $3M$. We can find such a p in $O(B \log B \log\log B)$ bit operations by using the sieve of Eratosthenes (cf the proof of the [GG99, theorem 18.10 part ii]). Then arithmetic operations in the residue field $\mathbb{F}_p$ will require $O(\log B)$ bit operations. Next, E_4 and E_6 can be computed mod p to precision $O(q^B)$ in $O(B \log B \log\log B)$ bit operations by using again the sieve of Eratosthenes, and u and dj can be computed in $O(B \log B)$ operations in $\mathbb{F}_p$ with fast series arithmetic. As ℓ is fixed, computing the short q-expansions and finding the equations Φ, which are of fixed degree, takes fixed time. Then, one Newton iteration takes $O(B \log B)$ operations in $\mathbb{F}_p$ with fast arithmetic, and reaching precision $O(q^B)$ requires $O(\log B)$ such iterations. Finally, we can lift back to K each coefficient because $p > 2M$. Each coefficient lift requires $O(\log B)$ bit operations, so lifting the forms requires $O(B \log B)$ bit operations, hence the result. $\square$

3.2 Computing the periods of $X_1(\ell)$

Computing the period lattice Λ amounts, by the Manin-Drinfeld theorem (cf [Lan95, chapter IV, theorem 2.1]), to compute integrals of newforms ω of weight 2 along modular symbols, such as

$$\int_{\infty}^{0} \omega(\tau) d\tau.$$

These integrals can be computed by integrating q-expansions term by term. However, we have to split the integration path so that the resulting series converges. Furthermore, to increase the convergence speed, we need the path ends to lie well-inside the convergence disks.

To reduce the number of integrals we compute, we use the adjointness property of the Hecke operators with respect to the integration pairing between modular symbols and cuspforms. In general, the modular symbol $\{\infty, 0\}$ alone does not span the rational homology of the modular curve, even over $\mathbb{T}_{2,\ell} \otimes \mathbb{Q}$. As a consequence, we introduce other modular symbols, the twisted winding elements w_p.

More precisely, define (cf [BosC6, section 6.3]), for every $p \neq \ell$ prime or $p = 1$, the twisted winding element

$$w_p = \sum_{a \bmod p} \epsilon_p(a) \left\{\infty, \frac{a}{p}\right\} \in \mathbb{M}_2\big(\Gamma_1(\ell)\big),$$

where $\epsilon_p = \left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol at p, which we define to be 1 if $p = 1$ for convenience. We can write each basis element γ_j of $H_1\big(X_1(\ell)(\mathbb{C}), \mathbb{Z}\big)$, seen as a linear form on $S_2\big(\Gamma_1(\ell)\big)$, as a $\mathbb{T}_{2,\ell} \otimes \mathbb{Q}$-linear combination

$$\gamma_j = \sum_p T_{j,p} w_p, \quad T_{j,p} \in \mathbb{T}_{2,\ell} \otimes \mathbb{Q}.$$

We can then compute the periods using the adjointness property of the integration pairing with respect to Hecke operators as follows:

$$\int_{\gamma_j} \omega(\tau) d\tau = \int_{\sum_p T_{j,p} w_p} \omega(\tau) d\tau = \sum_p \int_{w_p} (T_{j,p}\omega)(\tau) d\tau = \sum_p \lambda_{j,p} \int_{w_p} \omega(\tau) d\tau,$$

where $\lambda_{j,p} \in \mathbb{C}$ denotes the eigenvalue of the newform ω for the Hecke operator $T_{j,p}$. Consequently, all we need is to compute the integrals $\int_{w_p} \omega(\tau) d\tau$.

The Fricke involution W_ℓ transforms the form $\omega(\tau)$ into $\frac{1}{\ell\tau^2}\omega\left(\frac{-1}{\ell\tau}\right)$. It is useful for our purpose because it can be used to map a point τ with small imaginary part to $\frac{-1}{\ell\tau}$, which can have a much larger imaginary part. We read in [BosC6, section 6.2] that if $\omega = q + \sum_{n\geqslant 2} a_n q^n \in S_2\big(\Gamma_1(\ell), \varepsilon\big)$ is a newform with weight 2, level ℓ and character ε, then $W_\ell\omega$ is the newform with weight 2, level ℓ and conjugate character $\overline{\varepsilon}$ defined by

$$W_\ell\omega = \lambda_\ell(\omega)\left(q + \sum_{n\geqslant 2}\overline{a_n}q^n\right),$$

where $\lambda_\ell(\omega)$ is given by

$$\lambda_\ell(\omega) = \begin{cases} -\overline{a_\ell} & \text{if } \varepsilon \text{ is trivial,} \\ \dfrac{g(\varepsilon)\overline{a_\ell}}{\ell} & \text{if } \varepsilon \text{ is nontrivial,} \end{cases}$$

where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character. Moreover, if χ is a Dirichlet character modulo $p \neq \ell$, then

$$\omega \otimes \chi = \sum_{n\geqslant 1} a_n\chi(n)q^n.$$

is a cuspform of level ℓp^2 by [AL78, proposition 3.1], and we have the formula

$$W_{\ell p^2}(\omega\otimes\chi) = \frac{g(\chi)}{g(\overline{\chi})}\varepsilon(p)\chi(-\ell)\cdot(W_\ell\omega)\otimes\overline{\chi}.$$

An easy computation shows that

$$\sum_{a \bmod p}\overline{\chi}(a)\omega(\tau + a/p) = g(\overline{\chi})(\omega\otimes\chi)(\tau).$$

This yields the formula

$$\int_{w_p}\omega(\tau)d\tau = g(\epsilon_p)\int_\infty^0(\omega\otimes\epsilon_p)(\tau)d\tau$$

$$= g(\epsilon_p)\left(\int_\infty^{\frac{i}{p\sqrt{\ell}}}(\omega\otimes\epsilon_p)(\tau)d\tau + \int_{\frac{i}{p\sqrt{\ell}}}^0(\omega\otimes\epsilon_p)(\tau)d\tau\right)$$

$$= g(\epsilon_p)\left(\int_{\infty}^{\frac{i}{p\sqrt{\ell}}}(\omega\otimes\epsilon_p)(\tau)d\tau - \int_{\infty}^{\frac{i}{p\sqrt{\ell}}} W_{\ell p^2}(\omega\otimes\epsilon_p)(\tau)d\tau\right)$$

$$= \frac{g(\epsilon_p)}{2\pi i}\sum_{n=1}^{+\infty}\left(a_n - \varepsilon(p)\epsilon_p(-\ell)\lambda_\ell(\omega)\overline{a_n}\right)\frac{\epsilon_p(n)}{n}\left(e^{-\frac{2\pi}{p\sqrt{\ell}}}\right)^n,$$

which allows us to compute the integral of a newform along a twisted winding element, and thus to finally compute the period lattice of the modular curve $X_1(\ell)$. We sum power series at $q = e^{-\frac{2\pi}{p\sqrt{\ell}}}$ for primes p, which has small enough modulus to achieve fast convergence. We have indeed checked that $p \leqslant 3$ is very often sufficient for the w_p to span the rational homology of the modular curve over $\mathbb{T}_{2,\ell}$, and $p \leqslant 7$ is enough for all levels $\ell \leqslant 61$, except for $\ell = 37$ in which case we had to go up to $p = 19$.

3.3 Arithmetic in the jacobian $J_1(\ell)$

In order to efficiently compute in the jacobian $J_1(\ell)$, we use K. Khuri-Makdisi's algorithms [KM04, KM07]. This requires choosing an effective divisor D_0 of degree $d_0 \geqslant 2g+1$ for which we know how to compute the associated Riemann-Roch space

$$V = H^0\big(X_1(\ell), 3D_0\big).$$

A divisor class $x \in J_1(\ell)$ is then represented by an effective divisor D of degree d_0 such that the class of $D - D_0$ is x, and D is itself represented by the subspace

$$W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V;$$

in particular $0 \in J_1(\ell)$ can be represented by

$$W_0 = H^0\big(X_1(\ell), 2D_0\big) \subset V.$$

We also want D_0 to be defined other $\mathbb{Q}$, so that $(W_D)^\sigma = W_{D^\sigma}$ for all $\sigma \in \operatorname{Aut}\mathbb{C}$.

