An Interpretation of some congruences concerning Ramanujan's τ-function

Jean-Pierre Serre

September 11, 2003

1 Ramanujan's τ-function

Definition

Let us put

$$D(x) = x \prod_{m=1}^{\infty} (1 - x^m)^{24}. \tag{1}$$

The coefficient of x^n ($n \geq 1$) in the power series os $D(x)$ is denoted by $\tau(n)$. The function $n \longmapsto \tau(n)$ is *Ramanujan's τ-function* (cf. [5] and [16]). We have

$$D(x) = \sum_{n=1}^{\infty} \tau(n) x^n. \tag{2}$$

Here are a few values of τ, as computed by Lehmer [11]: $\tau(1) = 1$, $\tau(2) = -24$, $\tau(3) = 252$, $\tau(4) = -1472$, $\tau(5) = 4830$, $\tau(6) = -6048$, ...

Some properties of τ

If we put

$$\Delta(z) = D(e^{2\pi i z}), \quad \mathrm{Im}\,(z) > 0, \tag{3}$$

then it is known that the function Δ is, up to a constant factor, the unique cusp form of weight 12 for the group $\mathrm{SL}\,(2, \mathbb{Z})$. In particular, the function Δ is, for each prime number p, an eigenfunction of the Hecke operator T_p, with corresponding eigenvalue $\tau(p)$ (cf. e.g. Hecke [6], p. 644–671). This implies the following properties, which have been conjectured by Ramanujan [16] and proved by Mordell [14]:

$$\tau(mn) = \tau(m)\tau(n), \qquad \text{if } (m,n) = 1 \tag{4}$$

$$\tau(p^{n+1}) = \tau(p^n)\tau(p) - p^{11}\tau(p^{n-1}), \text{ if } p \text{ is prime.} \tag{5}$$

These formulas allow us to compute $\tau(n)$ from the values of $\tau(p)$ for primes p.

The Dirichlet series attached to τ

The Dirichlet series attached to τ is defined by

$$L_\tau(s) = \sum_{n=1}^{\infty} \tau(n) n^{-s}. \tag{6}$$

The formulas (4) and (5) are equivalent to the following:

$$L_\tau(s) = \prod_p \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}} = \prod_p \frac{1}{H_p(p^{-s})}, \tag{7}$$

where

$$H_p(X) = 1 - \tau(p)X + p^{11}X^2. \tag{8}$$

Moreover, Hecke's theory shows that $L_\tau(s)$ can be extended to a holomorphic function on the complex plane, and that the function

$$(2\pi)^{-s}\Gamma(s)L_\tau(s) \tag{9}$$

is invariant under the map $s \longmapsto 12 - s$.

We mention that the Conjecture of Ramanujan can be expressed by the following equivalent assertions:

- the roots of the polynomial $H_p(X)$ are conjugated complex numbers;
- the roots of the polynomial $H_p(X)$ have absolute value $p^{-11/2}$;
- we have $|\tau(p)| < 2p^{11/2}$.

2 Congruences involving τ

Results

There exist congruences for $\tau(n)$ modulo 2^{11}, 3^7, 5^3, 7, 23, and 691 (cf. Lehmer [13]).

2.1 Powers of 2.

In [2], Bambah gave the value of $\tau(n)$ modulo 2^5:

$$\tau(p) \equiv 1 + p^{11} \bmod 2^5, \quad p > 2. \tag{10}$$

Actually, this congruence holds modulo 2^8; more exactly, Lehmer [13] has shown

$$\tau(p) \equiv 1 + p^{11} + 8(41 + x)(p - x)^{2+x} \bmod 2^{11}, \tag{11}$$

where $x = (-1)^{(p-1)/2}$.

Swinnerton-Dyer (unpublished) has also obtained congruences modulo 2^{12}, 2^{13}, 2^{14} for primes $p \equiv 5, 3, 7 \bmod 8$.

2.2 Powers of 3.

In [15], $\tau(p)$ modulo 3 is given:

$$\tau(p) \equiv 1 + p \bmod 3, \quad p \neq 3. \tag{12}$$

Lehmer [13] gave $\tau(p) \bmod 3^5$; in particular,

$$\tau(p) \equiv p^2 + p^9 \bmod 3^3. \tag{13}$$

Swinnerton-Dyer (unpublished) obtained congruences modulo 3^6 and 3^7 for primes $p \equiv 1 \bmod 3$ and $p \equiv -1 \bmod 3$, respectively.

2.3 Powers of 5.

According to [2], we have

$$\tau(p) \equiv p + p^{10} \bmod 5^2 \tag{14}$$

Lehmer [13] gave a congruence modulo 5^3 (for primes $p \neq 5$):

$$\tau(p) \equiv -24p(1 + p^9) - 10p(1 + p^5) - 90p^2(1 + p^3) \bmod 5^3;$$

this can also be written in the form

$$\tau(p) \equiv p^{41} + p^{-30} \bmod 5^3, \quad (p \neq 5). \tag{15}$$

2.4 Powers of 7.

We have ([15])

$$\tau(p) \equiv p + p^4 \bmod 7 \tag{16}$$

Currently we do not know the value of $\tau(p) \bmod 7^2$, except when p is a quadratic non-residue modulo 7, and in this case $\tau(p) \equiv p + p^{10} \bmod 7^2$ according to Lehmer [13].

