# On some mathematical connections between Fermat's Last Theorem, Modular Functions, Modular Elliptic Curves and some sector of String Theory

**Michele Nardelli** [1,2]

[1] Dipartimento di Scienze della Terra – Università degli Studi di Napoli "Federico II"
Largo S. Marcellino, 10 – 80138 Napoli (Italy)

[2] Dipartimento di Matematica ed Applicazioni "R. Caccioppoli"
Università degli Studi di Napoli "Federico II" – Polo delle Scienze e delle Tecnologie
Monte S. Angelo, Via Cintia (Fuorigrotta), 80126 Napoli (Italy)

## Abstract

This paper is fundamentally a review, a thesis, of principal results obtained in some sectors of Number Theory and String Theory of various authoritative theoretical physicists and mathematicians.
Precisely, we have described some mathematical results regarding the Fermat's Last Theorem, the Mellin transform, the Riemann zeta function, the Ramanujan's modular equations, how primes and adeles are related to the Riemann zeta functions and the p-adic and adelic string theory.
Furthermore, we show that also the fundamental relationship concerning the Palumbo-Nardelli model (a general relationship that links bosonic string action and superstring action, i.e. bosonic and fermionic strings in all natural systems), can be related with some equations regarding the p-adic (adelic) string sector.
Thence, in conclusion, we have described some new interesting connections that are been obtained between String Theory and Number Theory, with regard the arguments above mentioned.

## Introduzione e riassunto

L'ultimo teorema di Fermat è una generalizzazione dell'equazione diofantea $a^2 + b^2 = c^2$. Già gli antichi Greci ed i Babilonesi sapevano che questa equazione ha delle soluzioni intere, come (3, 4, 5) $(3^2 + 4^2 = 5^2)$ o (5, 12, 13) $(5^2 + 12^2 = 13^2)$. Queste soluzioni sono conosciute come "terne pitagoriche" e ne esistono infinite, anche escludendo le soluzioni banali per cui a, b e c hanno un divisore in comune e quelle ancor più banali in cui almeno uno dei numeri è uguale a zero.
Secondo l'ultimo teorema di Fermat, non esistono soluzioni intere positive quando l'esponente 2 è sostituito da un numero intero maggiore. Il teorema è particolarmente noto per la sua correlazione con molti argomenti matematici che apparentemente non hanno nulla a che vedere con la Teoria dei Numeri. Inoltre, la ricerca di una dimostrazione è stata all'origine dello sviluppo di importanti aree della matematica, anche legate a moderni settori della fisica teorica, quali ad esempio la Teoria delle Stringhe.
L'ultimo teorema di Fermat può essere dimostrato per n = 4 e nel caso in cui n è un numero primo: se infatti si trova una soluzione $a^{kp} + b^{kp} = c^{kp}$, si ottiene immediatamente una soluzione $\left(a^k\right)^p + \left(b^k\right)^p = \left(c^k\right)^p$. Nel corso degli anni il teorema venne dimostrato per un numero sempre maggiore di esponenti speciali n, ma il caso generale rimaneva evasivo. Il caso n = 5 è stato

dimostrato da Dirichlet e Legendre nel 1825 ed il caso n = 7 da Gabriel Lamé nel 1839. Nel 1983 G. Faltings dimostrò la congettura di Mordell, che implica che per ogni n > 2, c'è al massimo un numero finito di interi "co-primi" a, b e c con $a^n + b^n = c^n$. (In matematica, gli interi a e b si dicono "co-primi" o "primi tra loro" se e solo se essi non hanno nessun divisore comune eccetto 1 e -1, o, equivalentemente, se il loro massimo comune divisore è 1).
Utilizzando i sofisticati strumenti della geometria algebrica (in particolare curve ellittiche e forme modulari), della teoria di Galois e dell'algebra di Hecke, il matematico di Cambridge Andrew John Wiles, dell'Università di Princeton, con l'aiuto del suo primo studente, Richard Taylor, diede una dimostrazione dell'ultimo teorema di Fermat, pubblicata nel 1995 nella rivista specialistica "Annals of Mathematics".
Nel 1986, Ken Ribet aveva dimostrato la "Congettura Epsilon" di Gerhard Frey secondo la quale ogni contro-esempio $a^n + b^n = c^n$ all'ultimo teorema di Fermat avrebbe prodotto una curva ellittica definita come: $y^2 = x \cdot (x - a^n) \cdot (x + b^n)$, che fornirebbe un contro-esempio alla "Congettura di Taniyama-Shimura". Quest'ultima congettura propone un collegamento profondo fra le curve ellittiche e le forme modulari. Wiles e Taylor hanno stabilito un caso speciale della Congettura di Taniyama-Shimura sufficiente per escludere tali contro-esempi in seguito all'ultimo teorema di Fermat. In pratica, la dimostrazione che le curve ellittiche semistabili sui razionali sono modulari, rappresenta una forma ridotta della Congettura di Taniyama-Shimura che tuttavia è sufficiente per provare l'ultimo teorema di Fermat.
Le curve ellittiche sono molto importanti nella Teoria dei Numeri e ne costituiscono il maggior campo di ricerca attuale. Nel campo delle curve ellittiche, i "numeri p-adici" sono conosciuti come "numeri l-adici", a causa dei lavori di Jean-Pierre Serre. Il numero primo p è spesso riservato per l'aritmetica modulare di queste curve.
Il sistema dei numeri p-adici è stato descritto per la prima volta da Kurt Hensel nel 1897. Per ogni numero primo p, il sistema dei numeri p-adici estende l'aritmetica dei numeri razionali in modo differente rispetto l'estensione verso i numeri reali e complessi. L'uso principale di questo strumento viene fatto nella Teoria dei Numeri. L'estensione è ottenuta da un'interpretazione alternativa del concetto di valore assoluto. Il motivo della creazione dei numeri p-adici era il tentativo di introdurre il concetto e le tecniche delle "serie di potenze" nel campo della Teoria dei Numeri. Più concretamente per un dato numero primo p, il campo $Q_p$ dei numeri p-adici è un'estensione dei numeri razionali. Se tutti i campi $Q_p$ vengono considerati collettivamente, si arriva al "principio locale-globale" di Helmut Hasse, il quale, a grandi linee, afferma che certe equazioni possono essere risolte nell'insieme dei numeri razionali se e solo se possono essere risolte negli insiemi dei numeri reali e dei numeri p-adici per ogni p. Il campo $Q_p$ possiede una topologia derivata da una metrica, che è, a sua volta, derivata da una stima alternativa dei numeri razionali. Questa metrica è "completa", nel senso che ogni serie di Cauchy converge.
Scopo del presente lavoro è quello di evidenziare le connessioni ottenute tra la matematica inerente la dimostrazione dell'ultimo teorema di Fermat ed alcuni settori della Teoria di Stringa, precisamente la supersimmetria p-adica e adelica in teoria di stringa.
I settori inerenti la dimostrazione dell'ultimo teorema di Fermat, riguardano quelle funzioni chiamate L p-adiche connesse alla funzione zeta di Riemann, quale estensione analitica al piano complesso della serie di Dirichlet. Tali funzioni sono strettamente correlate sia ai numeri primi, sia alla funzione zeta, i cui teoremi sono già stati connessi matematicamente con la teoria di stringa in alcuni precedenti lavori.
Quindi, per concludere, anche dalla matematica che riguarda l'ultimo teorema di Fermat è possibile ottenere, come vedremo nel corso del lavoro, ulteriori connessioni tra Teoria di Stringa (p-adic string theory), Numeri Primi, Funzione zeta di Riemann (numeri p-adici, funzioni L p-adiche) e Serie di Fibonacci (quindi identità e funzioni di Ramanujan), che, a loro volta, verranno correlate anche al modello Palumbo-Nardelli.

## Chapter 1.

## The mathematics concerning the Fermat's Last Theorem

### 1.1 The Wiles approach

An elliptic curve over Q is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over Q with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular. A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over Q is modular.
In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The Wiles approach to the study of elliptic curves is via their associated Galois representations. Suppose that $\rho_p$ is the representation of $Gal(\overline{Q}/Q)$ on the p-division points of an elliptic curve over Q, and suppose that $\rho_3$ is irreducible. The choice of 3 is critical because a crucial theorem of Langlands and Tunnell shows that if $\rho_3$ is irreducible then it is also modular. Thence, under the hypothesis that $\rho_3$ is semistable at 3, together with some milder restrictions on the ramification of $\rho_3$ at the other primes, every suitable lifting of $\rho_3$ is modular. Furthermore, Wiles has obtained that E is modular if and only if the associated 3-adic representation is modular.
The key development in the proof is a new and surprising link between two strong but distinct traditions in number theory, the relationship between Galois representations and modular forms on the one hand and the interpretation of special values of L-functions on the other.
The restriction that $\rho_3$ be irreducible at 3 is bypassed by means of an intriguing argument with families of elliptic curves which share a common $\rho_5$. Using this, we complete the proof that all semistable elliptic curves are modular. In particular, this yields to the proof of Fermat's Last Theorem.
Now we present the methods and results in more detail.
Let f be an eigenform associated to the congruence subgroup $\Gamma_1(N)$ of $SL_2(Z)$ of weight $k \geq 2$ and character $\chi$. Thus if $T_n$ is the Hecke operator associated to an integer n there is an algebraic integer $c(n,f)$ such that $T_n f = c(n,f)f$ for each n. We let $K_f$ be the number field generated over Q by the $\{c(n,f)\}$ together with the values of $\chi$ and let $\mathrm{O}_f$ be its ring of integers. For any prime $\lambda$ of $\mathrm{O}_f$ let $\mathrm{O}_{f,\lambda}$ be the completion of $\mathrm{O}_f$ at $\lambda$. The following theorem is due to Eichler and Shimura (for k > 2).

THEOREM 1.

*For each prime* $p \in Z$ *and each prime* $\lambda | p$ *of* $\mathrm{O}_f$ *there is a continuous representation*

$$\rho_{f,\lambda} : Gal(\overline{Q}/Q) \to GL_2(\mathrm{O}_{f,\lambda}) \quad (1)$$

*which is unramified outside the primes dividing Np and such that for all primes q | Np,*

$$trace\ \rho_{f,\lambda}(Frob\ q) = c(q,f), \quad \det\ \rho_{f,\lambda}(Frob\ q) = \chi(q)q^{k-1}. \quad (2)$$

We will be concerned with trying to prove results in the opposite direction, that is to say, with establishing criteria under which a $\lambda$-adic representation arises in this way from a modular form.
Assume

$$\rho_0 : Gal(\overline{Q}/Q) \to GL_2(\overline{F}_p) \qquad (3)$$

is a continuous representation with values in the algebraic closure of a finite field of characteristic p and that $\det \rho_0$ is odd. We say that $\rho_0$ is modular if $\rho_0$ and $\rho_{f,\lambda} \bmod \lambda$ are isomorphic over $\overline{F}_p$ for some $f$ and $\lambda$ and some embedding of $O_f / \lambda$ in $\overline{F}_p$. Serre has conjectured that every irreducible $\rho_0$ of odd determinant is modular.
If O is the ring of integers of a local field (containing $Q_p$) we will say that

$$\rho : Gal(\overline{Q}/Q) \to GL_2(O) \qquad (4)$$

is a lifting of $\rho_0$ if, for a specified embedding of the residue field of O in $\overline{F}_p$, $\overline{\rho}$ and $\rho_0$ are isomorphic over $\overline{F}_p$. We will restrict our attention to two cases:

(I) $\rho_0$ is ordinary (at p) by which we mean that there is a one-dimensional subspace of $\overline{F}_p^2$, stable under a decomposition group at p and such that the action on the quotient space is unramified and distinct from the action on the subspace.

(II) $\rho_0$ is flat (at p), meaning that as a representation of a decomposition group at p, $\rho_0$ is equivalent to one that arises from a finite flat group scheme over $Z_p$, and $\det \rho_0$ restricted to an inertia group at p is the cyclotomic character.

CONJECTURE.

*Suppose that $\rho : Gal(\overline{Q}/Q) \to GL_2(O)$ is an irreducible lifting of $\rho_0$ and that $\rho$ is unramified outside of a finite set of primes. There are two cases:*

(i) *Assume that $\rho_0$ is ordinary. Then if $\rho$ is ordinary and $\det \rho = \varepsilon^{k-1}\chi$ for some integer $k \geq 2$ and some $\chi$ of finite order, $\rho$ comes from a modular form.*

(ii) *Assume that $\rho_0$ is flat and that p is odd. Then if $\rho$ restricted to a decomposition group at p is equivalent to a representation on a p-divisible group, again $\rho$ comes from a modular form.*

Now we will assume that p is an odd prime, we have the following theorem:

THEOREM 2.

*Suppose that $\rho_0$ is irreducible and satisfies either (I) or (II) above. Suppose also that*

(i) *$\rho_0$ is absolutely irreducible when restricted to $Q\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.*

(ii) *If $q \equiv -1 \bmod p$ is ramified in $\rho_0$ then either $\rho_0 | D_q$ is reducible over the algebraic closure*

*where $D_q$ is a decomposition group at q or $\rho_0|I_q$ is absolutely irreducible where $I_q$ is an inertia group at q.*

*Then any representation $\rho$ as in the conjecture does indeed come from a modular form.*

The only condition which really seems essential to our method is the requirement that $\rho_0$ is modular. The most interesting case at the moment is when p = 3 and $\rho_0$ can be defined over $F_3$. Then since $PGL_2(F_3) \cong S_4$ every such representation is modular by the theorem of Langlands and Tunnell. In particular, every representation into $GL_2(Z_3)$ whose reduction satisfies the given conditions is modular. We deduce:

THEOREM 3.

*Suppose that E is an elliptic curve defined over Q and that $\rho_0$ is the Galois action on the 3-division points. Suppose that E has the following properties:*

- *(i) E has good or multiplicative reduction at 3.*
- *(ii) $\rho_0$ is absolutely irreducible when restricted to $Q(\sqrt{-3})$.*
- *(iii) For any $q \equiv -1 \mod 3$ either $\rho_0|D_q$ is reducible over the algebraic closure or $\rho_0|I_q$ is absolutely irreducible.*

*Then E should be modular.*

The important class of semistable curves, i.e., those with square-free conductor, satisfies (i) and (iii) but not necessarily (ii).

THEOREM 4.

*Suppose that E is a semistable elliptic curve defined over Q. Then E is modular.*

In 1986, Serre conjectured and Ribet proved a property of the Galois representation associated to modular forms which enabled Ribet to show that Theorem 4 implies "Fermat's Last Theorem". Furthermore, we have the following theorems:

THEOREM 5.

*Suppose that $u^p + v^p + w^p = 0$ with $u,v,w \in Q$ and $p \geq 3$ then $uvw = 0$. (Equivalently – there are no non-zero integers a,b,c,n with n > 2 such that $a^n + b^n = c^n$.)*

THEOREM 6.

*Suppose that $\rho_0$ is irreducible and satisfies the hypothesis of the conjecture, including (I) above. Suppose further that*

*(i) $\rho_0 = Ind_L^Q \kappa_0$ for a character $\kappa_0$ of an imaginary quadratic extension L of Q which is unramified at p.*

*(ii)* $\det \rho_0 \big| I_p = \omega$.

Then a representation $\rho$ as in the conjecture does indeed come from a modular form.

Wiles has worked on the Iwasawa conjecture for totally real fields and some applications of it, with the assumption that the reduction of a given $\ell$-adic representation was reducible and tried to prove under this hypothesis that the representation itself would have to be modular. Thence, we write p for $\ell$ because of the connections with Iwasawa theory.
In the solution to the Iwasawa conjecture for totally real fields, Wiles has introduced a new technique in order to deal with the trivial zeroes.
It involved replacing the standard Iwasawa theory method of considering the fields in the cyclotomic $Z_p$-extension by a similar analysis based on a choice of infinitely many distinct primes $q_i \equiv 1 \mod p^{n_i}$ with $n_i \to \infty$ as $i \to \infty$. Wiles has developed further the idea of using auxiliary primes to replace the change of field that is used in Iwasawa theory.

Let p be an odd prime. Let $\Sigma$ be a finite set of primes including p and let $Q_\Sigma$ be the maximal extension of $Q$ unramified outside this set and $\infty$. Throughout we fix an embedding of $\overline{Q}$, and so also of $Q_\Sigma$, in C. We will also fix a choice of decomposition group $D_q$ for all primes q in Z. Suppose that k is a finite field characteristic p and that

$$\rho_0 : Gal(Q_\Sigma / Q) \to GL_2(k) \qquad (5)$$

is an irreducible representation. We will assume that $\rho_0$ comes with its field of definition k and that $\det \rho_0$ is odd.
We will restrict our choice of $\rho_0$ further by assuming that either:

(i) $\rho_0$ is ordinary. The restriction of $\rho_0$ to the decomposition group $D_p$ has (for a suitable choice of basis) the form

$$\rho_0 \Big| D_p \approx \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} \qquad (6)$$

where $\chi_1$ and $\chi_2$ are homomorphisms from $D_p$ to $k^*$ with $\chi_2$ unramified. Moreover we require that $\chi_1 \neq \chi_2$.

(ii) $\rho_0$ is flat at p but not ordinary. Then $\rho_0 \big| D_p$ is the representation associated to a finite flat group scheme over $Z_p$ but is not ordinary in the sense of (i). We will assume also that $\det \rho_0 \big| I_p = \omega$ where $I_p$ is an inertia group at p and $\omega$ is the Teichmuller character giving the action on $p^{th}$ roots of unity.

Furthermore, we have the following restrictions on the deformations:

(i) (a) *Selmer deformations*. In this case we assume that $\rho_0$ is ordinary, with notion as above, and

that the deformation has a representative $\rho : Gal(Q_\Sigma / Q) \to GL_2(A)$ with the property that (for a suitable choice of basis)

$$\rho\Big|D_p \approx \begin{pmatrix} \tilde{\chi}_1 & * \\ 0 & \tilde{\chi}_2 \end{pmatrix}$$

with $\tilde{\chi}_2$ unramified, $\tilde{\chi} \equiv \chi_2 \mod m$, and $\det \rho\Big|I_p = \varepsilon\omega^{-1}\chi_1\chi_2$ where $\varepsilon$ is the cyclotomic character, $\varepsilon : Gal(Q_\Sigma / Q) \to Z_p^*$, giving the action on all p-power roots of unity, $\omega$ is of order prime to p satisfying $\omega \equiv \varepsilon \mod p$, and $\chi_1$ and $\chi_2$ are the characters of (i) viewed as taking values in $k^* \mapsto A^*$.