Let us first give an overview of how to find such a divisor D_0. Our strategy consists of choosing $D_0 = K + c_1 + c_2 + c_3$, where K is an effective canonical divisor defined over $\mathbb{Q}$ and the c_i are $\mathbb{Q}$-rational cusps, so for us d_0 is exactly $2g+1$. First, we compute the $(g+2)$-dimensional space

$$V_2 = H^0\big(X_1(\ell), \Omega^1(c_1 + c_2 + c_3)\big).$$

This space is the direct sum of all the cusp forms of weight 2 and of the scalar multiples of Eisenstein series $e_{1,2}$ and $e_{1,3}$ of weight 2 vanishing at all cusps except c_1 and c_2 for $e_{1,2}$ and except c_1 and c_3 for $e_{1,3}$, so we have

$$V_2 = S_2\big(\Gamma_1(\ell), \mathbb{C}\big) \oplus \mathbb{C}e_{1,2} \oplus \mathbb{C}e_{1,3} \subset M_2\big(\Gamma_1(\ell), \mathbb{C}\big).$$

The point of this is that by picking a cusp form $f_0 \in S_2\big(\Gamma_0(\ell), \mathbb{Q}\big)$ defined over $\mathbb{Q}$, we obtain a Galois-equivariant isomorphism

$$\begin{array}{ccc} V_2 & \xrightarrow{\sim} & H^0\big(X_1(\ell), K + c_1 + c_2 + c_3\big) \\ f & \longmapsto & \dfrac{f}{f_0} \end{array},$$

where K is the divisor of the differential 1-form over $X_1(\ell)$ associated to the cuspform f_0, which is indeed an effective canonical divisor. Now by [KM04, lemma 2.2], the map

$$\begin{array}{ccc} V_2^{\otimes 3} & \longrightarrow & H^0\big(X_1(\ell), 3(K + c_1 + c_2 + c_3)\big) \\ f_1 \otimes f_2 \otimes f_3 & \longmapsto & \dfrac{f_1 f_2 f_3}{f_0^3} \end{array}$$

is surjective. We may thus choose V to be the image of the multiplication map

$$\begin{array}{ccc} V_2^{\otimes 3} & \longrightarrow & M_6\big(\Gamma_1(\ell), \mathbb{C}\big) \\ f_1 \otimes f_2 \otimes f_3 & \longmapsto & f_1 f_2 f_3 \end{array}.$$

In this framework, the subspace W_0 representing $0 \in J_1(\ell)$ is the image of the map

$$\begin{array}{ccc} V_2^{\otimes 2} & \longrightarrow & M_6\big(\Gamma_1(\ell), \mathbb{C}\big) \\ f_1 \otimes f_2 & \longmapsto & f_1 f_2 f_0 \end{array}.$$

From now on, we will identify weight-6 modular form spaces with the corresponding modular function spaces obtained by dividing by f_0^3 without explicitly mentioning it.

We represent the weight-6 forms by their q-expansions at each cusp. To compute these q-expansions, we start from the q-expansion at ∞, and apply diamond operators and Fricke involutions in order to reach all the other cusps, as explained below. We could also have represented forms by their q-expansions at ∞ only, but we think using q-expansions at various cusps is better for numerical stability. Also we will later need to be able to evaluate

the forms at various points of the modular curve, hence it is better to know the q-expansions at various places.

The modular curve $X_0(\ell)$ has exactly two cusps, namely $\Gamma_0(\ell)\cdot\infty$ and $\Gamma_0(\ell)\cdot 0$, whereas the modular curve we are interested in, $X_1(\ell)$, has exactly $\ell-1$ cusps, half of which lie above $\Gamma_0(\ell)\cdot\infty$ while the other half lie above $\Gamma_0(\ell)\cdot 0$. We call the former cusps above ∞ and the latter cusps above 0. The cusps above 0 are all rational, whereas the cusps above ∞ make up a single Galois orbit. Now, the diamond operators $\langle d\rangle$, $d\in(\mathbb{Z}/\ell\mathbb{Z})^*$, which correspond to the action of the quotient group $\Gamma_0(\ell)/\Gamma_1(\ell)\simeq(\mathbb{Z}/\ell\mathbb{Z})^*$, map the cusp $\Gamma_1(\ell)\cdot\infty$ onto the cusps above ∞, and the cusp $\Gamma_1(\ell)\cdot 0$ onto the cusps above 0. Moreover, the Fricke operator W_ℓ swaps $\Gamma_1(\ell)\cdot\infty$ and $\Gamma_1(\ell)\cdot 0$. We know how the Fricke operator acts on newforms of weight 2 (cf subsection 3.2 on the periods), and on Eisenstein series (cf next subsection 3.4). Besides, all the forms we are dealing with have a nebentypus, so that the action of any diamond operator $\langle d\rangle$ on their q-expansions is easy to compute : it boils down to multiplying by the value of their character at d. Using these two kinds of operators, we thus get the q-expansions of the newforms and of the Eisenstein series at all cusps from their q-expansions at ∞.

3.4 Finding the appropriate Eisenstein series

We now explain how to choose the Eisenstein series $e_{1,2}$ and $e_{1,3}$. Let us first review some facts about Eisenstein series of weight 2 in general (not necessarily prime) level N. From [DS05, chapter 4], we know that the Eisenstein subspace of $M_2\big(\Gamma_1(N),\mathbb{C}\big)$ has a basis formed of the Eisenstein series

$$G_2^{\psi,\varphi}(\tau)=\sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\psi(r)\overline{\varphi}(s)\sum_{\substack{(c,d)\in\mathbb{Z}^2\\ c\equiv rv \bmod N\\ d\equiv s+tv \bmod N}}\frac{1}{(c\tau+d)^2},$$

where ψ and φ are Dirichlet characters not both trivial, of the same parity, and of respective conductors u and v such that $uv=N$ exactly, and of

$$G_2(N\tau)-NG_2(N\tau),\quad\text{where}\quad G_2(\tau)=\sum_{c\in\mathbb{Z}}\sum_{\substack{d\in\mathbb{Z}\\ (c,d)\neq(0,0)}}\frac{1}{(c\tau+d)^2}.$$

We furthermore have the q-expansions at ∞

$$E_2^{\psi,\varphi}(\tau) = -\mathbb{1}_{u=1}\frac{1}{2}\sum_{a=0}^{v-1}\varphi(a)a\left(\frac{a}{v}+1\right) + 2\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}}\psi(n/m)\varphi(m)m\right)q^n,$$

where $\mathbb{1}_{u=1}$ is 1 if $u=1$ and 0 else, $E_2^{\psi,\varphi}$ is the normalisation of $G_2^{\psi,\varphi}$ defined by the relation

$$G_2^{\psi,\varphi} = \frac{-4\pi^2 g(\overline{\varphi})}{v^2}E_2^{\psi,\varphi},$$

and where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character, and

$$E_2(\tau) = 1 - 24\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}} m\right)q^n, \quad G_2 = \frac{\pi^2}{3}E_2.$$

Also, $G_2^{\psi,\varphi} \in M_2\big(\Gamma_1(N), \psi\varphi\big)$ has nebentypus $\psi\varphi$, where $\psi\varphi$ is seen as a Dirichlet character modulo N, whereas $G_2(\tau) - NG_2(N\tau)$ has trivial nebentypus. In what follows, we will not use $G_2(\tau) - NG_2(N\tau)$ at all.

Consequently, in the case when $N = \ell$ is prime, we are left with only two cases, namely $G_2^{\chi,1}$ and $G_2^{1,\chi}$, where χ is a nontrivial even Dirichlet character modulo ℓ. Both have nebentypus χ, and $G_2^{\chi,1}$ vanishes at ∞ while $G_2^{1,\chi}$ does not.

