APPLICATIONS OF MASSIVE COMPUTATIONS: THE ARTIN CONJECTURE.

IAN KIMING

1. Introduction.

This lecture presents an overview of a joint work with J. Basmaji, G. Frey, X. Wang (all at IEM, Univ. Essen) and L. Merel (Paris). Details and numerical results will appear elsewhere.

1.1. The work concerns the simplest in general unproved case of 'Langlands' philosophy':

Consider equivalence classes of 2-dimensional, irreducible, continuous, odd Galois representations over $\mathbb{Q}$:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

with Artin conductor $N(\in \mathbb{N})$ and determinant character $\det \rho = \varepsilon$. Here $\mathbb{C}$ is endowed with the discrete topology and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has the natural topology as a profinite group so that 'continuous' implies 'having finite image'. The determinant character $\det \rho$ is the character on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ obtained by composing ρ with the determinant homomorphism

$$\det : \mathrm{GL}_2(\mathbb{C}) \longrightarrow \mathbb{C}^\times .$$

Then $\varepsilon = \det \rho$ is a character on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with class field theoretic conductor dividing N, and that ρ is odd means that ε has value -1 at a Frobenius infinity. By class field theory we may identify ε with a Dirichlet character modulo N which we will do in the following. With this identification, ρ is odd if and only if $\varepsilon(-1) = -1$.

It is conjectured that these equivalence classes are in 1-1 correspondence with the normalized newforms $f(z)$ of weight 1 and nebentypus ε on the congruence group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \ c \equiv 0 \quad (N) \right\}$$

(see for example [9] for definitions). More explicitly one expects the Fourier coefficients of f at ∞:

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

to coincide with the coefficients of the Artin L-series of ρ:

$$L(s, \rho) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad \mathrm{Re}(s) > 1.$$

The arithmetical interest of this conjecture is that it will, if true, constitute a natural extension of class field theory to a truly non-abelian situation.

A deep theorem of Deligne and Serre (cf. [3]) states that if $f(z) = \sum a_n q^n$ is a normalized newform on $\Gamma_0(N)$ of weight 1 and nebentypus ε, then there is a representation ρ of the above type with Artin conductor N, determinant character ε and Artin L-series $L(s,\rho) = \sum a_n n^{-s}$ (for $\mathrm{Re}(s) > 1$). A classical theorem of Hecke (cf. for example [9], chap. 4) now implies that this L-series, enlarged by the usual Γ-factor, has a holomorphic continuation to the whole complex plane.

With this, a theorem of Weil (cf. [16] or [7]) shows that the above conjecture conjunctively for all 2-dimensional, irreducible, continuous, odd representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is equivalent to the Artin conjecture for these representations. Recall that the Artin conjecture for the considered representations claims the existence of a holomorphic continuation of the associated (enlarged) Artin L-series. For more information in this connection the reader is referred to [11].

We want to make it clear that from an arithmetical point of view, the interest is not attached to the Artin conjecture itself. The Artin conjecture (in our case) should rather be regarded as a concentrated way of expressing a very deep conjecture of a truly arithmetical (and *not* analytical) nature.

1.2. Let us now introduce the following notation:

Fix $N \in \mathbb{N}$ and let ε be a Dirichlet character modulo N with $\varepsilon(-1) = -1$. Let $d(N,\varepsilon)$ denote the number of equivalence classes of irreducible, continuous, 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with Artin conductor N and determinant character ε. (This number is obviously finite.) Further let $S_1^+(N,\varepsilon)$ denote the complex vector space generated by the (finite number of) newforms of weight 1 and nebentypus ε on $\Gamma_0(N)$. From the discussion in 1.1 it follows that

$$(*) \qquad \dim S_1^+(N,\varepsilon) \le d(N,\varepsilon),$$

and that equality holds if and only if the conjecture in 1.1 is true for all representations ρ of the above type with Artin conductor N and determinant character ε. Hence this conjecture may be verified for all such representations simultaneously by computing the numbers $\dim S_1^+(N,\varepsilon)$ and $d(N,\varepsilon)$ and showing that they are equal. However, as we shall see, the question of determining these numbers leads to theoretical problems of independent interest. Before we proceed to the consideration of these, we shall briefly review in what cases the conjectured equality in $(*)$ is known to hold.

