Computational aspects of modular forms and Galois representations

Authors: Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, Johan Bosman

Reviewer: Capi Corrales Rodrigáñez, Department of Algebra, Mathematics, UCM, Madrid

"Modular forms are functions on the complex plane which are inordinately symmetric. They satisfy so many internal symmetries that their mere existence seems like an accident. But they do exist." (Barry Mazur interviewed by Simon Singh in *Fermat's Last Theorem*, BBC series Horizon, 1996.

"Modular forms can be viewed as functions on the set of elliptic curves with level structure. Modular forms can be viewed as pluricanonical forms on modular curves. By a construction of Eichler and Shimura, modular forms of weight 2 give rise to elliptic curves and abelian varieties. By the Taniyama-Shimura conjecture, elliptic curves give rise to modular forms of weight 2. By a construction of Pierre Deligne, modular forms give rise to two-dimensional p-adic Galois representations. Modular forms are a kind of automorphic form and thus give rise to automorphic representations." (Tom Weston, www.math.umass.edu/ weston/rs/mf.html)

Modular forms are complex analytic functions on the upper half plane satisfying certain conditions. Among other properties, they admit a Fourier expansion with coefficients having deep arithmetic significance, as illustrated by the nicest example of a modular form, involving Ramanujan's tau-function, which Ramanujan introduced in 1916 in the process of studying the representation of integers as sums of twenty four squares. Ramanujan's interest in the problem of representing integers as sums of squares is well known.

"I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways." " (G.H. Hardy, *Ramanujan*, London 1940)

In his most famous article ([3]), Ramanujan introduced the function $\tau : \mathbb{N} \to \mathbb{Z}$ by means of the equality

$$\sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{m=1}^{\infty} (1-q^m)^{24}, \ q = e^{2\pi i z}, z \in \mathcal{H}. \tag{1}$$

and he conjectured that $\tau(mn) = \tau(n)\tau(m)$ when n and m are relatively prime integers, and also that for each prime p, one has $|\tau(p)| < 2p^{11/2}$. The first of these properties was proved by Mordell in 1928 and the second one by Deligne in 1974, as a consequence of his proof of the Weil Conjectures. The product formula (1) for the Fourier expansion of τ, allows us to compute easily the first few coefficients, but it is very unpractical if we want to compute the pth coefficients for a very large p. Thus, from a computational point of view this product formula is quite useless.

Prior to the book under review, the fastest known algorithms for computing these Fourier coefficients took exponential time in $\log p$. Couveignes, Edixhoven and their collaborators present a deterministic polynomial time algorithm for computing coefficients of modular forms of level one in polynomial time which, for example, allows us to compute $\tau(p)$ in time bounded by a fixed power of the logarithm of the prime p. Such fast computation of Fourier coefficients is itself based on the main result of the book: the computation, in polynomial time, of Galois representations over finite fields attached to modular forms, a result which has been described as the start of an explicit Langlands program.

Just as our first example of a modular form, this book on modular forms is attached to a taxi ride: it gives an answer to a question raised in a Chicago taxi cab by Henri Cohen, Noam Elkies and René Schoof, during the celebration of the Atkin Conference in 1997. Let us start by first framing and then phrasing the question. References for the details of what follows can be found in [1] and [4].

1 Framing the taxi question: some definitions.

Let $\mathcal{H}$ denote the complex upper half-plane consisting of complex numbers with positive imaginary part. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ by fractional linear transformations, with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acting as $z \mapsto \frac{az+b}{cz+d}$.

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is said to be a congruence subgroup of level N if it contains $\Gamma(N)$ for some positive integer N, where

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod} N) \right\}$$

is called the principal congruence subgroup of level N. For example,

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod} N) \right\}$$

is a congruence subgroup containing $\Gamma(N)$.

Let k be a non-negative integer and Γ a congruence subgroup of level N. By a modular form of weight k with respect to Γ we mean a function $f : \mathcal{H} \to \mathbb{C}$ satisfying:

(i) f is holomorphic on H;

(ii) $(cz+d)^{-k} f(\gamma(z)) = f(z)$, all $z \in \mathcal{H}, \gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma$;

(iii) f is holomorphic at the cusps.

Let us explain this last condition. The group Γ contains a matrix $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ for some positive integer h, and so we have $f(z+h) = f(z)$. Thus, f has a Fourier expansion at ∞ of the type

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q_h^n, \; q_h = e^{\frac{2\pi i z}{h}} \tag{2}$$

We say that f is holomorphic (resp. vanishes) at the cusps if for all $\alpha = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ the function on $\mathcal{H}$ defined by $z \mapsto \det(\alpha)^{k-1}(cz+d)^{-k} f(\alpha(z))$, is holomorphic (resp. vanishes) at ∞. In order for f to be holomorphic (resp. vanish) at the cusps, we must have $a_n = 0$ for all $n < 0$ in (2) (resp. $n \leq 0$), and this condition is independent of the choice of h.