2.5 Powers of 23.

This result differs in form from the preceding congruences. We have (cf. Wilton [21]), for $p \neq 23$:

$$\tau(p) \equiv \begin{cases} 0 \bmod 23 & \text{if } (-23/p) = -1 \\ 2 \bmod 23 & \text{if } (-23/p) = +1 \text{ and } p = u^2 + 23v^2 \\ -1 \bmod 23 & \text{if } (-23/p) = +1 \text{ and } p \neq u^2 + 23v^2 \end{cases} \tag{17}$$

Remark. Let $K = \mathbb{Q}(\sqrt{-23})$. Then $(-23/p) = +1$ means that p splits in K into two distinct prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$; p has the form $u^2 + 23v^2$ if and only if $\mathfrak{p}$ is *principal* (recall that K has class number 3).

2.6 Powers of 691.

We know (Ramanujan [16])

$$\tau(p) \equiv 1 + p^{11} \bmod 691. \quad (18)$$

These are the known congruences for $\tau(p)$; of course, one can deduce congruences for $\tau(n)$, $n \in \mathbb{N}$, by using the equations (4) and (5).

Proofs

I will only give short indications; for more details, see [2],[12], [13], [15], [16], [21].

Consider the Eisenstein series of weight 6 and 12:

$$\left.\begin{array}{rcl} E_6(x) & = & 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)x^n \\ E_{12}(x) & = & 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)x^n \end{array}\right\} \text{ where } \sigma_q(n) = \sum_{d|n} d^q. \quad (19)$$

Since the square of E_6 is a modular form of weight 12, it must be a linear combination of E_{12} and D, and we find

$$E_6^2 = E_{12} - \frac{a}{691}D, \quad \text{with } a \equiv 65520 \bmod 691. \quad (20)$$

Multiplying through by 691, we get

$$0 \equiv 65520\Big(\sum_{n=1}^{\infty}\sigma_{11}(n)x^n - \sum_{n=1}^{\infty}\tau(n)x^n\Big) \bmod 691, \quad (21)$$

and this implies

$$\tau(n) \equiv \sigma_{11}(n) \bmod 691. \quad (22)$$

If $n = p$ is prime, this gives the congruence (18).

The congruences modulo 2^α, 3^β, 5^γ, 7 can be derived by analogous (but more complicated) arguments, using the functions

$$\Phi_{r,s}(x) = \sum_{m,n} m^r n^s x^{mn}$$

of Ramanujan (cf. Lehmer [13]).

The congruence mod 23 results easily from the following (cf. Wilton [21]):

$$\prod_{m=1}^{\infty}(1 - x^m)^{24} \equiv \theta(x)\theta(x^{23}) \bmod 23, \quad (23)$$

where

$$\theta(x) = \prod_{m=1}^{\infty}(1 - x^m) = \sum_{-\infty}^{\infty}(-1)^r x^{(3r^2+r)/2}.$$

Zeros of τ

Do there exist primes p such that $\tau(p)=0$? There are no examples known. In any case, the congruences given above imply (cf. Lehmer [12, 13]):

$$\text{If } \tau(p)=0, \text{ then } \left\{ \begin{array}{l} p \equiv -1 \bmod 2^{11}3^7 5^3 691, \\ p \equiv -1, 19, 31 \bmod 7^2, \\ (p/23) = -1. \end{array} \right\} \tag{24}$$

In particular, the density of the set of primes p such that $\tau(p)=0$ is at most 10^{-12}, and the smallest possible p has at least 15 digits.

3 The ℓ-adic representations attached to τ

Notation

Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$; for every prime ℓ, let K_ℓ denote the maximal subfield of $\overline{\mathbb{Q}}$ which is unramified outside ℓ. A finite subfield of $\overline{\mathbb{Q}}$ is contained in K_ℓ if and only if its discriminant is (up to sign) a power of ℓ.

The extension $K_\ell/\mathbb{Q}$ is normal; let $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ denote its Galois group. In the terminology of Grothendieck, $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ is the fundamental group of $\mathrm{Spec}\,(\mathbb{Z}) \setminus \{\ell\}$. If p is a prime $\neq \ell$, we associate to p its *Frobenius automorphism* F_p, which is an element of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ defined up to conjugation.

For a ring k and an integer N, let $\rho : \mathrm{Gal}\,(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}\,(N,k)$ be a linear representation of degree N of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ in k. For all primes $p \neq \ell$, the element $\rho(F_p) \in \mathrm{GL}\,(N,k)$ is defined up to conjugation; in particular, the polynomial $P_{p,\rho}(X) = \det(1-\rho(F_p)X)$ is well defined.