Together with a representation ρ of the above type, we consider its projectivisation

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{C})$$

obtained by composing ρ with the canonical homomorphism $\mathrm{GL}_2(\mathbb{C}) \longrightarrow \mathrm{PGL}_2(\mathbb{C})$. For group theoretical reasons the (finite) image of $\overline{\rho}$ is either isomorphic to a cyclic group, to a dihedral group, to the alternating group A_4, to the symmetric group S_4, or to the alternating group A_5, where however the cyclic case is excluded since ρ was assumed to be irreducible. We shall distinguish these cases by saying that ρ is of dihedral-, A_4-, S_4-, or A_5-type respectively.

Now, if ρ is of dihedral type, then one may by class field theory show that ρ is associated with a newform as in 1.1. By deep results of Langlands and Tunnell (cf. [6] and [14]) this is also the case if ρ is of A_4- or S_4-type. Thus the question of equality in $(*)$ is only of interest if there exists a ρ of A_5-type with Artin conductor N and determinant character ε. Here the question of computational verification of equality in $(*)$ (for some numerical cases) turns up, since the methods in [6] and [14] for associating a newform to a ρ of type A_4 or S_4 do not work, and cannot be made to work, in the case of a ρ of type A_5. We note that there is in the literature such a computational verification only for one single numerical case (cf. [1]; here $N = 800$). The method in [1] can however not be described as an algorithm.

This discussion may now serve as motivation for the following objectives:

(1) To develop an algorithm for verifying equality in $(*)$ (given N and ε). As has already been noted this leads to theoretical problems of independent interest.

(2) To provide more non-trivial examples of equality in $(*)$.

We proceed now to sketch the solution which has been obtained for (1).

2. Computation of $d(N, \varepsilon)$

2.1. We fix $N \in \mathbb{N}$ and ε a character on the idele class group of $\mathbb{Q}$ with conductor dividing N. In this section there is no reason to restrict our attention to the case of an odd ε. Furthermore, we shall fix a 2-dimensional, irreducible, continuous, projective representation

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{C}).$$

The image of $\bar{\rho}$ is finite, and we let K be the fixed field of the kernel of $\bar{\rho}$. Thus $\bar{\rho}$ may be perceived as a finite Galois extension $K/\mathbb{Q}$ together with an imbedding

$$\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{PGL}_2(\mathbb{C}).$$

In this section we want to ask the following question: What is the number of inequivalent *liftings* of $\bar{\rho}$, i.e. continuous representations ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{C})$ with Artin conductor N and determinant character ε, such that

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[d, "\rho"'] \arrow[dr, "\bar{\rho}"] & \\
\mathrm{GL}_2(\mathbb{C}) \arrow[r] & \mathrm{PGL}_2(\mathbb{C})
\end{tikzcd}$$

commutes?

2.2. We want to reduce this question to an analogous local one. For this purpose we introduce the following notation: For each prime number p denote by D_p resp. I_p the decomposition resp. inertia group of a place of $\mathbb{Q}$ above p; we identify D_p with $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Now consider the following theorem of Tate (cf. [11]):

Theorem. *(Tate): Let* $\theta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_n(\mathbb{C})$ *be an n-dimensional, continuous, projective representation. Suppose that for each prime number p there is given* *a continuous representation* $\theta_p : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ *which is a lifting of the restriction* $\bar{\theta} \mid D_p$*, i.e.*

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \arrow[d, "\theta_p"'] \arrow[dr, "\bar{\theta}|D_p"] & \\
\mathrm{GL}_n(\mathbb{C}) \arrow[r] & \mathrm{PGL}_n(\mathbb{C})
\end{tikzcd}$$

commutes, and such that the restriction $\theta_p \mid I_p$ *is trivial for almost all* p*.(Here* $\mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathrm{PGL}_n(\mathbb{C})$ *is the canonical projection.)*

Then there is a unique lifting $\theta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ *of* $\bar{\theta}$ *such that*

$$\theta \mid I_p = \theta_p \mid I_p \quad \textit{for all } p.$$

The theorem follows from another theorem of Tate on the vanishing of the Schur multiplier of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ together with the fact that $\mathbb{Q}$ has class number 1.