We easily check the formula

$$G_2^{\psi,\varphi}(\tau) = \sum_{(c,d)\in\mathbb{Z}^2}\frac{\psi(c)\overline{\varphi}(d)}{(vc\tau+d)^2},$$

from which it is clear that

$$W_N G_2^{\psi,\varphi} = \frac{u}{v}\psi(-1)G_2^{\overline{\varphi},\overline{\psi}},$$

and thus

$$W_N E_2^{\psi,\phi} = \frac{g(\psi)}{g(\overline{\varphi})}\frac{v}{u}\psi(-1)E_2^{\overline{\phi},\overline{\psi}}.$$

We construct Eisenstein series $e_{1,2}$ and $e_{1,3}$ as linear combinations of the $E_2^{\chi,1}$'s and the $E_2^{1,\chi}$'s, because they have nicer q-expansions than their G-counterparts. First, we choose the cusps c_1, c_2 and c_3 to be $c_1 = \Gamma_1(\ell)\cdot 0$, $c_2 =$

$\langle 2\rangle c_1$, and $c_3 = \langle 3\rangle c_1$, so that they are all $\mathbb{Q}$-rational. They are also all distinct since $\ell \geqslant 11$. The form $f_0 \in S_2\big(\Gamma_0(\ell), \mathbb{Q}\big)$ being defined over $\mathbb{Q}$ because its q-expansion at the $\mathbb{Q}$-rational cusp $\Gamma_1(\ell)\cdot 0$ has rational coefficients, its divisor K is defined over $\mathbb{Q}$, and so is our divisor $D_0 = K + c_1 + c_2 + c_3$. Next, we have from the above formulae

$$W_\ell E_2^{\chi,1} = \frac{g(\chi)}{\ell} E_2^{1,\overline{\chi}} \qquad \text{and} \qquad W_\ell E_2^{1,\chi} = \frac{\ell}{g(\overline{\chi})} E_2^{\overline{\chi},1},$$

from which we read that $E_2^{\chi,1}$ vanishes at the cusps above ∞ but not at the cusps above 0, while the opposite stands true for $E_2^{1,\chi}$. Consequently we construct $e_{1,2}$ and $e_{1,3}$ as linear combinations of the $E_2^{\chi,1}$ only. Now, it follows easily from the orthogonality relations between Dirichlet characters that the Eisenstein series

$$e_{1,2} = \sum_{\substack{\chi \text{ even} \\ \chi \neq 1}} \frac{1-\chi(2)}{g(\chi)\displaystyle\sum_{a=0}^{\ell-1} \overline{\chi}(a) a \left(\frac{a}{\ell}+1\right)} E_2^{\chi,1}$$

and

$$e_{1,3} = \sum_{\substack{\chi \text{ even} \\ \chi \neq 1}} \frac{1-\chi(3)}{g(\chi)\displaystyle\sum_{a=0}^{\ell-1} \overline{\chi}(a) a \left(\frac{a}{\ell}+1\right)} E_2^{\chi,1}$$

are the ones we were looking for, that is to say $e_{1,2}$ vanishes at all cusps but c_1 and c_2, and $e_{1,3}$ vanishes at all cusps but c_1 and c_3.

3.5 Computing an ℓ-torsion divisor

Recall that our goal is to find null-degree divisors D_1 and D_2 representing a basis of the eigenplane $V_{f,\mathfrak{l}} \subset J_1(\ell)[\ell]$. From our knowledge of the period lattice Λ and of a generator of the Hecke algebra $\mathbb{T}_{2,\ell}$, we can express the basis vectors x_k, $k \in \{1,2\}$ of $V_{f,\ell}$ as points in the analytic model $\mathbb{C}^g/\Lambda$ of the jacobian $J_1(\ell)(\mathbb{C})$. Lift x_k to $\widetilde{x_k} \in \mathbb{C}^g$. We will use Newton iteration to compute $2g$ points P_j and P'_j, $1 \leqslant j \leqslant g$, with each P'_j close to P_j, such that

$$\sum_{j=1}^{g} \left(\int_{P_j}^{P'_j} \omega_i(\tau) d\tau \right)_{1 \leqslant j \leqslant g} = \frac{\widetilde{x_k}}{2^m}. \qquad (\star)$$

Here $m \in \mathbb{N}$ is an integer, and we introduced the 2^m factor so as to help the Newton iteration to converge by ensuring that for each j, P'_j stays well-inside the coordinate disk containing P_j, namely the q-disk centered at the cusp c_j (see below). The integral from P_j to P'_j is understood to be along a path which stays inside this disk, so that the left-hand side of $(\star)$ is well-defined in $\mathbb{C}^g$. In practice we use $m \approx 10$.

More precisely, first pick g (not necessarily distinct) cusps $c_1, \cdots, c_g$. For each of these cusps, we have an analytic map, the "q-coordinate" around c_j

$$\kappa_j \colon \mathbb{E} \longrightarrow X_1(\ell)(\mathbb{C}),$$

where $\mathbb{E}$ stands for the open unit disk in $\mathbb{C}$, which maps 0 to the cusp c_j and which is a local diffeomorphism. Next, choose g complex numbers $q_1, \cdots, q_g$ of small moduli, so that each point $P_j = \kappa_j(q_j)$ is close to the cusp c_j. Consider another vector of g small complex numbers $\delta_1, \cdots, \delta_g$. We want to adjust this vector so that $(\star)$ be satisfied with $P'_j = \kappa_j(q_j + \delta_j)$. In a nutshell, the overall map we apply Newton iteration to is

$$\begin{array}{ccccccc} U & \xrightarrow{\prod \kappa_j} & X_1(\ell)^g & \longrightarrow & \operatorname{Div}^0 X_1(\ell) & \longrightarrow & \mathbb{C}^g \\ (\delta_j)_{1 \leqslant j \leqslant g} & \longmapsto & (P'_j)_{1 \leqslant j \leqslant g} & \longmapsto & \displaystyle\sum_{j=1}^{g} (P'_j - P_j) & \longmapsto & \displaystyle\sum_{j=1}^{g} \left(\int_{P_j}^{P'_j} \omega_i(\tau) d\tau \right)_{1 \leqslant j \leqslant g} \end{array},$$

where $U \subset \mathbb{E}$ is a neighbourhood of $0 \in \mathbb{E}^g$ such that $(q_j + \delta_j)_{1 \leqslant j \leqslant g}$ remains in $\mathbb{E}^g$ for all $(\delta_j)_{1 \leqslant j \leqslant g} \in U$. The differential of this map is given by the newforms f_i themselves evaluated at the P'_j, so using it for Newton iteration presents no difficulty.

Once this is done, we want to double the divisor class of

$$D_k^{(m)} = \sum_{j=1}^{g} (P'_j - P_j)$$

m times, using K. Khuri-Makdisi's algorithms. This is however not immediate, as these algorithms can only deal with divisors of the form $D - D_0$, where D is an effective divisor of degree d_0, and D_0 and d_0 are defined in the beginning of the section 3.3. To work around this, we fix what we call a padding divisor, that is to say an effective divisor C of degree $d_0 - g = g + 1$, we feed the divisors $\sum_{j=1}^{g} P'_j + C - D_0$ and $\sum_{j=1}^{g} P_j + C - D_0$ which are indeed of the form $D - D_0$ to K. Khuri-Makdisi's algorithm, and then use this algorithm to subtract these two divisor classes. Feeding a divisor $D - D_0$ to K. Khuri-Makdis's algorithm is easy : it amounts to computing the subspace $W_D = H^0\big(X_1(\ell), 3D_0 - D\big)$ of $V = H^0\big(X_1(\ell), 3D_0\big)$ consisting of functions of V which vanish at D. We do so by evaluating the q-series in the basis of V at the points of D and by doing linear algebra. Because we will have to evaluate q-series at C, it proves convenient to choose a divisor C supported by cusps, hence the notation C.

Finally, once the divisor $D_k^{(m)}$ is processed, we apply K. Khuri-Makdisi's chord algorithm $x \mapsto -2x$ on it, yielding $(-2)^m[D_k^{(m)}] = \pm x_k$. The $\pm$ sign is not a problem, because we get a basis vector for $V_{f,\mathfrak{l}}$ no matter what the sign is, and this is all we actually need.

3.6 Evaluating the torsion divisors

We must construct a Galois-equivariant function $\alpha \in \mathbb{Q}\big(J_1(\ell)\big)$ which can be efficiently evaluated at every point $x \in V_{f,\mathfrak{l}}$ given in Khuri-Makdisi form. We then evaluate α in each nonzero point of $V_{f,\mathfrak{l}}$, and form the polynomial

$$F(X) = \prod_{\substack{x \in V_{f,\mathfrak{l}} \\ x \neq 0}} \big(X - \alpha(x)\big) \in \mathbb{Q}[X]$$

which defines the Galois representation $\rho_{f,\mathfrak{l}}$. In order to recognise its coefficients as rational numbers, we compute the continued fraction expansion of each of them until we find a huge term. Clearly, the lower the height of $F(X)$ the better, as it requires less precision in $\mathbb{C}$. This means one should use an evaluation function α which is arithmetically well-behaved. In order

to try to quantify this, we may look at the class of its divisor of poles (or zeroes) in the Néron-Severi group of $J_1(\ell)$.