In the following, we are mainly interested in the case where the ring k is $\mathbb{Z}/\ell^n\mathbb{Z}$, $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$, or $\mathbb{Q}_\ell = \mathbb{Z}_\ell[\frac{1}{\ell}]$ and where the homomorphism ρ is continuous.

A conjecture

It's the following:

Conjecture 1. *For each prime ℓ, there exists a continuous linear representation*

$$\rho_\ell : \mathrm{Gal}\,(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{Aut}\,(V_\ell),$$

where V_ℓ is a $\mathbb{Q}_\ell$-vector space of dimension 2 which satisfies the following condition:
(C) For each prime $p \neq \ell$, the polynomial $P_{p,\rho}(X)$ equals the polynomial $H_p(X)$ defined in Sect. 1.

This condition (C) can also be expressed as
(C') For each prime $p \neq \ell$, we have

$$\mathrm{Tr}\,(\rho_\ell(F_p)) = \tau(p) \quad \text{and} \quad \det(\rho_\ell(F_p)) = p^{11}. \tag{25}$$

In the terminology of [17] (Chap. I, §2), the ρ_ℓ form a *strictly compatible system of ℓ-adic rational representations of* $\mathbb{Q}$, whose exceptional set is empty.

Remarks.
1. Let $\chi_\ell : \mathrm{Gal}\,(K_\ell/\mathbb{Q}) \longrightarrow \mathbb{Q}_\ell^\times$ be the ℓ-adic representation of degree 1 given by the action of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ on the l^n-th roots of unity (cf. [17], Chap. I, Sect. 1.2); we have $\chi_\ell(F_p) = p$. The second part of the condition (25) is therefore equivalent to

$$\det(\rho_\ell) = \chi_\ell^{11}. \tag{26}$$

2. Let $c \in \mathrm{Gal}\,(K_\ell/\mathbb{Q})$ be the element of order 2 induced by complex conjugation; c is defined up to conjugation. According to (26), we have $\det(\rho_\ell(c)) = -1$. We conclude that $\rho_\ell(c)$ has eigenvalues $+1$ and -1.
3. The representation ρ_ℓ which exists according to the conjecture above is *unique* up to conjugation. This follows from [17] (Chap. I, Sect. 2.3), combined with the fact that ρ_ℓ is irreducible (cf. Sect. 5 below).

Representations mod ℓ^n

We first observe that, if $\rho_\ell : \mathrm{Gal}\,(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{Aut}\,(V_\ell)$ exists, then there is a *lattice* in V_ℓ which is stable under $\mathrm{im}\,(\rho_\ell)$ (cf. [17], Chap. I, Sect. 1.1). In other words, we can view ρ_ℓ as a homomorphism of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ with image in $GL(2, \mathbb{Z}_\ell)$, not only in $GL(2, \mathbb{Q}_\ell)$ (Remark, however, that uniqueness is lost: different lattices can give rise to non-isomorphic representations). By reduction modulo ℓ^n, we obtain representations mod ℓ^n

$$\rho_{\ell,n} : \mathrm{Gal}\,(K_\ell/\mathbb{Q}) \longrightarrow GL(2, \mathbb{Z}/\ell^n\mathbb{Z})$$

such that

$$\left.\begin{array}{rcl} \mathrm{Tr}\,(\rho_{\ell,n}(F_p)) & \equiv & \tau(p) \bmod \ell^n, \\ \det(\rho_{\ell,n}(F_p)) & \equiv & p^{11} \bmod \ell^n. \end{array}\right\} \tag{27}$$

for all $p \neq \ell$.

Thus, for certain ℓ^n we know $\tau(p)$ modulo ℓ^n explicitly (cf. Sect. 2). A first verification of the conjecture consists therefore in trying to find representations mod ℓ^n with the properties listed above for those values of ℓ^n. This is what we will do now.

Representations corresponding to the congruences of Section 2

There are no difficulties mod 2^8, 3^3, 5^3, 7 and 691. In each case, we have

$$\tau(p) \equiv p^a + p^{11-a} \bmod \ell^n$$

for $p \neq \ell$ with $a = 0, 2, 41, 1$ and 0, respectively. Each triangular representation

$$\begin{pmatrix} \phi & * \\ 0 & \psi \end{pmatrix},$$

where $\phi, \psi : \mathrm{Gal}\,(K_\ell/\mathbb{Q}) \longrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ are congruent modulo ℓ^n to χ_ℓ^a and χ_ℓ^{11-a}, respectively, answers the question.

