Bounds for Arithmetic Multiplicities

W. Duke[1]

Abstract. This paper will describe some recent applications of techniques giving non-trivial upper bounds for multiplicities in certain arithmetic instances. These applications include estimates for dimensions of spaces of cusp forms of weight one, multiplicities of number fields with a given degree and discriminant, and the number of elliptic curves over the rationals whose reductions have the same number of points for a few small primes. The techniques share a common strategy, which combines approximate orthogonality with rigidity properties of arithmetic Fourier coefficients.

1991 Mathematics Subject Classification: 11F,11N
Keywords and Phrases: modular forms of weight one, number fields, class groups, elliptic curves

1 Introduction

A set of problems in Number Theory where analytic and algebraic techniques combine fruitfully concern finding upper bounds for arithmetic multiplicities. These problems are perhaps best introduced through a series of particular examples. They involve counting automorphic forms, number fields, class groups and elliptic curves under various conditions on associated eigenvalues. In most cases natural conjectures arise which appear to be quite difficult and the analytic method introduced provides non-trivial information but certainly not the final answer. The corresponding existence questions are left untreated here but present fascinating challenges.

2 Modular forms of weight one

In a variety of situations it is of interest to bound the multiplicity of an automorphic representation in an appropriate family (see [S-X]). Conjectured bounds for the multiplicities of certain Maass eigenvalues for congruence subgroups are crucial assumptions in the works of Philips and Sarnak [P-S] and of Wolpert [Wol] on the disappearance of cusp forms under perturbations. The main analytic tool which has been applied is the trace formula, but, in cases when the eigenvalue is

[1]Research supported in part by NSF Grant DMS-9500797.

not isolated, it only yields rough information since it is not capable by itself of effectively separating neighboring spectrum.

Perhaps the most classical instance of this problem is in determining the dimension of the space of holomorphic cusp forms of weight one for congruence subgroups as a function of the level. For forms of integral weight larger than one the dimension is well understood by means of either the Riemann–Roch theorem or the Selberg trace formula but the eigenvalue for weight one, $1/4$, is an accumulation point for the discrete spectrum when the level increases and thus the above problem intervenes.

For a positive integer N and χ a Dirichlet character (mod N) let $S_1(N,\chi)$ denote the space of holomorphic cusp forms for $\Gamma_0(N)$ of weight 1 with Nebentypus χ. If the order of χ is fixed a direct application of the trace formula gives

$$\dim S_1(N,\chi) \ll N$$

while Deshouillers/Iwaniec and Sarnak observed (unpublished) that a clever choice of test function yields the improvement

$$\dim S_1(N,\chi) \ll \frac{N}{\log N}.$$

Early on Hecke pointed out that weight one cusp forms for real χ may be constructed from non-real characters of class groups of imaginary quadratic fields. More generally, let ρ be a two-dimensional irreducible odd Galois representation and $\tilde{\rho}$ be the induced projective representation into $PGL(2,\mathbf{C})$. The image of $\tilde{\rho}$ is dihedral or isomorphic to one of A_4, S_4, or A_5. Langland's program predicts the existence of a newform $f = \sum a_f(n)e(nz) \in S_1(N,\chi)$ with

$$a_f(p) = \mathrm{tr}(\rho(\mathrm{Frob}_p)) \text{ and } \chi(p) = \det(\rho(\mathrm{Frob}_p))$$

for p not dividing N. The dihedral case corresponds to Hecke's construction. Langlands and Tunnell (see [Tu]) proved the existence of such a form in all but the A_5 case. Deligne and Serre [D-S] proved that every newform arises in this way.

Suppose for simplicity that N is prime and that χ is real. It can be shown that there are $(h-1)/2$ independent forms of dihedral type, where h is the class number of $\mathbf{Q}(\sqrt{-N})$ and thus there are $\ll N^{1/2}\log N$ such forms. Serre raised the question of bounding from above the number of non-dihedral forms. The following was proved in [Du].

Theorem 1 *For N prime*

$$\dim S_1(N,\chi) \ll_\varepsilon N^{11/12+\varepsilon}.$$

It appears reasonable to expect that in fact

$$\dim S_1(N,\chi) = \frac{1}{2}(h-1) + O(N^\varepsilon).$$

In particular, this would imply that $\dim S_1(N,\chi) \ll N^{1/2}\log N$. Since by Siegel's theorem

$$\dim S_1(N,\chi) \underset{\varepsilon}{\gg} N^{1/2-\varepsilon}$$

this would be essentially best-possible.