Let f be a modular form of weight k with respect to $\Gamma_0(N)$ that vanishes at the cusps and is normalized so that its Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n q^n,\ z \in \mathcal{H}, q = e^{2\pi i z}$$

satisfies $a_1 = 1$ and $a_{nm} = a_n a_m$ if $\gcd(n, m) = 1$. The coefficients a_n are algebraic integers, but not necessarily ordinary integers. The subfield K_f of $\mathbb{C}$ generated by the a_n is a number field, i.e., a finite extension of $\mathbb{Q}$, and the a_n lie in its integer ring $\mathcal{O}_f$. The Galois group $\mathrm{Gal}(K_f/\mathbb{Q})$ respects $\mathcal{O}_f$, so one obtains an induced action of $\mathrm{Gal}(K_f/\mathbb{Q})$ on the set of ideals of $\mathcal{O}_f$. Shimura associates to f and abelian variety (i.e., a projective variety endowed with a group law) A_f defined over $\mathbb{Q}$ whose dimension is the degree $[K_f : \mathbb{Q}]$ and which can be used to find a set of group representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ indexed by the prime ideals of $\mathcal{O}_f$: let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_f$; its residue field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_f/\mathfrak{p}$ is a finite field of characteristic p for some prime p. Using the abelian variety A_f, one can find a semisimple group representation $\rho_{f,\mathfrak{p}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$ which is characterized by the following property: if l is a prime number not dividing pN, then the image under $\rho_{f,\mathfrak{p}}$ of the element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ known as Frob_l (uniquely defined up to conjugacy), is a matrix with trace a_l mod $\mathfrak{p}$ and determinant l mod $\mathfrak{p}$.

2 The taxi question

Let f be a modular form of weight 2 with respect to $\Gamma_0(N)$ that vanishes at the cusps and is normalized so that its Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n q^n,\ z \in \mathrm{H}, q = e^{2\pi i z}$$

satisfies $a_1 = 1$, $a_{nm} = a_n a_m$ if $\gcd(n, m) = 1$ and $a_{p^{r+1}} = a_p a_{p^r} - p a_{p^{r-1}}$.

If the Fourier coefficients a_n of f are ordinary integers, then $K = \mathbb{Q}$ and the associated abelian variety A_f has dimension 1. This means that in this case A_f is simultaneously an abelian variety and a curve, what is known as an elliptic curve. According to a theorem of Eichler and Shimura, the coefficients a_p of f are reflected in the arithmetic of the elliptic cuve A_f in the following way: for each prime p not dividing N, its Weiestrass (minimal) equation, when viewed mod p, yields an elliptic curve over the finite field $\mathbb{Z}/p\mathbb{Z}$ and the number of points on this elliptic curve is given by $p + 1 - a_p$. Therefore, in this case computing the Fourier coefficient a_p of the modular form f is the same as counting the number of points on the elliptic curve A_f over the finite field $\mathbb{Z}/p\mathbb{Z}$, something which can be done in polynomial time using Schoof's deterministic algorithm ([5], [6]).

"Abstract. In this paper we present a deterministic algorithm to compute the number of $\mathbb{F}_q$-points on an elliptic curve that is defined over a finite field $\mathbb{F}_q$ and which is given by a Weierstrass equation. The algorithm takes $O(\log^9 q)$ elementary operations. As an application we give an algorithm to compute square roots mod p. For fixed $x \in \mathbb{Z}$, it takes $O(\log^9 p)$ elementary operations to compute $\sqrt{x}$ mod p." (René Schoof, [6]).

If the Fourier coefficients a_n of f are not rational integers, then the abelian variety A_f has dimension higher than 1, and one needs consider the group representations $\rho_{f,\mathfrak{p}}$ in order to compute the Fourier coefficients a_p. For modular forms of weight 2, this can be done in polynomial time using Pila's algorithm.

"Abstract. We give a generalization to Abelian varieties over finite fields of the algorithm of Schoof for elliptic curves. Schoof showed that for an elliptic curve E over $\mathbb{F}_q$, given by a Weierstrass equation, one can compute the number of $\mathbb{F}_q$ rational points of E in time $O((\log q)^9)$. Our result is the following. Let A be an Abelian variety over $\mathbb{F}_q$. Then one can compute the characteristic polynomial of the Frobenius endomorphism of A in time $O((\log p)^{\Delta})$, where Δ and the implied constant depend only on the dimension of the embedding space of A, the number of equations defining A and the addition law, and their degrees. The method, generalizing that of Schoof, is to use the machinery developed by Weil to prove the Riemann hypothesis for Abelian varieties. By means of this theory, the calculation is reduced to ideal-theoretic computations in a ring of polynomials in several variables over $\mathbb{F}_q$. As applications we show how to count the rational points on the reductions modulo primes p of a fixed curve over $\mathbb{Q}$ in time polynomial in $\log p$; we show also that, for a fixed prime l, we can compute the l-th roots of unity mod p, when they exist, in polynomial time in $\log p$. This generalizes Schoof's application of his algorithm to find square roots of a fixed integer x mod p." (Jonathan Pila, [2])

The question raised by Cohen, Elkies and Schoof during their taxi ride along the streets of Chicago in 1997 is the following: Could this situation be generalized to modular forms of weight larger that 2? Could it be possible to construct a polinomial time algorithm for computing the coefficients of a modular form of weight larger than 2?