The case $\ell = 23$ and $n = 1$ can be interpreted as follows: let E be the field obtained by adjoining to $\mathbb{Q}$ the roots of the polynomial $x^3 - x - 1 = 0$. This is a normal extension of $\mathbb{Q}$, ramified only at 23; its Galois group is the group S_3, the symmetric group of order 6. It is known that E is the Hilbert class field of the field $\mathbb{Q}(\sqrt{-23}\,)$. Let r be the unique irreducible representation of degree 2 of S_3; for $s \in S_3$, we have

$$\mathrm{Tr}\,(r(s)) = 0,\ 2, \quad \text{or} \ -1,$$

according as s has order 2, 1 or 3. Moreover, since $\mathrm{Gal}\,(E/\mathbb{Q})$ is a quotient of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$, we can consider r as a representation of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$. Equation (17) shows that ρ_{23} and r have the same characteristic polynomial modulo 23. Since r is irreducible mod 23, this implies

$$\rho_{23,1} \equiv r \bmod 23.$$

The case 2^{11} is much less evident than those above (and has even led me to doubt the conjecture!). Luckily, it has been treated by Swinnerton-Dyer (unpublished), and his result is in fact the most important numerical verification of the general conjecture. Swinnerton-Dyer has even obtained the complete structure of the group $\mathrm{im}\,(\rho_2)$, and not only the structure of its reduction modulo 2^{11}. According to what he told me, $\mathrm{im}\,(\rho_2)$ is an open subgroup of index $3 \cdot 2^{25}$ in $\mathrm{GL}\,(2, \mathbb{Z}_2)$.

The representation $\rho_{11,1}$

Although we don't know a congruence giving $\tau(p)$ mod 11 as a simple function of p (the reason for this will be explained in Sect. 4 below), Swinnerton-Dyer made me realize that the *existence of the representation* $\rho_{11,1}$ (i.e. ρ_{11} mod 11) can be demonstrated in the following way:

We start by observing

$$\begin{aligned} x \prod_{m=1}^{\infty} (1 - x^m)^{24} &= x \prod_{m=1}^{\infty} (1 - x^m)^2 \prod_{m=1}^{\infty} (1 - x^m)^{22} \\ &\equiv x \prod_{m=1}^{\infty} (1 - x^m)^2 \prod_{m=1}^{\infty} (1 - x^{11m})^2 \bmod 11. \end{aligned} \tag{28}$$

Thus $x \prod (1-x^m)^2 \prod (1-x^{11m})^2$ is a cusp form of weight 2 for $\Gamma_0(11)$. Moreover, we know (cf. Shimura [19]) that for every ℓ there exists a corresponding ℓ-adic representation: the one associated to the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20. \tag{29}$$

We conclude that $\rho_{11,1}$ is isomorphic to the representation of $\mathrm{Gal}\,(K_\ell/\mathbb{Q})$ in the group of 11-division points of this elliptic curve. It can be shown (cf. Shimura

[19]) that the image of $\rho_{11,1}$, which a priori is a subgroup of $\mathrm{GL}(2, \mathbb{F}_{11})$, is in fact the whole group $\mathrm{GL}(2, \mathbb{F}_{11})$. The situation here is therefore completely different from the situation before, where we only encountered *solvable groups*.

4 Applications

In this and the next chapter, we assume the truth of the conjecture made in Sect. 3, namely the existence of the representations ρ_ℓ and $\rho_{\ell,n}$. The results below can therefore not be considered as demonstrated unless the conjecture itself will be proved (which is imminent, cf. Section 6).

Density

The value of $\tau(p) \bmod \ell^n$ depends uniquely on the element

$$\rho_{\ell,n}(F_p) \in \mathrm{GL}(2, \mathbb{Z}/\ell^n\mathbb{Z}).$$

By the theorem of Chebotarev (cf. e.g. [17], Chap. I, Sect. 2.2), this implies:

> The set of primes $p \neq \ell$ such that $\tau(p)$ is congruent to a given integer $a \bmod \ell^n$, has a *density*; this density is > 0 if the set under consideration is non-empty.

More exactly, the density equals A/B, where B is the order of $\mathrm{im}(\rho_{\ell,n})$, and where A is the number of elements in $\mathrm{im}(\rho_{\ell,n})$ whose trace is congruent to a modulo ℓ^n.

Independence of certain primes

The extensions K_ℓ $(\ell = 2, 3, 5, \ldots)$ are linearly disjoint over $\mathbb{Q}$; this follows easily from the fact that $\mathbb{Q}$ has no unramified extensions $\neq \mathbb{Q}$. We conclude that the values of $\tau(p)$ modulo 2^a, $3^b, \ldots$ are independent: if the density of primes p such that $\tau(p) \equiv a_i \bmod \ell_i^{n_i}$ is d_i, then the density of the primes satisfying all these conditions is the *product* of the d_i. The same argument implies

> Let ℓ and p_0 be different primes, and $n \geq 1$ an integer. Then there exist infinitely many primes p such that
>
> $$\tau(p) \equiv \tau(p_0) \bmod \ell^n, \quad p \equiv p_0 \bmod \ell^n,$$
>
> even if we restrict p_0 to be in an arithmetic progression $an + b$ with $(a, b) = (a, \ell) = 1$.

