

Introduction to Vatsal's theorem on non vanishing L-functions.

Nicolas Templier

July 8, 2007

The organisers asked me to explain V.Vatsal's theorem since it is a beautiful application of Ratner's equidistribution theorem.

- ▶ Part I. Generalities.
- ▶ Part II. Proofs.
- ▶ Part III. How to catch the derivative?
- ▶ Part IV. What is a Landau-Siegel zero?

Thanks to Rodolphe Richard for enlighting discussions.

Main Theme.

Part I

Description of the setting.

Arithmetic data \rightsquigarrow Combinatorial data.

Asymptotic behaviour \rightsquigarrow Dynamics.

Data.

We give ourselves the following arithmetic data:

- ▶ A positive integer N . A modular newform f of level N and weight 2. One may view it as a holomorphic 1-form on the modular surface $\Gamma_0(N)\backslash\mathfrak{H}$.
- ▶ A fundamental negative discriminant $D \equiv 1 \pmod{4}$. The associated quadratic field $K = \mathbb{Q}(\sqrt{D})$. χ an anticyclotomic Größencharacter of K .

Langlands.

Huge machinery to create sequences of numbers (a_n) whose generating functions $\sum_{n \geq 1} \frac{a_n}{n^s}$ - that are denoted $L(s, \pi)$ - have

- ▶ nice properties: meromorphic continuation, finite number of poles, functional equation,
- ▶ deep properties: zero-free regions, Weyl's law, subconvex bounds, special values,
- ▶ desperately expected properties: GRH, GRP.

The good object π appears to be a so called *automorphic representation* of $G(\mathbb{A})$ in $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}))$, where G is a reductive group over \mathbb{Q} .

L-functions.

One can construct the L-function $L(s, f \times \chi)$. It is of degree 4. The completed L-function has a functional equation relating the values at s and $1 - s$ by an epsilon factor,

$$\Lambda(s, f \times \chi) = \epsilon(s, f \times \chi) \Lambda(1 - s, f \times \chi).$$

Rough idea of the construction:

f lives on GL_2/\mathbb{Q} .

χ lives on GL_1/K , and its associated theta series lives on GL_2/\mathbb{Q} .

The Rankin-Selberg convolution $f \times \chi$ lives on GL_4/\mathbb{Q} .

In our situation, the *root number* is given by the Kronecker symbol,

$$\epsilon\left(\frac{1}{2}, f \times \chi\right) = -\left(\frac{D}{N}\right) = \pm 1.$$

Problematic.

The order of vanishing at the critical point is expected to have deep arithmetic interpretation.

«An arithmetic property should be generically satisfied unless there is an obvious obstruction.»

From now on we place ourselves in the case

$$\epsilon\left(\frac{1}{2}, f \times \chi\right) = +1,$$

and then there is no particular reason for $L(\frac{1}{2}, f \times \chi)$ to vanish, and the conjecture is that it 'often' does not vanish. One needs to specify sets of choices $\{(f, \chi)\}$ for the data, and make explicit what is meant by 'often'.

remark: Another problem is worth mentioning. It is to exhibit an L-function that does vanish. For example the following is not yet proven:

There is an elliptic curve E/\mathbb{Q} whose L-function vanishes to order ≥ 4 at the critical point.

We consider two interesting choices.

In both cases, $f \in S_2(N)$ is fixed while the Grössencharacter χ will vary.

1. We consider the unramified χ 's. In other words χ is a character of the class group \mathbf{Cl}_D . Hence, for each D there are h_D such characters.

We want to estimate the number of nonvanishing twists when D tends to $-\infty$. Recall the size of the class group (Siegel's bound)

$$|D|^{\frac{1}{2}-\epsilon} \ll_{\epsilon} h_D \ll |D|^{\frac{1}{2}} \log |D|.$$

2. We fix the fundamental discriminant D and an auxiliary prime p . And we consider anticyclotomic Grössencharacters χ of conductor p^n . For each n , there are roughly $h_D p^n$ such characters.