(i) (b) *Ordinary deformations*. The same as in (i) (a) but with no condition on the determinant.

(i) (c) *Strict deformations*. This is a variant on (i) (a) which we only use when $\rho_0\Big|D_p$ is not semisimple and not flat. We also assume that $\chi_1\chi_2^{-1} = \omega$ in this case. Then a strict deformation is an in (i) (a) except that we assume in addition that $(\tilde{\chi}_1 / \tilde{\chi}_2)\Big|D_p = \varepsilon$.

(ii) *Flat (at p) deformations*. We assume that each deformations $\rho$ to $GL_2(A)$ has the property that for any quotient A / a of finite order $\rho\Big|D_p \mod a$ is the Galois representation associated to the $\overline{Q}_p$-points of a finite flat group scheme over $Z_p$.

In each of these four cases, as well as in the unrestricted case one can verify that Mazur's use of Schlessinger's criteria proves the existence of a universal deformation

$$\rho : Gal(Q_\Sigma / Q) \to GL_2(R) \quad (7)$$

With regard the primes $q \neq p$ which are ramified in $\rho_0$, we distinguish three special cases:

(A) $\rho_0\Big|D_q = \begin{pmatrix} \chi_1 & * \\ & \chi_2 \end{pmatrix}$ for a suitable choice of basis, with $\chi_1$ and $\chi_2$ unramified, $\chi_1\chi_2^{-1} = \omega$ and the fixed space of $I_q$ of dimension 1,

(B) $\rho_0\Big|I_q = \begin{pmatrix} \chi_q & 0 \\ 0 & 1 \end{pmatrix}$, $\chi_q \neq 1$, for a suitable choice of basis,

(C) $H^1(Q_q, W_\lambda) = 0$ where $W_\lambda = \{f \in Hom_k(U_\lambda, U_\lambda) : tracef = 0\} \cong (Sym^2 \otimes \det^{-1})\rho_0$.

Then in each case we can define a suitable deformation theory by imposing additional restrictions on those we have already considered, namely:

(A) $\rho\Big|D_q = \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix}$ for a suitable choice of basis of $A^2$ with $\psi_1$ and $\psi_2$ unramified and $\psi_1\psi_2^{-1} = \varepsilon$;

(B) $\rho\big|I_q = \begin{pmatrix} \chi_q & 0 \\ 0 & 1 \end{pmatrix}$ for a suitable choice of basis ( $\chi_q$ of order prime to p, so the same character as above);

(C) $\det\rho\big|I_q = \det\rho_0\big|I_q$, i.e., of order prime to p.

Thus if $\mathrm{M}$ is a set of primes in $\Sigma$ distinct from p and each satisfying one of (A), (B) or (C) for $\rho_0$, we will impose the corresponding restriction at each prime in $\mathrm{M}$.
Thus to each set of data $D=\{\cdot,\Sigma,\mathrm{O},\mathrm{M}\}$ where . is Se, str, ord, flat or unrestricted, we can associate a deformation theory to $\rho_0$ provided

$$\rho_0 : Gal(Q_\Sigma / Q) \to GL_2(k) \qquad (8)$$

is itself of type $D$ and $\mathrm{O}$ is the ring of integers of a totally ramified extension of $W(k)$; $\rho_0$ is ordinary if . is Se or ord, strict if . is strict and flat if . is flat; $\rho_0$ is of type $\mathrm{M}$, i.e., of type (A), (B) or (C) at each ramified primes $q \neq p$, $q \in \mathrm{M}$.

Suppose that q is a prime not dividing N. Let $\Gamma_1(N,q)=\Gamma_1(N)\cap\Gamma_0(q)$ and let $X_1(N,q)=X_1(N,q)_{/Q}$ be the corresponding curve. The two natural maps $X_1(N,q)\to X_1(N)$ induced by the maps $z\to z$ and $z\to qz$ on the upper half plane permit us to define a map $J_1(N)\times J_1(N)\to J_1(N,q)$. Using a theorem of Ihara, Ribet shows that this map is injective. Thus we can define $\varphi$ by

$$0 \to J_1(N)\times J_1(N) \xrightarrow{\varphi} J_1(N,q). \qquad (9)$$

Dualizing, we define B by

$$0 \to B \xrightarrow{\psi} J_1(N,q) \xrightarrow{\hat{\varphi}} J_1(N)\times J_1(N) \to 0\,.$$

Let $T_1(N,q)$ be the ring of endomorphism of $J_1(N,q)$ generated by the standard Hecke operators. One can check that $U_p$ preserves B either by an explicit calculation or by noting that B is the maximal abelian subvariety of $J_1(N,q)$ with multiplicative reduction at q. We set $J_2 = J_1(N)\times J_1(N)$. More generally, one can consider $J_H(N)$ and $J_H(N,q)$ in place of $J_1(N)$ and $J_1(N,q)$ (where $J_H(N,q)$ corresponds to $X_1(N,q)/H$ ) and we write $T_H(N)$ and $T_H(N,q)$ for the associated Hecke rings.
In the following lemma if $m$ is a maximal ideal of $\mathrm{T}_1(Nq^{r-1})$ or $\mathrm{T}_1(Nq^r)$ we use $m^{(q)}$ to denote the maximal ideal of $\mathrm{T}_1^{(q)}(Nq^r,q^{r+1})$ compatible with $m$, the ring $\mathrm{T}_1^{(q)}(Nq^r,q^{r+1})\subset\mathrm{T}_1(Nq^r,q^{r+1})$ being the sub-ring obtained by omitting $U_q$ from the list of generators.

LEMMA 1.

*If $q\neq p$ is a prime and $r\geq 1$ then the sequence of abelian varieties*

$$0 \to J_1(Nq^{r-1}) \xrightarrow{\xi_1} J_1(Nq^r)\times J_1(Nq^r) \xrightarrow{\xi_2} J_1(Nq^r,q^{r+1}) \qquad (10)$$

*where* $\xi_1=\left((\pi_{1,r}\circ\pi)^*,-(\pi_{2,r}\circ\pi)^*\right)$ *and* $\xi_2=\left(\pi_{4,r}^*,\pi_{3,r}^*\right)$ *induces a corresponding sequence of p-divisible groups which becomes exact when localized at any* $m^{(q)}$ *for which* $\rho_m$ *is irreducible*.

Now, we have the following theorem:

THEOREM 7.

*Assume that* $\rho_0$ *is modular and absolutely irreducible when restricted to* $Q\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$. *Assume also that* $\rho_0$ *is of type (A), (B) or (C) at each* $q\neq p$ *in* $\Sigma$. *Then the map* $\varphi_D:R_D\to \mathrm{T}_D$ *(remember that* $\varphi_D$ *is an isomorphism) is an isomorphism for all* $D$ *associated to* $\rho_0$, *i.e., where* $D=(\cdot,\Sigma,\mathrm{O},\mathrm{M})$ *with* $\cdot=Se$, *str, fl or ord. In particular if* $\cdot=Se$, *str or fl and* $f$ *is any newform for which* $\rho_{f,\lambda}$ *is a deformation of* $\rho_0$ *of type* $D$ *then*

$$\#H_D^1\left(Q_\Sigma/Q,V_f\right)=\#\left(\mathrm{O}/\eta_{D,f}\right)<\infty \quad (11)$$

*where* $\eta_{D,f}$ *is the invariant defined in the following equation* $(\eta)=\left(\eta_{D,f}\right)=(\hat{\pi}(1))$.

We assume that

$$\rho=Ind_L^Q\kappa:Gal\left(\overline{Q}/Q\right)\to GL_2(\mathrm{O}) \quad (12)$$

is the p-adic representation associated to a character $\kappa:Gal\left(\overline{L}/L\right)\to \mathrm{O}^\times$ of an imaginary quadratic field $L$.
Let $M_\infty$ be the maximal abelian p-extension of $L(\nu)$ unramified outside $p$.

PROPOSITION 1.

*There is an isomorphism*

$$H_{unr}^1\left(Q_\Sigma/Q,Y^*\right)\tilde{\to}Hom\left(Gal\left(M_\infty/L(\nu)\right),(K/\mathrm{O})(\nu)\right)^{Gal(L(\nu)/L)} \quad (13)$$

*where* $H_{unr}^1$ *denotes the subgroup of classes which are Selmer at p and unramified everywhere else.*

Now we write $H_{str}^1\left(Q_\Sigma/Q,Y_n^*\right)$ (where $Y_n^*=Y_{\lambda^n}^*$ and similarly for $Y_n$) for the subgroup of $H_{unr}^1\left(Q_\Sigma/Q,Y_n^*\right)=\left\{\alpha\in H_{unr}^1\left(Q_\Sigma/Q,Y_n^*\right):\alpha_p=0 in H^1\left(Q_p,Y_n^*/\left(Y_n^*\right)^0\right)\right\}$ where $\left(Y_n^*\right)^0$ is the first step in the filtration under $D_p$, thus equal to $\left(Y_n/Y_n^0\right)^*$ or equivalently to $\left(Y^*\right)_{\lambda^n}^0$ where $\left(Y^*\right)^0$ is the divisible submodule of $Y^*$ on which the action of $I_p$ is via $\varepsilon^2$. It follows from an examination of the action $I_p$ on $Y_\lambda$ that

$$H_{str}^1\left(Q_\Sigma/Q,Y_n\right)=H_{unr}^1\left(Q_\Sigma/Q,Y_n\right). \quad (14)$$

In the case of $Y^*$ we will use the inequality

$$\#H^1_{str}\left(Q_\Sigma/Q,Y^*\right)\le\#H^1_{unr}\left(Q_\Sigma/Q,Y^*\right). \quad (15)$$

Furthermore, for n sufficiently large the map

$$H^1_{str}\left(Q_\Sigma/Q,Y_n^*\right)\to H^1_{str}\left(Q_\Sigma/Q,Y^*\right) \quad (16)$$

is injective.
The above map is then injective whenever the connecting homomorphism

$$H^0\left(L_{p^*},(K/\mathrm{O})(\nu)\right)\to H^1\left(L_{p^*},(K/\mathrm{O})(\nu)_{\lambda^n}\right)$$

is injective, which holds for sufficiently large n. Furthermore, we have

$$\frac{\#H^1_{str}\left(Q_\Sigma/Q,Y_n\right)}{\#H^1_{str}\left(Q_\Sigma/Q,Y_n^*\right)}=\#H^0\left(Q_p,\left(Y_n^0\right)^*\right)\frac{\#H^0\left(Q,Y_n\right)}{\#H^0\left(Q,Y_n^*\right)}. \quad (17)$$

Thence, setting $t=\inf_q\#\left(\mathrm{O}/\left(1-\nu(q)\right)\right)$ if $\nu \bmod \lambda=1$ or $t=1$ if $\nu \bmod \lambda\neq 1$ (17b), we get

$$\#H^1_{Se}\left(Q_\Sigma/Q,Y\right)\le\frac{1}{t}\cdot\prod_{\in\Sigma}\ell_q\cdot\#Hom\left(Gal\left(M_\infty/L(\nu)\right),(K/\mathrm{O})(\nu)\right)^{Gal(L(\nu)/L)} \quad (18)$$

where $\ell_q=\#H^0\left(Q_q,Y^*\right)$ for $q\neq p$, $\ell_p=\lim_{n\to\infty}\#H^0\left(Q_p,\left(Y_n^0\right)^*\right)$. This follows from Proposition 1, (14)-(17) and the elementary estimate

$$\#\left(H^1_{Se}\left(Q_\Sigma/Q,Y\right)/H^1_{unr}\left(Q_\Sigma/Q,Y\right)\right)\le\prod_{q\in\Sigma-\{p\}}\ell_q, \quad (19)$$

which follows from the fact that $\#H^1\left(Q_q^{unr},Y\right)^{Gal\left(Q_q^{unr}/Q_q\right)}=\ell_q$. (Remember that $\ell$ is the $\ell$-adic representation).
Let $w_f$ denote the number of roots of unity $\zeta$ of $L$ such that $\zeta\equiv 1 \bmod f$ ($f$ an integral ideal of $\mathrm{O}_L$). We choose an $f$ prime to p such that $w_f=1$. Then there is a grossencharacter $\varphi$ of $L$ satisfying $\varphi((\alpha))=\alpha$ for $\alpha\equiv 1 \bmod f$. According to Weil, after fixing an embedding $\overline{Q}\mapsto\overline{Q}_p$ we can associate a p-adic character $\varphi_p$ to $\varphi$. We choose an embedding corresponding to a prime above $p$ and then we find $\varphi_p=\kappa\cdot\chi$ for some $\chi$ of finite order and conductor prime to p.
The grossencharacter $\varphi$ (or more precisely $\varphi\circ N_{F/L}$) is associated to a (unique) elliptic curve E defined over $F=L(f)$, the ray class field of conductor $f$, with complex multiplication by $\mathrm{O}_L$ and isomorphic over $C$ to $C/\mathrm{O}_L$. We may even fix a Weierstrass model of E over $\mathrm{O}_F$ which has good reduction at all primes above $p$. For each prime B of $F$ above $p$ we have a formal group $\hat{E}_\mathrm{B}$, and this is a relative Lubin-Tate group with respect to $F_\mathrm{B}$ over $L_p$. We let $\lambda=\lambda_{\hat{E}_\mathrm{B}}$ be the logarithm of this formal group.
Let $U_\infty$ be the product of the principal local units at the primes above $p$ of $L(fp^\infty)$; i.e.,

$$U_\infty = \prod_{\mathrm{B}|p} U_{\infty,\mathrm{B}} \quad \text{where} \quad U_{\infty,\mathrm{B}} = \lim_{\leftarrow} U_n, \mathrm{B}.$$

To an element $u = \lim_{\leftarrow} u_n \in U_\infty$ we can associate a power series $f_{u,\mathrm{B}}(\mathrm{T}) \in \mathrm{O}_\mathrm{B}[\mathrm{T}]^\times$ where $\mathrm{O}_\mathrm{B}$ is the ring of integers of $F_\mathrm{B}$. For B we will choose the prime above $p$ corresponding to our chosen embedding $\overline{Q} \mapsto \overline{Q}_p$. This power series satisfies $u_{n,\mathrm{B}} = (f_{u,\mathrm{B}})(\omega_n)$ for all $n > 0, n \equiv 0(d)$ where $d = [F_\mathrm{B} : L_p]$ and $\{\omega_n\}$ is chosen as an inverse system of $\pi^n$ division points of $\hat{E}_\mathrm{B}$. We define a homomorphism $\delta_k : U_\infty \to \mathrm{O}_\mathrm{B}$ by

$$\delta_k(u) := \delta_{k,\mathrm{B}}(u) = \left( \frac{1}{\lambda'_{\hat{E}_\mathrm{B}}(\mathrm{T})} \frac{d}{d\mathrm{T}} \right)^k \log f_{u,\mathrm{B}}(\mathrm{T})\big|_{\mathrm{T}=0}. \quad (20)$$

Then

$$\delta_k(u^\tau) = \theta(\tau)^k \delta_k(u) \quad (21) \quad \text{for} \quad \tau \in Gal(\overline{F}/F)$$

where $\theta$ denotes the action on $E[p^\infty]$. Now $\theta = \varphi_p$ on $Gal(\overline{F}/F)$. We want a homomorphism on $u_\infty$ with a transformation property corresponding to $\nu$ on all of $Gal(\overline{L}/L)$. We observe that $\nu = \varphi_p^2$ on $Gal(\overline{F}/F)$.

Let $S$ be a set of coset representatives for $Gal(\overline{L}/L)/Gal(\overline{L}/F)$ and define

$$\Phi_2(u) = \sum_{\sigma \in S} \nu^{-1}(\sigma) \delta_2(u^\sigma) \in \mathrm{O}_\mathrm{B}[\nu]. \quad (22)$$

Each term is independent of the choice of coset representative by (17b) and it is easily checked that

$$\Phi_2(u^\sigma) = \nu(\sigma) \Phi_2(u).$$

It takes integral values in $\mathrm{O}_\mathrm{B}[\nu]$. Let $U_\infty(\nu)$ denote the product of the groups of local principal units at the primes above $p$ of the field $L(\nu)$. Then $\Phi_2$ factors through $U_\infty(\nu)$ and thus defines a continuous homomorphism

$$\Phi_2 : U_\infty(\nu) \to C_p.$$

Let $C_\infty$ be the group of projective limits of elliptic units in $L(\nu)$. Then we have a crucial theorem of Rubin:

THEOREM 8.

*There is an equality of characteristic ideals as* $\Lambda = Z_p[[Gal(L(\nu)/L)]]$*-modules*:

$$char_\wedge(Gal(M_\infty / L(\nu))) = char_\wedge(U_\infty(\nu)/\overline{C}_\infty).$$

Let $\nu_0 = \nu \bmod \lambda$. For any $Z_p[Gal(L(\nu_0)/L)]$-module $X$ we write $X^{(\nu_0)}$ for the maximal quotient of $X \underset{Z_p}{\otimes} \mathrm{O}$ on which the action of $Gal(L(\nu_0)/L)$ is via the Teichmuller lift of $\nu_0$. Since $Gal(L(\nu)/L)$ decomposes into a direct product of a pro-p group and a group of order prime to p,

$$Gal(L(\nu)/L) \cong Gal(L(\nu)/L(\nu_0)) \times Gal(L(\nu_0)/L),$$

we can also consider any $Z_p[[Gal(L(\nu)/L)]]$-module also as a $Z_p[Gal(L(\nu_0)/L)]$-module. In particular $X^{(\nu_0)}$ is a module over $Z_p[Gal(L(\nu_0)/L)]^{(\nu_0)} \cong \mathrm{O}$. Also $\Lambda^{(\nu_0)} \cong \mathrm{O}[[\mathrm{T}]]$.