The approach used in [CEC3], [EdiC14], [Bos07] and [Zen12] consists in selecting a rational function ξ on $X_1(\ell)$ defined over $\mathbb{Q}$ and extending it to $J_1(\ell)$ by

$$\begin{array}{rccc} \Xi\colon & J_1(\ell) & \dashrightarrow & \mathbb{C} \\ & \displaystyle\sum_{i=1}^{g} P_i - gO & \longmapsto & \displaystyle\sum_{i=1}^{g} \xi(P_i), \end{array}$$

where $O \in X_1(\ell)(\mathbb{Q})$ is an origin for the Abel-Jacobi map. The divisor of the poles of this function Ξ is

$$(\Xi)_\infty = \sum_{Q \text{ pole of } \xi} \tau^*_{[Q-O]}\Theta,$$

where Θ is the theta divisor on $J_1(\ell)$ associated to the Abel-Jacobi map with origin O. We thus see that $(\Xi)_\infty$ is the sum of $\deg \xi$ translates of Θ. If we are to let this function Ξ play the role of α, then we want it to be be arithmetically well-behaved, so that ξ should be chosen to have degree as low as possible. However, this degree is at least the gonality of $X_1(\ell)$, which is roughly proportional to g (cf [Abr96, remark 0.2]).

We introduce a radically different method, which can be used on every algebraic curve X to construct a function $\alpha \in \mathbb{Q}\big(\operatorname{Jac}(X)\big)$. Let us denote the genus of X by g. Every point $x \in \operatorname{Jac}(X)$ can be written $[E_x - gO]$, where E_x is an effective divisor of degree g on X which is generically unique, and $O \in X$ is a fixed point. Let Π be a fixed divisor on X of degree $2g$. Then the space $H^0(X, \Pi - E_x)$ is generically 1-dimensional over $\mathbb{C}$, say spanned by $t_x \in \mathbb{C}(X)$. The divisor of t_x is of the form $(t_x) = -\Pi + E_x + R_x$, where R_x is a residual effective divisor of degree g on X, which is the image of E_x by the reflection

$$\begin{array}{rccc} R_\Pi\colon & \operatorname{Pic}^g(X) & \longrightarrow & \operatorname{Pic}^g(X) \\ & [E] & \longmapsto & [\Pi - E]. \end{array}$$

Let A and B be two points on X disjoint from the support of Π. We can then define

$$\begin{array}{rccc} \alpha\colon & \operatorname{Jac}(X) & \dashrightarrow & \mathbb{C} \\ & x & \longmapsto & \frac{t_x(A)}{t_x(B)}. \end{array}$$

This map is well-defined only on a Zariski-dense subset of $\mathrm{Jac}(X)$ because of the genericity assumptions, and it is defined over $\mathbb{Q}$ if X, Π, A, B and O are defined over $\mathbb{Q}$. Moreover, it is much better-behaved than the function Ξ used in the classical approach :

Theorem 2. *The divisor of poles of α is the sum of only two translates of the Θ divisor.*

Proof. α has a pole at $x \in \mathrm{Jac}(X)$ if and only if $[E_x - gO]$ or $[R_x - gO]$ are on the support of $\tau^*_{[B-O]}\Theta$. But $[R_x - gO]$ is the image of $[E_x - gO]$ by the involution $R_\Pi = \tau_{[\Pi-2gO]} \circ [-1]$ defined above, and $[-1]^*\Theta = \tau^*_{\mathcal{K}}\Theta$ is the translate of Θ by the image $\mathcal{K}$ of the canonical class, cf [HS00, theorem A.8.2.1.i]. $\square$

This is even in some sense optimal, as by the Riemann-Roch theorem for abelian varieties (cf [HS00, theorem A.5.3.3]), no nonconstant function on $\mathrm{Jac}(X)$ has a single translate of Θ as divisor of poles, whereas a generic curve X has $\mathrm{NS}\big(\mathrm{Jac}(X)\big) = \mathbb{Z}\Theta$.

In order to use this on the modular curve $X_1(\ell)$, there is a difficulty we have to overcome. In K. Khuri-Makdisi's algorithms, a divisor class $x \in J_1(\ell)$ is represented by a subspace $W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V$, where D is an effective divisor of degree $d_0 = 2g+1$ such that $[D - D_0] = x$, but such a D is far from being unique — by the Riemann-Roch theorem, there is a whole $(g+1)$-dimensional projective space of them ! Thus, the first thing to do is to rigidify the representation W_D of x into a representation which depends on x only. To do this, we compute the sub-subspace

$$W_{D,\mathrm{red}} = H^0\big(X_1(\ell), 3D_0 - D - C_1\big) \subset W_D,$$

where C_1 is a fixed effective divisor of degree $d_1 = 2d_0 - g$, so that $W_{D,\mathrm{red}}$ will generically be 1-dimensional by the Riemann-Roch theorem. Letting $s_D \in V$ be such that s_D spans $W_{D,\mathrm{red}}$ over $\mathbb{C}$, we know that the divisor of s_D is of the form

$$(s_D) = -3D_0 + D + C_1 + E_D,$$

where E_D is some effective divisor of degree g. Again by the Riemann-Roch theorem, E_D is generically alone in its linear equivalence class. But on the other hand, if W_D and $W_{D'}$ both represent the same point $x \in J_1(\ell)(\mathbb{C})$, then $D \sim D'$, so that $E_D \sim E_{D'}$ as D_0 and C_1 are fixed. Consequently, we

generically have $E_D = E_{D'}$, which shows that E_D only depends on x and not on D, so that the process $W_D \mapsto E_D$ is the rigidification we are looking for. We then use a trick *à la* Khuri-Makdisi: we first compute

$$s_D \cdot V = \{s_D v,\ v \in V\} = H^0\big(X_1(\ell), 6D_0 - D - C_1 - E_D\big),$$

after which we compute

$$H^0\big(X_1(\ell), 3D_0 - C_1 - E_D\big) = \{v \in V \mid vW_D \subset s_D \cdot V\},$$

all of this by linear algebra as in [KM04, KM07]. Next, we fix another effective divisor C_2 of degree $d_2 = d_0+1-g$, so that the subspace $H^0\big(X_1(\ell), 3D_0 - C_1 - C_2 - E_D\big)$ of the previously computed space $H^0\big(X_1(\ell), 3D_0 - C_1 - E_D\big)$ is generically one-dimensional. Letting $\Pi = 3D_0 - C_1 - C_2$, we thus have computed a function $t_D \in \mathbb{C}\big(X_1(\ell)\big)$ such that

$$\mathbb{C}t_D = H^0\big(X_1(\ell), \Pi - E_D\big),$$

as wanted. This allows us to compute the map α, which will be defined over $\mathbb{Q}$ if C_1, C_2, A and B are. As in the previous section, it proves convenient to choose the divisors C_1 and C_2 to be supported by cusps, so that the q-series are effortless to evaluate, hence the notation C_1 and C_2.

Evaluating α on $V_{f,\mathfrak{l}}$, we may thus hope to get a defining polynomial $F(X)$ of logarithmic height $g/2$ times less than if we had used the classical approach.

3.7 Finding the Frobenius elements

After evaluating a suitable function in the torsion divisors representing the points of $V_{f,\mathfrak{l}} \setminus \{0\}$, we get a polynomial $F(X) \in \mathbb{Q}[X]$ of degree $\ell^2 - 1$ whose decomposition field is the field L fixed by the kernel of the Galois representation. It is thus a Galois number field, and its Galois group over $\mathbb{Q}$ is embedded by the representation as a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. In order to completely specify the Galois representation, we would like to know the image of the Frobenius elements Frob_p in $\mathrm{GL}_2(\mathbb{F}_\ell)$. We now explain how to compute the similarity class of the image of Frob_p for almost all rational primes p (clearly, we have to exclude $p = \ell$, as L is ramified at ℓ, but we will shortly see that we actually have to exclude finitely many other primes as well). This can be used to get congruence relations modulo ℓ on the coefficients a_p of the cuspform f, by looking at the trace of the similarity class of Frob_p.