The proof of Theorem 1 extends to general N and χ as long as the order of χ is fixed. Recently S. Wong [Wo1] has carried this out and extended the arguments to apply to general χ as well. The idea behind the proof is to take advantage of two properties of the Fourier coefficients of non-dihedral newforms which cannot co-exist if there are too many of them. These are their approximate orthogonality, which is a consequence of their belonging to automorphic forms, and the finiteness of the number of their possible values at primes, which is a consequence of their coming from Galois representations of a known type. The technique could in principle be applied to estimate other eigenvalue multiplicities in other Galois cases. For example, it would bound nontrivially the multiplicity of the eigenvalue 1/4 of the weight zero Laplacian for congruence subroups if it were known that they come from Galois representations.

3 Number fields and class groups

A closely related problem concerns bounding from above the multiplicity of number fields of a given degree as a function of its discriminant. This in turn is, in cases covered by class field theory, tied to estimating the ranks of class groups.

For a positive integer n and an integer D let $M_n(D)$ be the number of number fields of degree n with discriminant D. Hermite showed that $M_n(D)$ is finite and Stickelberger observed that $M_n(D) = 0$ unless $D \equiv 0, 1 (\text{mod } 4)$. Except for the case $n = 2$ when $M_n(D) = 1$ exactly for D fundamental, little is known about the size of $M_n(D)$.

On average over $|D| \leq X$ a little more is known. Let

$$S_n(X) = \sum_{|D|\leq X} M_n(D) :$$

for $n = 2, 3$ we have that

$$S_n(X) \sim c_n X$$

where $c_n = 1/\zeta(n)$, the case $n = 3$ being a famous result of Davenport-Heilbronn [D-H]. The best general upper bound is due to Schmidt [Sch]

$$S_n(X) \ll X^{(n+2)/4}$$

using the geometry of numbers. Wright and Yukie have announced an asymptotic in the case of quartic fields.

Such results have motivated the conjectured bound for fixed n:

$$M_n(D) \ll |D|^{\varepsilon}$$

but, except for the case $n = 2$, this is open. A non-trivial upper bound for the multiplicity of quartic fields was obtained in [Du].

Theorem 2 *For $-D$ prime*

$$M_4(D) \ll_\varepsilon |D|^{7/8+\varepsilon}.$$

As in the case of Theorem 1, this result extends to more general quartic fields (see [Wo1].) Before Theorem 2, the only known upper bounds followed from trivial bounds for class numbers. By means of class field theory Heilbronn [He] showed that

$$M_4(D) = \frac{4}{3} \sum_k h_2(K),$$

where K runs over all cubic number fields of discriminant D. Here, for any ℓ and any number field K, $h_\ell(K)$ denotes the number of ideal classes of K of (exact) order ℓ. Furthermore, the number of cubic fields in the sum is $\frac{3}{2} h_3(\mathbf{Q}(\sqrt{D}))$. For the class number $h(K)$ of any number field K of degree $n > 1$ and discriminant D we have the bound

$$h(k) \ll |D|^{1/2} \log^{n-1} |D|$$

where the implied constant depends only on n. Since $h_\ell(K) \leq h(K)$ we deduce the "trivial" bound

$$M_4(D) \ll |D|^{1+\varepsilon}.$$

The improvement of this given in Theorem 2 requires both the classification of quartic fields of discriminant D by odd S_4– Galois representations of conductor $|D|$ and the proof in this case of the Artin conjecture given in [Tu]. If we assume the Artin conjecture for icosahedral representations then similarly we can prove that the number of non-real quintic fields of discriminant D^2 whose normal closure has Galois group A_5 is $O(|D|^{11/12+\varepsilon})$.