In less precise words: given relatively prime integers M and N, then no congruence on $p \bmod N$ can impose anything on the value of $\tau(p) \bmod N$.

Nonexistence of a congruence mod 11

The fact that the image of $\rho_{11,1}$ is the whole group $\mathrm{GL}\,(2, \mathbb{Z}/11\mathbb{Z})$ (cf. Sect. 3) implies (using Chebotarev's theorem again)

> No congruence on p can impose restrictions on the value of $\tau(p)$ mod 11.

More precisely: given integers a, b, c such that $(a, b) = 1$, there exist infinitely many primes p such that $p \equiv a \bmod b$ and $\tau(p) \equiv c \bmod 11$.

Of course, an analogous result holds whenever $\mathrm{im}\,(\rho_{\ell,1})$ contains $\mathrm{SL}\,(2, \mathbb{Z}/\ell\mathbb{Z})$, which can easily be verified numerically by the method indicated in [19].

Primes p such that $\tau(p) = 0$ have density 0

More generally, let $\Phi(X, Y)$ be a polynomial in two variables with coefficients in a field of characteristic 0, and assume that Φ does not identically vanish. Then the set of primes p such that $\Phi(p, \tau(p)) = 0$ has density zero.

In fact, this can be reduced by an easy argument to the case where Φ has the form $\Psi(X^{11}, Y)$, with Ψ having coefficients in $\mathbb{Q}$. Let ℓ be prime, and define the subgroup $H_\ell = \mathrm{im}\,(\rho_\ell)$ of $\mathrm{GL}\,(2, \mathbb{Q}_\ell)$. It can be shown (cf. Sect. 5 below) that H_ℓ is an *open* subgroup of $\mathrm{GL}\,(2, \mathbb{Q}_\ell)$. Let X be the set of all $s \in H_\ell$ such that $\Psi(\det(s), \mathrm{Tr}\,(s)) = 0$. The set X is a 'hypersurface' in the ℓ-adic variety H_ℓ, and its interior is *empty*; this implies that $\mu(X) = 0$, where μ is the Haar measure on H_ℓ. Now Chebotarev's theorem asserts that the set of primes such that $F_p \in X$ has density 0; this proves our claim.

(We have thus replaced the 10^{-12} from Sect. 2.6 by 0).

A congruence modulo 23^2

(I shall restrict myself to a trivial case here. In any case, as Swinnerton-Dyer has observed, we can certainly give the value of $\tau(p)$ modulo 23^2).

We have seen above that $\rho_{23,1}$ is congruent modulo 23 to the representation r of S_3. Consider, in particular, primes p of the form $p = u^2 + 23v^2$; then we have

$$\rho_{23}(F_p) \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 23.$$

Therefore we can write

$$\rho_{23}(F_p) = \begin{pmatrix} 1 + 23a & 23b \\ 23c & 1 + 23d \end{pmatrix},$$

with $a, b, c, d \in \mathbb{Z}_{23}$, and

$$\begin{aligned} \tau(p) &= 2 + 23(a + d), \\ p^{11} &= 1 + 23(a + d) + 23^2(ad - bc). \end{aligned}$$

Comparing yields

$$\tau(p) \equiv 1 + p^{11} \bmod 23^2, \tag{30}$$

for primes $p \neq 23$ of the form $u^2 + 23v^2$.
Example. $p = 59 = 6^2 + 23 \cdot 1^2$: here $\tau(p) = -5,189,203,740$; one can easily verify that $-5,189,203,740 \equiv 1 + 59^{11} \bmod 23^2$.

5 Remarks and Questions

The image of ρ_ℓ is an open subgroup of $\mathrm{GL}(2, \mathbb{Q}_\ell)$

This result has been mentioned above. It can be proved by a method analogous to the one used for the 'Tate modules' of elliptic curves ([17], Chap. IV, Sect. 2.2):

To begin with, we may assume that ρ_ℓ is semi-simple (if not, we can replace it by its semi-simplification). Let $\mathfrak{g}_\ell \subseteq M_2(\mathbb{Q}_\ell)$ be the Lie algebra of $\mathrm{im}(\rho_\ell)$, viewed as an ℓ-adic Lie algebra; since ρ_ℓ is semi-simple, $\mathfrak{g}_\ell$ is a *reductive* algebra, and hence has the form $\mathfrak{c} \times \mathfrak{s}$, with abelian $\mathfrak{c}$ and semi-simple $\mathfrak{s}$. If $\mathfrak{s} \neq 0$, then $\mathfrak{s}$ is necessarily equal to the Lie algebra of the group $\mathrm{SL}(2, \mathbb{Q}_\ell)$; using the fact that $\det(\rho_\ell) = \chi_\ell^{11}$, we deduce that $\mathfrak{g}_\ell = M_2(\mathbb{Q}_\ell)$, and this implies that $\mathrm{im}(\rho_\ell)$ is open.