We want to estimate the number of nonvanishing twists as n grows to infinity.

V. Vatsal's theorem

Theorem

If n is large enough, the critical values $L(\frac{1}{2}, f \times \chi)$ are nonzero for all anticyclotomic Grössencharacters of conductor p^n .

In other words, given the numbers (N, D, p) , only a finite number of $L(\frac{1}{2}, f \times \chi)$ do vanish.

Advertisement.

P. Michel, A. Venkatesh and myself have studied the first case and obtained partial results. The methods rely on Duke's equidistribution theorem and the tools are in the same flavour as those seen in Harcos' lectures.

With the current technology we can only reach a nonvanishing for $|D|^{\delta}$ class group characters, which is weak compared to other theorems on nonvanishing of lower degree L-functions. 'Usually' a positive proportion of nonvanishing twists is achieved by *mollifying* the family.

Asumptions.

The data $(f \in S_2(N), D, p)$ satisfy:

- ▶ $(N, D) = 1$.
- ▶ $(p, ND) = 1$.
- ▶ $(\frac{D}{N}) = -1$.

Furthermore, we assume the following to simplify the exposition:

- ▶ $p \nmid h_D$.
- ▶ $D \equiv 1 \pmod{4}$ and $|D|$ is prime.
- ▶ N is the product of an odd number of inert primes.
- ▶ $N \equiv 1 \pmod{12}$.
- ▶ $(\frac{D}{p}) = -1$.

Gross-Zagier formula.

- ▶ J-L. Walspurger prop.7 p.222 + local computations that no one ever did!
- ▶ B. Gross and D. Zagier by an explicit computation. Generalized by S-W. Zhang.
- ▶ K. Martin and D. Whitehouse using Jacquet's trace formula.

We have already seen the formula when f was a Maass form in Harcos' lecture and the period here has the same shape.

Theorem

$$L\left(\frac{1}{2}, f \times \chi\right) = \frac{c}{|D|^{\frac{1}{2}} \cdot p^n} \left| \sum_{\sigma \in G_n} \chi(\sigma) \psi(z^\sigma) \right|^2.$$

c is a constant - which is roughly $\frac{(f, f)}{(\psi, \psi)}$.

I'll explain what the ψ , G_n , z are in the next slides.

Heegner points.

Definition

A Heegner point $z = (f, R)$ of discriminant D is a B^\times -conjugacy class of ring embeddings $f : \mathcal{O}_K \rightarrow R$, where R is a maximal order of B . $f^{-1}(R)$ is an order \mathcal{O}_{Dc^2} in K whose level c is the level of z .

The Heegner points of discriminant D and level 1 on GL_2 are the ones we have seen in Harcos' lecture.

By forgetting the map f , we can associate to a Heegner point a conjugacy class of maximal orders. We write $\psi(z)$ for $\psi(R)$ when $z = (f, R)$.

The set of Heegner points of discriminant D and level p^n is acted upon freely and transitively by the group G_n . Hence after choosing such a point z , $\{z^\sigma\}_{\sigma \in G_n}$ is the set of Heegner points of level p^n .

Note that the period in the Gross-Zagier formula does not depend on this choice.

Eichler-Jacquet-Langlands correspondence.

Let B denote the quaternion algebra over \mathbb{Q} ramified at ∞ and at the primes dividing N . In terms of algebraic groups defined over \mathbb{Q} , B^\times is a compact inner form of GL_2 . Let's fix R_0 a maximal order of B .

The double coset

$$\mathcal{G} := B^\times \backslash \widehat{B}^\times / \widehat{R}_0^\times,$$

is finite and represents the set of conjugacy class of maximal orders in B .

To give $f \in S_2(N)$ is equivalent to give a function

$$\psi : \mathcal{G} \rightarrow \mathbb{R}.$$

Furthermore the fact that f is a cusp form translates into

$$\sum_{v \in \mathcal{G}} \psi(v) = 0.$$

One 'accident' explains why one can reach so strong a theorem. *If two characters are conjugate under $\text{Aut}(\mathbb{C})$, then the algebraic part of the L-values are also conjugate.*

Because of this new symmetry if one nonvanishing forces the nonvanishing of all the other conjugates.

With our assumptions, the set of characters of level p^n whose restriction to G_1 , $\chi|_{G_1}$ is a fixed character χ_1 , are all conjugate under $\text{Aut}(\mathbb{C})$. We'll actually check that the sum is non-zero.

$$\mathcal{N} := \sum_{\substack{\chi \text{ of level } p^n, \\ \chi|_{G_1} = \chi_1}} L\left(\frac{1}{2}, f \times \chi\right).$$

remark: The orbits of $\text{Aut}(\mathbb{C})$ are very large. Indeed there are less than $h_D(p+1)$ orbits in G_n which is of size $h_D(p+1)p^{n-1}$. On the other hand, the characters of $\text{Cl}_D \subset G_1$ need not be conjugate - this relies on the structure of the class group which is fairly unknown. This explains why we only reach $|D|^\delta$ nonvanishing of class group characters in our setting 1.

Observation.

$$\mathcal{M} := \sum_{\substack{\chi \text{ of level } \leq p^n, \\ \chi|_{G_1} = \chi_1}} (*) L\left(\frac{1}{2}, f \times \chi\right).$$

In preparing this talk, I found that one could simplify some technical computations in V.Vatsal Inventiones' paper with the following

Proposition

If \mathcal{M} has a limit as n tends to infinity, then \mathcal{N} does also and we have:

$$\lim_{n \rightarrow \infty} \mathcal{N} = \frac{(p-1)(p+1)}{p^2} \cdot \left[1 - \left(\frac{a_p}{p+1}\right)^2\right] \cdot \lim_{n \rightarrow \infty} \mathcal{M}.$$

Recall that the p^{th} -Fourier coefficient satisfies $|a_p| < p+1$ - a kind of *spectral gap* - and for modular forms we have Ramanujan's bound $|a_p| \leq 2\sqrt{p}$ which is stronger.

The proof of the proposition follows the computations p.19, but rearranging the terms in a better way.

Iwasawa's anticyclotomic setting.

$$\mathcal{O}_D = \mathbb{Z} + \frac{1 + \sqrt{D}}{2} \mathbb{Z} = \left\{ \frac{a + b\sqrt{D}}{2}, a \equiv b \pmod{2} \right\}$$

is the ring of integers or the unique maximal order of K , while

$$\mathcal{O}_{Dp^{2n}} = \left\{ \frac{a + bp^n\sqrt{D}}{2}, a \equiv b \pmod{2} \right\}$$

is the order of level p^n .

$$G_n = \text{Pic}(\mathcal{O}_{Dp^{2n}}) = K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}_{Dp^{2n}}}^\times = \text{Gal}(H_n/K).$$

One has $G_0 = \text{Cl}_D$ and $|G_n| = h_D(p+1)p^{n-1}$. Recall that χ is an anticyclotomic Grössencharacter of $\mathbb{Q}(\sqrt{D})$ of level p^n . We can now explain what that means:

χ is a character of G_n that does not factor through G_{n-1} .

By the Gross-Zagier formula, our partial average takes the form:

$$\begin{aligned} \mathcal{M} &\doteq \sum_{\substack{\chi : G_n \rightarrow S^1, \\ \chi|_{G_1} = \chi_1}} \left| \sum_{\sigma \in G_n} \chi(\sigma) \psi(z^\sigma) \right|^2 = \\ &= \sum_{\tau \in G_1} \chi_1(\tau) \sum_{\sigma \in G_n} \psi(z^{\sigma\tau}) \psi(z^\sigma) \doteq \sum_{\tau} \chi_1(\tau) \mathcal{M}_\tau. \end{aligned}$$

Proposition

(i) If $\tau = 1$, (resp. Frob_D) belongs to Gauss' genus group, then

$$\mathcal{M}_\tau \rightarrow 1 \quad (\text{resp. } \frac{a_D}{D+1}),$$

(ii) and if not,

$$\mathcal{M}_\tau \rightarrow 0,$$

where all the limits are taken as n grows to infinity.

This implies that \mathcal{M} has a positive limit using again the spectral bound $|a_D| < D+1$ and this implies Vatsal's theorem, as discussed before - this dichotomy between diagonal - $\tau = 1$ - and non diagonal terms - $\tau \neq 1$ - is very common in Analytic Number Theory.

More about galois groups.

$$G_0 = \text{Cl}_D.$$

$$G_n = G_1 \times \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

- ▶ $\text{Cl}_D = G_0 = \text{Gal}(H_K/K)$, where H_K is the Hilbert class field.
- ▶ G_1 has size $h_D(p+1)$. It is the torsion subgroup of G in our case.
- ▶ $G_n = \text{Pic}(\mathcal{O}_{Dp^{2n}})$. $G_n \simeq G_1 \times \mathbb{Z}/p^{n-1}\mathbb{Z}$.
- ▶ I_n is the inertia group. It acts on Heegner points by 'rotation'.
- ▶ $G = \varinjlim G_n \simeq G_1 \times \mathbb{Z}_p$.

$H_\infty^{G_1}$ is called the *anticyclotomic \mathbb{Z}_p -extension* of K .

Class Field Theory provides a complete description of abelian extension of number fields.

p -Unfolding.

For the moment we have not taken into account enough the given prime p . We now focus on this aspect.

Strong approximation shows that

$$\mathcal{G} = B^\times \backslash \widehat{B}^\times / \widehat{R}_0^\times = \Gamma \backslash PGL_2(\mathbb{Q}_p) / PGL_2(\mathbb{Z}_p),$$

where $\Gamma = (R \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{p}])^\times$ is a lattice in $PGL_2(\mathbb{Q}_p)$.

The symmetric space $\mathcal{T} = PGL_2(\mathbb{Q}_p) / PGL_2(\mathbb{Z}_p)$ is the Bruhat-Tits tree. It is the infinite $p + 1$ -regular tree. In this way, the set \mathcal{G} inherits the structure of a finite graph.

We have already seen this kind of construction when Elon was considering

$$PGL_2(\mathbb{Z}[\frac{1}{p}]) \backslash PGL_2(\mathbb{R}) \times PGL_2(\mathbb{Q}_p) / PGL_2(\mathbb{Z}_p) \simeq PGL_2(\mathbb{Z}) \backslash PGL_2(\mathbb{R}).$$

He projected everything on the real place. In our case, the group is compact and the real place is not interesting and we instead project to the place at p .

Expanders.

They are heavily used in applied mathematics (networks). The problem of their existence and explicit construction is a very interesting one. Its solution intricates group theoretic and arithmetic methods.

- ▶ They are shown to exist by a counting argument.
- ▶ First explicitly constructed by G. Margulis using Kazhdan's (T) property of semisimple groups of rank ≥ 2 .
- ▶ Ramanujan's graphs constructed before.
- ▶ Recently more combinatoric constructions have been provided by Reingold-Vadhan-Widgerson or by Bourgain-Gamburg-Sarnak.

□ A.Lubotzky *Discrete groups, expanding graphs and invariant measures*.

Aside.

The adjacency matrix of a k -regular graph \mathcal{G} , is the matrix indexed by the vertices whose entries are given by the edges. It is symmetric. All its eigenvalues are in $[-k, k]$. The eigenvalue k exists and is simple iff the graph is connected. The eigenvalue $-k$ exists iff the graph is bi-partite. *It has to be thought as the Laplacian or the Hecke operator.*

Definition

A k -regular graph is called *Ramanujan* iff the non-trivial eigenvalues λ of its adjacency matrix satisfy $|\lambda| \leq 2\sqrt{k-1}$.

Definition

Let $\delta > 0$ and k be fixed. A family of (δ, k) -*expander graphs* is an infinite family of k -regular graphs whose non-trivial eigenvalues λ satisfy $|\lambda| \leq k - \delta$.

Any infinite family of Ramanujan graphs is expanding.

They were called *Ramanujan* because this spectral bound is deduced from the Ramanujan conjecture for the Fourier coefficients of modular forms of arbitrary integral weight, proven by P. Deligne. The condition $|\lambda| \leq 2\sqrt{k-1}$ is best possible. (J. Friedman)

To avoid loops, multi-edges and non-free actions, one can replace Γ by a congruence sublattice. This is what V. Vatsal did - there is some confusion in Vatsal's paper at this point, but if one takes the integer M very large, everything is fine.

Note also that in our case the lattice Γ does act freely because of our assumption $N \equiv 1 \pmod{12}$. That's why we do not have any weights w_R corresponding to the order of the stabilizer in the Gross-Zagier formula.

Let's recall two theorems of Ihara (see e.g. [Serre, Trees])

- ▶ A group acts freely on a tree iff it is free.
- ▶ A lattice in $PGL_2(\mathbb{Q}_p)$ is cocompact.

Normal forms.

We do the same construction for the Heegner points by 'unfolding the Gross curve', a construction due to Bertolini-Darmon and Vatsal. In a certain sense, one can view Heegner points as vertices of the Bruhat-Tits tree. We do not get into the details but shall describe the situation in the next slide.

$$\begin{array}{c} \mathcal{T} \\ \cup \\ G_n \circlearrowleft \text{Heegner} \end{array}$$

The 'galois' action cannot be lifted to the whole symmetric space. However one can do it partially. It is a very key point.

«Ergodic methods can be applied efficiently if and only if the galois action 'extends' or 'looks like' a geometric action on the whole space.»

I guess A. Venkatesh will elaborate on this point next week.

Summary.

We are left with the following objects

- ▶ A finite graph covered by a $p + 1$ -regular tree,
 $\mathcal{T} \rightarrow \mathcal{G} = \Gamma \backslash \mathcal{T}$.
- ▶ A 'modular form' $\psi : \mathcal{G} \rightarrow \mathbb{R}$. $T_p \psi = \Delta \psi = a_p \psi$.
- ▶ A vertex 0 and a point z at distance n . The points $\{z^\sigma\}_{\sigma \in I_n}$ are all the vertices at distance n from 0.
- ▶ Elements $g_\tau \in PGL_2(\mathbb{Q}_p)$, $\tau \in G_1$ that act on the tree.

We need to evaluate, for each $\tau \in G_1$, the expression

$$\mathcal{M}_\tau \doteq \sum_{\sigma \in I_n} \psi(z^\sigma) \psi(g_\tau \cdot z^\sigma),$$

as n grows to infinity.

Γ and $g_\tau \Gamma g_\tau^{-1}$ are commensurable iff $\tau = 1$ or $\text{Frob}(D)$.

We fix a Heegner point z of conductor p^n .

$$G_n = I_n \cdot G_1.$$

We write an element of G_n as $\sigma\tau$, $\tau \in G_1$, $\sigma \in I_n$. This is not unique and introduces some redundancy, but it doesn't matter since $G_1 \cap I_n$ has fix cardinality.

- ▶ We view I_n acting by rotation on z around a fixed vertex 0.
- ▶ For each $\tau \in G_1$, we can pick a good element $g_\tau \in PGL_2(\mathbb{Q}_p)$ such that the Heegner point $z^{\sigma\tau}$ is then represented by $g_\tau \cdot z^\sigma$, for any $\sigma \in I_n$.

Part II

Proofs. (given on the blackboard)

Diagonal terms.

To prove the first assertion of the proposition, when $\tau = 1$, one needs to prove the following

Claim 1: The Heegner points $\{z^\sigma\}_{\sigma \in I_n}$ equidistributes on \mathcal{G} as n tends to infinity.

Proof. One interprets these Heegner points as the endpoints of nonbacktracking path of length n from the origin. Then the claim follows from properties of the adjacency matrix $A(\mathcal{G})$, which uses only the fact that the regular graph \mathcal{G} is connected and not bipartite.

The analysis when $\tau = \text{Frob}_D$ is the same and we now turn to the remaining cases where $\tau \neq 1, \text{Frob}_D$ so that Γ and $g_\tau \Gamma g_\tau^{-1}$ are not commensurable.

Long circles.

This last integral is reminiscent to others seen in different lectures (Eskin's convention is G/Γ while ours is $\Gamma \backslash G$.)

- ▶ In Eskin's talk about quantitative Oppenheim (prop. 7.12 p.50),

$$\int_K \tilde{f}(a_t k \Delta_Q) dk,$$

- ▶ about moduli space of translation surfaces (eq. (110) p.81),

$$\int_0^{2\pi} \hat{f}(g_t r_\theta S) d\theta,$$

- ▶ in Marklof's talk, ($E(x)$ vary in a compact group while Φ^t is the action of a diagonal matrix),

$$\int_\Omega f((1, \alpha)(M, O)(E(x), 0)\Phi^t) d\lambda(x).$$

Non-diagonal terms.

Claim 2: The Heegner points $\{(z^\sigma, g_\tau \cdot z^\sigma)\}_{\sigma \in I_n}$ equidistributes on $\mathcal{G} \times \mathcal{G}$ as n tends to infinity.

Proof. Let's introduce the lattice $\Gamma' := \Gamma \times g_\tau \Gamma g_\tau^{-1}$ in $G = PGL_2(\mathbb{Q}_p) \times PGL_2(\mathbb{Q}_p)$ and the homogeneous space $\Gamma' \backslash G$. We'll make use later of the action of the following 1-parameter unipotent subgroup,

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, x \in \mathbb{Q}_p \right\} \subset PSL_2(\mathbb{Q}_p) \subset PSL_2(\mathbb{Q}_p) \times PSL_2(\mathbb{Q}_p) \subset G,$$

where the middle inclusion of $PSL_2(\mathbb{Q}_p)$ is the diagonal one. We also introduce the compact group $PGL_2(\mathbb{Z}_p)$ that we also include diagonally in G and note for the moment that our main quantity may be expressed as

$$\mathcal{M}_\tau \doteq \int_{PGL_2(\mathbb{Z}_p)} (\psi \times \psi) \left(k \cdot \begin{pmatrix} p^n & 0 \\ 0 & 1 \end{pmatrix} \right) dk.$$

Unipotent flow.

The proof that it converges to $\int_{\Gamma' \backslash G} \psi \times \psi d\text{Haar}$ is the same: the long circle are well approximate by horocycles to which we apply Ratner. However our case is much simpler since our p-adic homogeneous space is compact, and no extra analysis of integrability nor use of Dani-Margulis theorem is needed.

To be precise, our claim 2 is a consequence of the following which is a consequence of Ratner's measure classification and equidistribution theorems.

Claim 3: For almost every $k \in PGL_2(\mathbb{Z}_p)$,

$\{k \cdot \begin{pmatrix} 1 & p^{-n} \cdot u \\ 0 & 1 \end{pmatrix}\}_{u \in \mathbb{Z}_p^\times}$ equidistributes on $\Gamma' \backslash G$.

Proof. The main point is to exclude periodic orbits under the diagonal embedded $PSL_2(\mathbb{Q}_p)$, which is achieved by showing that for almost every k , the conjugate $k\Gamma'k^{-1} \cap PSL_2(\mathbb{Q}_p)$ is not a lattice in $PSL_2(\mathbb{Q}_p)$.

Part III

$\epsilon = -1$. The special derivative $L'(\frac{1}{2}, f \times \chi)$.

Two proofs are available by C. Cornut and V. Vatsal. We'll present the quickest one that relies on the previous theorem on special values. ([Vatsal, Duke. Math. Journ.]).

I shall present briefly the steps of this rather indirect proof in order to show how tricky it is to catch the derivative.

Theorem (V. Vatsal and C. Cornut ; Mazur conjecture)

Let (N, D, p) with $\epsilon = -(\frac{N}{D}) = -1$ be given.

Then the critical derivatives $L'(\frac{1}{2}, f \times \chi)$ are non-zero for all but a finite number of anticyclotomic Größencharacters χ on $\mathbb{Q}(\sqrt{D})$ of level a power of p .

Step 1.

A Gross-Zagier formula relates the critical derivative to the canonical Néron-Tate height of a Heegner point on the modular curve viewed as an algebraic curve over \mathbb{Q} .

The derivative vanishes \Leftrightarrow the height vanishes \Leftrightarrow the Heegner point is torsion as divisor class.

Hence we need to prove that the Heegner point is not torsion.

Step 2.

We take a suitably chosen auxiliary large prime ℓ .

To check that the Heegner point is not torsion, it is enough to prove that it is not torsion $(\text{mod } \ell)$.

Step 3.

We choose another auxiliary prime q . We also choose a modular form g of level Nq that is congruent to $f \pmod{\ell}$. The theory of p -adic modular forms proves that many such examples indeed exist. (see e.g. [Serre])

For the modular form, the sign of the functional equation is $+1$ as in part I and we can look at the algebraic part of the special value. Then V. Vatsal proved *Jochnowitz congruences* in this setting: the Heegner point $\pmod{\ell}$ is 'related' to this special value $\pmod{\ell}$.

Part IV

$D \rightarrow -\infty$. [Laudau-Siegel zero.](#)

Step 4.

One needs to prove that the special value is a ℓ -adic unit for almost all characters. To achieve this, V. Vatsal redoes all the proof of part I, but taking the p -adic L-function instead of the classical one.

One main difficulty in dealing with the family of class group characters is that we do not know precisely the size of the class number h_D .

One can reverse the logic and say that if we gather enough informations about L-functions, we might be able to say something about the size of h_D .

This is what H. Iwaniec and P. Sarnak did ([*Isr. Jour. of Math.*, 2000]). Motivated by this goal, they invented a large number of new methods that are now standard in solving subconvexity and nonvanishing problems.

Theorem

- (i) (Dirichlet) For any Dirichlet character χ , $L(1, \chi) \neq 0$.
- (ii) (Landau) There exists a constant c - effectively computable - such that for any positive integer q , the L-functions $L(s, \chi)$ for χ a Dirichlet character of conductor q have no zero in the region

$$\sigma > 1 - \frac{c}{\log(q(|T| + 1))}, \quad s = \sigma + iT,$$

except perhaps for the real (=quadratic) character. If it happens, the zero is real and simple.

- (iii) (Siegel) For any $\epsilon > 0$ there exists a constant c_ϵ - not effectively computable when $\epsilon < \frac{1}{2}$ - such that the quadratic Dirichlet L-functions $L(s, (\frac{D}{\cdot}))$ have no zero on the interval

$$s > 1 - c_\epsilon \cdot |D|^{-\epsilon}, \quad s \in \mathbb{R}.$$

A Landau-Siegel zero is a potential zero of an L-function that lies in Landau's region $s > 1 - \frac{c}{\log q}$. It is however bounded away from 1 by Siegel's bound $s < 1 - c_\epsilon \cdot q^{-\epsilon}$.