Now according to results of Iwasawa, $U_\infty(\nu)^{(\nu_0)}$ is a free $\Lambda^{(\nu_0)}$-module of rank one. We extend $\Phi_2$ $\mathrm{O}$-linearly to $U_\infty(\nu) \otimes_{Z_p} \mathrm{O}$ and it then factors through $U_\infty(\nu)^{(\nu_0)}$. Suppose that u is a generator of $U_\infty(\nu)^{(\nu_0)}$ and $\beta$ an element of $\overline{C}_\infty^{(\nu_0)}$. Then $f(\gamma - 1)u = \beta$ for some $f(\mathrm{T}) \in \mathrm{O}[[\mathrm{T}]]$ and $\gamma$ a topological generator of $Gal(L(\nu)/L(\nu_0))$. Computing $\Phi_2$ on both $u$ and $\beta$ gives

$$f(\nu(\gamma) - 1) = \phi_2(\beta)/\Phi_2(u). \quad (23)$$

We have that $\nu$ can be interpreted as the grossencharacter whose associated p-adic character , via the chosen embedding $\overline{Q} \mapsto \overline{Q}_p$ , is $\nu$ , and $\overline{\nu}$ is the complex conjugate of $\nu$ .

Furthermore, we can compute $\Phi_2(u)$ by choosing a special local unit and showing that $\Phi_2(u)$ is a p-adic unit.

Now, if we have that

$$\#H^1_{Se}(Q_\Sigma/Q, Y) \le \#\left(\mathrm{O}/\Omega^{-2}L_{f_0}(2,\overline{\nu})\right) \cdot \prod_{q \in \Sigma} \ell_q ,$$

and

$$\#(\mathrm{O}/h_L) \cdot \prod_{q \in \Sigma - \{p\}} \ell_q , \quad (24)$$

where $\ell_q = \#H^0\left(Q_q, ((K/\mathrm{O})(\psi) \oplus K/\mathrm{O})^*\right)$ and $h_L$ is the class number of $\mathrm{O}_L$, combining these we obtain the following relation:

$$\#H^1_{Se}(Q_\Sigma/Q, V) \le \#\left(\mathrm{O}/\Omega^{-2}L_{f_0}(2,\overline{\nu})\right) \#(\mathrm{O}/h_L) \cdot \prod_{q \in \Sigma} \ell_q , \quad (25)$$

where $\ell_q = \#H^0(Q_q, V^*)$ (for $q \neq p$), $\ell_p = \#H^0\left(Q_p, (Y^0)^*\right)$. (Also here, we remember that $\ell$ is p-adic).

Let $\rho_0$ be an irreducible representation as in (5). Suppose that $f$ is a newform of weight 2 and level N, $\lambda$ a prime of $\mathrm{O}_f$ above p and $\rho_{f,\lambda}$ a deformation of $\rho_0$. Let $m$ be the kernel of the homomorphism $\mathrm{T}_1(N) \to \mathrm{O}_f/\lambda$ arising from $f$ .

We now give an explicit formula for $\eta$ developed by Hida by interpreting $\langle , \rangle$ in terms of the cup product pairing on the cohomology of $X_1(N)$, and then in terms of the Petersson inner product of $f$ with itself. Let

$$(,): H^1(X_1(N), \mathrm{O}_f) \times H^1(X_1(N), \mathrm{O}_f) \to \mathrm{O}_f \quad (26)$$

be the cup product pairing with $\mathrm{O}_f$ as coefficients. Let $p_f$ be the minimal prime of $\mathrm{T}_1(N)\otimes O_f$ associated to $f$, and let

$$L_f = H^1\left(X_1(N),\mathrm{O}_f\right)[p_f].$$

If $f=\sum a_n q^n$ let $f^\rho=\sum \bar{a}_n q^n$. Then $f^\rho$ is again a newform and we define $L_{f^\rho}$ by replacing $f$ by $f^\rho$ in the definition of $L_f$. Then the pairing $(,)$ induces another by restriction

$$(,): L_f \times L_{f^\rho} \to \mathrm{O}_f. \quad (27)$$

Replacing $\mathrm{O}$ by the localization of $\mathrm{O}_f$ at p (if necessary) we can assume that $L_f$ and $L_{f^\rho}$ are free of rank 2 and direct summands as $\mathrm{O}_f$-modules of the respective cohomology groups. Let $\delta_1,\delta_2$ be a basis of $L_f$. Then also $\bar{\delta}_1,\bar{\delta}_2$ is a basis of $L_{f^\rho}=\bar{L}_f$. Here complex conjugation acts on $H^1\left(X_1(N),\mathrm{O}_f\right)$ via its action on $\mathrm{O}_f$. We can then verify that

$$(\delta,\bar{\delta}) := \det\left(\delta_i,\bar{\delta}_j\right)$$

is an element of $\mathrm{O}_f$ whose image in $\mathrm{O}_{f,\lambda}$ is given by $\pi(\eta^2)$ (unit).

To give a more useful expression for $(\delta,\bar{\delta})$ we observe that $f$ and $\bar{f}^\rho$ can be viewed as elements of $H^1(X_1(N),C)\cong H^1_{DR}(X_1(N),C)$ via $f\mapsto f(z)dz$, $\bar{f}^\rho\mapsto \bar{f}^\rho d\bar{z}$. Then $\{f,\bar{f}^\rho\}$ form a basis for $L_f\otimes_{\mathrm{O}_f} C$. Similarly $\{\bar{f},f^\rho\}$ form a basis for $L_{f^\rho}\otimes_{\mathrm{O}_f} C$. Define the vectors $\omega_1=\left(f,\bar{f}^\rho\right)$, $\omega_2=\left(\bar{f},f^\rho\right)$ and write $\omega_1=C\delta$ and $\omega_2=\bar{C}\bar{\delta}$ with $C\in M_2(C)$. Then writing $f_1=f, f_2=\bar{f}^\rho$ we set

$$(\omega,\bar{\omega}) := \det\left(\left(f_i,\bar{f}_j\right)\right) = (\delta,\bar{\delta})\det\left(C\bar{C}\right).$$

Now $(\omega,\bar{\omega})$ is given explicitly in terms of the (non-normalized) Petersson inner product $\langle,\rangle$: $(\omega,\bar{\omega})=-4\langle f,f\rangle^2$ where $\langle f,f\rangle=\int_{\Im/\Gamma_1(N)} f\bar{f}dxdy$. Hence, we have the following equation:

$$(\omega,\bar{\omega}) = -4\left(\int_{\Im/\Gamma_1(N)} f\bar{f}dxdy\right)^2. \quad (28)$$

To compute $\det(C)$ we consider integrals over classes in $H_1\left(X_1(N),\mathrm{O}_f\right)$. By Poincaré duality there exist classes $c_1,c_2$ in $H_1\left(X_1(N),\mathrm{O}_f\right)$ such that $\det\left(\int_{c_j}\delta_i\right)$ is a unit in $\mathrm{O}_f$. Hence $\det C$ generates the same $\mathrm{O}_f$-module as is generated by $\left\{\det\left(\int_{c_j} f_i\right)\right\}$ for all such choices of classes $(c_1,c_2)$ and with $\{f_1,f_2\}=\{f,\bar{f}^\rho\}$. Letting $u_f$ be a generator of the $\mathrm{O}_f$-module $\left\{\det\left(\int_{c_j} f_i\right)\right\}$ we have the following formula of Hida:

$$\pi(\eta^2)=\langle f,f\rangle^2 / u_f\bar{u}_f \times (\text{unit in } \mathrm{O}_{f,\lambda}).$$

Now, we choose a (primitive) grossencharacter $\varphi$ on L together with an embedding $\overline{Q} \mapsto \overline{Q}_p$ corresponding to the prime $p$ above p such that the induced p-adic character $\varphi_p$ has the properties:

(i) $\varphi_p \bmod \overline{p} = \kappa_0$ ( $\overline{p} =$ maximal ideal of $\overline{Q}_p$ ).

(ii) $\varphi_p$ factors through an abelian extension isomorphic to $Z_p \oplus T$ with $T$ of finite order prime to p.

(iii) $\varphi((\alpha)) = \alpha$ for $\alpha \equiv 1(f)$ for some integral ideal $f$ prime to p.

Let $p_0 = \ker \psi_f : \mathrm{T}_1(N) \to \mathrm{O}_f$ and let $A_f = J_1(N)/\, p_0 J_1(N)$ be the abelian variety associated to f by Shimura. Over $F^+$ there is an isogeny $A_{f/F^+} \approx (E_{/F^+})^d$ where $d = [\mathrm{O}_f : \mathrm{Z}]$.

We have that the p-adic Galois representation associated to the Tate modules on each side are equivalent to $(Ind_F^{F^+} \varphi_0) \otimes_{\mathrm{Z}_p} K_{f,p}$ where $K_{f,p} = \mathrm{O}_f \otimes Q_p$ and where $\varphi_p : Gal(\overline{F}/F) \to \mathrm{Z}_p^\times$ is the p-adic character associated to $\varphi$ and restricted to $F$ .We now give an expression for $\langle f_\varphi, f_\varphi \rangle$ in terms of the L-function of $\varphi$. We note that $L_N(2,\overline{\nu}) = L_N(2,\nu) = L_N(2, \varphi^2 \overline{\hat{\chi}})$ and remember that $\nu$ is the p-adic character, and $\overline{\nu}$ is the complex conjugate of $\nu$, we have that:

$$\langle f_\varphi, f_\varphi \rangle = \frac{1}{16\pi^3} N^2 \left\{ \prod_{\substack{q|N \\ q \notin S_\varphi}} \left(1 - \frac{1}{q}\right) \right\} L_N(2, \varphi^2 \overline{\hat{\chi}}) L_N(1, \psi), \quad (29)$$

*where $\chi$ is the character of $f_\varphi$ and $\hat{\chi}$ its restriction to $L$; $\psi$ is the quadratic character associated to $L$; $L_N(\ )$ denotes that the Euler factors for primes dividing $N$ have been removed; $S_\varphi$ is the set of primes $q|N$ such that $q = qq'$ with $q \mid$ cond $\varphi$ and $q, q'$ primes of $L$, not necessarily distinct.*

THEOREM 9.

*Suppose that $\rho_0$ as in (5) is an irreducible representation of odd determinant such that $\rho_0 = Ind_L^Q \kappa_0$ for a character $\kappa_0$ of an imaginary quadratic extension $L$ of $Q$ which is unramified at p. Assume also that:*

(i) $\det \rho_0 \big|_{I_p} = \omega$;

(ii) $\rho_0$ *is ordinary.*

*Then for every $D = (\cdot, \Sigma, \mathrm{O}, \phi)$ such that $\rho_0$ is of type $D$ with $\cdot =$ Se or ord,*

$$R_D \cong \mathrm{T}_D$$

*and $\mathrm{T}_D$ is a complete intersection.*

COROLLARY.

*For any $\rho_0$ as in the theorem suppose that*

$$\rho : Gal(\overline{Q}/Q) \to GL_2(\mathrm{O})$$

*is a continuous representation with values in the ring of integers of a local field, unramified outside a finite set of primes, satisfying* $\overline{\rho} \cong \rho_0$ *when viewed as representations to* $GL_2(\overline{F}_p)$. *Suppose further that:*

(i) $\rho\big|_{D_p}$ *is ordinary;*

(ii) $\det \rho\big|_{I_p} = \chi\varepsilon^{k-1}$ *with* $\chi$ *of finite order,* $k \geq 2$.

*Then* $\rho$ *is associated to a modular form of weight* $k$.

THEOREM 10. (Langlands-Tunnell)

*Suppose that* $\rho : Gal(\overline{Q}/Q) \to GL_2(C)$ *is a continuous irreducible representation whose image is finite and solvable. Suppose further that* $\det \rho$ *is odd. Then there exists a weight one newform* $f$ *such that* $L(s, f) = L(s, \rho)$ *up to finitely many Euler factors.*

Suppose then that

$$\rho_0 : Gal(\overline{Q}/Q) \to GL_2(F_3)$$

is an irreducible representation of odd determinant. This representation is modular in the sense that over $\overline{F}_3$, $\rho_0 \approx \rho_{g,\mu} \bmod \mu$ for some pair $(g, \mu)$ with $g$ some newform of weight 2. There exists a representation

$$i : GL_2(F_3) \mapsto GL_2(\mathrm{Z}[\sqrt{-2}]) \subset GL_2(C).$$

By composing $i$ with an automorphism of $GL_2(F_3)$ if necessary we can assume that $i$ induces the identity on reduction $\bmod(1+\sqrt{-2})$. So if we consider $i \circ \rho_0 : Gal(\overline{Q}/Q) \to GL_2(C)$ we obtain an irreducible representation which is easily seen to be odd and whose image is solvable.
Now pick a modular form $E$ of weight one such that $E \equiv 1(3)$. For example, we can take $E = 6E_{1,\chi}$ where $E_{1,\chi}$ is the Eisenstein series with Mellin transform given by $\zeta(s)\zeta(s,\chi)$ for $\chi$ the quadratic character associated to $Q(\sqrt{-3})$. Then $fE \equiv f \bmod 3$ and using the Deligne-Serre lemma we can find an eigenform $g'$ of weight 2 with the same eigenvalues as $f$ modulo a prime $\mu'$ above $(1+\sqrt{-2})$. There is a newform $g$ of weight 2 which has the same eigenvalues as $g'$ for almost all $T_l$'s, and we replace $(g', \mu')$ by $(g, \mu)$ for some prime $\mu$ above $(1+\sqrt{-2})$. Then the pair $(g, \mu)$ satisfies our requirements for a suitable choice of $\mu$ (compatible with $\mu'$).
We can apply this to an elliptic curve $E$ defined over $Q$, and we have the following fundamental theorems:

THEOREM 11.

*All semistable elliptic curves over* $Q$ *are modular.*

THEOREM 12.

*Suppose that* $E$ *is an elliptic curve defined over* $Q$ *with the following properties:*
(i) $E$ *has good or multiplicative reduction at 3, 5,*

(ii) *For* $p = 3, 5$ *and for any prime* $q \equiv -1 \bmod p$ *either* $\bar{\rho}_{E,p}|D_q$ *is reducible over* $\bar{F}_p$ *or* $\bar{\rho}_{E,p}|I_q$ *is irreducible over* $\bar{F}_p$.

*Then* $E$ *is modular.*

## Chapter 2.

## Further mathematical aspects concerning the Fermat's Last Theorem

2.1 On the modular forms, Euler products, Shimura map and automorphic L-functions.

### A. Modular forms

We know that there is a direct relation with elliptic curves, via the concept of *modularity* of elliptic curves over $Q$.

Let $E$ be an elliptic curve over $Q$, given by some Weierstrass equation. Such a Weierstrass equation can be chosen to have its coefficients in $Z$. A Weierstrass equation for $E$ with coefficients in $Z$ is called *minimal* if its *discriminant* is minimal among all Weierstrass equations for $E$ with coefficients in $Z$; this discriminant then only depends on $E$ and will be denoted discr($E$). Thence, $E$ has a Weierstrass minimal model over $Z$, that will be denoted by $E_Z$.

For each prime number p, we let $E_{F_p}$ denote the curve over $F_p$ given by reducing a minimal Weierstrass equation modulo p; it is the fibre of $E_Z$ over $F_p$. The curve $E_{F_p}$ is smooth if and only if p does not divide discr($E$).

The possible singular fibres have exactly one singular point: an ordinary double point with rational tangents, or with conjugate tangents, or an ordinary cusp. The three types of reduction are called split multiplicative, non-split multiplicative and additive, respectively, after the type of group law that one gets on the complement of the singular point. For each p we then get an integer $a_p$ by requiring the following identity:

$$p + 1 - a_p = \#E(F_p). \quad (1)$$

This means that for all p, $a_p$ is the trace of $F_p$ on the degree one étale cohomology of $E_{\bar{F}_p}$, with coefficients in $F_l$, or in $Z/l^nZ$ or in the $l$-adic numbers $Z_l$. For p not dividing discr($E$) we know that $|a_p| \le 2p^{1/2}$. If $E_{F_p}$ is multiplicative, then $a_p = 1$ or $-1$ in the split and non-split case. If $E_{F_p}$ is additive, then $a_p = 0$. We also define, for each p an element $\varepsilon(p)$ in $\{0,1\}$ by setting $\varepsilon(p) = 1$ for p not dividing discr($E$). The Hasse-Weil L-function of $E$ is then defined as:

$$L_E(s) = \prod_p L_{E,p}(s), \quad L_{E,p}(s) = \left(1 - a_p p^{-s} + \varepsilon(p) p p^{-2s}\right)^{-1}, \quad (2)$$

for $s$ in $C$ with $R(s) > 3/2$. We note that for all p and for all $l \neq p$ we have the identity:

$$1 - a_p t + \varepsilon(p) t^2 = \det\left(1 - tF_p^*, H^1\left(E_{\bar{F},et}, Q_l\right)\right). \quad (3)$$

We use étale cohomology with coefficients in $Q_l$, the field of $l$-adic numbers, and not in $F_l$.

The function $L_E$ was conjectured to have a holomorphic continuation over all of $C$, and to satisfy a certain precisely given functional equation relating the values at $s$ and $2-s$. In that functional equation appears a certain positive integer $N_E$ called the conductor of $E$, composed of the primes p dividing discr($E$) with exponents that depend on the behaviour of $E$ at p, i.e., on $E_{Z_p}$. This conjecture on continuation and functional equation was proved for semistable $E$ (i.e., $E$ such that there is no p where $E$ has additive reduction) by Wiles and Taylor-Wiles, and in the general case by Breuil, Conrad, Diamond and Taylor. In fact, the continuation and functional equation are direct consequences of the modularity of $E$ that was proved by Wiles, Taylor-Wiles, etc.