It remains to show that $\mathfrak{s} = 0$ is impossible. Assume therefore that $\mathfrak{s} = 0$; then the Lie algebra $\mathfrak{g}_\ell$ is abelian and acts semi-simple on V_ℓ. If $\mathfrak{g}_\ell$ were the algebra of *homotheties* of V_ℓ, then there would exist an open subgroup of $\mathrm{im}(\rho_\ell)$ consisting of homotheties. Thus there would exist infinitely many primes p such that $\det(\rho_\ell(F_p)) = \mathrm{Tr}(\rho_\ell(F_p))^2/4$, i.e. such that $4p^{11} = \tau(p)^2$: this is a contradiction. With this case disposed of, we see that the centralizer of $\mathfrak{g}_\ell$ in $\mathrm{End}(V_\ell)$ is a *Cartan algebra* $\mathfrak{h}_\ell$, and that $\mathrm{im}(\rho_\ell)$ is contained in the normalizer N of $\mathfrak{h}_\ell$. In light of the structure of N, it follows that $\mathrm{im}(\rho_\ell)$ contains an open abelian subgroup of index 1 or 2. In other words, there exists an extension $E/\mathbb{Q}$ with $(E : \mathbb{Q}) \leq 2$ such that the representation ρ_ℓ is *abelian* over E. By applying the theorem of [17] (Chap. III, Sect. 3.1) to E and ρ_ℓ we find that ρ_ℓ is 'locally algebraic' over E. But according to the theorem in [17] (Chap. III, Sect. 2.3), this implies that all representations $\rho_{\ell'}$ (with respect to different primes ℓ') have the same property. In particular, each of the groups $\mathrm{im}(\rho_{\ell'})$ has an open abelian subgroup of index 1 or 2. This is absurd, since e.g. $\mathrm{im}(\rho_{11,1})$ is not solvable.

Questions

(a) Is it possible to determine the image of ρ_ℓ, as Swinnerton-Dyer has done for $\ell = 2$? More exactly, is $\mathrm{im}(\rho_\ell)$ contained in the subgroup H_ℓ of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ which consists of elements whose determinants are 11-th powers? Is is true that $\mathrm{im}(\rho_\ell) = H_\ell$ for almost all ℓ (or even for all $\ell \neq 2, 3, 5, 7, 23, 691$)?

It would be equally interesting to find a 'reason' explaining the special form of the representations modulo $2, 3, 5, 7, 23, 691$. There are (conjectural) indications at the end of Kuga's notes [9].

(b) Does the set of primes p such that $\tau(p) \equiv 0 \bmod p$ have density 0? Is it finite? Is it simply $\{2, 3, 5, 7\}$?

A (quite weak) analogy with the representations attached to elliptic curves suggests that $\tau(p) \equiv 0 \bmod p$ might have something to do with the structure of the *inertia subgroup* I_p of p in $\mathrm{im}\,(\rho_\ell)$, which is defined up to conjugacy. For example, is it true that I_p is *open* in $\mathrm{im}\,(\rho_\ell)$ if and only if $\tau(p) \equiv 0 \bmod p$?

For $p = 2, 3, 5, 7$, we have in fact $I_p = \mathrm{im}\,(\rho_\ell)$. [Proof: for these values of p, the congruences in Chap. 2 show that $\mathrm{im}\,(\rho_\ell)$ is a group extension of $(\mathbb{Z}/p\mathbb{Z})^\times$ by a prop-p group N[?]. The quotient group $(\mathbb{Z}/p\mathbb{Z})^\times$ corresponds to the cyclotomic field $\mathbb{Q}(\zeta_p)$. We conclude that I_p gets mapped *onto* $(\mathbb{Z}/p\mathbb{Z})^\times$, and it remains to show that $N \cap I_p = N$. Assume that $N \cap I_p \neq N$; then the elementary theory of p-groups shows the existence of a closed normal subgroup of index p in N which contains I_p; this subgroup corresponds to a cyclic unramified extension of degree p of $\mathbb{Q}(\zeta_p)$. According to class field theory, the class number of $\mathbb{Q}(\zeta_p)$ is divisible by p, and p is an irregular prime. But $p = 2, 3, 5, 7$ are regular: contradiction.]

Note that this argument does not apply to $p = 691$, which is an irregular prime (since it divides the numerator of the Bernoulli number B_{12}). In fact, it seems likely to me that, for $p = 691$, we have $I_p \neq \mathrm{im}\,(\rho_\ell)$, in other words, that the unramified extension of $\mathbb{Q}(\zeta_{691})$ really comes into play. Maybe one can attack this question by examining the values of $\tau(p) \bmod 691^2$.

(c) Does the restriction of ρ_p to the inertia subgroup I_p admit a 'Hodge decomposition' (cf. [17], Chap. III, Sect. 1.2) of type $(0, 11)$?