3 The book

As we find in this book, for modular forms of level one the answer to the taxi question is yes: there is a polynomial time algorithm invented by Couveignes and Edixhoven (and Bosman, De Jong and Merkl) that determines the coefficients of almost all such forms in polynomial time.

"Preface. This is a book about computational aspects of modular forms and the Galois representations attached to them. The main result is the following: Galois representations over finite fields attached to modular forms of level one can, in almost all cases, be computed in polynomial time in the weight and the size of the finite field. As a consequence, coefficients of modular forms can be computed fast via congruences, as in Schoof's algorithm for computing the number of points of elliptic curves over finite fields. The most important feature of the proof of the main result is that exact computations involving systems of polynomial equations in many variables are avoided by approximations and height bounds, that is, bounds for the accuracy that is necessary to derive exact values from the approximations." (Jean-Marc Couveignes, Bass Edixhoven, Preface to [1]).

The book, highly technical, gives a nice exposition of the material involved and should be accessible to graduate students or researchers with a sufficient background in number theory and algebraic geometry. It is well written and is divided into fifteen chapters. The first three give us an introduction to the subject, precise statements of the main results, the necessary background concerning modular curves and modular forms and a first informal description of the algorithms. The rest of the book is dedicated to presenting the tools and main ingredients for the proof of the main result (which can be found in Chapter 14) and some real computations of Galois representations attached to modular forms (Chapters 6, 7 and 15).

As a nice application of the algorithm described in the book, in the last chapter the special case of the modular form of weight 12 associated to Ramanujans's function is discussed.

To compute $\tau(p)$ mod l, the algorithm makes use of a certain two-dimensional $\mathbb{Z}/l\mathbb{Z}$- vector space V_l: for several small primes l they compute the action of the Frobenius endomorphism φ on V_l, an endomorphism with characteristic polynomial $X^2 - tX + p^{11}$, where $t \equiv \tau(p) \pmod{l}$.

As explained by René Schoof in the Workshop on Elliptic Curves and Computation which took place in 2010 at Microsoft Research in Redmond (see [7]), the key problem lies in the identification of the vector space V_l, an object which, having been first guessed by Serre in 1967 (see [8]) was defined by Deligne in 1969 as the 11th- étale cohomology group of the 10-th fold product $E^{(10)}$ of the universal elliptic curve with values in $\mathbb{Z}/l\mathbb{Z}$; that is, $V_l = H^{11}_{et}(E^{(10)}, \mathbb{Z}/l\mathbb{Z})$ an object which, somewhat more explicitly, is also equal to $V_l = H^1_{et}(\mathbb{P}^1, F)$ for some étale sheaf F. Unfortunately this definition is too abstract to be put in a computer. This illustrates the difficulty in the generalization of Schoof and Pila's algorithms to modular forms of higher weights: the fact that the definition of the two-dimensional vector spaces one must work on are too abstract.

Couveignes and Edixhoven solve the problem by identifying Deligne's vector space V_l as a subspace the cohomology group $H^1_{et}(X_1(l), \mathbb{Z}/l\mathbb{Z})$ of the modular curve $X_1(l)$. In other words V_l is a subspace of the l-torsion points of the Jacobian $J_1(l)$ of the modular curve $X_1(l)$. And this they can compute.

References

[1] Jean-Marc Couveignes, Bas Edixhoven (eds.), *Computational aspects of modular forms and Galois representations*,

[2] Jonathan Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. 55:192 (1990), 745-763.

[3] Srinivasan Ramanujan, *On certain arithmetical functions*, Trans. Camb. Phil. Soc. 22 (1916), pp 159-184.

[4] Kenneth A. Ribet, *Galois representations and modular forms*, Bulletin of the AMS vol. 32, no. 4 (1995), 375-402.

[5] René Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombre de Bordeaux **7** (1995), 219-254.

[6] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. 44 (1985), 483- 494.

[7] René Schoof, *Counting points on elliptic curves and beyond*, http://research.microsoft.com/apps/video/dl.aspx?id=140499

[8] Jean-Pierre Serre *Une interprétation des congruences relatives à la fonction de Ramanujan*, Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, no. 1 (1967-68), exp. 14, 1-17.