This discussion motivates another problem, which is to bound $h_\ell(K)$ and again, very little seems to be known. A famous exception is for quadratic fields $n = 2$ when $\ell = 2$, where Gauss' genus theory gives the formula

$$h_2(K) = 2^{\nu(D)-1} - 1$$

where $\nu(D)$ is the number of primes dividing D. Once again, it is suspected that in general for a given n, ℓ

$$h_\ell(K) \ll |D|^\varepsilon.$$

One may also a formulate the more precise possible bound (see [B-S])

$$\log h_\ell(K) \ll \log |D| / \log\log |D|.$$

4 Elliptic Curves

A basic multiplicity problem for elliptic curves is to bound the number $M(N)$ of elliptic curves over $\mathbf{Q}$ with conductor N. Recently Brumer and Silverman [B-S] have shown that

$$M(N) \ll N^{1/2+\varepsilon}.$$

They use that solutions to the discriminant equation for elliptic curves correspond to S-integral points on a curve

$$y^2 = x^3 + A$$

and that the number of such points is $\ll h_3(K)|N|^{\varepsilon}$ for some quadratic K with discriminant $\ll N$. Thus any improvement on the trivial bound for $h_3(K)$ would improve the bound for $M(N)$. In this case it was observed in [D-K] that on average

$$\sum_{N \leq X} M(N) \ll X^{1+\varepsilon}$$

since the Davenport-Heilbronn Theorem is applicable. Brumer and Silverman also showed that under standard conjectures about L-functions for elliptic curves (GRH, BSD) that

$$M(N) \ll N^{\varepsilon}.$$

Wong [Wo2] observed that under these hypotheses one may deduce that

$$h_3(k) \ll |D|^{1/4+\varepsilon}.$$

We turn to an enrichment of the question of counting all elliptic curves. It is connected to the problem of determining the extent to which an elliptic curve defined over $\mathbf{Q}$ is determined by the trace of Frobenius for a few small primes. This problem is analogous to bounding the least quadratic non-residue, a venerable problem in classical analytic number theory. Assuming the Riemann-Hypothesis for Artin L-functions, Serre [Se2] showed that $O((\log N)^2)$ primes suffice, where N is the conductor of the curve. No nontrivial unconditional results are known for this problem due in part to the difficulty in breaking convexity for the associated Rankin-Selberg L-function (see [D-F-I]).

The associated multiplicity problem is to estimate the maximal number of isogeny classes of curves which have the same trace of Frobenius for a few small primes, in terms of the conductor. Recently in a joint work with E. Kowalski we obtained an estimate which shows that "most" curves are determined by very few primes. Our proof uses modularity of the curves and hence we must restrict ourselves to curves for which the theorem of Wiles [Wi] or a generalization applies.

For example, let $M(X, \alpha)$ be the maximal number of isogeny classes of semi-stable elliptic curves over $\mathbf{Q}$ with conductor less than or equal to X which for every prime $p \leq (\log X)^{\alpha}$ have a fixed number of points modulo p. The following is proved in [D-K].

Theorem 3 *We have for any* $\varepsilon > 0$

$$M(X, \alpha) \ll_{\varepsilon} X^{8/\alpha+\varepsilon}.$$

It follows from this and the lower bound [F-N-T]

$$Ell(X) \gg X^{5/6}$$

for the number of isogeny classes of semi-stable elliptic curves with conductor less than X that the probability that two such elliptic curves have the same number of points (mod p) for all primes $p \leq (\log X)^\alpha$ tends to zero as X tends to infinity, if α is large enough. It may be viewed as an analogue of the classical result of Linnik bounding the number of primes with no small quadratic non-residues.

5 Approximate orthogonality

A unifying feature of the results outlined is the use of mean-value theorems which display in a quantitative form the orthogonality of the Fourier coefficients of newforms. Such theorems, already in extremely sophisticated form, were introduced and applied by Deshouillers and Iwaniec [D-I] and have been used extensively in the analytic theory of automorphic L-functions. The uses we are describing are more rudimentary in the sense that direct use is made of the coefficients.