This theorem allows us to reduce the question in 2.1 to certain analogous local problems: Let $\bar{\rho}$ be as in 2.1. If p is a prime number, denote by $\bar{\rho}_p$ the restriction of $\bar{\rho}$ to D_p as above. If $\bar{\rho}$ is going to have a lifting with Artin conductor N, then $\bar{\rho}_p$ must be unramified for $p \nmid N$. Assuming this to be the case, each $\bar{\rho}_p$ has a lifting r_p such that r_p is unramified for $p \nmid N$ (cf. [11] and [12]). The above theorem of Tate then gives us a unique lifting ρ of $\bar{\rho}$ such that:

$$\rho \mid I_p = r_p \mid I_p \quad \text{for all } p.$$

Now, any other lifting of $\bar{\rho}$ has the form $\rho \otimes \chi$, where χ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have:

$$\det(\rho \otimes \chi) = \det(\rho) \cdot \chi^2.$$

Concerning the question of equivalence of these 'twists' $\rho \otimes \chi$, one must know for what characters χ the representations ρ and $\rho \otimes \chi$ are equivalent. If χ is non-trivial, this can only happen if $\mathrm{Im}(\bar{\rho})$ is a dihedral group, and this case can be completely analyzed, as will become clear from the following, by use of the well-known theorem of Mackey concerning induced representations.

Now, in the above situation the determinant of ρ is given once one knows its restriction to I_p for all p, and this restriction is $\det(r_p) \mid I_p$. Viewing via local class field theory the character $\det(r_p)$ as a character on $\mathbb{Q}_p^{\times}$, this restriction is simply the restriction of $\det(r_p)$ to the group of units of $\mathbb{Z}_p$. Furthermore, if χ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we may by global class field theory view χ as an idele class character and consider its restriction χ_p to $\mathbb{Q}_p^{\times}$ for every p. The Artin conductor of $\rho \otimes \chi$ is the product of the Artin conductors of $r_p \otimes \chi_p$ for all p, and these latter conductors depend only on the restrictions of r_p and χ_p to I_p.

It follows from this discussion that we can answer the question of 2.1, if we can solve the following problem.

Problem: Given a prime number p and a continuous representation:

$$\bar{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{C}).$$

determine *some* lifting φ sufficiently explicitly so that:

(a) the restriction of $\det(\varphi)$ to the inertia group can be determined,

(b) the Artin conductor of $\varphi \otimes \chi$, for χ a character of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, can be computed in 'terms' of χ.

2.3. In [5] we have given a complete solution of this problem; in fact a slightly more general problem is considered in [5]. general problem is considered in [5]. This work is in turn based on results of Buhler and Zink ([1] and [19]; see also [17]). Since both the solution and the methods of obtaining it are rather technical, we shall, due to considerations of space, only give a very brief sketch of the ideas involved together with one (simple) example of the results obtained.

Let $\bar{\varphi}$ be as in the above problem.

Now one has to split up the discussion into two main cases: The image of $\bar{\varphi}$ is either a cyclic group, a dihedral group, or is isomorphic to A_4 or S_4. The 'A_5-type' is of course excluded, since any Galois extension of a local field has a solvable Galois group; also, the cyclic case is a priori not excluded since we have not required $\bar{\varphi}$ to be irreducible. The cyclic case is however easily seen to be trivial, so that one has the following two main cases:

(i) $\mathrm{Im}\bar{\varphi}$ is a dihedral group,
(ii) $\mathrm{Im}\bar{\varphi}$ is isomorphic to A_4 or S_4.