3.7.1 The Dockchitsers' resolvents

For this, we use Tim and Vladimir Dokchitser's work [Dok10]. Denoting by $(a_i)_{1 \leqslant i < \ell^2}$ the roots of F in L, if $h(X) \in \mathbb{Z}[X]$ is a polynomial with integer coefficients, then for each similarity class $C \subset \mathrm{GL}_2(\mathbb{F}_\ell)$, the resolvent

$$\Gamma_C(X) = \prod_{\sigma \in C} \left(X - \sum_{i=1}^{n} h(a_i)\sigma(a_i) \right)$$

lies in $\mathbb{Q}[X]$. Furthermore, these resolvents $\Gamma_C(X)$ are pairwise coprime over $\mathbb{Q}$ for a generic choice of $h(X)$ amongst the polynomials of degree at most $\ell^2 - 2$ with coefficients in $\mathbb{Z}$. Let p be a rational prime such that F is p-integral and squarefree modulo p. Define $u = \mathrm{Tr}_{\frac{\mathbb{F}_p[X]}{F(X)}/\mathbb{F}_p} h(a)a^p \in \mathbb{F}_p$, where a denotes the class of X in the quotient algebra $\mathbb{F}_p[X]/\big(F(X)\big)$. Then the resolvents Γ_C are also p-integral, and we have the implication

$$\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p) \in C \Longrightarrow \Gamma_C(u) = 0 \bmod p.$$

If the resolvents Γ_C are indeed pairwise coprime over $\mathbb{Q}$, and if p is very large, then it is likely that they remain pairwise coprime modulo p, and then we have the criterion

$$\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p) \in C \Longleftrightarrow \Gamma_C(u) = 0 \bmod p,$$

which allows us to find out which similarity class $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ lies in. If, however, the resolvents fail to be pairwise coprime modulo p, then $\Gamma_C(u)$ may vanish for several C, so that we cannot tell where $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ lies. Nonetheless, as the primary goal of our computations is to find the coefficients a_p of the q-expansion of f modulo $\mathfrak{l}$, and as naive methods compute a_p for small p in almost no time, the only case we are really interested in is the case in which p is extremely large, and in this case it is extremely likely that the resolvents $\Gamma_C(X)$ remain pairwise coprime modulo p if they are pairwise coprime over $\mathbb{Q}$. In practice, we choose $h(X) = X^2$, which has always yielded resolvents $\Gamma_C(X)$ which are pairwise coprime over $\mathbb{Q}$.

To compute the resolvents $\Gamma_C(X)$, we first start by computing the roots a_i, which we already know to a mildly high precision, to a very high precision in $\mathbb{C}$ by using Newton iteration. Then, we compute complex approximations of the resolvents $\Gamma_C(X)$ by enumerating matrices in the similarity classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Finally, we recognise their coefficients as rational numbers, using our knowledge of an *a priori* multiple of their denominators, namely $d^{|C|(1+\deg h)}$, where d is a common denominator for the coefficients of $F(X)$.

Once the resolvents are computed, it is easy to deduce what $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ is similar to, and hence to compute the coefficient a_p of f modulo $\mathfrak{l}$.

3.7.2 The quotient representation trick

Unfortunately, these computations, although simple, can be rather slow because they require performing operations on very high precision approximations of certain complex numbers. For instance, in level $\ell = 29$, about 5 million decimal digits after the decimal point are required to compute the resolvents. However, a simple trick allows us, in most cases, to sharply reduce the amount of computations needed. Indeed, we have not yet used the fact that we know in advance what the determinant of the image of the Frobenius element Frob_p is, namely $\varepsilon(p)p^{k-1}$, where k and ε denote respectively the weight and the nebentypus of the newform f.

The idea is then to compute a *quotient* representation, that is to say the representation $\rho_{f,\mathfrak{l}}$ composed with the projection map from $\mathrm{GL}_2(\mathbb{F}_\ell)$ onto one its quotient groups. The coarser the chosen quotient group, the smaller the computation, so we should use a quotient just fine enough to be able to lift correctly an element back to $\mathrm{GL}_2(\mathbb{F}_\ell)$ based on the knowledge of its determinant. Thus $\mathrm{PGL}_2(\mathbb{F}_\ell)$ for instance is slightly too coarse, because the knowledge of the image of a matrix in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and of its determinant

only determines this matrix up to sign — this is the very reason why J. Bosman, for computing only the projective Galois representation, determined the coefficients a_p of f only up to sign in [Bos07]. In the light of this example, it is clear that the right quotient to consider is

$$\widetilde{\mathrm{GL}_2(\mathbb{F}_\ell)} = \mathrm{GL}_2(\mathbb{F}_\ell)/S,$$

where S is the largest subgroup of $\mathbb{F}_\ell^*$. This subgroup S is the subgroup made up of the elements of odd order in $\mathbb{F}_\ell^*$, that is to say, the $2'$-subgroup of $\mathbb{F}_\ell^*$.

Computing the associated quotient Galois representation

$$G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \widetilde{\mathrm{GL}_2(\mathbb{F}_\ell)}$$

then amounts to describing the Galois action on the quotient space

$$\widetilde{V_{f,\mathfrak{l}}} = V_{f,\mathfrak{l}}/S.$$

We thus first begin by computing the polynomial $\widetilde{F}(X) \in \mathbb{Q}[X]$ defining $\widetilde{V_{f,\mathfrak{l}}}$ by tracing the roots $\alpha(x)$, $x \in V_{f,\mathfrak{l}}$ of $F(X)$ along their orbits under S :

$$\widetilde{F}(X) = \prod_{\substack{Sx \in \widetilde{V_{f,\mathfrak{l}}} \\ x \neq 0}} \left(X - \sum_{s \in S} \alpha(sx) \right).$$

This new polynomial has the same height as the original $F(X)$, but its degree is $|S|$ times smaller.

We must then compute the resolvents $\Gamma_{\widetilde{C}}(X)$ for each conjugacy class $\widetilde{C}$ of $\widetilde{\mathrm{GL}_2(\mathbb{F}_\ell)}$. As the subgroup S of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is central, these conjugacy classes are easy to describe.

Lemma 3. *Let* $\pi\colon \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \widetilde{\mathrm{GL}_2(\mathbb{F}_\ell)}$ *denote the projection map, let* $\widetilde{g} \in \widetilde{\mathrm{GL}_2(\mathbb{F}_\ell)}$*, and let* $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$ *such that* $\pi(g) = \widetilde{g}$*. Then* π *induces a bijection*

$$\begin{array}{rccc} \pi_g\colon & \textit{Conjugacy class of } g & \xrightarrow{\sim} & \textit{Conjugacy class of } \widetilde{g} \\ & hgh^{-1} & \longmapsto & \pi(hgh^{-1}). \end{array}$$

Proof. It is clear that the image of the conjugacy class of g by π is exactly the conjugacy class of $\widetilde{g}$, so that π_g is well-defined and surjective. To show that π_g is also injective, let h_1, $h_2 \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that $\pi(h_1 g h_1^{-1}) = \pi(h_2 g h_2^{-1})$, that is to say such that $h_1 g h_1^{-1} = s h_2 g h_2^{-1}$ for some $s \in S$. We must prove that $h_1 g h_1^{-1} = h_2 g h_2^{-1}$. By taking determinants, we see that $\det s = 1$. As s is scalar, this implies $s = \pm 1$. Since $-1 \notin S$, we conclude that $s = 1$, and therefore $h_1 g h_1^{-1} = h_2 g h_2^{-1}$. $\square$

A resolvent $\Gamma_{\widetilde{C}}(X)$ has therefore exactly the same degree as (each of) the corresponding $\Gamma_C(X)$, so we must still use the same very high precision in $\mathbb{C}$ to compute it. However, we have now $|S|$ times less such resolvents to compute. Furthermore, the roots $\sum_{i=1}^n h(a_i)\sigma(a_i)$ of these resolvents actually take $|S|^2$ less time to compute, since they are defined by sums $|S|$ times shorter and there are $|S|$ times less of them.