Let $S(N) = S_k^+(N,\chi)$ denote the set of newforms of integral weight k for $\Gamma_0(N)$ with character χ. Each $f \in S$ has the Fourier expansion at ∞

$$f(z) = \sum_{n\geq 1} a_f(n)\, e(nz)\,.$$

The Hecke eigenvalues are

$$\lambda_f(n) = n^{-(k-1)/2} a_f(n).$$

The simplest mean-value result is that applied in the proof of Theorem 1 and is the following. For arbitrary $c_n \in \mathbf{C}$ with $1 \leq n \leq X$ we have

$$\sum_{f\in S(N)} \Big|\sum_{n\leq X} c_n\, \lambda_f(n)\Big|^2 \ll (X+N)N^\varepsilon \sum_{n\leq X} |c_n|^2. \tag{1}$$

This result is proved by using a form of duality and the following estimate for any cusp form f, not necessarily a newform:

$$\sum_{n\leq X} |a_f(n)|^2 \ll (1+X/N)\langle f,f\rangle$$

where $\langle f,f\rangle$ is the Petersson inner product.

For the proof of Theorem 3 we need more sophisticated mean value theorems which average also over the level and are thus reminiscent of the classical large sieve inequality for primitive Dirichlet characters:

$$\sum_{q\leq Q} \sideset{}{^*}\sum_{\chi (\mathrm{mod}\ q)} \Big|\sum_{n\leq X} c_n \chi(n)\Big|^2 \leq (X+Q^2) \sum_{n\leq X} |c_n|^2$$

which gives a kind of approximate orthogonality for the truncated sequences $(\chi(n))_{1\leq n\leq X}$ considered as elements of a finite dimensional Hilbert space.

Suppose for simplicity that the Nebentypus character χ is trivial. The first inequality is

$$\sum_{N\leq X}^{\flat}\sum_{f\in S(N)}\Big|\sum_{n\leq X^{\beta}}c_n\lambda_f(n)\Big|^2\ll X^{\beta+\varepsilon}\sum_n|c_n|^2 \tag{2}$$

for any $\varepsilon>0$, and $\beta>4$, where $\sum^{\flat}$ indicates a sum over squarefree integers.

We also needed to use another inequality which is similar to the previous one except that it detects orthogonality along the squares:

$$\sum_{N\leq X}^{\flat}\sum_{f\in S(N)}\Big|\sum_{n\leq X^{\beta}}^{\flat}c_n\lambda_f(n^2)\Big|^2\ll X^{\beta+\varepsilon}\sum_n|c_n|^2 \tag{3}$$

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 $GL(3)$-automorphic forms defined by Gelbart and Jacquet [G-J].

These results are also proved using duality, but in a different form. The second one, which is by far the more difficult, reduces to proving a smoothed version of

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

where $\lambda_f^{(2)}$ denotes the coefficients of the L-function of the symmetric square $f^{(2)}$ of f. We are led 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 [J-P-S]. This comparison lemma gives us the analytic continuation of L_b up to the critical line, which is sufficient to get the result. Also used is the determination of the location of the poles of the Rankin-Selberg convolution, due to Moeglin and Waldspurger [M-W], and a result of Ramakrishnan according to which two newforms with squarefree levels cannot have the same symmetric square unless they are the same.

6 Rigidity of arithmetic coefficients

The essential idea behind the techniques for giving non-trivial upper bounds for arithmetic multiplicities is to show that the general approximate orthogonality of Fourier coefficients reflected in the mean value theorems of the previous section is not compatable with rigidity properties they possess by virtue of their arithmetic nature.

In the proof of Theorem 1 this rigidity comes from the finiteness of the set of possible values of $\lambda_f(p)$ when the associated Galois representation, whose existence was proved by Deligne and Serre, is not dihedral. For example, if it is of type A_5 then it is shown for $p\not|N$ that

$$\lambda_f(p^{12})-\lambda_f(p^8)-\chi(p)\lambda_f(p^2)=1. \tag{4}$$

This relation comes from the recurrence relations satisfied by the Hecke operators and the fact that

$$\chi(p)\lambda_f(p^2) \in \left\{-1, 0, 3, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}.$$

Letting $S(A_5)$ denote the set of f of type A_5 we deduce from (1) taking $X = N$ and using positivity that

$$\sum_{f \in S(A_5)} |\sum_{n \le X} c_n \, \lambda_f(n)|^2 \ll N^{1+\varepsilon} \sum_{n \le N} |c_n|^2. \tag{5}$$