In the first case one bases oneself on the following description of the liftings of $\bar{\varphi}$ (cf. [11]):

Suppose that the ground field is K. Then $\bar{\varphi}$ provides us with a Galois extension M/K such that $\mathrm{Gal}(M/K)$ is a dihedral group. Except when $[M:K]=4$, which case can be discussed separately, the field M contains a unique quadratic extension L/K, and $\mathrm{Gal}(M/L)$ is cyclic. Now, the restriction of $\bar{\varphi}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ has the form

$$\bar{\varphi}(g) = \begin{pmatrix} \psi(g) & 0 \\ 0 & 1 \end{pmatrix} \quad \text{modulo } \mathbb{C}^\times,$$

where ψ is a certain character on $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$. Suppose that σ is an element of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ which modulo $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ generates $\mathrm{Gal}(L/K)$. Now any lifting of $\bar{\varphi}$ is a representation of the form:

$$\varphi = \mathrm{Ind}_{L/K}(\omega)$$

representation induced by ω), where ω is a character on $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ such that

$$\omega(\sigma g \sigma^{-1}) = \omega(g)\psi(g) \quad \text{for all } g \in \mathrm{Gal}(\overline{\mathbb{Q}}/L).$$

The conductor of such a φ is:

$$D_{L/K} \cdot N_{L/K}(f(\omega)),$$

where $D_{L/K}$ is the discriminant of L/K and $f(\omega)$ is the conductor of ω. Viewing ω via local class field theory as a character on $L^\times$, we may consider its restriction to $K^\times : \omega \mid K^\times$. Denoting by α the character on $K^\times$ of order 2 corresponding to L/K, the determinant of φ is:

$$\det \varphi = \alpha \cdot (\omega \mid K^\times).$$

Using this description one can now by splitting the discussion into numerous cases according to the structure of $K^\times$, of L/K and of ψ, find answers to (a) and (b) above.

In case (ii) (the ‘primitive’ case) one knows that the residue characteristic of the ground field must be 2. Here we restrict the discussion to the case where the ground field is $\mathbb{Q}_2$ (this clearly suffices, as we have seen in 2.2, for the purpose of answering the question in 2.1). One can then find that there are exactly 4 possibilities for $\bar{\varphi}$: There is exactly 1 extension of $\mathbb{Q}_2$ with Galois group isomorphic to A_4, and exactly 3 extensions with Galois group isomorphic to S_4; see [17]. Now, for these cases one has some general theory: In the first place there is the determination of the minimal conductor of a lifting of $\bar{\varphi}$, together with an intrinsic characterization of those liftings which have minimal conductor; this is due to Buhler and Zink, see [1] and [19] (and also [17]). Secondly we have the answer to (b) above for a φ which has minimal conductor; see [19]. With this and a detailed analysis of each of the 4 cases above, one can find a satisfactory answer to (a) and (b) if one chooses for φ a certain lifting (depending on the case) with minimal conductor. Let us give just one example of the results:

The unique A_4-extension of $\mathbb{Q}_2$ is $K/\mathbb{Q}_2$ with

$$K = \mathbb{Q}_2\left(\theta, \sqrt{1+2\theta}, \sqrt{1+2\theta^2}, \sqrt{1+2\theta^4}\right),$$

where θ is a primitive 7’th root of unity. This gives us a unique representation:

$$\bar{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2) \longrightarrow \mathrm{PGL}_2(\mathbb{C})$$

of A_4-type, and this $\bar{\varphi}$ has a lifting φ with the following properties:

Let α be the character on $\mathbb{Q}_2^\times$ corresponding to $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$. We view a character ψ on $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ also as a character on $\mathbb{Q}_2^\times$ and write $f(\psi)$ for $\log_2$ of the conductor of ψ. Then the determinant of $\varphi \otimes \psi$ is $\alpha\psi^2$. Furthermore, $\log_2$ of the conductor of $\varphi \otimes \psi$ is 5 if $f(\psi) \leq 2$, and it is $2f(\psi)$ if $f(\psi) \geq 3$.

2.4. We now return to the situation and notation of 2.1. We have seen how to reduce the question asked in 2.1 to a finite number of local problems (one for each prime divisor in N), and we have indicated how one can solve these local problems. This reduces the problem of determining $d(N, \varepsilon)$ to the problem of finding the potential candidates for the field K in 2.1. Now, if the representation $\bar{\rho}$ has a lifting with conductor N, then trivially the smallest possible conductor of a lifting of $\bar{\rho}$ is $\leq N$; if one has the results of 2.3 at ones disposal, then one can easily from this derive explicit bounds for the discriminant of $K/\mathbb{Q}$. Thus it is in principle clear that one has an algorithm for determining the possible fields K (given N and ε). The question is how to do this as effectively as possible.