(d) If one assumes the truth of Ramanujan's conjecture that $|\tau(p)| < 2p^{11/2}$, is it possible to write the polynomial $H_p(X)$ of Sect. 1 in the form

$$H_p(X) = (1 - \alpha_p X)(1 - \overline{\alpha}_p X), \tag{31}$$

with $\alpha_p = p^{11/2} e^{i\phi_p}$, $0 < \phi_p < \pi$?

Is it true that the angles ϕ_p are equidistributed in the the interval $[0, \pi]$ with respect to the measure $\frac{2}{\pi} \sin^2 \phi d\phi$, as Sato and Tate have conjectured on the elliptic case without complex multiplication?

The question is connected ([17], Chap. I, A.2) with the question whether the Dirichlet series

$$L_m(s) = \prod_p \prod_{n=0}^{m} \frac{1}{1 - \alpha_p^n \overline{\alpha}_p^{m-n} p^{-s}}, \quad m = 1, 2, \ldots \tag{32}$$

can be extended to the complex plane. One would have to show that $L_m(s)$ can be extended to a holomorphic function such that $L_m(1 + \frac{11m}{2}) \neq 0$. Of course, it is also natural to conjecture that $L_m(s)$ has a functional equation of the usual type. More exactly, there should exist an 'infinite term' $\gamma_m(s)$ such that $\gamma_m(s)L_m(s)$ is invariant (or anti-invariant) under the transformation $s \longmapsto 11m + 1 - s$. We can even risk to conjecture the form of $\gamma_m(s)$:

$$\gamma_m(s) = \begin{cases} \frac{1}{(2\pi)^{ks}} \Gamma(s)\Gamma(s-11)\cdots\Gamma(s-11(k-1)), & \text{if} \quad m = 2k-1, \\ (\pi)^{-s/2}\Gamma(\frac{s-11k+\varepsilon}{2})\gamma_{m-1}(s), & \text{if} \quad m = 2k, \end{cases} \tag{33}$$

where $\varepsilon = 0$ if k is even, and $\varepsilon = 1$ otherwise. It seems that only the cases $m = 1$ and $m = 2$ are known; $L_1(s)$ coincides with the function $L_\tau(s)$ of Sect. 1, and $L_2(s)$ is connected by a simple formula with the function

$$f(s) = \sum_{n=1}^{\infty} \tau(n)^2 n^{-s} \tag{34}$$

studied by Rankin (cf. Hardy [5], p. 174–180).

Generalizations to modular forms

Everything we have said here about τ can also be said about the coefficients of any cusp form of weight k

$$\Phi(x) = \sum_{n=1}^{\infty} a_n x^n, \quad a_1 = 1, \tag{35}$$

which is an eigen function of Hecke operators, and whose coefficients are ordinary integers. Again, it is possible to prove that $\mathrm{im}\,(\rho_\ell)$ is *open* in $\mathrm{GL}\,(2, \mathbb{Q}_\ell)$.

According to Kuga ([9], last part), we should expect that the representations modulo $2, 3, 5, 7$ have special properties; it would be interesting to find these representations, and to study the case of other primes as well.

Example. Take $k = 16$; here we have

$$\Phi(x) = D(x)E_4(X) = \Big(\sum_{n=1}^{\infty} \tau(n)x^n\Big)\Big(1 + 240\sum_{n=1}^{\infty} \sigma_3(n)x^n\Big). \tag{36}$$

One observes easily that

$$a_p \equiv p + p^2 \bmod 7 \tag{37}$$

$$a_p \equiv 1 + p^{15} \bmod 3617. \tag{38}$$

(Observe that 3617 is the numerator of the Bernoulli number B_{16}; it is therefore an irregular prime).

As for cusp forms of $\mathrm{SL}\,(2, \mathbb{Z})$ which are eigen functions of Hecke operators but do not have integral coefficients, they should correspond to 'E-rational' representations in the sense of [17] (Chap. I, Sect. 2.3). Moreover, if the space of cusp forms has dimension h, it should be possible to find ℓ-adic representations of degree $2h$ on which the Hecke operators T_p act, and by reducing these representations of the Hecke algebra one should find the representations of degree 2 we are interested in.

6 History

The idea of viewing certain arithmetic functions as traces of the action of the Frobenius goes back to Davenport-Hasse. There, only exponential sums were treated whose properties were already known (Gauss and Jacobi sums). The note of Weil goes further: he gives a 'Frobenius interpretation' of all exponential sums in one variable, and he obtained (thanks to the 'Riemann hypothesis for curves') an upper bound which was not known before. For example, for the Kloosterman sums

$$S_p(a,b) = \sum_{x=1}^{p-1} \exp\Big(\frac{2\pi i}{p}(ax + bx^{-1})\Big), \quad p \nmid ab \tag{39}$$

one finds

$$|S_p(a,b)| \leq 2p^{1/2}. \tag{40}$$

Weil has remarked long ago the analogy of Ramanujan's conjecture

$$|\tau(n)| \leq 2p^{11/2} \tag{41}$$

with the inequality (40). Weil suggested that $\tau(p)$ can be written as $\tau(p) = \alpha_p + \overline{\alpha}_p$, where α_p and $\overline{\alpha}_p$ are the eigenvalues of a Frobenius endomorphism which acts on a suitable cohomology of dimension 11. On the other hand, he asked me in 1960 about the interpretation of the known congruences on $\tau(p)$ in this connection (I was not able to answer his question then, because I had not understood the relation between 'cohomology' and 'ℓ-adic representations').