The weak Birch and Swinnerton-Dyer conjecture says that the dimension of the $Q$-vector space $Q \otimes E(Q)$ is equal to the order of vanishing of $L_E$ at 1. Anyway, the function $L_E$ gives us integers $a_n$ for all $n \geq 1$ as follows:

$$L_E(s) = \sum_{n \geq 1} a_n n^{-s}, \quad \text{for} \quad R(s) > 3/2. \quad (4)$$

From these $a_n$ one can then consider the following function:

$$f_E : H = \{\tau \in C \mid \Im(\tau) > 0\} \to C, \quad \tau \mapsto \sum_{n \geq 1} a_n e^{2\pi i n \tau}. \quad (5)$$

Equivalently, we have:

$$f_E = \sum_{n \geq 1} a_n q^n, \quad \text{with} \quad q : H \to C, \quad \tau \mapsto e^{2\pi i \tau}. \quad (6)$$

A more conceptual way to state the relation between $L_E$ and $f_E$ is to say that $L_E$ is obtained, up to elementary factors, as the *Mellin transform* of $f_E$:

$$\int_0^\infty f_E(it) t^s \frac{dt}{t} = (2\pi)^{-s} \Gamma(s) L_E(s), \quad \text{for} \quad R(s) > 3/2. \quad (7)$$

Hence, we can finally state what the modularity of $E$ means:

*$f_E$ is a modular form of weight two for the congruence subgroup $\Gamma_0(N_E)$ of $SL_2(Z)$.*

The last statement means that $f_E$ has an enormous amount of symmetry.

A typical example of a modular form of weight higher than two is the *discriminant* modular form, usually denoted $\Delta$. One way to view $\Delta$ is as the holomorphic function on the upper half plane $H$ given by:

$$\Delta = q \prod_{n \geq 1} \left(1 - q^n\right)^{24}, \quad (8)$$

where $q$ is the function from $H$ to $C$ given by $z \mapsto \exp(2\pi i z)$. The coefficients in the power series expansion:

$$\Delta = \sum_{n \geq 1} \tau(n) q^n \quad (9)$$

define the famous *Ramanujan* $\tau$ *-function*.
To say that $\Delta$ is a modular form of weight 12 for the group $SL_2(Z)$ means that for all elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $SL_2(Z)$ the following identity holds for all $z$ in $H$:

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z), \quad (10)$$

which is equivalent to saying that the multi-differential form $\Delta(z)(dz)^{\otimes 6}$ is invariant under the action of $SL_2(Z)$. As $SL_2(Z)$ is generated by the elements $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, it suffices to check the identity in (10) for these two elements. The fact that $\Delta$ is $q$ times a power series in $q$ means that $\Delta$ is a *cusp form*: it vanishes at "$q = 0$". It is a fact that $\Delta$ is the first example of a non-zero cusp form for $SL_2(Z)$: there is no non-zero cusp form for $SL_2(Z)$ of weight smaller than 12, i.e., there are no non-zero holomorphic functions on $H$ satisfying (10) with the exponent 12 replaced by a smaller integer, whose Laurent series expansion in $q$ is $q$ times a power series. Moreover, the $C$-vector space of such functions of weight 12 is one-dimensional, and hence $\Delta$ is a basis of it.
The one-dimensionality of this space has as a consequence that $\Delta$ is an eigenform for certain operators on this space, called *Hecke operators*, that arise from the action on $H$ of $GL_2(Q)^+$, the subgroup of $GL_2(Q)$ of elements whose determinant is positive. This fact explains that the coefficients $\tau(n)$ satisfy certain relations which are summarised by the following identity of Dirichlet series:

$$L_\Delta(s) := \sum_{n\geq 1}\tau(n)n^{-s} = \prod_p \left(1-\tau(p)p^{-s}+p^{11}p^{-2s}\right)^{-1}. \quad (11)$$

These relations:

$$\begin{aligned} &\tau(mn) = \tau(m)\tau(n) && \text{if } m \text{ and } n \text{ are relatively prime;} \\ &\tau(p^n) = \tau(p^{n-1})\tau(p) - p^{11}\tau(p^{n-2}) && \text{if } p \text{ is prime and } n \geq 2 \end{aligned}$$

were conjectured by Ramanujan, and proved by Mordell. Using these identities, $\tau(n)$ can be expressed in terms of the $\tau(p)$ for $p$ dividing $n$. As $L_\Delta$ is the Mellin transform of $\Delta$, $L_\Delta$ is holomorphic on $C$, and satisfies the functional equation (Hecke):

$$(2\pi)^{-(12-s)}\Gamma(12-s)L_\Delta(12-s) = (2\pi)^{-s}\Gamma(s)L_\Delta(s). \quad (12)$$

The famous *Ramanujan conjecture* states that for all primes $p$ one has the inequality:

$$|\tau(p)| < 2p^{11/2}, \quad (13)$$

or, equivalently, that the complex roots of the polynomial $x^2 - \tau(p)x + p^{11}$ are complex conjugates of each other, and hence are of absolute value $p^{11/2}$.

**B. Euler products**

We know that the infinite series

$$\sum_{n=1}^{\infty}\frac{1}{n^s}, \quad (14)$$

converges for $R(s)>1$ and gives rise by analytic continuation to a meromorphic function $\zeta(s)$ in $C$. For $R(s)>1$ $\zeta(s)$ admits the absolutely convergent infinite product expansion

$$\prod_{p}\frac{1}{1-p^{-s}}, \quad (15)$$

taken over the set of primes. This "Euler product" may be regarded as an analytic formulation of the principle of unique factorization in the ring $Z$ of integers. It is, as well, the product taken over all the non-Archimedean completions of the rational field $Q$ (which completions $Q_p$ are indexed by the set of primes) of the "Mellin transform" in $Q_p$

$$\xi_p(s)=\frac{1}{1-p^{-s}}, \quad (16)$$

(where the Mellin transform is, more or less, Fourier transform on the multiplicative group. Classically, the Mellin transform $\varphi$ of $f$ is given formally by $\varphi(s)=\int_0^{\infty} f(x)x^s(dx/x)$. (17)) of the canonical "Gaussian density" $\Phi_p(x)=$ 1 if $x\in$ closure of $Z$ in $Q_p$; 0 otherwise, which Gaussian density is equal to its own Fourier transform. For the Archimedean completion $Q_\infty = R$ of the rational field $Q$ one forms the classical Mellin transform

$$\xi_\infty(s)=\pi^{-(s/2)}\Gamma(s/2) \quad (18)$$

of the classical Gaussian density

$$\Phi_\infty(x)=e^{-\pi x^2}, \quad (19)$$

(which also is equal to its own Fourier transform). Then the function

$$\xi(s)=\xi_\infty(s)\zeta(s)=\prod_{p\le\infty}\xi_p(s) \quad (20)$$

is meromorphic in $C$, and satisfies the functional equation

$$\xi(1-s)=\xi(s). \quad (21)$$

The connection of Riemann's $\zeta$-function with the subject of modular forms begins with the observation that $\zeta(2s)$ is essentially the Mellin transform of $\theta_I(x)=\theta(ix)-1$, where $\theta$, which is a modular form of weight 1/2 and level 8, is defined in the upper-half plane $H$ by the formula

$$\theta(\tau)=\sum_{m\in Z}\exp(\pi i\tau m^2). \quad (22)$$

In fact, one of the classical proofs of the functional equation (21) is given by applying the Poisson summation formula to the function $x \mapsto \exp(\pi i \tau x^2)$, while observing that the substitution $s \mapsto (1/2) - s$ for $\zeta(2s)$ corresponds in the upper-half plane to the substitution $\tau \mapsto -1/\tau$ for the theta series. If $f$ is a cuspform for a congruence group $\Gamma$ containing

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (23)$$

and so, consequently, $f(\tau+1) = f(\tau)$, then one has the following Fourier expansion

$$f(\tau) = \sum_{m=1}^{\infty} c_m e^{2\pi i m \tau} . \quad (24)$$

The Mellin transform $\varphi(s)$ of $f_I$ leads to the Dirichlet series

$$\varphi(s) = \sum_{m=1}^{\infty} c_m m^{-s} , \quad (25)$$

which may be seen to have a positive abscissa of convergence.
For the "modular group" $\Gamma(1)$ the Dirichlet series associated to every cuspform of weight $w$ admits an analytic continuation with functional equation under the substitution $s \mapsto w - s$. Since $\Gamma(1)$ is generated by the two matrices $T$ and

$$W = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (26)$$

and since the functional equation of a modular form $f$ relative to $T$ is reflected in the formation of the Fourier series (24), the condition that an absolutely convergent series (24) is a modular form for $\Gamma(1)$ is the functional equation for a modular form relative solely to $W$.
Observing that the formula

$$ds^2 = \frac{dx^2 + dy^2}{y^2} \quad \text{for} \quad \tau = x + iy \in H , \quad (27)$$

gives a (the hyperbolic) $SL_2(R)$-invariant metric in $H$ with associated invariant measure

$$d\mu = \frac{dxdy}{y^2} , \quad (28)$$

one introduces the Petersson (Hermitian) inner product in the space of cuspform of weight $w$ for $\Gamma$ with the definition:

$$\langle f, g \rangle = \int_{H/\Gamma} f(\tau)\overline{g}(\tau)\Im(\tau)^w d\mu(\tau) . \quad (29)$$ (see also page 13 eq. (28))

(Integration over the quotient $H/\Gamma$ makes sense since the integrand $f(\tau)\overline{g}(\tau)y^w$ (30) is $\Gamma$-invariant).

For the modular group $\Gamma(1)$ the $n^{th}$ Hecke operator $T(n)=T_w(n)$ is the linear endomorphism of the space of cuspforms of weight $w$ arising from the following considerations. Let $S_n$ be the set of $2\times 2$ matrices in $Z$ with determinant $n$. For

$$M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in S_n \quad (31)$$

and for a function $f$ in $H$ one defines

$$(M\cdot_w f)(\tau)=\det(M)^{w-1}(c\tau+d)^{-w}f(\tau), \quad (32)$$

and then, observing that $\Gamma(1)$ under $\cdot_w$ acts trivially on the modular forms of weight $w$, one may define the Hecke operator $T_w(n)$ by

$$T_w(n)(f)=\sum_{M\in S_n/\Gamma(1)}(M\cdot_w f)(\tau), \quad (33)$$

where the quotient $S_n/\Gamma(1)$ refers to the action of $\Gamma(1)$ by left multiplication on the set $S_n$. One finds for $m,n$ coprime that

$$T(mn)=T(m)T(n), \quad (34)$$

and furthermore one has

$$T(p^{e+1})=T(p^e)T(p)-p^{w-1}T(p^{e-1}). \quad (35)$$

Consequently, the operators $T(n)$ commute with each other, and, therefore, generate a commutative algebra of endomorphisms of the space of cusp forms of weight $w$ for $\Gamma(1)$. It is not difficult to see that the Hecke operators are self-adjoint for the Petersson inner product on the space of cuspforms. Consequently, the space of cuspforms of weight $w$ admits a basis of simultaneous eigenforms for the Hecke algebra. A "Hecke eigencuspform" is said to be *normalized* if its Fourier coefficient $c_1=1$. If $f$ is a normalized Hecke eigencuspform, then:

(i) The Fourier coefficient $c_m$ of $f$ is the eigenvalue of $f$ for $T(m)$.

(ii) The Fourier coefficients $c(m)=c_m$ of $f$ satisfy
$c(mn)=c(m)c(n)$ for $m,n$ coprime, and
$c(p^{e+1})=c(p^e)c(p)-p^{w-1}c(p^{e-1})$ for $p$ prime.

Consequently, the Dirichlet series associated with a simultaneous Hecke eigencuspform of level 1 and weight $w$ admits an Euler product

$$\varphi(s)=\prod_p \frac{1}{1-c_p p^{-s}+p^{w-1-2s}}. \quad (36)$$

For example, when $f$ is the unique normalized cuspform $\Delta$ of level 1 and weight 12, one has

$$\varphi(s)=\prod_p \frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}, \quad (37) \qquad \text{(in fact, if } w=12\text{, then } w-1-2s=11-2s\text{)}$$

where $c_p=\tau(p)$ is the function $\tau$ of Ramanujan.

**C. Shimura map**

Shimura showed for a given $W_N$-compatible Hecke eigencuspform $f$ of weight 2 for the group $\Gamma_0(N)$ with rational Fourier coefficients how to construct an elliptic curve $E_f$ defined over $Q$ such that the Dirichlet series $\varphi(s)$ associated with $f$ is the same as the $L$-function $L(E_f,s)$.
Let $\Gamma$ be a congruence subgroup of $SL_2(Z)$, and let $X(\Gamma)$ denote the compact Riemann surface $H^*/\Gamma$. The inclusion of $\Gamma$ in $\Gamma(1)$ induces a "branched covering"

$$X(\Gamma)\to X(1)\cong P^1. \quad (38)$$

One may use the elementary Riemann-Hurwitz formula from combinatorial topology to determine the Euler number, and consequently the genus, of $X(\Gamma)$. The genus is the dimension of the space of cuspforms of weight 2. Even when the genus is zero one obtains embeddings of $X(\Gamma)$ in projective spaces $P^r$ through holomorphic maps

$$\tau\mapsto(f_0(\tau),f_1(\tau),...,f_r(\tau)), \quad (39)$$

where $f_0,f_1,...,f_r$ is a basis of the space of modular forms of weight $w$ with $w$ sufficiently large.
Using the corresponding projective embedding one finds a *model* for $X_0(N)=X(\Gamma_0(N))$ over $Q$, i.e., an algebraic curve defined over $Q$ in projective space that is isomorphic as a compact Riemann surface to $X_0(N)$.
Associated with any "complete non-singular" algebraic curve $X$ of genus $g$ is a complex torus, the "Jacobian" $J(X)$ of $X$, that is the quotient of $g$-dimensional complex vector space $C^g$ by the lattice $\Omega$ generated by the "period matrix", which is the $g\times 2g$ matrix in $C$ obtained by integrating each of the $g$ members $\omega_i$ of a basis of the space of holomorphic differentials over each of the $2g$ loops in $X$ representing the members of a homology basis in dimension 1. Furthermore, if one picks a base point $z_0$ in $X$, then for any $z$ in $X$, the path integral from $z_0$ to $z$ of each of the $g$ holomorphic differentials is well-defined modulo the periods of the differential. One obtains a holomorphic map $X\to J(X)$ from the formula

$$z\mapsto\left(\int_{z_0}^{z}\omega_1,...,\int_{z_0}^{z}\omega_g\right)\bmod\Omega. \quad (40)$$

This map is universal for pointed holomorphic maps from $X$ to complex tori. Furthermore, the Jacobian $J(X)$ is an algebraic variety that admits definition over any field of definition for $X$ and $z_0$, and the universal map also admits definition over any such field. The complex tori that admit embeddings in projective space are the abelian group objects in the category of projective varieties. They are called *abelian varieties*. Every abelian variety is isogenous to the product of "simple" abelian varieties: abelian varieties having no abelian subvarieties. Shimura showed that one of the simple isogeny factors of $J(X_0(N))$ is an elliptic curve $E_f$ defined over $Q$ characterized by the fact that its one-dimensional space of holomorphic differentials induces on $X_0(N)$, via the composition of the universal map with projection on $E_f$, the one-dimensional space of differentials on $X_0(N)$ determined by the cuspform $f$.
He showed further that $L(E_f, s)$ is the Dirichlet series $\varphi(s)$ with Euler product given by $f$. An elliptic curve $E$ defined over $Q$ is said to be *modular* if it is isogenous to $E_f$ for some $W_N$-compatible Hecke eigencuspform of weight 2 for $\Gamma_0(N)$. Equivalently $E$ is modular if and only if $L(E,s)$ is the Dirichlet series given by such a cuspform. The Shimura-Taniyama-Weil Conjecture states that every elliptic curve defined over $Q$ is modular. Shimura showed that this conjecture is true in the special case where the $Z$-module rank of the ring of endomorphisms of $E$ is grater than one. In this case the point $\tau$ of the upper-half plane corresponding to $E(C)$ is a quadratic imaginary number, and $L(E,s)$ is a number-theoretic $L$-function associated with the corresponding imaginary quadratic number field.

**D. Automorphic $L$-functions**

Talking about zeta functions in general one inevitably is led to start with the Riemann zeta function $\zeta(s)$. It is defined as a *Dirichlet series*:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad (41)$$

which converges for each complex number $s$ of real part greater than one. In the same region it possesses a representation as a *Mellin integral*:

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{1}{e^t - 1} t^s \frac{dt}{t}. \quad (42)$$

Let $f$ be a cusp form of weight $2k$ for some natural number $k$, i.e., the function $f$ is holomorphic on the upper half plane $H$ in $C$, and has a certain invariance property under the action of the modular group $SL_2(Z)$ on $H$. Then $f$ admits a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i z n}. \quad (43)$$

Define its $L$-function for $\mathrm{Re}(s) > 1$ by

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \quad (44)$$

The easily established integral representation

$$\hat{L}(f,s)=(2\pi)^{-s}\Gamma(s)L(f,s)=\int_0^\infty f(it)t^s\frac{dt}{t}, \quad (45)$$

implies that $L(f,s)$ extends to an entire function satisfying the functional equation $\hat{L}(f,s)=(-1)^k\hat{L}(f,2k-s)$. With $\Lambda(f,s)=\hat{L}(f,2ks)$ this becomes

$$\Lambda(f,s)=(-1)^k\Lambda(f,1-s). \quad (46)$$

This construction can be extended to cusp forms for suitable subgroups of the modular group. These $L$-functions look like purely analytical objects. Thus it was particularly daring of A. Weil, G. Shimura, and Y. Taniyama in 1955 to propose the conjecture that the zeta function of any elliptic curve over $Q$ coincides with a $\Lambda(f,s)$ for a suitable cusp form $f$. This conjecture was proved in part by A. Wiles and R. Taylor providing a proof of Fermat's Last Theorem as a consequence.
The upper half plane is a homogeneous space of the group $SL_2(R)$, and so cusp forms may be viewed as functions on this group, in particular, they are vectors in the natural unitary representation of $SL_2(R)$ on the space

$$L^2(SL_2(Z)\backslash SL_2(R)). \quad (47)$$

Going even further one can extend this quotient space to the quotient of the adele group $GL_2(A)$ modulo its discrete subgroup $GL_2(Q)$, so cusp forms become vectors in

$$L^2\left(GL_2(Q)\backslash GL_2(A)^1\right), \quad (48)$$

where $GL_2(A)^1$ denotes the set of all matrices in $GL_2(A)$ whose determinant has absolute value one. Now $GL_2$ can be replaced by $GL_n$ for $n\in N$ and one can imitate the methods of Tate's thesis (the case n = 1) to arrive at a much more general definition of an automorphic $L$-function: this is an Euler product $L(\pi,s)$ attached to an automorphic representation $\pi$ of $GL_n(A)^1$, i.e., an irreducible subrepresentation $\pi$ of $L^2\left(GL_n(Q)\backslash GL_n(A)^1\right)$. As in the $GL_1$-case it has an integral representation as a Mellin transform and it extends to a meromorphic representation, which is entire if $\pi$ is cuspidal and $n>1$. Furthermore it satisfies a functional equation

$$L(\pi,s)=\varepsilon(\pi,s)L(\tilde{\pi},1-s), \quad (49)$$

where $\tilde{\pi}$ is the contragredient representation and $\varepsilon(\pi,s)$ is a constant multiplied by an exponential. We conclude remember that extending the Weil-Shimura-Taniyama conjecture, R.P. Langlands conjectured in the 1960s that any motivic $L$-function coincides with $L(\pi,s)$ for some cuspidal $\pi$.