If $\mathrm{Gal}(K/\mathbb{Q})$ is a dihedral group or isomorphic to A_4 or S_4, then the use of class field theory is the most efficient method for determining the candidates K. The use of class field theory is possible since $\mathrm{Gal}(K/\mathbb{Q})$ is in each of these cases a solvable group.

Of course this method does not work if $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$. In this case one can, given N and ε, find explicit bounds, not only for the discriminant of $K/\mathbb{Q}$, but also for the discriminant of a root field of K by which we mean an extension of degree 5 over $\mathbb{Q}$ contained in K. This gives us the problem to be considered in the next section.

3. Enumeration of A_5-fields

3.1. It is not hard to see that a projective representation $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{C})$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$ where K is the fixed field of the kernel of $\bar{\rho}$, has a lifting $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$ with *odd* determinant character if and only if K is not real.

From this and from the results of section 2 we conclude that we have to confront the following problem: Determine all non-real Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to A_5 and for which the discriminant of a root field is $\leq D^2$ for some fixed number D.

Here the number D has to be chosen so large that such fields actually occur, and secondly so that one of the (2-dimensional) projective representations associated with one of the occurring A_5-field has a lifting with odd determinant character and Artin conductor of a 'moderate' size. The reason for the second condition will become apparent in the next section. It turns out (from the table described below) that one must with these requirements choose D to be at least ≈ 500.

Now, the A_5-fields in the above problem will be obtained as splitting fields of polynomials

$$f(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5,$$

where $a_i \in \mathbb{Z}$, and the problem is to find good bounds for the $|a_i|$ so that we may use computer power to eliminate the uninteresting $f's$. Of course, the classical theory of geometry of numbers according to Minkowski provides us with bounds on the $|a_i|$ in terms of D, but the reader may convince himself that these bounds lead even for $D = 500$ to such a large number of possibilities for $f(x)$ that a computer search on this basis is absolutely impossible. Hence we have to do better than this.

3.2. We took our starting point in the following theorem of Hunter:

Theorem. *(cf. [4]). Suppose that $F/\mathbb{Q}$ is an extension of degree 5 with discriminant D. Then there is an algebraic integer θ in F such that $F = \mathbb{Q}(\theta)$, such that*

$$|\mathrm{Tr}_{F/\mathbb{Q}}(\theta)| \leq 2,$$

and such that, denoting by $\theta_1 = \theta, \theta_2, \theta_3, \theta_4, \theta_5$ the conjugates of θ,

$$\left(\sum_{i=1}^{5} |\theta_i|^2\right)^4 \leq \frac{8}{5} \cdot |D|.$$

Using this theorem and the fact that the potential $f's$ in 3.1 must have precisely one real root (since the splitting field should be a non-real extension of $\mathbb{Q}$ with Galois group isomorphic to A_5) it is not hard to derive rather 'reasonable' bounds for the $|a_i|$. We shall not here write down these bounds but merely be content to note that they enabled us to solve the problem in 3.1 for the following value of D:

$$D = 2083.$$

The reason for choosing this value, which is a prime number, will be recognized at the end of this section.

With this value of D and the above bounds for the $|a_i|$ one then gets a priori $\sim 7,7 \cdot 10^9$ possibilities for $f(x)$, and one then applies computer power to eliminate the uninteresting $f's$ through the following steps:

Step 1: Require the discriminant of $f(x)$ to be a square modulo the primes $3, 5, 7, 11, 13, 17, 19, 23$ and 29.

Step 2: Require the discriminant of $f(x)$ to be a square in $\mathbb{Z}$.

Step 3: Require $f(x)$ to be irreducible over $\mathbb{Z}$.

Step 4: Require the discriminant of a root field of the splitting field of $f(x)$ to be $\leq 2083^2$.

Step 5: Require the Galois group of a splitting field of $f(x)$ to be isomorphic to A_5.

Step 6: Distribute the remaining $f's$ into classes with identical splitting fields.

There is for each step a standard algorithm. Of these, perhaps only the algorithm involved in step 6 is less well known. For this algorithm the reader may consult [18].

