Centre de Recherches Mathématiques
CRM Proceedings and Lecture Notes
Volume **19**, 1999

Automorphic L-Functions in Level Aspect

W. Duke

ABSTRACT. This is an exposition of some recent developments in the theory of automorphic L-functions in "level aspect". It includes a discussion of joint work with J. Friedlander and H. Iwaniec on breaking convexity and with E. Kowalski on distinguishing elliptic curves by small primes.

1. Introduction

A well known task of analytic number theory is to understand the behavior of various objects associated to Dirichlet characters as the conductor varies, for example character sums and L-functions. In recent years it has become clear that analogous questions from $\mathrm{GL}(n)$ for $n > 1$ are also of great interest, although they are in general much more difficult to attack. A particularly interesting set of problems of this type concerns the variation of quantities associated to elliptic curves over $\mathbb{Q}$ as the level changes. In this largely expository article I will discuss a few of these questions in relation to their more classical counterparts.

2. Breaking convexity

Let χ be a primitive Dirichlet character with conductor q and

$$L(s,\chi) = \sum \chi(n) n^{-s}$$

be the associated Dirichlet L-function. As is familiar,

$$\Lambda(s,\chi) = q^{s/2}\pi^{-s/2}\Gamma\left(\frac{s+a}{2}\right) L(s,\chi)$$

is entire when $q > 1$ and satisfies the functional equation $\Lambda(s,\chi) = \epsilon\Lambda(1-s,\bar{\chi})$ where $|\epsilon| = 1$ and $a = 0$ or 1 according to whether χ is even or odd. From this and the convexity principle of Phragmén-Lindelöf it follows that

$$L(s,\chi) \ll q^{1/4+\varepsilon}$$

for $\mathrm{Re}(s) = \frac{1}{2}$, the implied constant depending on s and ϵ. This is the basic example of a *convexity bound* in the conductor (or level) aspect. If one assumes the Generalized Riemann Hypothesis (GRH) for $L(s,\chi)$ then one may replace the $\frac{1}{4}$ by 0, which

1991 *Mathematics Subject Classification.* 11F66, 11G40.
Research supported in part by NSF Grant No. DMS-9507797.
This is the final version of the paper.

is the Lindelöf hypothesis in the level aspect. *Breaking convexity* in this example was accomplished by Burgess [**B**] in 1962 when he reduced the exponent from $\frac{1}{4}$ to 3/16. His proof employed the Riemann Hypothesis for curves established by Weil and remains today the best known estimate. In 1992 Friedlander and Iwaniec [**FI**] obtained in an elementary way the exponent 5/22 by using a method which could be called the *amplification technique.* Very roughly speaking, the idea is to improve the general mean-value estimate

$$\sum_{\chi \mod q} \left| \sum_{n \le N} c_n \chi(n) \right|^2 \le (q+N) \sum_{n\le N} |c_n|^2,$$

which holds for any complex numbers c_n, when certain special c_n are chosen. This technique has proven to be more adaptable to different situations than that of Burgess and its variations have been successful in breaking convexity in the setting of GL(2).

An important point is that breaking convexity often has qualitative consequences and it may be irrelevant by how much the exponent in the convexity bound is improved. Let me illustrate this with a classical example from the theory of minima of positive integral binary quadratic forms. Suppose that $Q(x,y) = ax^2+bxy+cy^2$ is such a form with (negative) fundamental discriminant $d = b^2-4ac$ and associated CM point

$$z_Q = \frac{-b+\sqrt{d}}{2a}.$$

If $Q(x,y)$ is reduced, that is $|b| \le a \le c$, then the minimum positive value taken by $Q(x,y)$ is

$$\min Q = a = \frac{\sqrt{|d|}}{2\,\mathrm{Im}(z_Q)}.$$

Since Q being reduced is equivalent to z_Q being in the (closure of the) standard fundamental domain $\mathcal{F}$ for $\mathrm{PSL}(2,\mathbb{Z})$, the well known bound $\min Q \le \sqrt{|d|/3}$ follows. A consequence of convexity breaking for the Dirichlet L-function in level aspect is the following result giving the existence of a form with a (relatively) large minimum when $|d|$ is large.