2.2 On some mathematical applications of the Mellin transform.

Harmonic sums are sums of the form

$$G(x)=\sum_k \lambda_k g(\mu_k x), \quad (50)$$

where the $\lambda_k$ are the *amplitudes*, the $\mu_k$ are the *frequencies* and $g(x)$ is the *base function*. We consider harmonic sums because we wish to evaluate $G(x)$ at a set of particular points $x_0, x_1, \ldots$ or at all $x \in R$.

*Definition of the harmonic sum and computation of the appropriate Mellin transform.*

Now, let $\lambda_k = 1/k$, $\mu_k = 1/k$ and $g(x) = x/(1+x) = 1/(1+1/x)$; and we consider the harmonic sum

$$h(x)=\sum_x \lambda_k g(\mu_k x)=\sum \frac{1}{k}\frac{x/k}{1+x/k}=\sum\left(\frac{1}{k}-\frac{1}{x+k}\right). \quad (51)$$

This sum is of interest because

$$h(n)=\sum\left(\frac{1}{k}-\frac{1}{n+k}\right)=\sum\frac{1}{k}-\sum_{k=n+1}\frac{1}{k}=\sum_{k=1}^{n}\frac{1}{k}=H_n, \quad (52)$$

the $n$ th harmonic number.
The principal operation in the evaluation of harmonic sums is the computation of the Mellin transform of the base function $g(y)$ and the computation of the Dirichlet generating function $\Lambda(s)$.
We first compute the transform of the base function. We have $\mathrm{M}[1/(1+x);s]=\pi/\sin(\pi s)$ and hence

$$\mathrm{M}\left[\frac{x}{1+x};s\right]=-\frac{\pi}{\sin(\pi s)}. \quad (53)$$

Now we compute the Dirichlet generating function $\Lambda(s)$. We have

$$\Lambda(s)=\sum\frac{1}{k}k^s=\sum\frac{1}{k^{1-s}}=\zeta(1-s). \quad (54)$$

We conclude that the Mellin transform of $h(x)$ is

$$-\frac{\pi}{\sin(\pi s)}\zeta(1-s). \quad (55)$$

*Inversion of the map.*

Now, by Mellin inversion we obtain:

$$\mathrm{M}^{-1}\left[-\frac{\pi}{\sin(\pi s)}\zeta(1-s);x\right]=h(x). \quad (56)$$

This is equivalent to the inversion integral

$$\int_{c-i\infty}^{c+i\infty}\left(-\frac{\pi}{\sin(\pi s)}\zeta(1-s)\right)x^{-s}ds = h(x). \quad (57)$$

This integral representation permits the computation of $h(x)$, because the integral can evaluated by the Cauchy Residue theorem, i.e., it is a sum of residues of $h^*(s)x^{-s}$.

*Computation of the poles of the transform function and the corresponding terms in the asymptotic expansion.*

We use the fact that

$$h(x) \approx -\sum_{\varsigma \in Sing\left(h^*(s)x^{-s}\right)\cap H} \operatorname{Res} s\left(h^*(s)x^{-s}; s=\varsigma\right), \quad (58)$$

where $H$ is the right half-plane, chosen for an expansion at infinity. We must compute the set of poles $Sing\left(h^*(s)x^{-s}\right)\cap H$ and map them back to the terms of the expansion of $h(x)$. The poles of $h^*(s)$ in the right half-plane are at $s=0$, where we have a double pole and

$$h^*(s) = \frac{1}{s^2} - \frac{\gamma}{s} + \ldots \quad (59)$$

and at $s=k, k \in Z^+$, where we have

$$h^*(s) = -(-1)^k \frac{\zeta(1-k)}{s-k} + \ldots. \quad (60)$$

These poles map back to $-\log x - \gamma$ (61) and $-\frac{1}{2x}$ for $k=1$, $-\frac{(-1)^k B_k}{k}\frac{1}{x^k}$ for $k \geq 2$. (62)

We conclude that Harmonic numbers satisfy the asymptotic expansion

$$H_n \approx \log n + \gamma + \frac{1}{2n} + \sum_{k\geq 2}\frac{(-1)^k B_k}{k}\frac{1}{n^k}. \quad (63)$$

This expansion is exact; it converges for $n \geq 1$.
The Mellin transform maps the space of functions that are integrable along the positive real line to that of complex functions that are analytic on a vertical strip of the complex plane. This strip may in many cases be extended to a larger domain. The map is given by the fundamental formula:

$$\mathrm{M}[f(x); s] = f^*(s) = \int_0^{+\infty} f(x)x^{s-1}dx. \quad (64)$$

The Mellin-Perron formula is a specific instance of generalized Mellin summation. The traditional proof uses the "discontinuous factor" described by the following lemma:

$$\phi(y) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{y^s}{s(s+1)\ldots(s+m)}ds = \frac{1}{m!}\left(1-\frac{1}{y}\right)^m \quad \text{if} \quad 1 \leq y;$$

$$\phi(y)=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{y^s}{s(s+1)...(s+m)}ds=0 \text{ if } 0<y\le 1, \qquad (65)$$

where $y\in R^+, m\in Z^+$ and $c\ge 1$.
The above equality for the discontinuous factor $\phi(y)$ is easily verified with the Cauchy residue theorem.
Hence, there are two cases.

*Case 1.* $1\le y$.

The term $\frac{y^s}{s(s+1)...(s+m)}$ (66) is meromorphic with residues

$$\frac{y^{-k}}{(-k)(-k+1)...(-k+k-1)(-k+k+1)...(-k+m)}=y^{-k}\frac{(-1)^k}{k!(m-k)!} \qquad (67)$$

where $0\le k\le m$. Therefore the sum of these residues is

$$\sum_{k=0}^{m}y^{-k}\frac{(-1)^k}{k!(m-k)!}=\frac{1}{m!}\sum_{k=0}^{m}\binom{m}{k}\left(-\frac{1}{y}\right)^k 1^{m-k}=\frac{1}{m!}\left(1-\frac{1}{y}\right)^m. \qquad (68)$$

Now consider the left contour. The integral along the vertical segment at $c$ in the right-half plane approaches

$$\int_{c-i\infty}^{c+i\infty}\frac{y^s}{s(s+1)...(s+m)}ds \qquad (69)$$

as $T$ goes to infinity. Along the two horizontal segments from $-T\pm iT$ to $c\pm iT$, the integrand is bounded by $\frac{y^\sigma}{T^m}$ and because the term $\frac{1}{1+\sigma}\frac{y^{1+\sigma}}{T^m}$ with $\sigma=-T$, $\sigma=c$ vanishes as $T$ goes to infinity (recall that $1\le y$), the contribution from these two segments is zero. The integrand is bounded by $\frac{y^{-T}}{T(T-1)...(T-m)}$ on the vertical segment in the left half-plane; hence the integral is bounded by $\frac{2y^{-T}}{(T-1)...(T-m)}$ and its contribution is zero also.

*Case 2.* $0<y\le 1$.

Consider the contour in the right half-plane. Along the horizontal segments we may use the same bound as in the first case, with $\sigma=c$ and $\sigma=T$; hence these integrals vanish $(0<y\le 1)$. The integrand is bounded by $\frac{y^T}{T(T+1)...(T+m)}$ on the vertical segment in the right half-plane; its contribution is zero because $0<y\le 1$.
The principal feature of the "discontinuous factor" is that it can be used to evaluate finite sums. Suppose we have a finite sum over the indices $k$ from 1 to $n-1$. Evidently $\phi(y)$ is non-zero if $1/y$

lies in $(0,1)$ and zero otherwise. We need only find a map such that the set $\{1,...n-1\}$ maps to a subrange of $(0,1)$ and $\{n,n+1...\}$ to a subrange of $[1,\infty)$. Clearly $1/y = k/n$ is such a map. We obtain

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{1}{k^s}\frac{n^s}{s(s+1)...(s+m)}ds = \frac{1}{m!}\left(1-\frac{k}{n}\right)^m \quad \text{if} \quad k<n$$

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{1}{k^s}\frac{n^s}{s(s+1)...(s+m)}ds = 0 \quad \text{if} \quad n\le k \qquad (70)$$

By a formal argument we finally have

$$\frac{1}{m!}\sum_{k=1}^{n-1}\lambda_k\left(1-\frac{k}{n}\right)^m = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(\sum\frac{\lambda_k}{k^s}\right)\frac{n^s}{s(s+1)...(s+m)}ds\,. \qquad (71)$$

This is the **Mellin-Perron formula**.
The Mellin-transform view adds two additional perspectives. One, that the Mellin-Perron formula is a specific instance of harmonic sum formulas, and hence, two, that its evaluation corresponds to Mellin inversion.

We wish to evaluate the harmonic sum $\sum_{1\le k<n}\lambda_k\left(1-\frac{k}{n}\right)^m$ (72) where $m,n\in Z^+$. This is equivalent to $\sum_1^\infty\lambda_k g\left(\frac{k}{n}\right)$ (73) where $g(x)=(1-x)^m$ if $0<x\le 1$; $g(x)=0$ otherwise. It is no difficult to see that $\mathrm{M}[g(x);s]=\frac{1}{s(s+1)...(s+m)}$. (74)

Evidently the sum $\sum_1^\infty\lambda_k g\left(\frac{k}{n}\right)$ is a harmonic sum $G(x)$ of the form $\sum_1^\infty\lambda_k g(kx)$ with amplitudes $\lambda_k$, frequencies $\mu_k = k$ and evaluated at $x = 1/n$. Therefore the transform function $G^*(s)$ is

$$\Lambda(s)\frac{1}{s(s+1)...(s+m)}\,. \qquad (75)$$

By Mellin inversion we thus have

$$G(x)=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\Lambda(s)\frac{x^{-s}}{s(s+1)...(s+m)}ds \qquad (76)$$

and in particular

$$G\left(\frac{1}{n}\right)=\sum_{1\le k<n}\lambda_k\left(1-\frac{k}{n}\right)^m=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\Lambda(s)\frac{n^s}{s(s+1)...(s+m)}ds\,. \qquad (77)$$

This is the Mellin-Perron formula.

***The Mellin transform: Definitions, Theorems and Lemmas***

**Definition 2.2.1**

The open strip of complex numbers $\langle \alpha, \beta \rangle$ is the set $\{s = \sigma + it | \alpha < \sigma < \beta\}$.

**Definition 2.2.2**

Let $f(x)$ be locally Lebesgue integrable over $(0,+\infty)$. The Mellin transform of $f(x)$ is defined by

$$\mathrm{M}[f(x);s] = f^*(s) = \int_0^{+\infty} f(x) x^{s-1} dx. \quad (78)$$

The fundamental strip is the largest open strip where the integral converges.

**Lemma 2.2.1**

The conditions $f(x)_{x\to 0^+} \in \mathrm{O}(x^u), \quad f(x)_{x\to+\infty} \in \mathrm{O}(x^v), \quad (79)$

when $u > v$, guarantee that $f^*(x)$ exists in the strip $\langle -u, -v \rangle$.

**Definition 2.2.3**

Let $H_0(x) = 1$ if $x \in [0,1]$; $H_0(x) = 0$ if $x > 1$ (80) be defined on $[0,+\infty)$ and let

$$H_m(x) = (1-x)^m H_0(x) \text{ when } m \in Z^+. \quad (81)$$

Note that $H_0(x)$ has a discontinuity at $x = 1$; we have $\lim_{x\to 1-} H_0(x) = 1$ and $\lim_{x\to 1+} H_0(x) = 0$. Note also that $\lim_{x\to 1-} H_m(x) = \lim_{x\to 1+} H_m(x) = 0$ when $m \in Z^+$; $H_m(x)$ is continuous at $x = 1$.

**Lemma 2.2.2**

The Mellin transform $H_m^*(x)$ of $H_m(x)$, where $m \in N$, exists in $\langle 0,+\infty \rangle$ and is given by

$$H_m^*(x) = \frac{m!}{s(s+1)...(s+m)}. \quad (82)$$

We have $H_m(x)_{x\to 0+} \in \mathrm{O}(1)$ and $H_m(x)_{x\to+\infty} \in \mathrm{O}(x^{-b})$ for any $b > 0$ and for $m \in N$, hence $H_m^*(x)$ exists in $\langle 0,+\infty \rangle$. Note that

$$H_0^*(x) = \int_0^1 x^{s-1} dx = \frac{1}{s}\left[x^s\right]_0^1 = \frac{1}{s}. \quad (83)$$

We also have

$$H_m^*(s) = \int_0^1 H_m(x) x^{s-1} dx = \int_0^1 H_{m-1}(x) x^{s-1} dx - \int_0^1 H_{m-1}(x) x^s dx =$$

$$= H_{m-1}^*(x) - \int_0^1 \frac{(1-x)^m}{m} s x^{s-1} dx = H_{m-1}^*(x) - \frac{s}{m} H_m^*(x). \quad (84)$$

This gives $$H_m^*(x)=\frac{m}{s+m}H_{m-1}^*(x) \quad (85)$$

Now, we will be concerned with the linearity and the rescaling property of the Mellin transform.

**Theorem 2.2.1**

Let $\mathrm{K}\subset Z$ be a finite set of integers; let $\mu_k,\lambda_k\in R^+$. Let the fundamental strip of $\mathrm{M}[f(x);s]$ be $\langle\alpha,\beta\rangle$. We have

$$\mathrm{M}\left[\sum_k \lambda_k f(\mu_k x);s\right]=\left(\sum_k \frac{\lambda_k}{\mu_k^s}\right)\mathrm{M}[f(x);s], \quad (86)$$

where $s\in\langle\alpha,\beta\rangle$.
Let $y=\mu_k x$ and $dy=\mu_k dx$. Note that

$$\int_0^\infty\left(\sum_k \lambda_k f(\mu_k x)\right)x^{s-1}dx=\sum_k \lambda_k\int_0^\infty f(\mu_k x)x^{s-1}dx=\sum_k \lambda_k\int_0^\infty f(y)y^{s-1}\frac{dy}{\mu_k^s}=\left(\sum_k \frac{\lambda_k}{\mu_k^s}\right)f^*(s). \quad (87)$$

We were able to exchange the integral with the summation because $\mathrm{K}$ is finite. It can be shown that this operation extends to infinite $\mathrm{K}$ as long as $\sum_k \lambda_k/\mu_k^s$ converges absolutely. The extended property holds in the intersection of the half-plane of convergence of $\sum_k \lambda_k/\mu_k^s$ and the fundamental strip $\langle\alpha,\beta\rangle$ of $f(x)$.

**Definition 2.2.4**

*1.* (Lebesgue integration)

Let $f(x)$ be integrable with fundamental strip $\langle\alpha,\beta\rangle$. If $c\in(\alpha,\beta)$ and $f^*(c+it)$ is integrable, then

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}f^*(s)x^{-s}ds=f(x) \quad (88)$$

almost everywhere. If $f(x)$ is continuous, the equality holds everywhere on $(0,+\infty)$.

*2.* (Riemann integration.)

Let $f(x)$ be locally integrable with fundamental strip $\langle\alpha,\beta\rangle$ and be of bounded variation in a neighbourhood of $x_0$. Then

$$\lim_{T\to\infty}\frac{1}{2\pi i}\int_{c-iT}^{c+iT}f^*(s)x^{-s}ds\Big|_{x_0}=\frac{f(x_0^+)+f(x_0^-)}{2} \quad (89)$$

for $c\in(\alpha,\beta)$. Of course if $\lim_{x\to x_0^+}f(x)=\lim_{x\to x_0^-}f(x)$ then

$$\frac{f\left(x_0^+\right)+f\left(x_0^-\right)}{2}=f\left(x_0\right). \quad (90)$$

**Theorem 2.2.2** (Mellin-Perron formula)

Let $c\in R^+$ lie in the half-plane of absolute convergence of $\sum_k \lambda_k / k^s$. Then we have

$$\frac{1}{m!}\sum_{1\le k<n}\lambda_k\left(1-\frac{k}{n}\right)^m=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(\sum_{k\ge 1}\frac{\lambda_k}{k^s}\right)n^s\frac{ds}{s(s+1)...(s+m)} \quad (91)$$

for $m\in Z^+$. We have

$$\sum_{1\le k<n}\lambda_k+\frac{\lambda_n}{2}=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(\sum_{k\ge 1}\frac{\lambda_k}{k^s}\right)n^s\frac{ds}{s} \quad (92)$$

when $m=0$.
This theorem is a straightforward application of Mellin inversion.