Using these resolvents $\Gamma_{\widetilde{C}}(X)$, we can then compute the conjugacy class of the image of the Frobenius element Frob_p in $\widetilde{\mathrm{GL}_2(\mathbb{F}_\ell)}$ as above, and, since $-1 \notin S$, we can deduce the similarity class of the image of the Frobenius element in $\mathrm{GL}_2(\mathbb{F}_\ell)$ using our knowledge of its determinant. Consequently, with this trick, we can still compute the full, non-quotient representation $\rho_{f,\mathfrak{l}}$, and we have saved a factor $|S|^2$ in the computation of the roots of the resolvent, and a factor $|S|$ in their expansion and in the identification of their coefficients as rational numbers. Since

$$|S| = \frac{\ell - 1}{2^{\mathrm{ord}_2(\ell-1)}},$$

this prevents this final step of the Galois representation computation from being the slowest one, see the complexity section after the results.

4 Results

We have implemented the above algorithms in [SAGE, version 5.3], and have run them on PlaFRIM, the Bordeaux 1 university computing cluster.

As our algorithms compute the full Galois representation, we get results which are more complete than the ones from [Bos07]. For instance, picking $\ell = 19$ (which implies dealing with genus $g = 7$), we can compute the Galois representation $\rho_{\Delta,19}$ modulo 19 associated to the newform

$$f = \Delta = q \prod_{n=1}^{+\infty} (1 - q^n)^{24} = \sum_{n=1}^{+\infty} \tau(n) q^n$$

of level 1 and weight 12, find the similarity class in $\mathrm{GL}_2(\mathbb{F}_{19})$ of the images of Frobenius elements, and hence find the signs which were missing in the table on the very first page of [EC11] :

- The image of the Frobenius at $p = 10^{1000}+1357$ is similar to $\begin{bmatrix} 17 & 1 \\ 0 & 17 \end{bmatrix}$, therefore $\tau(10^{1000} + 1357) \equiv -4 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000} + 7383$ is similar to $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, therefore $\tau(10^{1000} + 7383) \equiv +2 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+21567$ is similar to $\begin{bmatrix} 11 & 1 \\ 0 & 11 \end{bmatrix}$, therefore $\tau(10^{1000} + 21567) \equiv +3 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+27057$ is similar to $\begin{bmatrix} 10 & 0 \\ 0 & 9 \end{bmatrix}$, therefore $\tau(10^{1000} + 27057) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+46227$ is similar to $\begin{bmatrix} 0 & 14 \\ 1 & 0 \end{bmatrix}$, therefore $\tau(10^{1000} + 46227) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+57867$ is similar to $\begin{bmatrix} 17 & 0 \\ 0 & 2 \end{bmatrix}$, therefore $\tau(10^{1000} + 57867) \equiv 0 \bmod 19$,

- The image of the Frobenius at $p = 10^{1000}+64749$ is similar to $\begin{bmatrix} 13 & 1 \\ 0 & 13 \end{bmatrix}$, therefore $\tau(10^{1000} + 64749) \equiv +7 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+68367$ is similar to $\begin{bmatrix} 14 & 0 \\ 0 & 5 \end{bmatrix}$, therefore $\tau(10^{1000} + 68367) \equiv 0 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+78199$ is similar to $\begin{bmatrix} 15 & 1 \\ 0 & 15 \end{bmatrix}$, therefore $\tau(10^{1000} + 78199) \equiv -8 \bmod 19$,
- The image of the Frobenius at $p = 10^{1000}+128647$ is similar to $\begin{bmatrix} 0 & 8 \\ 1 & 0 \end{bmatrix}$, therefore $\tau(10^{1000} + 128647) \equiv 0 \bmod 19$.

The surprising number of occurrences of non-semi-simple matrices — by the Chebotarev theorem, non-semi-simple matrices should occur with density about $1/\ell$ only — and of $\tau(p) \equiv 0 \bmod 19$ above can be explained by the fact that J. Bosman purposely chose special values of p (cf [BosC7, section 7.4]). For instance, for the other few first primes above 10^{1000}, we have computed the following:

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 19$
$10^{1000}+453$	$\begin{bmatrix} 15 & 0 \\ 0 & 10 \end{bmatrix}$	6
$10^{1000}+2713$	$\begin{bmatrix} 11 & 0 \\ 0 & 4 \end{bmatrix}$	15
$10^{1000}+4351$	$\begin{bmatrix} 6 & 0 \\ 0 & 4 \end{bmatrix}$	10
$10^{1000}+5733$	$\begin{bmatrix} 16 & 0 \\ 0 & 1 \end{bmatrix}$	17
$10^{1000}+10401$	$\begin{bmatrix} 0 & 15 \\ 1 & 8 \end{bmatrix}$	8
$10^{1000}+11979$	$\begin{bmatrix} 16 & 0 \\ 0 & 13 \end{bmatrix}$	10
$10^{1000}+17557$	$\begin{bmatrix} 0 & 5 \\ 1 & 11 \end{bmatrix}$	11
$10^{1000}+22273$	$\begin{bmatrix} 13 & 0 \\ 0 & 1 \end{bmatrix}$	14
$10^{1000}+24493$	$\begin{bmatrix} 14 & 0 \\ 0 & 10 \end{bmatrix}$	5
$10^{1000}+25947$	$\begin{bmatrix} 0 & 4 \\ 1 & 5 \end{bmatrix}$	5
$10^{1000}+29737$	$\begin{bmatrix} 0 & 12 \\ 1 & 7 \end{bmatrix}$	7
$10^{1000}+41599$	$\begin{bmatrix} 18 & 0 \\ 0 & 15 \end{bmatrix}$	14

This agrees with the Chebotarev theorem.

The computation times were as follows: computing the q-expansion of the cuspforms and the Eisenstein series $\big(\text{to } O(q^{5000})\big)$, the period lattice, and finally initialising K. Khuri-Makdisi's algorithms by computing the spaces V and W_0 took 11 minutes, computing the two 19-torsion divisors took 24 minutes each, and computing all the points in the $\mathbb{F}_{19}$-plane spanned by them took about 40 minutes. We found a polynomial $F(X) \in \mathbb{Q}[X]$ defining the representation, of degree $360 = 19^2 - 1$ and with a common denominator of 142 decimal digits, and finally, computing the resolvents $\Gamma_{\widetilde{C}}(X)$ took a little less than 20 minutes thanks to the quotient representation trick and to massive parallelisation, after which deducing the similarity classes of the image of a Frobenius element at $p \approx 10^{1000}$ takes about 30 minutes. Overall, the whole computation thus lasted about 2 hours, thanks to parallelisation. We used a precision of 1500 bits in $\mathbb{C}$ to compute the defining polynomial $F(X)$, and a precision of 600 kbits to compute the resolvents $\Gamma_{\widetilde{C}}(X)$.

Level $\ell = 23$ (genus $g = 12$)

The Galois representation modulo $\ell = 23$ associated to $f = \Delta$ degenerates since its image is a subgroup of $\mathrm{GL}_2(\mathbb{F}_{23})$ isomorphic to $\mathfrak{S}_3$ ([Gro90, top of section 17]). This phenomenon is related to Ramanujan-type congruences for $\tau(n)$ mod 23, cf [EdiC1, top of page 5]. The prime $\ell = 23$ is indeed one of the finitely many primes we have to exclude for $f = \Delta$, as we mentioned in the beginning of the introduction. As a consequence, we computed the representation associated to the newform $f = E_4\Delta$ of level 1 and weight 16 instead. We obtained a defining polynomial $F(X)$ of degree $528 = 23^2 - 1$ with a common denominator of 508 decimal digits. Computing the period lattice took a little less than 2 hours, computing each of the two 23-torsion divisors took 5 hours and a half, and computing the $\mathbb{F}_{23}$-plane spanned by them took a little more than 11 hours. Overall, getting the polynomial $F(X)$ took less than 20 hours. After having computed the resolvents $\Gamma_C(X)$, we got the following results, where we denote the Fourier coefficients of $E_4\Delta$ by $\tau_{16}(n)$:

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p) \bmod 23$
$10^{1000}+453$	$\begin{bmatrix} 15 & 0 \\ 0 & 5 \end{bmatrix}$	20
$10^{1000}+1357$	$\begin{bmatrix} 19 & 0 \\ 0 & 15 \end{bmatrix}$	11
$10^{1000}+2713$	$\begin{bmatrix} 0 & 2 \\ 1 & 12 \end{bmatrix}$	12
$10^{1000}+4351$	$\begin{bmatrix} 0 & 12 \\ 1 & 16 \end{bmatrix}$	16
$10^{1000}+5733$	$\begin{bmatrix} 18 & 0 \\ 0 & 14 \end{bmatrix}$	9
$10^{1000}+7383$	$\begin{bmatrix} 13 & 0 \\ 0 & 6 \end{bmatrix}$	19
$10^{1000}+10401$	$\begin{bmatrix} 0 & 16 \\ 1 & 19 \end{bmatrix}$	19
$10^{1000}+11979$	$\begin{bmatrix} 15 & 0 \\ 0 & 7 \end{bmatrix}$	22
$10^{1000}+17557$	$\begin{bmatrix} 0 & 22 \\ 1 & 15 \end{bmatrix}$	15
$10^{1000}+21567$	$\begin{bmatrix} 0 & 17 \\ 1 & 15 \end{bmatrix}$	15
$10^{1000}+22273$	$\begin{bmatrix} 17 & 0 \\ 0 & 5 \end{bmatrix}$	22

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p) \bmod 23$
$10^{1000} + 24493$	$\begin{bmatrix} 8 & 0 \\ 0 & 5 \end{bmatrix}$	13
$10^{1000} + 25947$	$\begin{bmatrix} 21 & 0 \\ 0 & 13 \end{bmatrix}$	11
$10^{1000} + 27057$	$\begin{bmatrix} 8 & 0 \\ 0 & 2 \end{bmatrix}$	10
$10^{1000} + 29737$	$\begin{bmatrix} 0 & 6 \\ 1 & 11 \end{bmatrix}$	11
$10^{1000} + 41599$	$\begin{bmatrix} 20 & 0 \\ 0 & 7 \end{bmatrix}$	4
$10^{1000} + 46227$	$\begin{bmatrix} 9 & 0 \\ 0 & 2 \end{bmatrix}$	11
$10^{1000} + 57867$	$\begin{bmatrix} 0 & 2 \\ 1 & 7 \end{bmatrix}$	7
$10^{1000} + 64749$	$\begin{bmatrix} 0 & 12 \\ 1 & 7 \end{bmatrix}$	7
$10^{1000} + 68367$	$\begin{bmatrix} 0 & 20 \\ 1 & 21 \end{bmatrix}$	21
$10^{1000} + 78199$	$\begin{bmatrix} 0 & 2 \\ 1 & 17 \end{bmatrix}$	17
$10^{1000} + 128647$	$\begin{bmatrix} 6 & 0 \\ 0 & 4 \end{bmatrix}$	10

Level $\ell = 29$ (genus $g = 22$)

We have also computed the polynomial $F(X)$ for the Galois representation modulo $\ell = 29$ associated to $f = \Delta$, which took about 10 days. This polynomial has degree $840 = 29^2 - 1$, and a common denominator of 1793 decimal digits. Computing the periods took a little more than 6 hours, computing each of the two 29-torsion divisors took 120 hours, and computing the $\mathbb{F}_{29}$-plane spanned by them took about 100 hours.

Then, thanks to the quotient representation trick, computing the resolvents $\Gamma_{\widetilde{C}}(X)$ took about 60 hours, and finally, deducing the image of the Frobenius at the same primes $p \approx 10^{1000}$ as in level 19 took 2 hours. Overall, the whole computation thus took less than two weeks.

We used a precision of 15 kbits in $\mathbb{C}$ for the computation of the defining polynomial $F(X)$, and a precision of 18 Mbits for the computation of the resolvents $\Gamma_{\widetilde{C}}(X)$.

Our results are the following :

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 29$
$10^{1000}+453$	$\begin{bmatrix} 0 & 5 \\ 1 & 21 \end{bmatrix}$	21
$10^{1000}+1357$	$\begin{bmatrix} 0 & 28 \\ 1 & 8 \end{bmatrix}$	8
$10^{1000}+2713$	$\begin{bmatrix} 0 & 9 \\ 1 & 11 \end{bmatrix}$	11
$10^{1000}+4351$	$\begin{bmatrix} 0 & 26 \\ 1 & 0 \end{bmatrix}$	0
$10^{1000}+5733$	$\begin{bmatrix} 20 & 0 \\ 0 & 2 \end{bmatrix}$	22
$10^{1000}+7383$	$\begin{bmatrix} 19 & 0 \\ 0 & 10 \end{bmatrix}$	0
$10^{1000}+10401$	$\begin{bmatrix} 7 & 0 \\ 0 & 2 \end{bmatrix}$	9
$10^{1000}+11979$	$\begin{bmatrix} 0 & 7 \\ 1 & 7 \end{bmatrix}$	7
$10^{1000}+17557$	$\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$	0
$10^{1000}+21567$	$\begin{bmatrix} 23 & 0 \\ 0 & 3 \end{bmatrix}$	26
$10^{1000}+22273$	$\begin{bmatrix} 0 & 26 \\ 1 & 14 \end{bmatrix}$	14

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 29$
$10^{1000} + 24493$	$\begin{bmatrix} 0 & 13 \\ 1 & 4 \end{bmatrix}$	4
$10^{1000} + 25947$	$\begin{bmatrix} 27 & 0 \\ 0 & 15 \end{bmatrix}$	13
$10^{1000} + 27057$	$\begin{bmatrix} 0 & 6 \\ 1 & 7 \end{bmatrix}$	7
$10^{1000} + 29737$	$\begin{bmatrix} 23 & 0 \\ 0 & 10 \end{bmatrix}$	4
$10^{1000} + 41599$	$\begin{bmatrix} 13 & 0 \\ 0 & 5 \end{bmatrix}$	18
$10^{1000} + 46227$	$\begin{bmatrix} 0 & 26 \\ 1 & 22 \end{bmatrix}$	22
$10^{1000} + 57867$	$\begin{bmatrix} 13 & 0 \\ 0 & 11 \end{bmatrix}$	24
$10^{1000} + 64749$	$\begin{bmatrix} 0 & 1 \\ 1 & 15 \end{bmatrix}$	15
$10^{1000} + 68367$	$\begin{bmatrix} 0 & 3 \\ 1 & 3 \end{bmatrix}$	3
$10^{1000} + 78199$	$\begin{bmatrix} 17 & 0 \\ 0 & 14 \end{bmatrix}$	2
$10^{1000} + 128647$	$\begin{bmatrix} 0 & 27 \\ 1 & 24 \end{bmatrix}$	24

Putting together the results in level $\ell = 19$ and $\ell = 29$, we see that $\tau(p) \neq 0$ for each value of p we have tested. This agrees with Lehmer's conjecture.

Complexity estimates

The most time-consuming part of the computation of the polynomial $F(X) \in \mathbb{Q}[X]$ defining the representation is the arithmetic in the jacobian $J_1(\ell)$. To perform these operations, K. Khuri-Makdisi's algorithms rely on linear algebra on matrices of size $O(g) \times O(g)$; as $g = O(\ell^2)$, and we have $O(\ell^2)$ points to compute in the jacobian, this implies a complexity of $O(\ell^8)$ operations in $\mathbb{C}$ to compute the Galois representation. Let H be the logarithm of the common denominator of $F(X)$, so that computing $F(X)$ with our method requires a precision of $O(H)$ bits in $\mathbb{C}$. Then the complexity of our method to find $F(X)$ is $\widetilde{O}(\ell^8 H)$ bit operations. The experiments we have run seem to indicate that H is $O(\ell^3)$, but we do not try to refine this estimate, because we do not know a proven sharp bound on H.