Choosing $c_{p^{12}} = 1, c_{p^8} = -1, c_{p^2} = -\chi(p)$ for primes p and all other $c_n = 0$, by means of (4) the prime number theorem gives

$$\sum_{n \le N} c_n \lambda_f(n) \sim \frac{12N^{1/12}}{\log N} \qquad \text{for } f \in S(A_5),$$

while

$$\sum_{n \le N} |c_n|^2 \sim \frac{36N^{1/12}}{\log N}.$$

Hence we get from (5) the bound

$$\#S(A_5) \ll N^{11/12+\varepsilon}.$$

Similar arguments give better bounds for the other non-dihedral forms. In particular, we get that the number of S_4–forms is $\ll N^{7/8+\varepsilon}$ and then Theorem 2 follows from the classification of quartic fields by S_4–Galois representations (see [Se1]) and Tunnell's proof of the Artin conjecture for them.

The proof of Theorem 3 makes use of the simpler Hecke relation

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

for unramified p in combination with (2) and (3). Of crucial importance is the essential independence of the level of these relations. After using positivity to restrict to modular elliptic curves, assuming the equality of just a few traces of Frobenius is enough to produce a contradiction in the approximate orthogonality of (2) and (3) by expanding their number through multiplicativity.

References

[B-S] A. Brumer and J. Silverman, *The number of elliptic curves over Q with conductor N*, Manuscripta Math. 91, 95–102 (1996).

[D-H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II.* Proc. Roy. Soc. London Ser. A 322 (1971), no. 1551, 405–420.

[D-S] P. Deligne and J–P. Serre, *Formes modulaires de poids 1,* Ann. Sci. Ec. Norm. Sup. 7 (1974) 507–530, in Serre's Collected Papers, III, 193–216.

[D-I] J.-M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms.* Invent. Math. 70 (1982/83), no. 2, 219–288.

[Du] W. Duke, *The dimension of the space of cusp forms of weight one*, Internat. Math. Res. Notices 1995, no. 2, 99–109

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

[D-K] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, appendix by D. Ramakrishnan, to appear in Inventiones Math..

[F-N-T] É. Fouvry, M. Nair and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France 120 (1992) no 4, 483-506.

[G-J] Gelbart, S. and Jacquet, H.: A relation between automorphic representations of $GL(2)$ and $GL(3)$, Ann. Sci. E.N.S 4ème série 11, 471-552 (1978).

[He] H. Heilbronn, *On the 2–classgroup of cubic fields,* in Studies in Pure Math. (L. Mirsky, ed.), Academic Press 1971, 117–119.

[J-P-S] H. Jacquet, I.I. Piatetskii-Shapiro, and J.A. Shalika, *Rankin-Selberg convolutions*, Amer. Jour. of Math. 105, 367-464 (1983).

[M-W] C. Moeglin and J.L. Waldspurger, *Pôles des fonctions L de paires pour $GL(N)$, appendice to Le spectre résiduel de $GL(n)$*, Ann. Sci. ENS (4ème série) 22, 605-674 (1989).

[P-S] R. Phillips and P. Sarnak, *Cusp forms for character varieties*, Geom. Funct. Anal. 4 (1994), no. 1, 93–118.

[S-X] P. Sarnak, and X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J. 64 (1991), no. 1, 207–227.

[Sch] W. Schmidt, *Number fields of given degree and bounded discriminant*, Columbia University Number Theory Seminar (New York, 1992). Astérisque No. 228 (1995), 4, 189–195.

[Se1] J–P Serre, *Modular forms of weight one and Galois representations,* Algebraic Number Fields, ed. by A. Fröhlich, Academic Press 1977, 193–268, in Serre's Collected Papers, III, 292–367.

[Se2] J–P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Pub. Math. I.H.E.S 54, 123-201 (1981).

[Tu] J. Tunnell, *Artin's conjecture for representations of octahedral type,* Bull. A.M.S. 5 (1981), 173–175.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141, 443-551 (1995).

[Wol] S.A. Wolpert, *Disappearance of cusp forms in special families*, Ann. of Math. (2) 139 (1994), no. 2, 239–291.

[Wo1] S. Wong, *Automorphic forms on $GL(2)$ and the rank of class groups*, Preprint.

[Wo2] S. Wong, *On the rank of ideal class groups*, Preprint.

William Duke
Department of Mathematics
Hill Center
Rutgers University
110 Frelinghuysen RD
Piscataway, NJ 08854-8019 USA
duke@math.rutgers.edu