**Proof**.

Let $F(x)=\sum_k \lambda_k f(\mu_k x)$ and use the rescaling property to obtain

$$\mathrm{M}[F(x);s]=F^*(s)=\left(\sum_k\frac{\lambda_k}{\mu_k^s}\right)f^*(s). \quad (93)$$

Consider Riemann-integrable $f(x)$ and apply the Mellin inversion formula

$$\sum_k\lambda_k\frac{f\left(\mu_k x^+\right)+f\left(\mu_k x^-\right)}{2}=\lim_{T\to\infty}\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left(\sum_k\frac{\lambda_k}{\mu_k^s}\right)f^*(s)x^{-s}ds. \quad (94)$$

Let $f(x)=H_m(x)$, $m\in N$ and let $\mu_k=k$. Recall that the fundamental strip of $H_m(x)$ is $\langle 0,\infty\rangle$; let $x=1/n$. This gives

$$\sum_k\lambda_k\frac{f\left(\mu_k x^+\right)+f\left(\mu_k x^-\right)}{2}=\sum_k\lambda_k\frac{H_m\left(\frac{k}{n^-}\right)+H_m\left(\frac{k}{n^+}\right)}{2}=$$

$$=\sum_{1\le k<n}\lambda_k\frac{\left(1-\frac{k}{n^-}\right)^m+\left(1-\frac{k}{n^+}\right)^m}{2}+\lambda_n\frac{H_m\left(1^+\right)+H_m\left(1^-\right)}{2}=\sum_{1\le k<n}\lambda_k\left(1-\frac{k}{n}\right)^m+\lambda_n\frac{H_m\left(1^+\right)+H_m\left(1^-\right)}{2}. \quad (95)$$

Note that

$$\lambda_n\frac{H_m\left(1^+\right)+H_m\left(1^-\right)}{2}=\lambda_n/2 \text{ if } m=0; \quad \lambda_n\frac{H_m\left(1^+\right)+H_m\left(1^-\right)}{2}=0 \text{ if } m\in Z^+. \quad (96)$$

Continuing the substitution, we have

$$\lim_{T\to\infty}\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left(\sum_k\frac{\lambda_k}{\mu_k^s}\right)f^*(s)x^{-s}ds=\lim_{T\to\infty}\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left(\sum_k\frac{\lambda_k}{k^s}\right)\frac{m!}{s(s+1)...(s+m)}n^s ds=$$

$$=\frac{m!}{2\pi i}\int_{c-i\infty}^{c+i\infty}\left(\sum_k\frac{\lambda_k}{k^s}\right)n^s\frac{ds}{s(s+1)...(s+m)}. \quad (97)$$

This concludes the proof. Because the fundamental strip of $H_m(x)$ is $\langle 0,\infty\rangle$, the choice of $c>0$ is determined by the half-plane of convergence of $\sum_k \lambda_k/k^s$ only.

Now we presents two Mellin-Perron formulae for the generalized $\zeta$-function. We apply the Mellin inversion theorem to $F(x)=\sum_k\lambda_k f(\mu_k x)$ with $x=r/n$, $r,n\in Z^+$, $\mu_k=k+a$, $\lambda_k=1$, $a\in R$, $a\in(0,1]$, $f(x)=H_1(x)=(1-x)H_0(x)$. As we require $\mu_k\in R^+$ we take $k\in N$. We have

$$F(x)=\sum_{k\in N}\left(1-(k+a)\frac{r}{n}\right)H_0\left((k+a)\frac{r}{n}\right) \quad (98)$$

and

$$F^*(s)=\left(\sum_{k\in N}\frac{1}{(k+a)^s}\right)f^*(s)=\frac{\zeta(s,a)}{s(s+1)} \quad (99)$$

where $\sigma>1$. We need to evaluate $F(x)$. $H_0(x)$ vanishes outside of $[0,1)$, hence we require $0\le(k+a)r/n<1$ or $k<n/r-a$. Let $N(u)=\{v<u|v\in N\}$ where $u\in R^+$. We have

$$F(x)=\sum_{k\in N(n/r-a)}\left(1-(k+a)\frac{r}{n}\right). \quad (100)$$

With these settings the Mellin inversion formula yields the following theorem.

**Theorem 2.2.3**

Let $c>1$.

$$\sum_{k\in N(n/r-a)}\left(1-(k+a)\frac{r}{n}\right)=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{1}{r^s}\zeta(s,a)\frac{n^s}{s(s+1)}ds. \quad (101)$$

This theorem has several useful corollaries. The first of these is obtained by setting $r=1$. Let $\alpha\in(-1,0)$.

**Corollary 2.2.3**

Let $n\in N$.

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\zeta(s,a)\frac{n^s}{s(s+1)}ds=0. \quad (102)$$

Let $c=1$. The set of poles of $\zeta(s,a)n^s/(s(s+1))$ in $\langle\alpha,c\rangle$ is $\{1,0\}$. We apply the shifting lemma with $\Phi(s)=n^s$ and $T_j=j$. Because $|n^s|=n^\sigma$ we can take $M=n^c$.

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\zeta(s,a)\frac{n^s}{s(s+1)}ds=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\zeta(s,a)\frac{n^s}{s(s+1)}$$
$$-\operatorname{Re}s\left(\zeta(s,a)\frac{n^s}{s(s+1)};s=1\right)-\operatorname{Re}s\left(\zeta(s,a)\frac{n^s}{s(s+1)};s=0\right)$$
$$=\sum_{0\le k<n}\left(1-(k+a)\frac{1}{n}\right)-\frac{n}{2}-\zeta(0,a)=n-n\frac{a}{n}-\frac{1}{n}\frac{1}{2}(n-1)n-\frac{n}{2}-\zeta(0,a)=\frac{1}{2}-a-\zeta(0,a)=0. \quad (103)$$

The second corollary results from taking $r=4$.

**Corollary 2.2.4**

Let $n\in N$.

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\frac{1}{4^s}\zeta(s,a)\frac{n^s}{s(s+1)}ds. \quad (104)$$

We let $c=1$ as before and consider the poles of $\zeta(s,a)n^s/\left(4^s s(s+1)\right)$ in $\langle\alpha,c\rangle$, which are at 1 and 0. We apply the shifting lemma with $\Phi(s)=(n/4)^s$, $T_j=j$ and take $M=(n/4)^c$.

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\zeta(s,a)\frac{n^s}{4^s s(s+1)}ds=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\zeta(s,a)\frac{n^s}{4^s s(s+1)}$$
$$-\operatorname{Re}s\left(\zeta(s,a)\frac{n^s}{4^s s(s+1)};s=1\right)-\operatorname{Re}s\left(\zeta(s,a)\frac{n^s}{4^s s(s+1)};s=0\right)$$
$$=\sum_{k\in N(n/4-a)}\left(1-(k+a)\frac{4}{n}\right)-\frac{n}{8}-\zeta(0,a)=\varepsilon(n,a)-\frac{n}{8}-\zeta(0,a). \quad (105)$$

Suppose $n=4m+m_1$ where $m_1\in\{0,1,2,3\}$. We have $n/4-a=[n/4]+m_1/4-a$. If $m_1/4<a$, the sum over $N(n/4-a)$ ranges from 0 to $[n/4]-1$. If $m_1/4\ge a$ the sum includes $[n/4]$. We have two cases:

$$\varepsilon(n,a)=\left[\frac{n}{4}\right]-a\frac{4}{n}\left[\frac{n}{4}\right]-\frac{2}{n}\left(\left[\frac{n}{4}\right]-1\right)\left[\frac{n}{4}\right] \qquad \text{if } \frac{m_1}{4}<a$$
$$\varepsilon(n,a)=\left[\frac{n}{4}\right]+1-a\frac{4}{n}\left(\left[\frac{n}{4}\right]+1\right)-\frac{2}{n}\left(\left[\frac{n}{4}\right]+1\right)\left[\frac{n}{4}\right] \qquad \text{if } \frac{m_1}{4}\ge a.$$

We note that $[n/4]=(n-m_1)/4$ and $[n/4]4/n=1-m_1/n$. Hence the two terms evaluate to

$$\frac{1}{8}n+\frac{1}{2}-a+\frac{1}{n}\left(am_1-\frac{1}{2}m_1-\frac{1}{8}m_1^2\right) \quad \text{and} \quad \frac{1}{8}n+\frac{1}{2}-a+\frac{1}{n}\left(a(m_1-4)+\frac{1}{2}m_1-\frac{1}{8}m_1^2\right).$$

We conclude that

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\zeta(s,a)\frac{n^s}{4^s s(s+1)}ds=\varepsilon(n,a)-\frac{1}{8}n-\frac{1}{2}+a. \quad (106)$$

2.3 The zeta-function quantum field theory and the quantum L-functions.

The Riemann zeta-function is defined as

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad s=\sigma+i\tau,\quad \sigma>1 \qquad (107)$$

and there is an Euler adelic representation

$$\zeta(s)=\prod_{p}\left(1-p^{-s}\right)^{-1}. \qquad (108)$$

Now, we have the Riemann $\xi$-function

$$\xi(s)=\frac{s(s-1)}{2}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) \qquad (109)$$

which is an entire function. The zeros of the $\xi$-function are the same as the nontrivial zeros of the $\zeta$-function. There is the functional equation

$$\xi(s)=\xi(1-s) \qquad (110)$$

and the Hadamard representation for the $\xi$-function

$$\xi(s)=\frac{1}{2}e^{as}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{s/\rho}. \qquad (111)$$

Here $\rho$ are nontrivial zeros of the zeta-function and

$$a=-\frac{1}{2}\gamma-1+\frac{1}{2}\log 4\pi \qquad (112)$$

where $\gamma$ is Euler's constant.
If $F(\tau)$ is a function of a real variable $\tau$ then we define a pseudo-differential operator $F(\Box)$ by using the Fourier transform

$$F(\Box)\phi(x)=\int e^{ixk}F\left(k^2\right)\tilde{\phi}(k)dk. \qquad (113)$$

Here $\Box$ is the d'Alambertian operator

$$\Box=-\frac{\partial^2}{\partial x_0^2}+\frac{\partial^2}{\partial x_1^2}+\ldots+\frac{\partial^2}{\partial x_{d-1}^2}, \qquad (114)$$

$\phi(x)$ is a function from $x\in R^d$, $\tilde{\phi}(k)$ is the Fourier transform and $k^2=k_0^2-k_1^2-\ldots-k_{d-1}^2$.
We assume that the integral (113) converges.

One can introduce a natural field theory related with the real valued function $F(\tau)=\xi\left(\frac{1}{2}+i\tau\right)$ defined by means of the zeta-function. We consider the following Lagrangian

$$L=\phi\xi(1/2+i\,\square)\,\phi\,, \quad (115)$$

the integral

$$\xi(1/2+i\,\square)\,\phi\,(x)=\int e^{ixk}\xi(1/2+i\,\square)\,\tilde{\phi}(k)dk \quad (116)$$

converges if $\phi(x)$ is a decreasing function since $\xi\left(\frac{1}{2}+i\tau\right)$ is bounded.

The operator $\xi(1/2+i\,\square)$ (or $\zeta(1/2+i\,\square)$) is the first quantization the Riemann zeta-function. From the Hadamard representation (111) we get

$$\xi\left(\frac{1}{2}+i\tau\right)=\frac{C}{2}\prod_{n=1}^{\infty}\left(1-\frac{\tau^2}{m_n^4}\right). \quad (117)$$

It is possible to write the formula (117) in the form

$$\xi\left(\frac{1}{2}+i\tau\right)=\frac{C}{2}\prod_{\varepsilon,n}\left(1+\frac{\tau}{\varepsilon m_n^2}\right) \quad (118)$$

where $\varepsilon=\pm1$ and a regularization is assumed.

To quantize the zeta-function classical field $\phi(x)$ which satisfies the equation in the Minkowski space

$$F\,(\square)\,\phi(x)=0 \quad (119)$$

where $F\,(\square)=\xi(1/2+i\,\square)$ we can try to interpret $\phi(x)$ as an operator valued distribution in a Hilbert space $\mathrm{H}$ which satisfies the equation (119). We suppose that there is a representation of the Poincare group and an invariant vacuum vector $|0\rangle$ in $\mathrm{H}$. Then the Wightman function

$$W(x-y)=\langle 0|\phi(x)\phi(y)|0\rangle$$

is a solution of the equation

$$F\,(\square)\,W(x)=0\,. \quad (120)$$

By using (118) we can write the formal Kallen-Lehmann representation

$$W(x)=\sum_{\varepsilon n}\int e^{ixk}f_{\varepsilon n}(k)\delta\left(k^2+\varepsilon m_n^2\right)dk\,. \quad (121)$$

One introduces also another useful function

$$Z(\tau)=\pi^{-i\tau/2}\frac{\Gamma\left(\frac{1}{4}+\frac{i\tau}{2}\right)}{\left|\Gamma\left(\frac{1}{4}+\frac{i\tau}{2}\right)\right|}\zeta\left(\frac{1}{2}+i\tau\right)=e^{i\vartheta(\tau)}\zeta\left(\frac{1}{2}+i\tau\right). \quad (122)$$

Here $\Gamma(z)$ is the gamma function. The function $Z(\tau)$ is called the Riemann-Siegel (or Hardy) function. It is known that $Z(\tau)$ is real for real $\tau$ and there is a bound

$$Z(\tau)=O\left(|\tau|^{\varepsilon}\right), \quad \varepsilon>0. \quad (123)$$

One can introduce a natural field theory related with the real valued functions $Z(\tau)$ defined by means of the zeta-function by considering the following Lagrangian

$$L=\phi Z(\Box)\phi.$$

The integral (113) converges if $\phi(x)$ is a decreasing function since there is the bound (123).
Thence, we have the following connection:

$$\pi^{-i\tau/2}\frac{\Gamma\left(\frac{1}{4}+\frac{i\tau}{2}\right)}{\left|\Gamma\left(\frac{1}{4}+\frac{i\tau}{2}\right)\right|}\zeta\left(\frac{1}{2}+i\tau\right)=e^{i\vartheta(\tau)}\zeta\left(\frac{1}{2}+i\tau\right)=O\left(|\tau|^{\varepsilon}\right)\Rightarrow$$

$$\Rightarrow F(\Box)\phi(x)=\int e^{ixk}F\left(k^2\right)\tilde{\phi}(k)dk, \quad \varepsilon>0. \quad (124)$$

For any character to modulus $q$ one defines the corresponding Dirichlet L-function by setting

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \quad (\sigma>1). \quad (125)$$

If $\chi$ is primitive then $L(s,\chi)$ has an analytic continuation to the whole complex plane. The zeros lie in the critical strip and symmetrically distributed about the critical line $\sigma=1/2$.
If we quantize the L-function by considering the pseudo-differential operator

$$L(\sigma+i\Box,\chi) \quad (126)$$

then we can try to avoid the appearance of tachyons and/or ghosts by choosing an appropriate character $\chi$.
The Taniyama-Weil conjecture relates elliptic curves and modular forms. It asserts that if E is an elliptic curve over $Q$, then there exists a weight-two cusp form $f$ which can be expressed as the Fourier series

$$f(z)=\sum a_n e^{2\pi inz} \quad (127)$$

with the coefficients $a_n$ depending on the curve E. Such a series is a modular form if and only if its Mellin transformation, i.e. the Dirichlet L-series

$$L(s,f)=\sum a_n n^{-s} \quad (128)$$

has a holomorphic extension to the full s-plane and satisfies a functional equation. For the elliptic curve E we obtain the L-series $L(s,E)$. The Taniyama-Weil conjecture was proved by Wiles and Taylor for semistable elliptic curves and it implies Fermat's Last Theorem.
Quantization of the L-functions can be performed similarly to the quantization of the Riemann zeta-function discussed above by considering the corresponding pseudo-differential operator $L(\sigma + i\square)$.

## Chapter 3.

## How primes and adeles are related to the Riemann zeta function

A. Connes has reduced the Riemann hypothesis for L-function on a global field k to the validity of a trace formula for the action of the idele class group on the noncommutative space quotient of the adeles of k by the multiplicative group of k.
Connes has devised a Hermitian operator whose eigenvalues are the Riemann zeros on the critical line. Connes gets a discrete spectrum by making the operator act on an abstract space where the primes appearing in the Euler product for the Riemann zeta function are built in; the space is constructed from collections of p-adic numbers (adeles) and the associated units (ideles).
Hence, the geometric framework involves the space X of Adele classes, where two adeles which belong to the same orbit of the action of $GL_1(k)$ ($k$ a global field), are considered equivalent. The group $C_k = GL_1(A)/GL_1(k)$ of Idele classes (which is the class field theory counterpart of the Galois group) acts by multiplication on X.
We have a trace formula (Theorem 3) for the action of the multiplicative group $K^*$ of a local field $K$ on the Hilbert space $L^2(K)$, and (Theorem 4) a trace formula for the action of the multiplicative group $C_s$ of Idele classes associated to a finite set $S$ of places of a global field $k$, on the Hilbert space of square integrable functions $L^2(X_S)$, where $X_S$ is the quotient of $\prod_{v\in S} k_v$ by the action of the group $O_S^*$ of S-units of $k$. The validity of the trace formula for any finite set of places follows from Theorem 4, but in the global case is left open and shown (Theorem 5) to be equivalent to the validity of the Riemann Hypothesis for all $L$ functions with Grossencharakter.

H. Montgomery has proved (assuming RH) a weakening of the following conjecture (with $\alpha,\beta>0$),

$$Card\{(i,j);i,j\in 1,...,M;x_i-x_j\in[\alpha,\beta]\}\approx M\int_\alpha^\beta\left(1-\left(\frac{\sin(\pi u)}{\pi u}\right)^2\right)du \quad (1)$$

This law, i.e. the equation (1), is precisely the same as the correlation between eigenvalues of hermitian matrices of the gaussian unitary ensemble. Moreover, numerical tests due to A. Odlyzko have confirmed with great precision the behaviour (1) as well as the analogous behaviour for more than two zeros. N. Katz and P. Sarnak has proved an analogue of the Montgomery-Odlyzko law for zeta and L-functions of function fields over curves.
It is thus an excellent motivation to try and find a natural pair $(\mathrm{H},D)$ where naturality should mean for instance that one should not even have to define the zeta function, let alone its analytic continuation, in order to obtain the pair (in order for instance to avoid the joke of defining H as the $\ell^2$ space built on the zeros of zeta).

