RESEARCH STATEMENT OF LIANGYI ZHAO

I. Research Overview

My research interests mainly lie in analytic number theory and include mean-value type theorems, exponential and character sums, $L$-functions, elliptic curves and automorphic forms.

II. Research to Date

i. Low-lying Zeros of Families of $L$-functions. The distribution of the zeros near the central point $s = 1/2$ (low-lying zeros) of a family of $L$-functions is a topic of great interest in number theory, as it often is believed to encode a lot of arithmetic information (e.g. Birch-Swinnerton-Dyer conjecture which relates the order of vanishing at that point to the rank of an elliptic curve). The density conjecture of Katz and Sarnak suggests that the distribution of the low-lying zeros of a family of $L$-functions is the same as that of eigenvalues near 1 of a corresponding classical compact group. This philosophy has received much attention recently and has been confirmed for various families.

In [10], we proved an unconditional density theorem for the low-lying zeros of Hasse-Weil $L$-functions for the family of all elliptic curves. Results of this flavor were known in [19, 32, 53], all under the assumptions of various kinds of generalized Riemann Hypotheses (GRH). These assumptions were removed in our density result. If we assume GRH for these Hasse-Weil $L$-functions (and only for these $L$-functions), the unconditional density theorem implies that the average analytic rank of all elliptic curves is at most $27/14$ which is strictly less than 2. The previous result [53] that gives an average rank strictly less than 2 required additionally GRH for Dirichlet and symmetric square $L$-functions. As noted in [32], knowing the average rank is strictly less than 2 is of “paramount importance” since from this we can infer that a positive proportion of elliptic curves have algebraic ranks equal to their analytic ranks and finite Tate-Shafarevich groups, due to the celebrated works in [28, 40].

Furthermore, in a joint project with P. Gao [26], we established and extended density theorems for the low-lying zeros of families automorphic $L$-functions twisted with quadratic Dirichlet characters as well as families of cubic and quartic Dirichlet $L$-functions. Our result for the quadratic twists automorphic $L$-functions improved that in [49] under GRH and we proved in [26] unconditional results for the other families mentioned.

ii. Convolutions of $d_3(n)$ on Average. The study of the Riemann zeta-function has been one of the focal points of number theory. The estimation of the moments of the function on the critical line are among the most important and open problems in the field. This can be translated into the investigation of the shifted convolution of the divisor function $d_k(n)$ (the number of ways of writing $n$ as a product of $k$ natural numbers). Thanks to the work of A. E. Ingham [36], $k = 2$ is the only non-trivial case for which an asymptotic formula is known and the cases with $k \geq 3$ still remain unresolved conjectures.

In [3], we studied the first and second moments of the shifted convolution of the divisor function $d_3(n)$. We proved that the error terms in the asymptotic formula must be small on average, when the lengths of shift in the convolution vary over some range, confirming the relevant conjectures. The first moment result has been improved in certain ranges and extended to $d_k(n)$ for all $k \geq 3$ in [37].

iii. Primes in Polynomial Progressions on Average. The prime values of polynomials are among the central issues of number theory. It is due to Dirichlet that any linear polynomial in one variable with integer coefficients that are coprime represents infinitely many primes. No such polynomial of degree two or higher is known to represent infinitely many primes, although it has long been conjectured by Hardy and Littlewood [29], with asymptotic formulas, that any quadratic polynomial which may conceivably represent infinitely many primes indeed does. We proved in [7, 11] that the conjectured asymptotic formula holds on average, up to some uniformity constraints, for the family of quadratic polynomials of the form $n^2 + k$, verifying the afore-mentioned conjecture in this respect. From this one can immediately deduce that the Hardy-Littlewood asymptotics holds, subject to the same uniformity constraints as before, for almost all polynomials in the said family. Moreover, the result in [7] has been extended to a family of cubic polynomials in [21].
iv. Hecke Eigenvalues at Primes. The estimations of averages of arithmetic functions over the set of primes or over sparse sets are often very hard, yet they frequently are the central issues of many problems in number theory. Among the most noteworthy arithmetic functions, there are the eigenvalues of the Hecke operators on the space of cusp forms which are known to be connected to many interesting number theoretic objects. Some very surprising conjectural heuristics for the mean values over the prime numbers of these eigenvalues twisted with the function \( e(\alpha \sqrt{p}) \) has been given in [38] under some hypotheses. In [57], we studied this afore-mentioned mean value, under some very strong hypotheses. We proved some unconditional upper bound of this average. The results and methods of this paper have been extended to other context by various authors [41, 45, 46, 50].

