Symmetries in Algebra and Number Theory
(I. KERSTEN, R. MEYER eds.), p. 11–26
Georg-August Universität Göttingen, 2008

L-FUNCTIONS, AUTOMORPHIC FORMS, AND ARITHMETIC

Valentin Blomer

Department of Mathematics, University of Toronto
E-mail : `vblomer@math.toronto.edu`

Gergely Harcos

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences
E-mail : `gharcos@renyi.hu`

***Abstract*.** We give a short, informal survey on the role of automorphic L-functions in number theory. We present the strongest currently known subconvexity bounds for twisted L-functions over number fields due to the authors and give various arithmetic applications. This is based on a talk of the first author.

1. L-functions

Suppose you are given an interesting sequence $a(n)$, $n \in \mathbb{N}$, of complex numbers that you would like to investigate. The method of analytic number theory is to encode this sequence in a generating function. There are several choices, and if some multiplicativity is involved, one might consider the Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}. \tag{1}$$

If we assume $a(n) \ll_\varepsilon n^\varepsilon$ for all $\varepsilon > 0$, or even only an average bound $\sum_{n\le x} |a(n)| \ll_\varepsilon x^{1+\varepsilon}$, then (1) converges absolutely and uniformly on compacta in $\Re s > 1$, and thus defines a holomorphic function. We can hope that in this way we translate the arithmetic of the sequence $a(n)$ into analytic properties of the function $L(s)$, and

2000 ***Mathematics Subject Classification*.** Primary: 11-02, Secondary: 11F66, 11E25.

The first author was supported by an NSERC grant and the second author was supported by European Community grant MEIF-CT-2006-040371 under the Sixth Framework Programme and by OTKA grants K 72731 and PD 75126.

indeed there is very often a remarkable interplay between arithmetic and analysis. Let us look at a few examples (see also [**21, 27, 32**]):

1) Let $a(n) = 1$ for all n. While it is debatable if this is an interesting sequence, it gives no doubt an interesting object: the Riemann ζ-function

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \qquad \Re s > 1.$$

The Euler product shows that $\zeta(s) \neq 0$ in $\Re s > 1$, and it is a classical fact that the non-vanishing of ζ on the line $\Re s = 1$ is equivalent[(1)] to the prime number theorem

$$\pi(x) := \#\{p \leq x \mid p \text{ prime}\} \sim \frac{x}{\log x}, \qquad x \to \infty.$$

The ζ-function can be extended meromorphically to all of $\mathbb{C}$, and one has more precisely an equivalence[(2)]

$$\begin{aligned} &\zeta(s) \neq 0 \text{ in } \Re s > 1 - \delta \text{ for some } 0 < \delta \leq 1/2 \\ \Longleftrightarrow\ &\pi(x) = \int_2^x \frac{dt}{\log t} + O(x^{1-\delta+\varepsilon}) \text{ for some } 0 < \delta \leq 1/2 \text{ and all } \varepsilon > 0. \end{aligned}$$

This shows a very precise translation of an arithmetic statement (distribution of prime numbers) into an analytic statement (location of zeros).

2) Let $K/\mathbb{Q}$ be a number field and let $a(n) := \#\{\text{integral ideals } \mathfrak{a} \mid \mathcal{N}\mathfrak{a} = n\}$. This gives the Dedekind ζ-function

$$\zeta_K(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \sum_{\mathfrak{a}} \frac{1}{(\mathcal{N}\mathfrak{a})^s},$$

which has a simple pole at $s = 1$. The analytic class number formula states

$$\operatorname*{res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} Rh}{w\sqrt{|D|}},$$

where as usual r_1, r_2 are the number of real resp. pairs of complex embeddings of K into $\mathbb{C}$, R is the regulator, h is the class number, w is the number of roots of unity in K and D is the discriminant. In other words, we find all algebraic invariants of K in the Laurent expansion of ζ_K at $s = 1$.

[(1)] Of course, since both statements are true, they are in particular equivalent. But even without knowing the truth of either of these statements one can deduce one from the other.

[(2)] Here it is unknown if either of these statement holds for some $\delta > 0$.

3) Let χ be a primitive Dirichlet character to some large modulus q. This gives rise to a Dirichlet L-function

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

which again can be continued to an entire function. In practice, one often encounters character sums of the type $\sum_{n\leq x}\chi(n)$, and one would expect that there is a lot of cancellation in such a sum. For example, for $x=q$ one even has $\sum_{n\leq q}\chi(n)=0$. Cancellation becomes a very delicate matter if the sum is short, i.e. if x is small compared to q. The Lindelöf hypothesis for $L(s,\chi)$ states that $L(1/2+it,\chi)\ll_\varepsilon ((1+|t|)q)^\varepsilon$ for all $\varepsilon>0$. This is not known, but it would imply

$$\sum_{n\leq x}\chi(n)\ll_\varepsilon x^{1/2+\varepsilon}$$

for all $\varepsilon>0$ and for all $x>0$. Again there is an intimate connection between an arithmetic statement (equidistribution of character values to small arguments) and an analytic statement (growth on vertical lines).

4) If $E/\mathbb{Q}$ is an elliptic curve, we know by Mordell's theorem that the set of rational points on E is a finitely generated Abelian group, $E(\mathbb{Q})\cong\mathbb{Z}^r\oplus E_{\text{tor}}(\mathbb{Q})$. The rank r seems to be an elusive object; however, it is relatively simple to count points on (the reduction of) E over finite fields, and we can define

$$a_E(p) := \frac{p+1-\#E(\mathbb{F}_p)}{\sqrt{p}}$$

for a prime p. This can be extended in a more or less natural way to all integers, and yields an L-function $L_E(s)=\sum a_E(n)n^{-s}$. It is, in general, very hard to prove that this can be extended to an entire function, and is part of the seminal work of Wiles (and others) [**9, 39, 43**]. Given that $L_E(1/2)$ exists, the Birch and Swinnerton-Dyer conjecture states (among other things) that the rank can be recovered from the Laurent expansion at $1/2$, namely $\operatorname{ord}_{s=1/2}L_E(s)=r$.

We observe that all four examples depend on an appropriate analytic continuation of the respective L-function and provide a connection between the arithmetic input and some analytic properties outside the region of absolute convergence.

Every decent L-function has a functional equation of the form

$$L(s)G(s)=\eta\overline{L(1-\bar{s})}G(1-s) \tag{2}$$

where $|\eta| = 1$ and

$$G(s) = N^{s/2} \prod_{j=1}^{d} \pi^{-s/2} \Gamma\left(\frac{s+\mu_j}{2}\right)$$

for some integer $N \in \mathbb{N}$ and some complex numbers $\mu_1, \dots, \mu_d$. The complexity of an L-function is measured by its *analytic conductor*

$$C := C(t) := N \prod_{j=1}^{d} (1 + |t + \mu_j|), \qquad t = \Im s. \tag{3}$$

Since we are assuming that $L(s)$ converges absolutely in $\Re s > 1$, we have $L(s) \ll 1$ in $\Re s = 1 + \varepsilon$. The functional equation (2) and Stirling's formula translate this into[(3)] $L(s) \ll C^{1/2+\varepsilon}$ on $\Re s = -\varepsilon$. If we assume in addition that L is of finite order (in the sense of complex analysis), which is always satisfied in applications, then a standard argument shows

$$L(1/2 + it) \ll C(t)^{1/4+\varepsilon}. \tag{4}$$

This is usually referred to as the *convexity bound*, and any exponent smaller than $1/4$ is called a *subconvexity bound*. If the generalized Riemann hypothesis holds for the L-function in question, then $1/4$ can be replaced with 0.

2. Automorphic forms on GL_2

Let $G := \mathrm{PSL}_2(\mathbb{R})$. We have the Iwasawa decomposition $G = NAK$ where

$$N := \left\{ \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \,\middle|\, x \in \mathbb{R} \right\}, \quad A := \left\{ \begin{pmatrix} y^{1/2} & \\ & y^{-1/2} \end{pmatrix} \,\middle|\, y > 0 \right\},$$
$$K := \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \,\middle|\, \theta \in [0, \pi) \right\}.$$

The group $K = \mathrm{PSO}_2(\mathbb{R})$ is a maximal compact subgroup of G. Let

$$\Gamma := \Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) \mid c \equiv 0 \,(\mathrm{mod}\, N) \right\}.$$

[(3)] Throughout this note, $\varepsilon > 0$ denotes an arbitrarily small constant, not necessarily the same on each occurrence.

Then G acts on $L^2(\Gamma\backslash G)$ by the right regular representation, $\rho(g)(\phi)(x) := \phi(xg)$ for $\phi \in L^2(\Gamma\backslash G)$, and we have a G-equivariant decomposition

$$L^2(\Gamma\backslash G) = \mathbb{C}\cdot\mathbf{1} \oplus \bigoplus_{\pi} V_\pi \oplus \sum_{\mathfrak{a}} \int_{\mathbb{R}} H_{\mathfrak{a}}(t)\,dt \tag{5}$$

into the constant functions, cuspidal irreducible representations (π, V_π) and Eisenstein series for the cusps $\mathfrak{a}$ (that enter the picture because $\Gamma\backslash G$ is not compact). Each V_π decomposes further according to the characters of K:

$$V_\pi = \bigoplus_{q\in 2\mathbb{Z}} V_{\pi,q}$$

(in the Hilbert space sense), and it is known that $\dim V_{\pi,q} \le 1$. The left and right G-invariant Laplace operator

$$\Delta := -y^2(\partial_x^2 + \partial_y^2) + y\partial_x\partial_\theta$$

acts (by a generalized version of Schur's lemma) on each V_π as a scalar $\lambda_\pi \in \mathbb{R}$. In algebraic terms, this is the Casimir element (up to normalization) of the universal enveloping algebra $U(\mathfrak{g})$. Sometimes we need a variant of the space $L^2(\Gamma\backslash G)$. For a character χ of modulus dividing N let $L^2(\Gamma\backslash G)$ denote the L^2-space of functions $G \to \mathbb{C}$ that transform under Γ as $f((\begin{smallmatrix} a & b \\ c & d\end{smallmatrix})g) = \chi(d)f(g)$ for $(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}) \in \Gamma$.

Why is the space $L^2(\Gamma\backslash G)$ interesting? One reason is that it is equipped with additional structure. In general there is no left action of G an $L^2(\Gamma\backslash G)$: if f is Γ-invariant, then $f(g\cdot.)$ is only $g^{-1}\Gamma g$-invariant. However, if $\Gamma = \Gamma_0(N)$ and $g \in \mathrm{PSL}_2(\mathbb{Q})$, then $g^{-1}\Gamma g$ contains some finite index subgroup of $\Gamma_0(N)$, and using a suitable average, we can get back to $\Gamma_0(N)$. This is a special feature of groups like $\Gamma_0(N)$ (as opposed to arbitrary discrete subgroups of G) and yields a family of naturally defined operators $\{T_n \mid n \in \mathbb{N}\}$ that forms a commutative algebra, which also commutes with Δ, since Δ is left G-invariant. Mostly for technical reasons we consider only the subspace $L^2_{\text{new}}(\Gamma\backslash G)$ whose irreducible representations are generated by so-called newforms, i.e. they do not come from subgroups with smaller index in $\mathrm{PSL}_2(\mathbb{Z})$. Then each operator T_n acts on each $V_\pi \subseteq L^2_{\text{new}}(\Gamma\backslash G)$ as a scalar $\lambda_\pi(n)$, and a function $\phi \in V_{\pi,q}$ has a Fourier-Whittaker expansion

$$\phi\left(\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2}\end{pmatrix}\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta\end{pmatrix}\right) \\ = e^{iq\theta}\sum_{n\neq 0}\frac{\lambda_\pi(n)}{\sqrt{|n|}} W_{\operatorname{sgn}(n)q/2,\sqrt{1/4-\lambda_\pi}}(4\pi|n|y)\,e(nx),$$

where as usual $e(x)$ denotes the additive character $e^{2\pi i x}$, $W_{\alpha,\beta}$ is the Whittaker function[(4)] [**42**, Chapter 16] and $\lambda(-n) = \eta\lambda(n)$ with $\eta \in \{-1,0,1\}$. This is relevant for us, because the Hecke eigenvalues $\lambda_\pi(n)$ carry often number theoretic information.

Examples. 1) Hecke [**25**] - Maaß [**31**]: Let N be the discriminant of the field $K = \mathbb{Q}(\sqrt{N})$ and χ the character of the extension $K/\mathbb{Q}$. Then there is a representation $(\pi, V_\pi) \subseteq L^2_{\text{new}}(\Gamma\backslash G, \chi)$ with $\lambda_\pi = 1/4$, such that $\lambda_\pi(n) = \#\{\text{ideals } \mathfrak{a} \subseteq \mathcal{O}_K \mid \mathcal{N}\mathfrak{a} = n\}$.

2) Wiles et al. [**9, 39, 43**]: Let $E/\mathbb{Q}$ be an elliptic curve. Then there is a representation $(\pi, V_\pi) \subseteq L^2_{\text{new}}(\Gamma\backslash G)$ with $\lambda_\pi = 0$, such that $\lambda_\pi(p) = (p+1-\#E(\mathbb{F}_p))/\sqrt{p}$ for all primes p.

Langlands' philosophy suggests that "all interesting objects" arise in this way for suitable Γ and G. In any case, for each representation $(\pi, V_\pi) \subseteq L^2_{\text{new}}(\Gamma\backslash G)$ we can define an L-function

$$L(\pi, s) := \sum_{n=1}^{\infty} \frac{\lambda_\pi(n)}{n^s},$$

and we hope to learn more about Hecke eigenvalues by studying $L(\pi, s)$ from an analytic point of view.

If we work over a number field $K/\mathbb{Q}$ with class number $h > 1$, the above setup is not appropriate. One could work with h copies of G modulo certain conjugates of Γ, but it is better to work adelically. For each place v of K let K_v be the completion and $\mathcal{O}_v$ the ring of integers (if $v \mid \infty$, then $\mathcal{O}_v = K_v$). Then the adele ring is the restricted product

$$\mathbb{A} = \prod_v{}' K_v$$

with respect to the sets $\mathcal{O}_v$, with K embedded diagonally. There is a natural surjection from $\mathbb{A}^\times$ to the group of non-zero fractional ideals of K, and we often do not distinguish between an idele and its image. Again $\mathrm{GL}_2(\mathbb{A})$ acts by the right regular representation on $L^2(\mathbb{A}^\times \mathrm{GL}_2(K)\backslash \mathrm{GL}_2(\mathbb{A}))$ where $\mathbb{A}^\times$ is identified with the center of $\mathrm{GL}_2(\mathbb{A})$. This setting has no dependence on the level of the subgroup any more, since it treats simultaneously all subgroups $\Gamma_0(\mathfrak{c})$, with $\mathfrak{c}$ an ideal in K. If we want to make the level explicit, we define

$$\mathcal{K}(\mathfrak{c}) := \prod_{\mathfrak{p} \text{ finite}} \mathcal{K}(\mathfrak{c}_\mathfrak{p}) \subseteq \mathrm{GL}_2(\mathbb{A}_{\text{fin}})$$

[(4)] In the special case $q = 0$, this reduces essentially to a Bessel K-function.

for a nonzero ideal $\mathfrak{c}$, where

$$\mathcal{K}(\mathfrak{c}_\mathfrak{p}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K_\mathfrak{p}) \,\middle|\, a, d \in \mathcal{O}_\mathfrak{p},\ b \in \mathfrak{d}_\mathfrak{p}^{-1},\ c \in \mathfrak{d}_\mathfrak{p}\mathfrak{c},\ ad - bc \in \mathcal{O}_\mathfrak{p}^\times \right\}$$

with $\mathfrak{d}$ the different of K. The conductor of an irreducible representation (π, V_π) contained in $L^2(\mathbb{A}^\times \mathrm{GL}_2(K)\backslash \mathrm{GL}_2(\mathbb{A}))$ is the smallest ideal such that V_π contains a right $K(\mathfrak{c})$-invariant vector (which is automatically a "newvector"). The Fourier expansion in the adelic setting reads

$$\phi\left(\begin{pmatrix} y & x \\ & 1 \end{pmatrix}\right) = \sum_{r \in K^\times} \frac{\lambda_\pi(r y_{\mathrm{fin}})}{\sqrt{\mathcal{N}(r y_{\mathrm{fin}})}} W_\phi(r y_\infty)\psi(r x),$$

where $y = y_\infty \times y_{\mathrm{fin}} \in \mathbb{A}^\times$, $x \in \mathbb{A}$, ϕ a smooth vector in some cuspidal irreducible representation π, $\mathcal{N}$ the norm, W_ϕ a product of Whittaker functions, ψ the standard additive character on $\mathbb{A}$, and $\lambda_\pi(r y_{\mathrm{fin}})$ depends only on the fractional ideal represented by $r y_{\mathrm{fin}}$ and is non-zero only if this ideal is integral.

How can we get new automorphic forms out of given ones? A typical way is twisting, and the simplest twist is by a character (that is, by an automorphic form on GL_1). Let $\chi : K^\times \backslash \mathbb{A}^\times \to S^1$ be a Hecke character of conductor $\mathfrak{q}$ (that is, $\mathfrak{q}$ is the largest ideal such that χ is trivial on finite ideles $\equiv 1 \bmod \mathfrak{q}$), and define the twist of a representation π on GL_2 with χ by

$$\pi \otimes \chi(g) := \chi(\det g)\pi(g).$$

This is another representation on GL_2, and if the integral ideal $\mathfrak{a}$ is coprime to the conductors of π and χ, then $\lambda_{\pi\otimes\chi}(\mathfrak{a}) = \lambda_\pi(\mathfrak{a})\chi(\mathfrak{a})$. If χ has conductor $\mathfrak{q}$ and π has conductor $\mathfrak{c}$ coprime to $\mathfrak{q}$, then $\pi \otimes \chi$ has conductor $\mathfrak{c}\mathfrak{q}^2$, so the conductor of the character enters quadratically.

3. Subconvexity for automorphic L-functions

The following result is a combination of the results in [**7, 6, 5**]. We are interested in bounding a twisted automorphic L-functions in terms of the conductor of the twisting character, where the other parameters are essentially kept fixed.

Theorem 1. *Let K be a totally real number field of degree d, π an irreducible cuspidal representation on* $\mathrm{GL}_2(\mathbb{A})$*, χ a Hecke character of conductor* $\mathfrak{q}$ *and $C = C(t,\pi)$ the analytic conductor of $L(s,\pi)$ in the sense of* (3)*. Then*

$$L(\pi \otimes \chi, 1/2 + it) \ll C^A(\mathcal{N}\mathfrak{q})^{1/2-\delta+\varepsilon}$$

where $\mathcal{N}$ denotes the norm, A is some absolute constant, $\varepsilon > 0$ is arbitrarily small, and $\delta = \frac{1}{11}$ in general, and $\delta = \frac{1}{8}$ if $K = \mathbb{Q}$.

More precisely, the constant δ in the general case[(5)] is $\frac{1}{8}(1-2\theta) > \frac{1}{11}$ where θ is the a bound towards the Ramanujan conjecture (currently $\theta \leq 1/9$ is known [**29**] and $\theta = 0$ is conjectured).

The convexity bound in this context is $L(\pi \otimes \chi, 1/2 + it) \ll_{t,\pi,\varepsilon} (\mathcal{N}\mathfrak{q})^{1/2+\varepsilon}$. The first subconvex bound in this direction was $\delta = 1/22$ for $K = \mathbb{Q}$ by Duke, Friedlander and Iwaniec [**19**] and an important contribution came from Bykovskiĭ [**12**] that inspired both [**16**] and [**6**]. Our bound $\delta = 1/8$ matches the quality of Burgess' celebrated bound [**11**], where the case π an Eisenstein series is treated.

Over a number field K other than $\mathbb{Q}$ a subconvexity bound was for a long time an open problem. In an unpublished manuscript [**13**] (see also [**14**]), Cogdell, Piatetskii-Shapiro and Sarnak obtained $\delta = 1/18$ for holomorphic Hilbert cusp forms using deep bounds for triple products [**35**]. As an application of an ingenious and very flexible geometric method, Venkatesh [**40**] (see also [**34**]) proved recently – among other things – Theorem 1 with $\delta = 1/24$. Our method is quite different from all of these works and will yield in particular as a by-product a solution of a problem of Selberg, see Theorem 2 below.

We will only sketch briefly the ideas that go into the proof; it rests on the following ingredients[(6)]:

- the amplification method [**19**] and an approximate functional equation [**23**] (this is essentially standard),
- the spectral decomposition of Dirichlet series associated with a shifted convolution sum [**7**] (solving a problem of Selberg) which makes good use of
- the Kirillov model and Sobolev norms [**2**].

Let us look at the first point. To start with, we have to find a way to work conveniently with the values $L(\pi \otimes \chi, 1/2 + it)$ since a priori they exist only by analytic continuation (or perhaps as a conditionally convergent series which is not useful in practice either). However, often a suitably truncated part of a divergent or conditionally convergent series gives a good approximation of the quantity that one

[(5)] At the time of writing, we need some technical assumptions that can most likely be removed with a little extra work.

[(6)] The proof for $K = \mathbb{Q}$ uses a somewhat different methods which avoid the dependence on Ramanujan bounds, see [**6**].

is interested in. For L-functions this can be made precise with an approximate functional equation, and in fact the first about $C^{1/2}$ terms of an L-function with analytic conductor C are a very good approximation on the critical line $\Re s = 1/2$. In other words, for all practical purposes

$$L(1/2, \pi \otimes \chi) \sim \sum_{\mathcal{N}\mathfrak{a} \sim \mathcal{N}\mathfrak{q}} \frac{\lambda_\pi(\mathfrak{a})\chi(\mathfrak{a})}{(\mathcal{N}\mathfrak{a})^{1/2}} \tag{6}$$

and similarly for other points on the critical line, where $\sim$ has to be understood in a very broad sense. Note by the way, that the trivial bound would recover the convexity estimate. Now that we have an explicit description of $L(s, \pi \otimes \chi)$ as a finite sum, let us try to exhibit cancellation in such sums. Let us first look at a simple example[7]. Suppose you want to prove that $|\sin x + \cos x| \leq \sqrt{2}$. There are certainly many ways of proving this. Here is one: Square the left hand side and add a “spectrally useful" nonnegative quantity:

$$|\sin x + \cos x|^2 + |\sin x - \cos x|^2 = 2.$$

Now drop the second term, and the proof is complete. In a similar way, it is useful to embed an L-function into a family. First let us cut the sum (6) into h pieces according to the ideal class of the ideal $\mathfrak{a}$. For simplicity we will only work with the principal class. We consider now the second moment

$$\sum_{\omega \in \Omega} |L(\pi \otimes \omega, 1/2 + it)|^2,$$

where Ω is a family of characters containing χ, for example the family of all characters of $(\mathcal{O}/\mathfrak{q})^\times$. These characters are in general not Hecke characters, because they may not be trivial on units, and so strictly speaking the expression $L(\pi \otimes \omega, 1/2 + it)$ does not make sense as a value of an automorphic L-function. It is typical in this context to consider such “fake-moments"; after all, we are free to add to our original quantity $L(\pi \otimes \chi, 1/2 + it)$ whatever we want as long as it is non-negative. Here the expression $L(\pi \otimes \omega, 1/2 + it)$ is just a notation for a suitable Dirichlet polynomial whose coefficients behave roughly like $\lambda_\pi((\alpha))\omega(\alpha)$ on principal ideals (α). This family is of size about $\mathcal{N}\mathfrak{q}$; so even if we assume a sort of Generalized Lindelöf hypothesis in the sense $L(\pi \otimes \omega, 1/2 + it) \ll_{t,\pi} 1$, we can bound the above sum only by $\mathcal{N}\mathfrak{q}$ which after taking the square-root just recovers the convexity bound. The problem here is that our family, although very convenient to work with, is quite

[7] which can be viewed as an instance of arts and science in mathematics: it is art to find the second term, and it is science to prove the trigonometric identity

large. One could try to evaluate a fourth moment instead of a second moment, in which case one could take the fourth root at the end, but our current analytic techniques are not strong enough to estimate a fourth moment appropriately. The idea of Duke-Friedlander-Iwaniec [**19**] is to weight the sum in our favor so as to highlight the one term we are interested in, but not the other ones that we drop at the end anyway. Hence as a refinement, we consider

$$\sum_{\omega\in\Omega} |A(\omega)|^2 |L(\pi\otimes\omega, 1/2+it)|^2, \tag{7}$$

where $A(\omega)$ is an "amplifier" that is large for $\omega=\chi$, and rather small otherwise. In practice, $A(\omega)$ will be a short Dirichlet polynomial, e.g.

$$A(\omega) = \sum_{\mathcal{N}(\alpha)\sim L} \chi(\alpha)\bar{\omega}(\alpha),$$

where L is a parameter that we can optimize later. Now we open the square and sum over ω. This shows that we have to bound nontrivally sums roughly of the form

$$\sum_{\substack{n_1,n_2\in\mathcal{O}_K\cap\mathcal{B}\\ \alpha_1 n_1\equiv\alpha_2 n_2 \,(\mathrm{mod}\ \mathfrak{q})}} \lambda_\pi(n_1)\bar{\lambda}_\pi(n_2), \tag{8}$$

where α_1, α_2 are of norm about L (they come from the amplifier), and $\mathcal{B}$ is a box in Minkowski space of the form

$$n^{\sigma_1},\dots,n^{\sigma_d} \asymp (\mathcal{N}\mathfrak{q})^{1/d}$$

with $\sigma_1,\dots,\sigma_d$ the embeddings of K into $\mathbb{R}$. We break this sum into pieces according to the value of

$$q := \alpha_1 n_1 - \alpha_2 n_2 \in \mathfrak{q}. \tag{9}$$

The term $q=0$ is the diagonal term, and pretty straightforward to handle. Let us now assume $q\neq 0$. Expressions of the type (8) with a summation condition of type (9) are usually called shifted convolution sums. Selberg [**37**] considered in 1965 Dirichlet series (over $\mathbb{Q}$) of the type

$$D_q(s) := \sum_{n_1-n_2=q} \frac{\lambda_\pi(n_1)\bar{\lambda}_\pi(n_2)}{(n_1+n_2)^s}$$

(which is not an automorphic L-function!) and proved in some cases an analytic continuation to some right half plane $\Re s > 1-\delta$ with $\delta>0$, however, without good control of the size in s and q (which is crucial for all known applications). Progress in this respect has been made by Good [**22**], Jutila [**28**], Sarnak [**35**] and Motohashi [**33**]. Our method, based on the Kirillov model and Sobolev norms gives not only the analytic continuation with good growth estimates, but also the pleasing structural insight that the series $D_q(s)$ can be decomposed according to the decomposition (5). We present the result in the simplest case [**7**]. The general case is treated in [**5**].

Theorem 2. *Let $k > 60$ and $q > 0$ be any integers, and $\lambda(n)$ Hecke eigenvalues of any irreducible cuspidal representation on* GL_2 *of conductor* 1*. Then there exist holomorphic functions F_π in the strip* $1/2 < \Re s < 3/2$ *(depending on k) such that*

$$\sum_{m-n=q} \frac{\lambda(n)\overline{\lambda(m)}(nm)^{(k-1)/2}}{(n+m)^{s+k-1}} = q^{1/2-s} \int \lambda_\pi(q) F_\pi(s)\, d\pi, \qquad \Re s > 1,$$

and

$$\int |F_\pi(s)|\, d\pi \ll_\varepsilon |s|^{22}, \qquad \frac{1}{2} + \varepsilon \le \Re s \le \frac{3}{2},$$

where the integral is taken over the union of the discrete spectrum and the continuous spectrum.

Armed with Theorem 2 (or rather a slight generalization thereof) it is relatively straightforward to complete the proof of Theorem 1.

4. Applications

Although at first sight Theorem 1 may seem as some purely analytic trickery, it has, in accordance with the general philosophy of L-functions, interesting arithmetic applications. Perhaps the most appealing application of Theorem 1 is in combination with the formula of Waldspurger [**41**] and its extensions to number fields. More precisely, let $\tilde{\pi}$ be a cuspidal representation on the double cover $\widetilde{\mathrm{SL}}_2$, generated by a half-integral weight modular form satisfying some technical assumptions, and π the representation on GL_2 given by theta correspondence (“Shimura lift"). Then for squarefree m, Waldspurger’s formula relates the square of the m-th Fourier coefficient of $\tilde{\pi}$ to $L(\pi \otimes \chi_m, 1/2)$ where χ_m is the quadratic character corresponding to the extension $K(\sqrt{m})/K$. In this way, Theorem 1 yields the currently best known bounds for Fourier coefficients of half-integral weight Hilbert modular forms.

One particular situation where such bounds are needed, are asymptotic formulae for the number of representations of totally positive integers by ternary quadratic forms, see [**3**] for an overview of this topic over $\mathbb{Q}$. Hilbert’s eleventh problem asks more generally which integers are (integrally) represented by a given n-ary quadratic form Q over a number field K. If Q is a binary form, it corresponds to some element in the class group of a quadratic extension of K (see [**17**] for a nice account over $\mathbb{Q}$).

If Q is indefinite at some archimedean place, Siegel [**38**] for $n \geq 4$ and Kneser [**30**] and Hsia [**26**] for $n = 3$ proved a local-to-global principle, so Siegel's mass formula tells us exactly which integers are represented by Q. If Q is positive definite at every archimedean place and $n \geq 4$, again Siegel's mass formula and simple bounds for Fourier coefficients of Hilbert modular forms give a complete answer (some care has to be taken in the case $n = 4$). The only remaining case of Q positive definite and $n = 3$ was solved by Duke and Schulze-Pillot [**20**] for $K = \mathbb{Q}$. For arbitrary totally real K, the result was announced in [**13**] with a sketch of the proof being given in [**14**] in the class number one case. Combining the argument in [**14**] with Theorem 1 and Waldspurger's formula e.g. in the version of Baruch-Mao [**1**] one derives:

***Theorem 3* (cf. [14, 13]).** *Let K be a totally real number field and let Q be a positive integral ternary quadratic form over K. Then there is an ineffective constant $c > 0$ such that every totally positive squarefree integer $m \in \mathcal{O}_K$ with $\mathcal{N} m \geq c$ is represented integrally by Q if and only if it is integrally represented over every completion of K.*

The representation of non-squarefree integers is quite subtle, but in principle can again be characterized by more involved local considerations, cf. e.g. [**36**].

Theorem 3 can be refined in various ways and also made quantitative, which yields for example applications of the following type: Gauß proved in his Disquisitiones that a rational integer n can be written as a sum of three squares if and only if it is not of the form $4^k(8m + 7)$, and if it is in addition not divisible by a very high power of 2, the number of such representations is about $L(1, \chi_n)\sqrt{n}$ which by Siegel's theorem is $n^{1/2+o(1)}$. Hence one may ask if all integers satisfying some natural congruence conditions can still be written as a sum of three squares of numbers with certain restrictions, e.g. sums of three squares of primes, or sums of three squares of squarefree numbers or sums of three squares of smooth numbers etc. Combining the previous results with a carefully designed sieve (the vector sieve as developed by Brüdern and Fouvry [**10**]) one can for example prove [**4, 3**]:

***Theorem 4*.** *Let*[8] *$n \equiv 3$ (mod 24), $5 \nmid n$, be sufficiently large, and let $\gamma = 1/567$. Then n is the sum of three squares of integers with all their prime factors greater than n^{γ}. The number of such representations exceeds $\gg n^{1/2-\varepsilon}$. In particular, every such n is the sum of three squares having at most 284 prime factors.*

[8] In [**3**, Proposition 3.1] the condition $n \equiv 3$ (mod 8) has to be replaced by $n \equiv 3$ (mod 24).

For similar results of this flavor see [**3**].

A different type of application of Theorem 1 can be found in [**15**] (cf. also [**40, 44**]) that generalizes work of Duke [**18**]: Under the assumption of a subconvex bound as above it is proved that a certain family of Heegner points and certain d-dimensional subvarieties are equidistributed on the Hilbert modular variety $\mathrm{PSL}_2(\mathscr{O}_K)\backslash\mathscr{H}^d$. For example, if $K=\mathbb{Q}$, and $-D$ is the discriminant of an imaginary quadratic field, then each ideal class $\mathfrak{a}=(a,\frac{1}{2}(b-\sqrt{-D}))$, say, in the class group of $\mathbb{Q}(\sqrt{-D})$ gives a Heegner point $z=(b-\sqrt{-D})/(2a)$ in $X:=\mathrm{PSL}_2(\mathbb{Z})\backslash\mathscr{H}$. If $D\to\infty$, these points become denser and denser in X, and the above statement says that they become actually equidistributed (with an explicit rate of decay) with respect to the standard measure $y^{-2}dxdy$ on X. In order to prove this, one has to sum the values of a test function at these Heegner points, and by a spectral decomposition one can assume that the test function is an eigenform of the Laplacian. This leads to certain Weyl sums, which can be expressed as central values of twisted L-functions. Using bounds for the L-values as in Theorem 1, one derives an equidistribution statement.

Finally we note that the subconvex bound in Theorem 1 (in particular for $K=\mathbb{Q}$) is a crucial input for certain subconvex bounds of higher degree L-functions, which in turn have other arithmetic applications. We refer the reader to [**24, 8**] for more details.

References

[1] E. M. Baruch & Z. Mao – "Central value of automorphic L-functions", *Geom. Funct. Anal.* **17** (2007), no. 2, p. 333–384.

[2] J. Bernstein & A. Reznikov – "Sobolev norms of automorphic functionals", *Int. Math. Res. Not.* (2002), no. 40, p. 2155–2174.

[3] V. Blomer – "Ternary, quadratic forms, and sums of three squares with restricted variables", Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, p. 1–17.

[4] V. Blomer & J. Brüdern – "A three squares theorem with almost primes", *Bull. London Math. Soc.* **37** (2005), no. 4, p. 507–513.

[5] V. Blomer & G. Harcos – "Twisted L-functions over number fields, and Hilbert's eleventh problem", preprint.

[6] ______, "Hybrid bounds for twisted L-functions", *J. Reine Angew. Math.* **621** (2008), p. 53–79.

[7] ______, "The spectral decomposition of shifted convolution sums", *Duke Math. J.* **144** (2008), no. 2, p. 321–339.

[8] V. Blomer, G. Harcos & P. Michel – "Bounds for modular L-functions in the level aspect", *Ann. Sci. École Norm. Sup. (4)* **40** (2007), no. 5, p. 697–740.

[9] C. Breuil, B. Conrad, F. Diamond & R. Taylor – "On the modularity of elliptic curves over **Q**: wild 3-adic exercises", *J. Amer. Math. Soc.* **14** (2001), no. 4, p. 843–939 (electronic).

[10] J. Brüdern & É. Fouvry – "Lagrange's four squares theorem with almost prime variables", *J. Reine Angew. Math.* **454** (1994), p. 59–96.

[11] D. A. Burgess – "On character sums and L-series", *Proc. London Math. Soc. (3)* **12** (1962), p. 193–206.

[12] V. A. Bykovskiĭ – "A trace formula for the scalar product of Hecke series and its applications", *translated in J. Math. Sci. (New York)* **89** (1998), p. 915–932.

[13] J. Cogdell, I. Piatetskii-Shapiro & P. Sarnak – "Estimates on the critical line for Hilbert modular L-functions and applications", unpublished.

[14] J. W. Cogdell – "On sums of three squares", *J. Théor. Nombres Bordeaux* **15** (2003), no. 1, p. 33–44, Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[15] P. B. Cohen – "Hyperbolic equidistribution problems on Siegel 3-folds and Hilbert modular varieties", *Duke Math. J.* **129** (2005), no. 1, p. 87–127.

[16] J. B. Conrey & H. Iwaniec – "The cubic moment of central values of automorphic L-functions", *Ann. of Math. (2)* **151** (2000), no. 3, p. 1175–1216.

[17] D. A. Cox – *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[18] W. Duke – "Hyperbolic distribution problems and half-integral weight Maass forms", *Invent. Math.* **92** (1988), no. 1, p. 73–90.

[19] W. Duke, J. Friedlander & H. Iwaniec – "Bounds for automorphic L-functions", *Invent. Math.* **112** (1993), no. 1, p. 1–8.

[20] W. Duke & R. Schulze-Pillot – "Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids", *Invent. Math.* **99** (1990), no. 1, p. 49–57.

[21] J. B. Friedlander – "Bounds for L-functions", *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)* (Basel), Birkhäuser, 1995, p. 363–373.

[22] A. Good – "Beiträge zur Theorie der Dirichletreihen, die Spitzenformen zugeordnet sind", *J. Number Theory* **13** (1981), no. 1, p. 18–65.

[23] G. Harcos – "Uniform approximate functional equation for principal L-functions", *Int. Math. Res. Not.* (2002), no. 18, p. 923–932.

[24] G. Harcos & P. Michel – "The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. II", *Invent. Math.* **163** (2006), no. 3, p. 581–655.

[25] E. Hecke – "Zur Theorie der elliptischen Modulfunktionen", *Math. Ann.* **97** (1927), no. 1, p. 210–242.

[26] J. S. Hsia – "Representations by spinor genera", *Pacific J. Math.* **63** (1976), no. 1, p. 147–152.

[27] H. Iwaniec & P. Sarnak – "Perspectives on the analytic theory of L-functions", *Geom. Funct. Anal.* (2000), no. Special Volume, Part II, p. 705–741, GAFA 2000 (Tel Aviv, 1999).

[28] M. JUTILA – “The additive divisor problem and its analogs for Fourier coefficients of cusp forms. I”, *Math. Z.* **223** (1996), no. 3, p. 435–461.

[29] H. H. KIM & F. SHAHIDI – “Cuspidality of symmetric powers with applications”, *Duke Math. J.* **112** (2002), no. 1, p. 177–197.

[30] M. KNESER – “Darstellungsmasse indefiniter quadratischer Formen”, *Math. Z.* **77** (1961), p. 188–194.

[31] H. MAASS – “Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen”, *Math. Ann.* **121** (1949), p. 141–183.

[32] P. MICHEL – “Analytic number theory and families of automorphic L-functions”, Automorphic forms and applications, IAS/Park City Math. Ser., vol. 12, Amer. Math. Soc., Providence, RI, 2007, p. 181–295.

[33] Y. MOTOHASHI – “A note on the mean value of the zeta and L-functions. XIV”, *Proc. Japan Acad. Ser. A Math. Sci.* **80** (2004), no. 4, p. 28–33.

[34] A. V. P. MICHEL – “The subconvexity problem for GL_2”, preprint.

[35] P. SARNAK – “Integrals of products of eigenfunctions”, *Internat. Math. Res. Notices* (1994), no. 6, p. 251 ff., approx. 10 pp. (electronic).

[36] R. SCHULZE-PILLOT – “Darstellungsmaße von Spinorgeschlechtern ternärer quadratischer Formen”, *J. Reine Angew. Math.* **352** (1984), p. 114–132.

[37] A. SELBERG – “On the estimation of Fourier coefficients of modular forms”, Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, p. 1–15.

[38] C. L. SIEGEL – “Indefinite quadratische Formen und Funktionentheorie. II”, *Math. Ann.* **124** (1952), p. 364–387.

[39] R. TAYLOR & A. WILES – “Ring-theoretic properties of certain Hecke algebras”, *Ann. of Math. (2)* **141** (1995), no. 3, p. 553–572.

[40] A. VENKATESH – “Sparse equidistribution problems, period bounds, and subconvexity”, to appear.

[41] J.-L. WALDSPURGER – “Sur les coefficients de Fourier des formes modulaires de poids demi-entier”, *J. Math. Pures Appl. (9)* **60** (1981), no. 4, p. 375–484.

[42] E. T. WHITTAKER & G. N. WATSON – *A course of modern analysis*, Cambridge University Press, Cambridge, 4th edition.

[43] A. WILES – “Modular elliptic curves and Fermat’s last theorem”, *Ann. of Math. (2)* **141** (1995), no. 3, p. 443–551.

[44] S.-W. ZHANG – “Equidistribution of CM-points on quaternion Shimura varieties”, *Int. Math. Res. Not.* (2005), no. 59, p. 3657–3689.