THEOREM 1. *Fix any $\kappa < \frac{1}{2}$. Then, for sufficiently large $|d|$, there is some form Q with fundamental discriminant d such that*

$$\min Q \ge \kappa\sqrt{|d|}.$$

A proof of this is easily sketched. Take a nice function ϕ supported in $(2\kappa, 1)$ and form the automorphic kernel $\Phi(z) = \sum \phi(\mathrm{Im}(\gamma z)^{-1})$, the sum being over $\gamma \in \Gamma_\infty\backslash\Gamma$ with $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$ and Γ_∞ the stabilizer of infinity. Clearly, if $S = \sum_{z_Q\in\mathcal{F}} \Phi(z_Q) > 0$ then we have the desired existence. Inverting the Mellin tranform

$$\tilde{\phi}(s) = \int_0^\infty \phi(y) y^s \frac{dy}{y}$$

we get, after interchanging summation and integration,

$$S = \frac{1}{2\pi i}\int_{Re(s)=2} \tilde{\phi}(s) \sum_{z_Q} E(z_Q, s)\, ds$$

where $E(z,s)$ is the classical Eisenstein series. Now the inner sum may be expressed in terms of the Dedekind zeta function of $\mathbb{Q}(\sqrt{d})$, which in turn factors as the product of the Riemann zeta function and a Dirichlet L-function. Upon shifting the contour we get

$$S - c\,h(d) \ll |d|^{1/4} \int_{\mathrm{Re}(s)=1/2} |\tilde{\phi}(s)|\,|L(s,\chi)|\,ds$$

for $\chi(n) = (d/n)$ and some $c > 0$. By Siegel's theorem for the class number $h(d) \gg |d|^{1/2-\varepsilon}$, so the eventual (though non-effective) positivity of S follows from any bound of the form $L(s,\chi) \ll |d|^{1/4-\delta}$ for $\delta > 0$ with some (weak) dependence of the bound on s, thus giving the result.

It follows from [**D**] that Theorem 1 actually holds for any $\kappa < 1/\sqrt{3}$ and then it is best-possible (although it retains the defect of being non-effective). For this one needs to be able to produce CM points in the fundamental domain $\mathcal{F}$ which have imaginary part less than 1, and this cannot be accomplished using only the Eisenstein series but requires the use of (non-holomorphic) cusp forms as well. This result of [**D**] may be viewed as an example of breaking convexity for GL(2) since the resulting Weyl type sums are in fact closely related to special values of twisted L-functions.

The question of breaking convexity for automorphic L-functions in the level aspect was taken up in earnest in the papers [**DFI**]. For even integral $k \geq 2$ let $S_k^+(q)$ be the set of holomorphic newforms for $\Gamma_0(q)$ of weight k with trivial character. For $f \in S_k^+(q)$ write

$$f(z) = \sum_{n\geq 1} \lambda_f(n) n^{(k-1)/2} e(nz).$$

The associated L-function is $L(f,s) = \sum_{n\geq 1} \lambda_f(n) n^{-s}$. It is entire and satisfies a functional equation which yields the convexity bound $L(f,s) \ll |q|^{1/4+\varepsilon}$ for $\mathrm{Re}(s) = \frac{1}{2}$, the critical line in this normalization. Among the results of the second paper of [**DFI**] is the following.

THEOREM 2. *For* $\mathrm{Re}(s) = \frac{1}{2}$ *we have the bound*

$$L(f,s) \ll |q|^{1/4-1/192+\varepsilon}.$$

The implied constant depends only on ε *and* s.

This estimate may be used to give a new proof of results in [**DS**] on the representability of large integers by positive ternary quadratic forms. For such applications the exact exponent obtained is unimportant as long as it is strictly less than that of the convexity bound.