Average values of arithmetic functions over a sparse set of prime number are even harder to fathom. Studying the prime values of polynomials of degree two or higher, as mentioned in the previous section, can be thought of as a problem of this kind. In [13], we studied the mean values of the afore-mentioned Hecke eigenvalues over the Piatetski-Shapiro primes. These are primes of the form \([n^c]\) with \( n \in \mathbb{N} \) and \( c > 1 \) fixed. Note that these are primes from a sparse set of integers. We showed that if \( 1 < c < 8/7 \), then the average of the Hecke eigenvalues satisfies a prime-number-theorem-like upper bound. Moreover, if we also assume an expected asymptotics for the square mean value of Hecke eigenvalues at these primes, then it can be inferred that Hecke eigenvalues change sign infinitely often at Piatetski-Shapiro primes. This result was generalized to primes of the form \([y(n)]\) in [14], where \( y \) is some rapidly increasing function satisfying certain properties.

v. Sato-Tate Conjecture on Average. Let \( E \) be an elliptic curve over \( \mathbb{Q} \). For any prime number \( p \) of good reduction, let \( \lambda_E(p) \) be the trace of the Frobenius morphism of \( E/\mathbb{F}_p \). Then the number of point on \( E \) modulo \( p \) is \( p + 1 - \lambda_E(p) \). The study of \( \lambda_E(p) \) lies at the center of the subject of elliptic curves. It is due to H. Hasse that \( |\lambda_E(p)| < 2\sqrt{p} \) and the Sato-Tate conjectures gives a formula for the distribution of the values of \( \lambda_E(p) \), that is, for a fixed curves \( E \) without complex multiplication, the number of primes \( p \) not exceeding \( x \) with \( \lambda_E(p) \) lying in a fixed interval can be approximated by an asymptotic formula. In works in [52], settled the Sato-Tate conjecture for all elliptic curves \( E \) over totally real fields satisfying the some mild conditions.

In [12], we proved, subject to some uniformity conditions, that the first and second moments of the error term in the Sato-Tate conjecture over a family of elliptic curves are majorized by the respective main terms divided by an arbitrary power of logarithm of the relevant parameter when the angles of the trace of Frobenius morphisms are restricted in a small range. A consequence of these results is that the asymptotics in the Sato-Tate conjecture holds for small angles and for almost all curves in the said family with error terms that are majorized by the main terms divided by an arbitrary power of logarithm. These results, with their upper bounds for the error terms, are not consequence of the work in [52] (as there is no error term in [52]) and they improve some earlier results in [39]. Moreover, these results have been improved in certain cases in [16].

vi. Bombieri-Vinogradov and Barban-Davenport-Halberstam Type Theorems. The study of the distribution of prime number is clearly at the center of number theory. Two imperfections in the study of the number of primes not exceeding \( x \) in an arithmetic progression modulo \( q \) are the size of the error term in the asymptotic formula (related to the GRH) and the uniformity of \( q \) ( \( q \) must be very small compared to \( x \)). These deficiencies would go away if one studies the primes in arithmetic progressions on average as \( q \) runs over an interval. These average results are the theorems mentioned in the title of this section and are often sufficient in applications.

In [6], we extended these above-mentioned theorems to sparse sets of moduli, among which the most interesting is the set of squares. The key input here is the large sieve for sparse sets of moduli, which is discussed in the next section. The results in [6] improve some earlier results [20, 44]. Our result has recently been improved by R. C. Baker. As an application of the Bombieri-Vinogradov theorem for square moduli, we proved, with a minorant of essentially the correct order of magnitude, the infinitude of primes of the form \( p = am^2 + 1 \) where \( a \) is square-free and \( O(p^{5/9+\varepsilon}) \). This approximates the very difficult problem that \( n^2 + 1 \) represents infinitely many primes which is equivalent to the infinitude of primes of the form \( p = am^2 + 1 \) with \( a = 1 \). It is also noteworthy that we are exhibiting primes in quite a sparse set of natural numbers, something that is often quite difficult, as mentioned before. Our result has been improved in [43].
vii. Extensions of Classical Large Sieve. It is often the case that one needs to study a family of objects (characters, $L$-functions, curves, etc.) in analytic number theory. The investigation is then often turned into the study of characters sums over same families of characters for which the large sieve inequality is an important tool. Many of the problems mentioned in the previous sections are examples of this paradigm. The large sieve was an idea originated by J. V. Linnik [42] in 1941. As it appears today, it may be thought of as an estimate on mean-values of characters sums as the moduli of the characters run over some set. As different families of objects are studied, different types of large sieves inequalities are needed. We have extended the classical result into many different contexts.

We proved in [54] a large sieve inequality for characters to square moduli. Applications of results of this kind can be found in the the problems mentioned in earlier sections. The result in question was derived from a lemma which states that the Farey fractions with square denominators are, with some discrepancy, uniformly distributed. The theorem is generalizable to higher power moduli via similar means. Conjectures were also made in [54] concerning what one should expect the best possible majorant may be. The above results have been improved by S. Baier and myself in a series of papers [2,5,8].

Large sieve results for Dirichlet characters with a fixed order are particularly useful in analytic number theory. Results for quadratic and cubic Dirichlet characters have been established in [4, 30], respectively. In a joint work with P. Gao [27], we to proved the analogous result for quartic Dirichlet characters. This will have applications to the study of orders of vanishing of various $L$-functions at special points.