**Theorem 1**.

*Let $K$ be a local field with basic character $\alpha$. Let $h\in S(K^*)$ have compact support. Then $R_\Lambda U(h)$ is a trace class operator and when $\Lambda\to\infty$, one has*

$$Trace(R_\Lambda U(h))=2h(1)\log'\Lambda+\int'\frac{h(u^{-1})}{|1-u|}d^*u+o(1) \quad (2)$$

*where $2\log'\Lambda=\int_{\lambda\in K^*,|\lambda|\in[\Lambda^{-1},\Lambda]}d^*\lambda$, and the principal value $\int'$ is uniquely determined by the pairing with the unique distribution on $K$ which agrees with $\frac{du}{|1-u|}$ for $u\neq 1$ and whose Fourier transform vanishes at 1.*

*Proof.*

We normalize the additive Haar measure to be the selfdual one on $K$. Let the constant $\rho>0$ be determined by the equality,

$$\int_{1\le|\lambda|\le\Lambda}\frac{d\lambda}{|\lambda|}\approx\rho\log\Lambda \quad \text{when} \quad \Lambda\to\infty, \quad (3)$$

so that $d^*\lambda=\rho^{-1}\frac{d\lambda}{|\lambda|}$. Let $L$ be the unique distribution, extension of $\rho^{-1}\frac{du}{|1-u|}$ whose Fourier transform vanishes at 1, $\hat{L}(1)=0$. One then has by definition,

$$\int'\frac{h(u^{-1})}{|1-u|}d^*u=\left\langle L,\frac{h(u^{-1})}{|u|}\right\rangle, \quad (4)$$

where $\frac{h(u^{-1})}{|u|}=0$ for $u^{-1}$ outside the support of $h$. Let $T=U(h)$. We can write the Schwartz kernel of $T$ as,

$$k(x,y)=\int h(\lambda^{-1})\delta(y-\lambda x)d^*\lambda\,. \quad (5)$$

Given any such kernel $k$ we introduce its symbol,

$$\sigma(x,\xi)=\int k(x,x+u)\alpha(u\xi)du \quad (6)$$

as its partial Fourier transform. The Schwartz kernel $r_\Lambda^t(x,y)$ of the transpose $R_\Lambda^t$ is given by,

$$r_\Lambda^t(x,y)=\rho_\Lambda(x)(\hat{\rho}_\Lambda)(x-y)\,. \quad (7)$$

Thus, the symbol $\sigma_\Lambda$ of $R_\Lambda^t$ is simply,

$$\sigma_\Lambda(x,\xi)=\rho_\Lambda(x)\rho_\Lambda(\xi)\,. \quad (8)$$

The operator $R_\Lambda$ is of trace class and one has,

$$\mathrm{Trace}\,(R_\Lambda T)=\int k(x,y)r_\Lambda^t(x,y)dxdy\,. \quad (9)$$

Using the Parseval formula we thus get,

$$\mathrm{Trace}\,(R_\Lambda T)=\int_{|x|\le\Lambda,|\xi|\le\Lambda}\sigma(x,\xi)dxd\xi\,. \quad (10)$$

Now the symbol $\sigma$ of T is given by,

$$\sigma(x,\xi)=\int h(\lambda^{-1})\left(\int\delta(x+u-\lambda x)\alpha(u\xi)du\right)d^*\lambda\,. \quad (11)$$

One has,

$$\int\delta(x+u-\lambda x)\alpha(u\xi)du=\alpha((\lambda-1)x\xi), \quad (12)$$

thus (11) gives,

$$\sigma(x,\xi)=\rho^{-1}\int_K g(\lambda)\alpha(\lambda x\xi)d\lambda \quad (13)$$

where,

$$g(\lambda)=h\left((\lambda+1)^{-1}\right)|\lambda+1|^{-1}\,. \quad (14)$$

Since $h$ is smooth with compact support on $K^*$ the function $g$ belongs to $C_c^\infty(K)$. Thus $\sigma(x,\xi)=\rho^{-1}\hat{g}(x\xi)$ and

$$\mathrm{Trace}\,(R_\Lambda T)=\rho^{-1}\int_{|x|\le\Lambda,|\xi|\le\Lambda}\hat{g}(x\xi)dxd\xi\,. \quad (15)$$

With $u=x\xi$ one has $dxd\xi=du\dfrac{dx}{|x|}$ and, for $|u|\le\Lambda^2$,

$$\rho^{-1}\int_{\frac{|u|}{\Lambda}\le|x|\le\Lambda}\frac{dx}{|x|}=2\log'\Lambda-\log|u|\,. \quad (16)$$

Thus we can rewrite (15) as,

$$\mathrm{Trace}\left(R_\Lambda T\right)=\int_{|u|\le\Lambda^2}\hat{g}(u)\left(2\log'\Lambda-\log|u|\right)du\,. \quad (17)$$

Since $g\in C_c^\infty(K)$ one has,

$$\int_{|u|\ge\Lambda^2}\left|\hat{g}(u)\right|du=O\left(\Lambda^{-N}\right)\qquad\forall N \quad (18)$$

and similarly for $\left|\hat{g}(u)\log|u|\right|$. Thus

$$\mathrm{Trace}\left(R_\Lambda T\right)=2g(0)\log'\Lambda-\int\hat{g}(u)\log|u|du+o(1). \quad (19)$$

Now for any local field $K$ and basic character $\alpha$, if we take for the Haar measure $da$ the selfdual one, the Fourier transform of the distribution $\varphi(u)=-\log|u|$ is given outside 0 by

$$\hat{\varphi}(a)=\rho^{-1}\frac{1}{|a|}, \quad (20)$$

with $\rho$ determined by (3). To see this one lets $P$ be the distribution on $K$ given by,

$$P(f)=\lim_{\substack{\varepsilon\to0\\ \varepsilon\in Mod(K)}}\left(\int_{|x|\ge\varepsilon}f(x)d^*x+f(0)\log\varepsilon\right). \quad (21)$$

One has $P(f_a)=P(f)-\log|a|f(0)$ which is enough to show that the function $\hat{P}(x)$ is equal to $-\log|x|+\mathrm{cst}$, and $\hat{\varphi}$ differs from $P$ by a multiple of $\delta_0$. Thus the Parseval formula gives, with the convention of Theorem 3,

$$-\int\hat{g}(u)\log|u|du=\frac{1}{\rho}\int'g(a)\frac{da}{|a|}. \quad (22)$$

Replacing $a$ by $\lambda-1$ and applying (14) gives the desired result.

Now, let $k$ be a global field and $S$ a finite set of places of $k$ containing all infinite places. The group $O_S^*$ of $S$-units is defined as the subgroup of $k^*$, $O_S^*=\left\{q\in k^*,|q_v|=1,v\notin S\right\}$. It is co-compact in $J_S^1$ where, $J_S=\prod_{v\in S}k_v^*$ and, $J_S^1=\left\{j\in J_S,|j|=1\right\}$. Thus the quotient group $C_S=J_S/O_S^*$ plays the same role as $C_k$, and acts on the quotient $X_S$ of $A_S=\prod_{v\in S}k_v$ by $O_S^*$.

**Theorem 2**.

*Let $A_S$ be as above, with basic character $\alpha=\prod\alpha_v$. Let $h\in S(C_S)$ have compact support. Then when $\Lambda\to\infty$, one has*

$$Trace\left(R_\Lambda U(h)\right) = 2h(1)\log'\Lambda + \sum_{v\in S}\int'_{k_v^*}\frac{h\left(u^{-1}\right)}{|1-u|}d^*u + o(1) \quad (23)$$

*where* $2\log'\Lambda = \int_{\lambda\in C_S,|\lambda|\in[\Lambda^{-1},\Lambda]}d^*\lambda$, *each* $k_v^*$ *is embedded in* $C_S$ *by the map* $u\to(1,1,...,u,...,1)$ *and the principal value* $\int'$ *is uniquely determined by the pairing with the unique distribution on* $k_v$ *which agrees with* $\frac{du}{|1-u|}$ *for* $u\neq 1$ *and whose Fourier transform relative to* $\alpha_v$ *vanishes at 1.*

*Proof.*

We normalize the additive Haar measure $dx$ to be the selfdual one on the abelian group $A_S$. Let the constant $\rho>0$ be determined by the equality,

$$\int_{\lambda\in D,1\le|\lambda|\le\Lambda}\frac{d\lambda}{|\lambda|}\approx\rho\log\Lambda \quad \text{when} \quad \Lambda\to\infty,$$

so that $d^*\lambda=\rho^{-1}\frac{d\lambda}{|\lambda|}$. We let $f$ be a smooth compactly supported function on $J_S$ such that

$$\sum_{q\in O_S^*}f(qg)=h(g) \quad \forall g\in C_S. \quad (24)$$

The existence of such an $f$ follows from the discreteness of $O_S^*$ in $J_S$. We then have the equality $U(f)=U(h)$, where

$$U(f)=\int f(\lambda)U(\lambda)d^*\lambda. \quad (25)$$

Now, for an operator T, acting on functions on $A_S$, which commutes with the action of $O_S^*$ and is represented by an integral kernel,

$$T(\xi)=\int k(x,y)\xi(y)dy, \quad (26)$$

the trace of its action on $L^2(X_S)$ is given by,

$$Tr(T)=\sum_{q\in O_S^*}\int_D k(x,qx)dx, \quad (27)$$

where $D$ is a fundamental domain for the action of $O_S^*$ on the subset $J_S$ of $A_S$, whose complement is negligible. Let $T=U(f)$. We can write the Schwartz kernel of $T$ as,

$$k(x,y)=\int f\left(\lambda^{-1}\right)\delta(y-\lambda x)d^*\lambda, \quad (28)$$

by construction one has,

$$k(qx,qy)=k(x,y) \qquad q\in O_S^*. \quad (29)$$

For any $q\in O_S^*$, we shall evaluate the integral,

$$I_q=\int_{x\in D} k(qx,y)r_\Lambda^t(x,y)dydx \quad (30)$$

where the Schwartz kernel $r_\Lambda^t(x,y)$ for the transpose $R_\Lambda^t$ is given by,

$$r_\Lambda^t(x,y)=\rho_\Lambda(x)(\hat{\rho}_\Lambda)(x-y). \quad (31)$$

To evaluate the above integral, we let $y=x+a$ and perform a Fourier transform in $a$. For the Fourier transform in $a$ of $r_\Lambda^t(x,x+a)$, one gets,

$$\sigma_\Lambda(x,\xi)=\rho_\Lambda(x)\rho_\Lambda(\xi). \quad (32)$$

For the Fourier transform in $a$ of $k(qx,x+a)$, one gets,

$$\sigma(x,\xi)=\int f(\lambda^{-1})\left(\int \delta(x+a-\lambda qx)\alpha(a\xi)da\right)d^*\lambda. \quad (33)$$

One has,

$$\int \delta(x+a-\lambda qx)\alpha(a\xi)da=\alpha((\lambda q-1)x\xi), \quad (34)$$

thus (33) gives,

$$\sigma(x,\xi)=\rho^{-1}\int_{A_S} g_q(u)\alpha(ux\xi)du \quad (35)$$

where,

$$g_q(u)=f\left(q(u+1)^{-1}\right)|u+1|^{-1}. \quad (36)$$

Since $f$ is smooth with compact support on $A_S^*$ the function $g_q$ belongs to $C_c^\infty(A_S)$.
Thus $\sigma(x,\xi)=\rho^{-1}\hat{g}_q(x\xi)$ and, using the Parseval formula we get,

$$I_q=\int_{x\in D,|x|\le\Lambda,|\xi|\le\Lambda}\sigma(x,\xi)dxd\xi. \quad (37)$$

This gives,

$$I_q=\rho^{-1}\int_{x\in D,|x|\le\Lambda,|\xi|\le\Lambda}\hat{g}_q(x\xi)dxd\xi. \quad (38)$$

With $u=x\xi$ one has $dxd\xi=du\dfrac{dx}{|x|}$ and, for $|u|\le\Lambda^2$,

$$\rho^{-1}\int_{x\in D,\frac{|u|}{\Lambda}\le|x|\le\Lambda}\frac{dx}{|x|}=2\log'\Lambda-\log|u|. \quad (39)$$

Thus we can rewrite (38) as,

$$\text{Trace}\left(R_\Lambda T\right)=\sum_{q\in O_S^*}\int_{|u|\le\Lambda^2}\hat{g}_q(u)\left(2\log'\Lambda-\log|u|\right)du\,. \quad (40)$$

Now $\log|u|=\sum_{v\in S}\log|u_v|$, and we shall first prove that,

$$\sum_{q\in O_S^*}\int\hat{g}_q(u)du=h(1), \quad (41)$$

while for any $v\in S$,

$$\sum_{q\in O_S^*}\int\hat{g}_q(u)\left(-\log|u_v|\right)du=\int_{k_v^*}'\frac{h\left(u^{-1}\right)}{|1-u|}d^*u\,. \quad (42)$$

In fact all the sums in $q$ will have only finitely many non zero terms. It will then remain to control the error term, namely to show that,

$$\sum_{q\in O_S^*}\int\hat{g}_q(u)\left(\log|u|-2\log'\Lambda\right)^+du=0\left(\Lambda^{-N}\right), \quad (43)$$

for any $N$, where we used the notation $x^+=0$ if $x\le 0$ and $x^+=x$ if $x>0$.
Now recall that for (36), $g_q(u)=f\left(q(u+1)^{-1}\right)|u+1|^{-1}$, so that $\int\hat{g}_q(u)du=g_q(0)=f(q)$. Since $f$ has compact support in $A_S^*$, the intersection of $O_S^*$ with the support of $f$ is finite and by (24) we get the equality (41). To prove (42), we consider the natural projection $pr_v$ from $\prod_{l\in S}k_l^*$ to $\prod_{l\ne v}k_l^*$. The image $pr_v\left(O_S^*\right)$ is still a discrete subgroup of $\prod_{l\ne v}k_l^*$, thus there are only finitely many $q\in O_S^*$ such that $k_v^*$ meets the support of $f_q$, where $f_q(a)=f(qa)$ for all $a$.
For each $q\in O_S^*$ one has,

$$\int\hat{g}_q(u)\left(-\log|u_v|\right)du=\int_{k_v^*}'\frac{f_q\left(u^{-1}\right)}{|1-u|}d^*u\,, \quad (44)$$

and this vanishes except for finitely many $q's$, so that by (24) we get the equality (42).

**Theorem 3**.

*Let $k$ be a global field of positive characteristic and $Q_\Lambda$ be the orthogonal projection on the subspace of $L^2(X)$ spanned by the $f\in S(A)$ such that $f(x)$ and $\hat{f}(x)$ vanish for $|x|>\Lambda$. Let $h\in S(C_k)$ have compact support. Then the following conditions are equivalent*,

a) *When $\Lambda\to\infty$, one has*

$$\mathrm{Trace}\left(Q_\Lambda U(h)\right) = 2h(1)\log'\Lambda + \sum_v \int_{k_v^*}' \frac{h\left(u^{-1}\right)}{|1-u|} d^*u + o(1). \quad (45)$$

b) *All L functions with Grossencharakter on k satisfy the Riemann Hypothesis.*

To prove that (a) implies (b), we shall prove (assuming (a)) the positivity of the Weil distribution,

$$\Delta = \log\left|d^{-1}\right|\delta_1 + D - \sum_v D_v . \quad (46)$$

We have that for $\delta = 0$, the map $E$,

$$E(f)(g) = |g|^{1/2} \sum_{q \in k^*} f(qg) \qquad \forall g \in C_k , \quad (47)$$

defines a surjective isometry from $L^2(X)_0$ to $L^2(C_k)$ such that,

$$EU(a) = |a|^{1/2} V(a) E , \quad (48)$$

where the left regular representation $V$ of $C_k$ on $L^2(C_k)$ is given by,

$$(V(a)\xi)(g) = \xi\left(a^{-1}g\right) \qquad \forall g, a \in C_k . \quad (49)$$

Let $S_\Lambda$ be the subspace of $L^2(C_k)$ given by,

$$S_\Lambda = \left\{\xi \in L^2(C_k); \xi(g) = 0, \forall g, |g| \notin \left[\Lambda^{-1}, \Lambda\right]\right\}. \quad (50)$$

We shall denote by the same letter the corresponding orthogonal projection.
Let $B_{\Lambda,0}$ be the subspace of $L^2(X)_0$ spanned by the $f \in S(A)_0$ such that $f(x)$ and $\hat{f}(x)$ vanish for $|x| > \Lambda$ and $Q_{\Lambda,0}$ be the corresponding orthogonal projection. Let $f \in S(A)_0$ be such that $f(x)$ and $\hat{f}(x)$ vanish for $|x| > \Lambda$, then $E(f)(g)$ vanishes for $|g| > \Lambda$, and the equality

$$E(f)(g) = E\left(\hat{f}\right)\left(\frac{1}{g}\right) \qquad f \in S(A)_0 , \quad (51)$$

shows that $E(f)(g)$ vanishes for $|g| < \Lambda^{-1}$.
This shows that $E\left(B_{\Lambda,0}\right) \subset S_\Lambda$, so that if we let $Q'_{\Lambda,0} = EQ_{\Lambda,0}E^{-1}$, we get the inequality,

$$Q'_{\Lambda,0} \le S_\Lambda \quad (52)$$

and for any $\Lambda$ the following distribution on $C_k$ is of positive type,

$$\Delta_\Lambda(f)=\mathrm{Trace}\left(\left(S_\Lambda-Q'_{\Lambda,0}\right)V(f)\right),\quad (53)$$

i.e. one has,

$$\Delta_\Lambda\left(f*f^*\right)\geq 0\,,\quad (54)$$

where $f^*(g)=\bar{f}\left(g^{-1}\right)$ for all $g\in C_k$.

Let then $f(g)=|g|^{-1/2}h\left(g^{-1}\right)$, so that by (48) one has $EU(h)=V\left(\tilde{f}\right)E$ where $\tilde{f}(g)=f\left(g^{-1}\right)$ for all $g\in C_k$. Then, we have:

$$\sum_v D_v(f)-\log\left|d^{-1}\right|=\sum_v\int'_{k_v^*}\frac{h\left(u^{-1}\right)}{|1-u|}d^*u\,.\quad (55)$$

One has $\mathrm{Trace}\left(S_\Lambda V(f)\right)=2f(1)\log'\Lambda$, thus using (a) we see that the limit of $\Delta_\Lambda$ when $\Lambda\to\infty$ is the Weil distribution $\Delta$. The term $D$ in the latter comes from the nuance between the subspaces $B_\Lambda$ and $B_{\Lambda,0}$. This shows using (53), that the distribution $\Delta$ is of positive type so that (b) holds.

Let us now show that (b) implies (a). We shall compute from the zeros of $L$-functions and independently of any hypothesis the limit of the distributions $\Delta_\Lambda$ when $\Lambda\to\infty$.