An important step towards the cohomological interpretation of $\tau(p)$ was done by Eichler [4]; he showed how the coefficients of the cusp forms of weight 2 (for certain congruence subgroups of the modular group) are connected to the Tate modules of the corresponding modular curve. His results have been taken up by Shimura [19] and been completed in an essential point by Igusa [7].

For arbitrary weight k, Sato (cf. [10], Introduction) had the idea of considering the fibered variety, whose fibers are the product of $k-2$ copies of the generic elliptic curve (the base being the modular curve). The ideas of Sato have been made precise by Kuga and Shimura [10]:
1. they talk about the 'number of points' instead of 'cohomology groups'; thus they do not obtain ℓ-adic representations;
2. the group they consider is not the modular group $\mathrm{SL}(2,\mathbb{Z})$, but a unit group of the quaternions, which has a compact quotient (this simplifies their task).

Nevertheless, one could hope that the ideas of Sato, Kuga and Shimura, combined with general theorems form ℓ-adic cohomology due to Grothendieck and Artin [1], allow us to construct a theory which can be applied to the modular group and its congruence subgroups. This hope seems to be at the point of becoming real: P. Deligne succeeded in showing more than what is needed for establishing the conjecture in Sect. 3 and for reducing Ramanujan's conjecture to 'standard conjectures' of Weil (this last point has already been treated by Ihara [8] by using an extremely ingenious method). For more details, see the seminar of Deligne at I.H.E.S., 'Conjecture de Ramanujan et représentations ℓ-adiques', which begins on February 28m 1968.

References

[1] M. Artin, A. Grothendieck, *Cohomologie étale des schémas*, Séminaire de Géométrie Algébrique, I.H.E.S. 1963/64 13

[2] R. P. Bambah, *Two congruence properties of Ramanujan's function $\tau(n)$*, J. London Math. Soc. **21** (1946), 91–93 2, 3, 4

[3] H. Davenport, H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182

[4] M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Arch. Math. **5** (1954), 355–366 13

[5] G. H. Hardy, *Ramanujan. Twelve lectures on subjects suggested by his life and his work*, Cambridge Univ. Press 1940 1, 12

[6] E. Hecke, *Mathematische Werke*, Göttingen 1959 1

[7] J. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. **81** (1959), 561–577 13

[8] Y. Ihara, *Hecke polynomials as congruence ζ functions in elliptic modular case*, Annals Math. **85** (1967), 267–295 13

[9] M. Kuga, *Fiber varieties over a symmetric space whose fibers are abelian varieties*, lecture notes Chicago, 1963/64 10, 12

[10] M. Kuga, G. Shimura, *On the zeta function of a fibre variety whose fibers are abelian varieties*, Annals Math. **82** (1965), 478–539 13

[11] D. H. Lehmer, *Ramanujan's function $\tau(n)$*, Duke Math. J. **10** (1943), 483–492 1

[12] D. H. Lehmer, *The vanishing of Ramanujan's function $\tau(n)$*, Duke Math. J. **14** (1947), 429–433 4, 5

[13] D. H. Lehmer, *Notes on some arithmetical properties of elliptic modular functions*, unpublished lecture notes 2, 3, 4, 5

[14] L. J. Mordell, *On Mr. Ramanujan's empirical expressions of modular functions*, Proc. Cambr. Phil. Soc. **19** (1917), 117–124 1

[15] K. G. Ramanathan, *Congruence properties of Ramanujan's function $\tau(n)$ (II)*, J. Indian Math. Soc. **9** (1945), 55–59 3, 4

[16] S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Phil. Soc. **22** (1916), 159–184 1, 4

[17] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, New York 1968 6, 8, 10, 11, 12

[18] G. Shimura, *Correspondances modulaires et les fonctions zêtas des courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1–28

[19] G. Shimura, *A reciprocity law in non-solvable extensions*, J. Reine Angew. Math. **221** (1966), 209–220 7, 8, 9, 13

[20] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA **34** (1948), 204–207

[21] J. R. Wilton, *Congruence properties of Ramanujan's function* $\tau(n)$, Proc. London Math. Soc. **31** (1930), 1–10 3, 4

The original appeared as
Une interpretation des congruences rélatives a la fonction de Ramanujan, Semin. Delange-Pisot-Poitou 9 (1967/68), Théorie Nombres, No.14, 17p. (1969).

Translated by Franz Lemmermeyer