3. Distinguishing characters or elliptic curves by small primes

Another classical problem which brings into the forefront the level aspect of automorphic L-functions is that of the least quadratic non-residue modulo a prime q. This deals with the structure of the seemingly well-known group $(\mathbb{Z}/q\mathbb{Z})^*$ of invertible elements modulo q. Let $N(q)$ be the smallest positive integer N such that N is not a square modulo q; the problem is to estimate this number as q varies. Write for any $n \geq 1$

$$\chi_q(n) = \left(\frac{n}{q}\right)$$

so that χ_q is a primitive Dirichlet character modulo q (if $q \geq 3$). Then $N(q)$ is also the smallest positive N such that

$$\left|\sum_{1\leq n\leq N} \chi_q(n)\right| < N$$

so we can estimate $N(q)$ by obtaining non-trivial bounds for this character sum. From the Polya-Vinogradov inequality

$$\left|\sum_{1\leq n\leq N} \chi_q(n)\right| \leq 2q^{1/2}\log q$$

it follows that $N(q) \ll q^{1/2+\varepsilon}$ for any $\varepsilon > 0$, and using an elementary trick this was improved by Vinogradov to give

$$N(q) \ll q^{1/(2\sqrt{e})+\varepsilon}$$

for any $\varepsilon > 0$. The same trick, when applied to the improvement of the Polya-Vinogradov inequality by Burgess, which gives a non-trivial bound for $N \gg q^{1/4+\epsilon}$, yields the current best known result for an *individual* character:

$$N(q) \ll q^{1/(\sqrt[4]{e})+\epsilon}$$

for any $\epsilon > 0$. On the other hand the GRH implies (see [**Mon**])

$$N(q) \ll (\log q)^2. \tag{1}$$

This shows how far we are from the true order of magnitude!

This problem was one of the motivations which brought Linnik to create the large-sieve [**Lin**] as a possible substitute for the Riemann Hypothesis *on average.* His idea was to estimate the number of exceptions to a bound such as (1), and was the first step on the road which led ultimately to results as important as the Bombieri-Vinogradov theorem on primes in arithmetic progressions, which can actually replace the Generalized Riemann Hypothesis in many interesting applications.

Let us write $N(\alpha, Q)$ for the number of primitive Dirichlet characters χ modulo q, for all positive integers $q \leq Q$, which satisfy

$$\chi(p) = 1 \quad \text{for all } p \leq (\log Q)^\alpha. \tag{2}$$

Then, by a variation of Linnik's original method, we derive:

THEOREM 3. *For any $\varepsilon > 0$ it holds that*

$$N(\alpha, Q) \ll Q^{2/\alpha+\varepsilon}. \tag{3}$$

Since the total number of possible χ modulo $q \leq Q$ is about Q^2, this shows that the number of exceptional characters is relatively small if $\alpha > 1$. Furthermore, if $\alpha > 2$ then almost all prime moduli $q \leq Q$ have quadratic non-residues $p \leq (\log Q)^\alpha$.

Here is a sketch of the proof of this result. It is based on the large-sieve inequality for Dirichlet characters, namely

$$\sum_{q\leq Q} \sum_{\chi \bmod q}{}^{*} \left|\sum_{n\leq N} c_n\chi(n)\right|^2 \leq (N+Q^2)\sum_{n\leq N}|c_n|^2. \tag{4}$$

To exploit this, consider the set $\mathcal{N}$ of all products of m distinct prime factors all less than $(\log Q)^\alpha$, where

$$m = \left[\frac{2\log Q}{\alpha \log\log Q}\right].$$

Then $N = \operatorname{Max}\mathcal{N} \ll Q^2$, and on the other hand an easy computation gives

$$|\mathcal{N}| \gg Q^{2(\alpha-1)/\alpha-\varepsilon}$$

for any $\varepsilon > 0$. Take then

$$c_n = \begin{cases} 1, & n \in \mathcal{N} \\ 0, & \text{otherwise} \end{cases}$$

in (4); the inner sum is then $|\mathcal{N}|$ for all those characters, and by positivity this gives

$$N(\alpha, Q)|\mathcal{N}|^2 \ll Q^2|\mathcal{N}|$$

whence, as claimed

$$N(\alpha, Q) \ll Q^{2-2(\alpha-1)/\alpha+\varepsilon} = Q^{2/\alpha+\varepsilon}.$$