We choose an isomorphism

$$C_k\cong C_{k,1}\times N\,.\quad (56)$$

where $N=\mathrm{range}\,|\,|\subset R_+^*$, $N\cong Z$ is the subgroup $q^Z\subset R_+^*$. For $\rho\in C$ we let $d\mu_\rho(z)$ be the harmonic measure of $\rho$ with respect to the line $iR\subset C$. It is a probability measure on the line $iR$ and coincides with the Dirac mass at $\rho$ when $\rho$ is on the line.

The implication (b)$\Rightarrow$(a) follows immediately from the explicit formulas and the following lemma,

**Lemma 1**.

*The limit of the distributions $\Delta_\Lambda$ when $\Lambda\to\infty$ is given by,*

$$\Delta_\infty(f)=\sum_{\substack{L\left(\tilde{\chi},\frac{1}{2}+\rho\right)=0\\ \rho\in B/N^\perp}}N\left(\tilde{\chi},\frac{1}{2}+\rho\right)\int_{z\in iR}\hat{f}(\tilde{\chi},z)d\mu_\rho(z)\quad (57)$$

*where $B$ is the open strip $B=\left\{\rho\in C;\mathrm{Re}(\rho)\in\left]\frac{-1}{2},\frac{1}{2}\right[\right\}$, $N\left(\tilde{\chi},\frac{1}{2}+\rho\right)$ is the multiplicity of the zero, $d\mu_\rho(z)$ is the harmonic measure of $\rho$ with respect to the line $iR\subset C$, and the Fourier transform $\hat{f}$ of $f$ is defined by*

$$\hat{f}(\tilde{\chi},\rho)=\int_{C_k}f(u)\tilde{\chi}(u)|u|^\rho d^*u\,.\quad (58)$$

Let us first recall the Weil explicit formulas. One lets $k$ be a global field. One identifies the quotient $C_k/C_{k,1}$ with the range of the module,

$$N = \{|g|; g \in C_k\} \subset R_+^*. \quad (59)$$

One endows $N$ with its normalized Haar measure $d^*x$. Given a function $F$ on $N$ such that, for some $b > \frac{1}{2}$,

$$|F(\nu)| = 0(\nu^b) \quad \nu \to 0, \quad |F(\nu)| = 0(\nu^{-b}), \quad \nu \to \infty, \quad (60)$$

one lets,

$$\Phi(s) = \int_N F(\nu)\nu^{1/2-s} d^*\nu. \quad (61)$$

Given a Grossencharakter $\chi$, i.e. a character of $C_k$ and any $\rho$ in the strip $0 < \mathrm{Re}(\rho) < 1$, one lets $N(\chi, \rho)$ be the order of $L(\chi, s)$ at $s = \rho$. One lets,

$$S(\chi, F) = \sum_\rho N(\chi, \rho)\Phi(\rho) \quad (62)$$

where the sum takes place over $\rho$'s in the above open strip. One then defines a distribution $\Delta$ on $C_k$ by,

$$\Delta = \log|d^{-1}|\delta_1 + D - \sum_v D_v, \quad (63)$$

where $\delta_1$ is the Dirac mass at $1 \in C_k$, where $d$ is a differential idele of $k$ so that $|d|^{-1}$ is up to sign the discriminant of $k$ when char $(k) = 0$ and is $q^{2g-2}$ when $k$ is a function field over a curve of genus $g$ with coefficients in the finite field $F_q$. The distribution $D$ is given by,

$$D(f) = \int_{C_k} f(w)\left(|w|^{1/2} + |w|^{-1/2}\right) d^*w \quad (64)$$

where the Haar measure $d^*w$ is normalized. The distributions $D_v$ are parametrized by the places $v$ of $k$ and are obtained as follows. For each $v$ one considers the natural proper homomorphism,

$$k_v^* \to C_k, \quad x \to \text{class of } (1,...,x,1...) \quad (65)$$

of the multiplicative group of the local field $k_v$ in the idele class group $C_k$. One then has,

$$D_v(f) = Pfw \int_{k_v^*} \frac{f(u)}{|1-u|} |u|^{1/2} d^*u \quad (66)$$

where the Haar measure $d^*u$ is normalized, and where the Weil Principal value $Pfw$ of the integral is obtained as follows, for a local field $K = k_v$,

$$Pfw \int_{k_v^*} 1_{R_v^*} \frac{1}{|1-u|} d^*u = 0, \quad (67)$$

if the local field $k_v$ is non Archimedean, and otherwise:

$$Pfw\int_{k_v^*}\varphi(u)d^*u = PF_0\int_{R_+^*}\psi(\nu)d^*\nu\,, \quad (68)$$

where $\psi(\nu)=\int_{|u|=\nu}\varphi(u)d_\nu u$ is obtained by integrating $\varphi$ over the fibers, while

$$PF_0\int\psi(\nu)d^*\nu = 2\log(2\pi)c+\lim_{t\to\infty}\left(\int\left(1-f_0^{2t}\right)\psi(\nu)d^*\nu-2c\log t\right), \quad (69)$$

where one assumes that $\psi - cf_1^{-1}$ is integrable on $R_+^*$, and $f_0(\nu)=\inf\left(\nu^{1/2},\nu^{-1/2}\right)\quad \forall\nu\in R_+^*$, $f_1=f_0^{-1}-f_0$. The Weil explicit formula is then,

**Theorem 4**.

*With the above notations one has* $S(\chi,F)=\Delta\left(F(|w|)\chi(w)\right)$.

Let $K$ be non Archimedean, furthermore, let $\alpha$ be a character of $K$ such that,

$$\alpha/R=1\,,\quad \alpha/\pi^{-1}R\neq 1\,. \quad (70)$$

Then, for the Fourier transform given by,

$$(Ff)(x)=\int f(y)\alpha(y)dy\,, \quad (71)$$

with $dy$ the selfdual Haar measure, one has

$$F(1_R)=1_R\,. \quad (72)$$

**Lemma 2**.

*With the above choice of* $\alpha$ *one has*

$$\int'\frac{h\left(u^{-1}\right)}{|1-u|}d^*u = Pfw\int\frac{h\left(u^{-1}\right)}{|1-u|}d^*u \quad (73)$$

*with the notations of theorem 1.*

By construction the two sides can only differ by a multiple of $h(1)$. Let us recall from theorem 1 that the left hand side is given by

$$\left\langle L,\frac{h\left(u^{-1}\right)}{|u|}\right\rangle, \quad (74)$$

where $L$ is the unique extension of $\rho^{-1}\dfrac{du}{|1-u|}$ whose Fourier transform vanishes at 1, $\hat{L}(1)=0$. Thus from (67) we just need to check that (74) vanishes for $h=1_{R^*}$, i.e. that

$$\left\langle L,1_{R^*}\right\rangle=0. \quad (75)$$

Equivalently, if we let $Y=\{y\in K;|y-1|=1\}$ we just need to show, using Parseval, that,

$$\left\langle \log|u|,\hat{1}_Y\right\rangle=0. \quad (76)$$

One has $\hat{1}_Y(x)=\int_Y\alpha(xy)dy=\alpha(x)\hat{1}_{R^*}(x)$, and $1_{R^*}=1_R-1_P$, $\hat{1}_{R^*}=1_R-|\pi|1_{\pi^{-1}R}$, thus, with $q^{-1}=|\pi|$,

$$\hat{1}_Y(x)=\alpha(x)\left(1_R-\frac{1}{q}1_{\pi^{-1}R}\right)(x). \quad (77)$$

We now need to compute $\int\log|x|\hat{1}_Y(x)dx=A+B$,

$$A=-\frac{1}{q}\int_{\pi^{-1}R^*}\alpha(x)(\log q)dx,\quad B=\left(1-\frac{1}{q}\right)\int_R\log|x|dx. \quad (78)$$

Let us show that $A+B=0$. One has $\int_R dx=1$, and

$$A=-\int_{R^*}\alpha(\pi^{-1}y)(\log q)dy=-\log q\left(\int_R\alpha(\pi^{-1}y)dy-\int_P dy\right)=\frac{1}{q}\log q, \quad (79)$$

since $\int_R\alpha(\pi^{-1}y)dy=0$ as $\alpha/\pi^{-1}R\neq 1$.

To compute $B$, note that $\int_{\pi^nR^*}dy=q^{-n}\left(1-\dfrac{1}{q}\right)$ so that

$$B=\left(1-\frac{1}{q}\right)\int_R\log|x|dx=\left(1-\frac{1}{q}\right)^2\sum_{n=0}^{\infty}(-n\log q)q^{-n}=-q^{-1}\log q=-\frac{1}{q}\log q, \quad (80)$$

and $A+B=0$.
Let us now treat the case of Archimedean fields. We take $K=R$ first, and we normalize the Fourier transform as,

$$(Ff)(x)=\int f(y)e^{-2\pi ixy}dy \quad (81)$$

so that the Haar measure $dx$ is selfdual.
With the notations of (68) one has,

$$Pfw\int_{R^*} f_0^3(|u|)\frac{|u|^{1/2}}{|1-u|}d^*u = \log\pi + \gamma \quad (82)$$

where $\gamma$ is Euler's constant, $\gamma = -\Gamma'(1)$. Indeed integrating over the fibers gives $f_0^4 \times (1-f_0^4)^{-1}$, and one gets,

$$PF_0\int_{R_+^*} f_0^4 \times (1-f_0^4)^{-1} d^*u = \left[\log(2\pi) + \lim_{t\to\infty}\left(\int_{R_+^*}(1-f_0^{2t})f_0^4(1-f_0^4)^{-1}d^*u - \log t\right)\right] = \log 2\pi + \gamma - \log 2\,. \quad (83)$$

Now let $\varphi(u) = -\log|u|$, it is a tempered distribution on $R$ and one has,

$$\left\langle \varphi, e^{-\pi u^2}\right\rangle = \frac{1}{2}\log\pi + \frac{\gamma}{2} + \log 2\,, \quad (84)$$

as one obtains from $\frac{\partial}{\partial s}\int |u|^{-s} e^{-\pi u^2} du = \frac{\partial}{\partial s}\left[\pi^{\frac{s-1}{2}}\Gamma\left(\frac{1-s}{2}\right)\right]$ evaluated at $s=0$, using $\frac{\Gamma'\left(\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2}\right)} = -\gamma - 2\log 2$. Thus by the Parseval formula one has,

$$\left\langle \hat{\varphi}, e^{-\pi x^2}\right\rangle = \frac{1}{2}\log\pi + \frac{\gamma}{2} + \log 2\,, \quad (85)$$

which gives, for any test function $f$,

$$\left\langle \hat{\varphi}, f\right\rangle = \lim_{\varepsilon\to 0}\left[\int_{|x|\geq\varepsilon} f(x)d^*x + (\log\varepsilon)f(0)\right] + \lambda f(0) \quad (86)$$

where $\lambda = \log(2\pi) + \gamma$. In order to get (86) one uses the equality,

$$\lim_{\varepsilon\to 0}\left[\int_{|x|\geq\varepsilon} f(x)d^*x + (\log\varepsilon)f(0)\right] = \lim_{\varepsilon\to 0}\left[\int f(x)|x|^{\varepsilon} d^*x - \frac{1}{\varepsilon}f(0)\right], \quad (87)$$

which holds since both sides vanish for $f(x) = 1$ if $|x| \leq 1$, $f(x) = 0$ otherwise. Thus from (86) one gets,

$$\int_R f(u)\frac{1}{|1-u|}d^*u = \lambda f(1) + \lim_{\varepsilon\to 0}\left[\int_{|1-u|\geq\varepsilon}\frac{f(u)}{|1-u|}d^*u + (\log\varepsilon)f(1)\right]. \quad (88)$$

Taking $f(u) = |u|^{1/2} f_0^3(|u|)$, the right hand side of (88) gives $\lambda - \log 2 = \log\pi + \gamma$, thus we conclude using (82) that for any test function $f$,

$$\int_R^{'} f(u)\frac{1}{|1-u|}d^*u = Pfw\int_R f(u)\frac{1}{|1-u|}d^*u\,. \quad (89)$$

Let us finally consider the case $K = C$. We choose the basic character $\alpha$ as

$$\alpha(z) = \exp 2\pi i(z+\bar{z}), \quad (90)$$

the selfdual Haar measure is $dzd\bar{z} = |dz \wedge d\bar{z}|$, and the function $f(z) = \exp -2\pi|z|^2$ is selfdual. The normalized multiplicative Haar measure is

$$d^*z = \frac{|dz \wedge d\bar{z}|}{2\pi|z|^2}. \quad (91)$$

Let us compute the Fourier transform of the distribution

$$\varphi(z) = -\log|z|_C = -2\log|z|\,. \quad (92)$$

One has

$$\left\langle \varphi, \exp -2\pi|z|^2 \right\rangle = \log 2\pi + \gamma, \quad (93)$$

as is seen using $\frac{\partial}{\partial\varepsilon}\left(\int e^{-2\pi|z|^2}|z|^{-2\varepsilon}|dz \wedge d\bar{z}|\right) = \frac{\partial}{\partial\varepsilon}\left[(2\pi)^{\varepsilon}\Gamma(1-\varepsilon)\right]$.

Thus $\left\langle \hat{\varphi}, \exp -2\pi|u|^2 \right\rangle = \log 2\pi + \gamma$ and one gets,

$$\left\langle \hat{\varphi}, f \right\rangle = \lim_{\varepsilon\to 0}\left[\int_{|u|_C \geq \varepsilon} f(u)d^*u + \log\varepsilon f(0)\right] + \lambda' f(0) \quad (94)$$

where $\lambda' = 2(\log 2\pi + \gamma)$.

To see this one uses the analogue of (87) for $K = C$, to compute the right hand side of (94) for $f(z) = \exp -2\pi|z|^2$. Thus, for any test function $f$, one has,

$$\int_C^{'} f(u)\frac{1}{|1-u|_C}d^*u = \lambda' f(1) + \lim_{\varepsilon\to 0}\left[\int_{|1-u|_C \geq \varepsilon}\frac{f(u)}{|1-u|_C}d^*u + (\log\varepsilon)f(1)\right]. \quad (95)$$

Let us compare it with $Pfw$. When one integrates over the fibers of $C^* \xrightarrow{|\ |_C} R_+^*$ the function $|1-z|_C^{-1}$ one gets,

$$\frac{1}{2\pi}\int_0^{2\pi}\frac{1}{|1-e^{i\theta}z|^2}d\theta = \frac{1}{1-|z|^2} \text{ if } |z|<1, \text{ and } \frac{1}{|z|^2-1} \text{ if } |z|>1. \quad (96)$$

Thus for any test function $f$ on $R_+^*$ one has by (68)

$$Pfw\int f\left(|u|_C\right)\frac{1}{|1-u|_C}d^*u = PF_0\int f(v)\frac{1}{|1-v|}d^*v \quad (97)$$

with the notations of (69). With $f_2(v)=v^{\frac{1}{2}}f_0(v)$ we thus get, using (69),

$$Pfw\int f_2\left(|u|_C\right)\frac{1}{|1-u|_C}d^*u = PF_0\int f_0 f_1^{-1}d^*v = 2(\log 2\pi+\gamma). \quad (98)$$

We shall now show that,

$$\lim_{\varepsilon\to 0}\left[\int_{|1-u|_C\geq\varepsilon}\frac{f_2\left(|u|_C\right)}{|1-u|_C}d^*u+\log\varepsilon\right]=0, \quad (99)$$

it will then follow that, using (95),

$$\int_C' f(u)\frac{1}{|1-u|_C}d^*u = Pfw\int f(u)\frac{1}{|1-u|_C}d^*u. \quad (100)$$

To prove (99) it is enough to investigate the integral,

$$\int_{|z|\leq 1,|1-z|\geq\varepsilon}\left[(1-z)(1-\bar{z})\right]^{-1}|dz\wedge d\bar{z}| = j(\varepsilon) \quad (101)$$

and show that $j(\varepsilon)=\alpha\log\varepsilon+o(1)$ for $\varepsilon\to 0$. A similar statement then holds for

$$\int_{|z|\leq 1,|1-z^{-1}|\geq\varepsilon}\left[(1-z)(1-\bar{z})\right]^{-1}|dz\wedge d\bar{z}|.$$

One has $j(\varepsilon)=\int_D|dZ\wedge d\bar{Z}|$, where $Z=\log(1-z)$ and the domain $D$ is contained in the rectangle,

$$\left\{Z=(x+iy);\log\varepsilon\leq x\leq\log 2,-\frac{\pi}{2}\leq y\leq\pi/2\right\}=R_\varepsilon \quad (102)$$

and bounded by the curve $x=\log(2\cos y)$ which comes from the equation of the circle $|z|=1$ in polar coordinates centred at $z=1$. One thus gets,

$$j(\varepsilon)=4\int_{\log\varepsilon}^{\log 2}Arc\cos\left(e^x/2\right)dx, \quad (103)$$

when $\varepsilon\to 0$ one has $j(\varepsilon)\approx 2\pi\log(1/\varepsilon)$, which is the area of the following rectangle (in the measure $|dz\wedge d\bar{z}|$),

$$\{Z=(x+iy);\log\varepsilon\leq x\leq 0,-\pi/2\leq y\leq\pi/2\}. \quad (104)$$

One has $|R_\varepsilon|-2\pi\log 2=2\pi\log(1/\varepsilon)$. When $\varepsilon\to 0$ the area of $R_\varepsilon\setminus D$ converges to

$$4\int_{-\infty}^{\log 2} Arc\sin\left(e^x/2\right)dx = -4\int_0^{\pi/2}\log(\sin u)du = 2\pi\log 2\,, \quad (105)$$

so that $j(\varepsilon) = 2\pi\log(1/\varepsilon) + o(1)$ when $\varepsilon \to 0$.

Thus we can assert that with the above choice of basic characters for local fields one has, for any test function $f$,

$$\int_K^{\cdot} f(u)\frac{1}{|1-u|}d^*u = Pfw\int f(u)\frac{1}{|1-u|}d^*u\,. \quad (106)$$

Now, we have the following

**Lemma 3**.

*Let $K$ be a local field, $\alpha_0$ a normalized character as above and $\alpha$, $\alpha(x) = \alpha_0(\lambda x)$ an arbitrary character of $K$.*

Hence, we obtain that:

$$\int_K^{\cdot} f(u)\frac{1}{|1-u|}d^*u = \log|\lambda| f(1) + Pfw\int f(u)\frac{1}{|1-u|}d^*u\,. \quad (107)$$