The total computing time required to perform the six steps was about 280 hours. The second step was the most time consuming, requiring about 200 hours of computing time. The machine used was an Apollo DN 10000.

The final result of this computation is the complete table of all non-real A_5-extensions of $\mathbb{Q}$ for which the discriminant of a root field is bounded by 2083^2. The table contains 238 fields; we shall not reproduce the table here, but be content to give one example of the use of it.

3.3. Consider $N = 2083$. This is a prime number $\equiv 3\ (4)$. Let ε be the Legendre symbol $\varepsilon(\cdot) = \left(\frac{\cdot}{2083}\right)$. It is not hard to deduce that if the representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$ is of A_5-type with Artin conductor $N = 2083$ and determinant character ε, then the discriminant of a root field of the corresponding A_5-extension of $\mathbb{Q}$ is 2083^2. The aforementioned table shows that there is exactly one such A_5- extension of $\mathbb{Q}$, namely the splitting field of

$$x^5 + 8x^3 + 7x^2 + 172x + 53. \tag{$**$}$$

Now, there are exactly two non-equivalent representations $A_5 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ for which the fixed field of the kernel of $\bar{\rho}$ is the splitting field of $(**)$; furthermore a straightforward analysis shows that each of these has exactly two non-equivalent liftings (to $\mathrm{GL}_2(\mathbb{C})$) with Artin conductor $N = 2083$ and determinant character ε.

It is not a problem to see that there are no representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$ with Artin conductor 2083 and determinant character ε of type A_4 or S_4; on the other hand there are exactly 3 such representations of dihedral type. The last fact is deduced from the fact that $\mathbb{Q}\left(\sqrt{-2083}\right)$ has class number 7 (cf. [11]). Hence we may conclude that

$$d(2083, \varepsilon) = 2 \cdot 2 + 3 = 7.$$

There are examples of a similar nature for many other values of N, for example

$$4 \cdot 487,\ 4 \cdot 751,\ 4 \cdot 887,\ 4 \cdot 919,\ 2^5 \cdot 73,\ 2^5 \cdot 193\ .$$

4. $\dim S_1^+(N,\varepsilon)$

4.1. For $k, M \in \mathbb{N}$ and δ a Dirichlet character modulo M with $\delta(-1) = (-1)^k$, we denote by $S_k(M,\delta)$ the complex vector space of cusp forms of weight k and nebentypus δ on

$$\Gamma_0(M) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) |\ c \equiv 0 \quad (M) \right\}.$$

These spaces are finite-dimensional. The space $S_k(M,\delta)$ always has an *integral basis* by which we mean a basis $(f_1, \ldots, f_d)$ over $\mathbb{C}$ such that the Fourier coefficients of any f_i are rational integers (cf. [13], Chap. 3).

4.2. Now let us once again fix $N \in \mathbb{N}$ and let ε be a Dirichlet character modulo N with $\varepsilon(-1) = -1$.

In order to compute $\dim S_1^+(N,\varepsilon)$ it obviously suffices to have a general algorithm for the determination of $\dim S_1(N,\varepsilon)$. The problem here is that a 'formula' for this dimension is not available; this is in contrast to the situation for weight ≥ 2 where such formulas exist and are classical (see for example [2]). To compute the dimension of $S_1(N,\varepsilon)$ we shall therefore use the following trick:

For the sake of simplicity, suppose that N has a prime divisor $\equiv 3$ (4); let p be such a prime divisor and let η be the Legendre symbol $\eta(\cdot) = \left(\frac{\cdot}{p}\right)$. Consider the Eisenstein series

$$E = \frac{1}{2}h + \sum_{n=1}^{\infty} \left(\sum_{d|n} \eta(d) \right) q^n \ , \qquad q := e^{2\pi i z},$$

where h is the class number of $\mathbb{Q}(\sqrt{-p})$. Then E is a modular form of weight 1 and nebentypus η on $\Gamma_0(p)$. The form $2E$ has integers as Fourier coefficients at ∞ and does not vanish at ∞.