It is natural now to investigate the analogue of these problems for modular forms, which are the GL(2)-analogues of the Dirichlet characters. The question is then the following: suppose we fix k and are given two new-forms $f \in S_k^+(q_1)$ and $g \in S_k^+(q_2)$ of squarefree levels q_1 and q_2, with $f \neq g$. Then how large, compared to the levels, is the smallest prime p such that $\lambda_f(p) \neq \lambda_g(p)$? Again a suitable Riemann Hypothesis (for the Rankin-Selberg convolution $L(f \otimes g, s)$ this time) implies by means of a standard argument that this is true for some $p \ll (\log q)^2$ where $q = \operatorname{lcm}(q_1, q_2)$. In this case the convexity bound (or a look at the order of vanishing of $f - g$ at ∞) gives $p \ll q^{1+\varepsilon}$ and this is substantially the best known unconditional result. Indeed, it seems very hard to break the convexity bound for $L(f \otimes g, s)$.

However, turning to the analogue of Linnik's result, it is possible to obtain good estimates for the number of exceptions. This is joint work with E. Kowalski [**DK**]. Letting $M(\alpha, Q)$ denote the maximal number of new-forms f of squarefree level $q \leq Q$ which all have the same Hecke eigenvalues for primes $p \leq (\log Q)^\alpha$, we obtain the following result:

THEOREM 4. *For any $\varepsilon > 0$, it holds that*

$$M(\alpha, Q) \ll Q^{10/\alpha+\varepsilon}.$$

As a corollary, using the modularity of semistable elliptic curves proved by Wiles, we get also:

COROLLARY 1. *The number of isogeny classes of semistable elliptic curves over $\mathbb{Q}$ with conductor less than Q which may have the same number of points modulo p for all $p \leq (\log Q)^\alpha$ is*

$$\ll Q^{8/\alpha+\varepsilon}$$

for any $\varepsilon > 0$.

To get the exponent 8 instead of 10 we need an upper bound for the number $\mathrm{Ell}(Q)$ of isogeny classes of semistable elliptic curves over $\mathbb{Q}$ with conductor less than Q, which is an improvement on average of a recent result of Brumer and Silverman [**BS**]:

$$\mathrm{Ell}(Q) \ll Q^{1+\varepsilon}$$

for any $\varepsilon > 0$. Note also that the corollary is non-trivial because there is also a lower bound for this number [**FNT**]

$$\mathrm{Ell}(Q) \gg Q^{5/6}.$$

The proof follows the same strategy as Linnik's result. However, various twists appear. First, we require a partial analogue of (4):

$$\sum_{q\leq Q}^{\flat} \sum_{f\in S_k(q)^+} \Big| \sum_{n\leq Q^\beta} c_n \lambda_f(n) \Big|^2 \ll Q^{\beta+\varepsilon} \sum_n |c_n|^2 \tag{5}$$

for any $\varepsilon > 0$, and $\beta > 4$ ($\sum^\flat$ indicates a sum over squarefree integers). But then, arguing as before, we cannot finish, because we do not have á lower bound for $\lambda_f(p)$ which is as convenient as $|\chi(p)| = 1$. Using results on average is not possible here because we use very small primes, compared to the level, and we need uniformity in f also. Such difficulties have already appeared in other problems, and we use the same trick as in [**DFI**]. The useful formula

$$\lambda_f(p)^2 - \lambda_f(p^2) = 1$$

(for all unramified p) implies that if $\lambda_f(p)$ is too small, then $\lambda_f(p^2)$ cannot be! This leads us to use another inequality which is similar to the previous one except that it detects orthogonality along the squares:

$$\sum_{q\leq Q}^{\flat} \sum_{f\in S_k(q)^+} \Big| \sum_{n\leq Q^\beta}^{\flat} c_n \lambda_f(n^2) \Big|^2 \ll Q^{\beta+\varepsilon} \sum_n |c_n|^2 \tag{6}$$

for any $\varepsilon > 0$, and this time $\beta > 10$. This may be interpreted as a partial large-sieve inequality for the symmetric squares of the new-forms, which are $\mathrm{GL}(3)$-automorphic forms defined by Gelbart and Jacquet [**GJ**]. We also need a result of Ramakrishnan according to which two newforms with squarefree levels can't have the same symmetric square unless they are the same. Now with (6), the proof of the theorem is easily completed.