Next, if we do not use the quotient representation trick (cf section 3.7.2), computing a root $\sum_{i=1}^{n} h(a_i)\sigma(a_i)$ of a Dokchitsers' resolvent $\Gamma_C(X)$ requires $O(n) = O(\ell^2)$ operations in $\mathbb{C}$. As there is one such root for each $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)$, computing all these roots requires $O(\ell^6)$ operations in $\mathbb{C}$. Then, computing a resolvent $\Gamma_C(X)$ from its roots requires $\widetilde{O}\big(\deg \Gamma_C(X)\big) = \widetilde{O}(\ell^2)$ operations in $\mathbb{C}$ using a fast Fourier transform. As there are $O(\ell^2)$ similarity classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$, we see that computing all the resolvents $\Gamma_C(X)$ from their roots requires $\widetilde{O}(\ell^4)$ operations in $\mathbb{C}$. Thus computing all the resolvents overall requires $O(\ell^6)$ operations in $\mathbb{C}$, the slow part being the computation of their roots. The precision in $\mathbb{C}$ we have to work at for this is $O(\ell^2 H)$, so that the total complexity of the computation of the resolvents $\Gamma_C(X)$ is $\widetilde{O}(\ell^8 H)$ bit operations, which is the same as the rest of the computation.

However, with the quotient representation trick, computing the resolvent roots $\sum_{i=1}^{n} h(a_i)\sigma(a_i)$ requires only $O(\ell^6/|S|^2) = O(\ell^4 \ell_2^2)$ operations in $\mathbb{C}$, where $\ell_2 = 2^{\mathrm{ord}_2(\ell-1)}$ is the 2-primary part of ℓ, and then computing the resolvents $\Gamma_{\widetilde{C}}(X)$ from these roots takes only $\widetilde{O}(\ell^4/|S|) = \widetilde{O}(\ell^3 \ell_2)$ operations in $\mathbb{C}$. Therefore, computing the resolvents $\Gamma_{\widetilde{C}}(X)$ overall requires $\widetilde{O}(\ell^6 \ell_2^2 H)$ bit operations, since the precision in $\mathbb{C}$ we have to work at is still $O(\ell^2 H)$. So, for instance, the use of this trick allows us to reduce the complexity of the computation of the resolvents $\Gamma_{\widetilde{C}}(X)$ by a factor ℓ^2 if we restrict to the primes $\ell \equiv -1 \bmod 4$. Note that restricting to such ℓ does not worsen the complexity of the computation of coefficients a_p of f by Chinese remainders. On the other hand, in the worst cases $\ell = 2^\lambda + 1$ for some $\lambda \in \mathbb{N}$, this trick unfortunately does not help at all.

References

[Abr96] Abramovich, Dan, **A linear lower bound on the gonality of modular curves**. Internat. Math. Res. Notices 1996, no. 20, 10051011.

[AG90] Allgower, Eugene L.; Georg, Kurt, **Introduction to numerical continuation methods**. Reprint of the 1990 edition [Springer-Verlag, Berlin; MR1059455 (92a:65165)]. Classics in Applied Mathematics, 45. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2003. xxvi+388 pp. ISBN:0-89871-544-X.

[AL78] Atkin, A. O. L.; Li, Wen Ch'ing Winnie, **Twists of newforms and pseudo-eigenvalues of W-operators**. Invent. Math. 48 (1978), no. 3, 221–243.

[Bos07] Bosman, Johan, **On the computation of Galois representations associated to level one modular forms**. arXiv:0710.1237

[Bos07a] Bosman, Johan, **A polynomial with Galois group $SL_2(\mathbb{F}_{16})$**. LMS J. Comput. Math. 10 (2007), 1461–1570.

[Bos11] Bosman, Johan, **Modular forms applied to the computational inverse Galois problem**. arXiv:1109.6879

[BosC6] Bosman, Johan, **Computations with modular forms and Galois representations**. Chapter 6 of the book [EC11].

[BosC7] Bosman, Johan, **Polynomials for projective representations of level one forms**. Chapter 7 of the book [EC11].

[CEC3] Couveignes, Jean-Marc; Edixhoven, Bas, **First description of the algorithms**. Chapter 3 of the book [EC11].

[CouC12] Couveignes, Jean-Marc, **Approximating V_f over the complex numbers**. Chapter 12 of the book [EC11].

[CouC13] Couveignes, Jean-Marc, **Computing V_f modulo p**. Chapter 13 of the book [EC11].

[Cre97] Cremona, J. E., **Algorithms for modular elliptic curves**. Second edition. Cambridge University Press, Cambridge, 1997. vi+376 pp. ISBN: 0-521-59820-6.

[CR62] Curtis, Charles W.; Reiner, Irving, **Representation theory of finite groups and associative algebras**. Pure and Applied Mathematics, Vol. XI Interscience Publishers, a division of John Wiley & Sons, New York-London. 1962, xiv+685 pp.

[Del71] Deligne, Pierre, **Formes modulaires et représentations l-adiques**. Lecture Notes in Math. 179 (1971), pp 139–172.

[Dok10] Dokchitser, Tim and Vladimir, **Identifying Frobenius elements in Galois groups**. September 2010 preprint, to appear in Algebra and Number Theory.

[DS05] Diamond, Fred; Shurman, Jerry, **A first course in modular forms**. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp. ISBN: 0-387-23229-X.

[EC11] **Computational aspects of modular forms and Galois representations**. Edited by Bas Edixhoven and Jean-Marc Couveignes, with contributions by Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong, and Franz Merkl. Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, NJ, 2011.

[Edi92] Edixhoven, Bas, **The weight in Serre's conjectures on modular forms**. Invent. Math. 109 (1992), no. 3, 563–594.

[EdiC1] Edixhoven, Bas, **Introduction, main results, contexts**. Chapter 1 of the book [EC11].

[EdiC14] Edixhoven, Bas, **Computing the residual Galois representations**. Chapter 14 of the book [EC11].

[EdJC11] Edixhoven, Bas; de Jong, Robin, **Bounds for Arakelov invariants of modular curves**. Chapter 11 of the book [EC11].

[GG99] von zur Gathen, Joachim; Gerhard, Jürgen, **Modern computer algebra**. Cambridge University Press, New York, 1999. xiv+753 pp. ISBN: 0-521-64176-4.

[Gro90] Gross, Benedict H., **A tameness criterion for Galois representations associated to modular forms (mod p)**. Duke Math. J. 61 (1990), no. 2, 445–517.

[HW08] Hardy, G. H.; Wright, E. M., **An introduction to the theory of numbers**. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp. ISBN: 978-0-19-921986-5.

[HS00] Hindry, Marc; Silverman, Joseph H., **Diophantine geometry - An introduction**. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1.

[KW09] Khare, Chandrashekhar; Wintenberger, Jean-Pierre, **Serres modularity conjecture (I and II)**. Inventiones Mathematicae 178 (3), 485–504 and 505–586.

[KM04] Khuri-Makdisi, Kamal, **Linear algebra algorithms for divisors on an algebraic curve**. Math. Comp. 73 (2004), no. 245, 333–357.

[KM07] Khuri-Makdisi, Kamal, **Asymptotically fast group operations on Jacobians of general curves**. Math. Comp. 76 (2007), no. 260, 2213–2239.

[Lan95] Lang, Serge, **Introduction to modular forms**. With appendices by D. Zagier and Walter Feit. Corrected reprint of the 1976 original. Grundlehren der Mathematischen Wissenschaften, 222. Springer-Verlag, Berlin, 1995. x+261 pp. ISBN: 3-540-07833-9.

[Rib85] Ribet, Kenneth A., **On l-adic representations attached to modular forms II**. Glasgow Math. J. 27 (1985), 185–194.

[SAGE] **SAGE mathematics software**. `http://sagemath.org/`

[Sch95] Schoof, René, **Counting points on elliptic curves over finite fields**. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993). J. Théor. Nombres Bordeaux 7 (1995), no. 1, 219–254.

[Ser87] Serre, Jean-Pierre, **Sur les représentations modulaires de degré 2 de** $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. Volume 54, Number 1 (1987), 179–230.

[Sop10] Soprounov, Ivan, **A short proof of the Prime Number Theorem for arithmetic progressions**. 2010 preprint available at http://academic.csuohio.edu/soprunov_i/pdf/primes.pdf

[Ste07] Stein, William, **Modular forms, a computational approach**. With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007. xvi+268 pp. ISBN: 978-0-8218-3960-7; 0-8218-3960-8.

[Swi72] Swinnerton-Dyer, H. P. F., **On ℓ-adic representations and congruences for coefficients of modular forms**. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1–55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[Zen12] Zeng, Jinxiang, **On the computation of coefficients of modular forms: the p-adic approach**. arXiv:1211.1124