On the other hand we consider the series

$$\theta_2(z) = \sum_{m \equiv 1 \quad (2)} q^{m^2/8} \ , \qquad q := e^{2\pi i z}.$$

Then θ_2^8 is a modular form of weight 4 and trivial nebentypus on $\Gamma_0(2)$; furthermore, θ_2^8 does not vanish in the upper half plane, and among the cusps it vanishes only at ∞, where it has integers as Fourier coefficients (cf. [10], chap. 1). Defining N' to be N if N is even, and $N' = 2N$ if N is odd, it is now clear that the map

$$f \longmapsto (2Ef, \theta_2^8 f)$$

maps $S_1(N,\varepsilon)$ isomorphically onto the subspace of

$$S_2(N,\varepsilon\eta) \times S_5(N',\varepsilon)$$

consisting of pairs (h_1, h_2) with

$$(+) \qquad h_1\theta_2^8 = h_2 \cdot 2E \ .$$

Here we have viewed η as a Dirichlet character modulo N and ε also as a Dirichlet character modulo N'. Now, for $h_1 \in S_2(N,\varepsilon\eta)$ and $h_2 \in S_5(N',\varepsilon\eta)$ the forms $h_1\theta_2^8$

and $h_2 \cdot 2E$ are elements of $S_6(N', \varepsilon\eta)$. Denote for $M \in \mathbb{N}$ by $m(M)$ the index of $\Gamma_0(M)$ in $\mathrm{SL}_2(\mathbb{Z})$; one has

$$m(M) = M \cdot \prod_{p|M} \left(1 + \left(\tfrac{1}{p}\right)\right)$$

(cf. [13], chap. 1). For a non-zero element of $S_k(M, \delta)$ its order of 0 at ∞ is less than $km(N)/12$ (see [10], chap. 1). Hence condition (+) simply means that the first $\frac{1}{2}m(N')$ Fourier coefficients of $h_1\theta_2^8 - h_2 \cdot 2E$ are all 0. If now d and e are the dimensions of the spaces $S_2(N, \varepsilon\eta)$ and $S_5(N', \varepsilon)$ respectively, we then see that if we have an algorithm for finding (i.e. computing Fourier coefficients of) an integral basis for each of these spaces, then the problem of computing the dimension of $S_1(N, \varepsilon)$ has been reduced to the computation of the rank of a certain $d + e$ by $\frac{1}{2}m(N')$ matrix with coefficients in $\mathbb{Z}$.

If N does not have a prime divisor $\equiv 3$ (4), one can replace the level N by $8N$ in the above, but then the discussion becomes somewhat more complicated.

4.3. We then turn to the problem of determining an integral basis for a space $S_k(M, \delta)$ where $k \geq 2$. Here again we have to be very brief and give only a rough sketch of the ideas involved.

Let $R = \mathbb{Z}\left[\frac{1}{6}\right]$. We consider a certain $R[\Gamma_0(M)]$-module $L_{k,\delta}$. As R-module $L_{k,\delta}$ is the R-module of homogeneous polynomials of degree $k - 2$ in two variables over R:

$$L_{k,\delta} = \left\{ \sum_{i=0}^{k-2} \; a_i x^i y^{k-2-i} | \; a_i \in R \right\} \; .$$

The action of $\Gamma_0(N)$ on $L_{k,\delta}$ is given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x^i y^{k-2-i} = \delta(d)(ax + cy)^i (bx + dy)^{k-2-i}.$$

Now, the Eichler-Shimura isomorphism gives us an exact sequence:

$$0 \to S_k(M, \delta) \oplus \overline{S_k(M, \delta)} \to H^1(\Gamma_0(M), L_{k,\delta} \otimes \mathbb{C}) \xrightarrow{r} L \to 0 \; .$$

Here, $\overline{S_k(M, \delta)}$ is the space obtained from $S_k(M, \delta)$ by complex conjugating Fourier coefficients at ∞, and L is a certain space which will not be described here.

This gives an embedding of $S_k(M, \delta)$ into the group of fixed points of $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in $H^1(\Gamma_0(M), L_{k,\delta} \otimes \mathbb{C})$. Now one constructs a concrete model W of the latter group. The Hecke operators T_m can be defined on the above cohomology group in a way which is compatible with the embedding of $S_k(M, \delta)$ in W.