The proofs of (5) and (6) are similar (actually, we prove a general mean-value estimate for families of $\mathrm{GL}(n)$-automorphic representations for any $n \geq 1$). Using duality, we reduce (6) (for instance) to proving

$$\sum_{n\leq Q^\beta} \lambda_f^{(2)}(n)\lambda_g^{(2)}(n) \ll \begin{cases} Q^{\beta-2+\varepsilon}, & \text{if } f \neq g \\ Q^{\beta+\varepsilon}, & \text{if } f = g \end{cases} \tag{7}$$

(where $\lambda_f^{(2)}$ denotes the coefficients of the L-function of the symmetric square $f^{(2)}$ of f) which we attack by means of Mellin inversion. We then have to study the analytic properties of the "bilinear convolution" L-function

$$L_b(f^{(2)} \otimes g^{(2)}, s) = \sum_{n\geq 1} \lambda_f^{(2)}(n)\lambda_g^{(2)}(n)n^{-s}$$

which we do by relating it to the true Rankin-Selberg convolution $L(f^{(2)} \otimes g^{(2)}, s)$, defined by Jacquet, Piatetskii-Shapiro and Shalika [**JPS**]. This comparison lemma gives us the analytic continuation of L_b up to the critical line, which is sufficient to get (7). *En route*, we have to use the determination of the location of the poles of the Rankin-Selberg convolution, due to Mœglin and Waldspurger [**MW**].

Acknowledgements

This article is a slightly expanded version of my lecture at the Fifth Conference of the CNTA. I thank the organizing commitee for providing financial support for this most enjoyable conference. I also thank E. Kowalski for his help in preparing this manuscript.

References

[BS] A. Brumer and J. Silverman, *The number of elliptic curves over* $\mathbb{Q}$ *with conductor* N, Manuscripta Math. **91** (1996), no. 1, 95–102.

[B] D. A. Burgess, *On character sums and L-series.* I, Proc. London Math. Soc (3) **12** (1962), 193–206; II, Proc. London Math. Soc (3) **13** (1963), 524–536 .

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

[DFI] W. Duke, J. Friedlander, and H. Iwaniec, *Bounds for automorphic L-functions.* I, Invent. Math. **112** (1993), no. 1, 1–8; II, Invent. Math. **115** (1994), no. 2, 219–239.

[DK] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, appendix by D. Ramakrishnan, 1996 (preprint).

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

[FNT] É. Fouvry, M. Nair, and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France **120** (1992) no. 4, 485–506.

[FI] J. Friedlander and H. Iwaniec, *A mean-value theorem for character sums*, Michigan Math. J. **39** (1992), no. 1, 153–159.

[GJ] S. Gelbart and H. Jacquet, *A relation between automorphic representations of* GL(2) *and* GL(3), Ann. Sci. École Norm. Sup. (4) **11** (1978), no. 4, 471–552.

[JPS] H. Jacquet, I. I. Piatetskii-Shapiro, and J. A. Shalika, *Rankin-Selberg convolutions*, Amer. J. Math. **105** (1983), no. 2, 367–464.

[Lin] Yu. V. Linnik, *The large sieve*, Dokl. Akad. Nauk. SSSR **30** (1941), 292–294 (Russian).

[MW] C. Mœglin and J.-L. Waldspurger, *Le spectre résiduel de* GL(n), Ann. Sci. École Norm. Sup. (4) **22** (1989), 605–674.

[Mon] H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Math., vol. 227, Springer-Verlag, Berlin-New York, 1971.

Department of Mathematics, Rutgers University, Piscataway, NJ 08854-8019, U.S.A.
E-mail address: duke@math.rutgers.edu