In the manner of Postnikov and Gallagher [24, 47], the group of characters $G$ on $(\mathbb{Z}/q\mathbb{Z})^*$ contains the subgroup $H$ which consists of characters on $(\mathbb{Z}/q\mathbb{Z})^*$. In [55], we proved a large sieve inequality for characters in a coset of $H$ in $G$. Note that the characters in question are not necessarily primitive, a feature that the classical large sieve inequality does not possess. We obtained a result that is superior to the trivial bound in certain ranges.

We proved, in [58], the large sieve inequality for the quadratic amplitude $f(n) = an^2 + \beta n + \gamma$ with $\beta/\alpha = u/v \in \mathbb{Q}$ and $\gcd(u,v) = 1$. We obtained a non-trivial bound in certain ranges. This result can also be derived if $\beta/\alpha \notin \mathbb{Q}$, but the new estimate depends on the Diophantine nature of $\beta/\alpha$. Furthermore, we gave examples from which one can deduce that our result here is essentially optimal. This work has been further extended in [1,48].

In [56], we proved a large sieve inequality for additive characters in high dimensions when the additive orders of $k$-tuple Farey fractions in the amplitudes are restricted. It was shown that the result is the best possible. This improves the large sieve inequality used in [25] which is a consequence of a theorem in [35].

III. Future Research

i. Applications of Large Sieve. In the short term, we plan to study the applications of various type of large sieve inequalities that I have developed, especially that for quartic characters. These inequalities are known to be very useful in the proof of mean-value type theorems. Recently, we developed the large sieve inequalities for quartic symbols [27] and quartic Dirichlet characters. We aim to apply our results to establish mean values of $L$-functions twisted by both the quartic symbols and the quartic Dirichlet characters. Another possible application of our quartic large sieve would be zero density estimates for quartic $L$-functions. These estimates are often needed in the study of the moments distribution of special values of $L$-functions at the edge of the critical strip. Moreover, we plan to obtain zero density estimates for quartic Hecke $L$-functions.

ii. Distribution of Square-Full Numbers. Another project that I would like to work on in the short term is the following. A natural number $n$ is said to be square-full if $p | n$ implies $p^2 | n$. An asymptotic formula for the distributions of these numbers has been proved by Bateman and Grosswald [17] and the error in this asymptotic formula has been studied by Suryanarayana [51]. In a joint project with T. H. Chan, we aim to prove a Bombieri-Vinogradov type theorem for these square-full numbers.

iii. Bateman-Horn Conjecture on Average. Another short term project is joint with S. Baier. We aim to prove that the Bateman-Horn [18] conjecture for $k$-tuples of quadratic polynomials holds on average over...
families of quadratic polynomials. To this end, we want to use the circle method and the techniques developed in [15] on the prime \( k \)-tuples conjecture on average. The starting point will be an average result on primes in quadratic progressions which has already been established in [7].

iv. Low-Lying Zeros of Families of L-Functions. In the medium term, we aim to continue the study of the low-lying zeros of families of \( L \)-functions. It will be of great interest to improve the previously known in the density theorems, (e.g. [10]). Moreover, it would also be desirable to remove the dependency on varying GRH's in some of the existing results and develop density results for more families of \( L \)-functions. This would provide further evidence of the deep links between the zeros of \( L \)-functions and random matrix theory and confirm the Katz-Sarnak philosophy in their density conjecture, as discussed earlier. The families of \( L \)-function that we have in mind are those associated with elliptic curves with fixed torsion groups and with Dirichlet characters with fixed orders. These problems often require the use of various types of large sieve inequalities, a topic on which I have had many publications.

v. Primes in Sparse Sets of Integers. In the long term, we would like to investigate the distribution of primes in sparse sets of integers. As discussed earlier, this is among the hardest and most interesting kinds of problems in number theory. Some of the most celebrated results in this direction are the infinitude of primes of the form \( x^2 + y^2 \) [22] and the analogous statement for for \( x^2 + 2y^2 \) [31]. The most remarkable feature of these results is that they break the parity barrier. In brief, this parity problem prevented all previous uses of sieve methods to produce primes in arithmetically interesting sets of natural numbers; instead the methods gave only almost-primes (products of a uniformly bounded number of primes). The result in [31] has been subsequently generalized to certain families of cubic forms [33, 34]. We aim to generalize the result in [22] to \( Q(x, y^2) \) where \( Q(x, y) \) is a quadratic form satisfying some appropriate conditions. Moreover, we would consider this problem is finding primes of the form \( Q(x, y^2) \) as a starting point for studying primes in other sparse and arithmetically interesting sets of natural numbers, as the methods should be applicable to other situations.

REFERENCES


[56] ———, An improvement on a large sieve inequality in high dimensions, Mathematika 52 (2005), 93–100.