In the model W one can find a basis $\{b_i\}$ such that $T_m b_i \in \oplus_i \mathbb{Z} b_i$ for all i and m. It is now shown (L. Merel) that if $w \in W$ is a $\mathbb{Z}$-linear combination of the $b_i's$ and if we define the integers $a_m^{(i)}$ by:

$$T_m w = \sum_i a_m^{(i)} b_i \; ,$$

then for all i, $a_0^{(i)} + \sum_m \; a_m^{(i)} q^m$ defines a modular form on $\Gamma_0(M)$ with weight k and nebentypus δ for some constant $a_0^{(i)}$. We have here ignored some technicalities concerning the definition of T_m if m is not prime to M. Furthermore, it is shown that these forms for 'generic' w provide us with an integral basis for the space of modular forms on $\Gamma_0(M)$ with weight k and nebentypus δ.

The constant $a_0^{(i)}$ in the above cannot be computed directly, but by explication of the homomorphism r above, one can easily isolate the cusp forms, and one thus obtains an integral basis for $S_k(M, \delta)$.

This algorithm has been completely implemented (by X. Wang) in Essen and is working very effectively.

Following the strategy outlined in the above, we have obtained 7 new non-trivial verifications of the Artin conjecture (corresponding to the 7 values of N mentioned in 3.3). We shall report on this elsewhere.

Acknowledgements: This work was supported by the Deutsche Forschungsgemeinschaft.

References

[1] J. P. Buhler: 'Icosahedral Galois Representations.' Lecture Notes in Mathematics **654**, Springer-Verlag 1978.

[2] H. Cohen, J. Oesterlé: 'Dimensions des espaces de formes modulaires.' In: J.-P. Serre, D.B. Zagier (eds.): 'Modular Functions of One Variable VI.' Lecture Notes in Mathematics **627**, Springer-Verlag 1977.

[3] P. Deligne, J.-P. Serre: 'Formes modulaires de poids 1.' Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530.

[4] J. Hunter: 'The minimum discriminants of quintic fields.' Proc. Glasgow Math. Assoc. **3** (1957), 57–67.

[5] I. Kiming: 'On the liftings of 2-dimensional, projective Galois representations over $\mathbb{Q}$.' J. Number Theory **56** (1996), 12–35.

[6] R.P. Langlands: 'Base change for $GL(2)$.' Annals of Mathematics Studies **96**, Princeton University Press 1980.

[7] W. Li: 'On converse theorems for $GL(2)$ and $GL(1)$.' Amer. J. Math. 103 (1981), 851–885.

[8] L. Merel: 'An elementary theorem about Hecke operators and periods of modular forms.' Preprint, 1992.

[9] T. Miyake: 'Modular Forms.' Springer-Verlag, 1989.

[10] H. Petersson: 'Modulfunktionen und quadratische Formen.' Ergebnisse der Mathematik und ihrer Grenzgebiete **100**. Springer-Verlag, 1982.

[11] J.-P. Serre: 'Modular forms of weight one and Galois representations.' In: A. Fröhlich: Algebraic Number Fields. Academic Press 1977.

[12] J.-P. Serre: 'Cohomologie Galoisienne.' Lecture Notes in Mathematics **5**, Springer-Verlag, 1986.

[13] G. Shimura: 'Introduction to the arithmetical theory of automorphic functions.' Princeton University Press, 1970.

[14] J. Tunnell: 'Artin's conjecture for representations of octahedral type.' Bull. Amer. Math. Soc. (N.S.) 5 (1981), 173–175.

[15] X. Wang: 'The Hecke algebra on the cohomology of $\Gamma_0(p_0)$.' Nagoya Math. J. **121** (1991), 97–125.

[16] A. Weil: 'Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen.' Math. Ann. **168** (1967), 149–156.

[17] A. Weil: 'Exercises dyadiques.' Invent. Math. **27** (1974), 1–22.

[18] Weinberger, Rothschild: 'Factoring polynomials over algebraic number fields.' ACM Transactions on Mathematical Software **2** (1976), 335–350.

[19] E.-W. Zink: 'Ergänzungen zu Weils Exercises dyadiques.' Math. Nachr. 92 (1979), 163–183.

kiming@math.ku.dk

Dept. of math., Univ. of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark.