OVERVIEW OF THE WORK OF KUMAR MURTY

AMIR AKBARY, SANOLI GUN AND M. RAM MURTY

1. Introduction

The role of the scholar in society is foundational for the growth of human civilization. In fact, one could argue that without the scholar, civilizations crumble. The transmission of knowledge from generation to generation, to take what is essential from the past, to transform it into a new shape and arrangement relevant to the present and to stimulate future students to add to this knowledge is the primary role of the teacher. Spanning more than four decades, Kumar Murty has been the model teacher and researcher, working in diverse areas of number theory and arithmetic geometry, expanding his contributions to meet the challenges of the digital age and training an army of students and post-doctoral fellows who will teach the future generations. On top of this, he has also given serious attention to how mathematics, and mathematical thought can be applied to dealing with large-scale economic problems and the emergence of "smart villages". We will not discuss this latter work here, nor his other work in the field of Indian philosophy. We will only focus on giving a synoptic overview of his major contributions to mathematics.

Kumar completed his PhD at Harvard University in 1982 under the direction of John Tate. After a year at the Institute for Advanced Study in Princeton, and another year at the Tata Institute for Fundamental Research in Mumbai, India, he accepted a position at Concordia University in Montreal, Canada. In 1987, he moved to the University of Toronto as Associate Professor and quickly advanced to Full Professor and later as Department Head. He has written more than 100 research papers, three books, and supervised more than a dozen doctoral students and post-doctoral fellows. His first book, "Introduction to Abelian Varieties" published by the American Mathematical Society in 1993 provides a gentle initiation into the study of this important topic in arithmetic geometry. His second book,"Non-vanishing of L-functions and applications," published by Birkhauser and written jointly with M. Ram Murty, won the 1996 Balaguer Prize. His third book, "The Mathematical Legacy of Srinivasa Ramanujan" (also written with M. Ram Murty) and published by Springer has been praised for its panoramic overview of Ramanujan's work making it accessible to non-specialists even outside of mathematics. In 1991, he was awarded the Coxeter-James Prize by the Canadian Mathematical Society. In 1995, he was awarded the E.W.R. Steacie Fellowship by the Natural Sciences and Engineering Research Council of Canada and was elected to the Royal Society of Canada. He also holds adjunct professorships at various universities in India that allow him to maintain academic contacts that foster the growth of mathematics there.

Kumar's work reflects his broad interests and covers aspects of number theory and algebraic geometry, as well as applications to problems that arise from information technology, such as data integrity, privacy and security. We will give a brief overview of his contributions to each of these areas.

2. Algebraic cycles

2.1. **The Hodge conjecture.** In his thesis work, Kumar became interested in various questions about algebraic cycles. Let X be a smooth projective algebraic variety defined over the complex numbers $\mathbb{C}$, and consider its singular cohomology $H^*(X(\mathbb{C}), \mathbb{Q})$. To any algebraic subvariety Z of X, one can associate a cohomology class $[Z] \in H^{2k}(X(\mathbb{C}), \mathbb{Q})$ where k is the codimension $\dim X - \dim Z$ of Z. By a fundamental theorem of Hodge, the complexified cohomology

$$H^*(X(\mathbb{C}), \mathbb{C}) = H^*(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{C}$$

has the property that every class in $H^k(X(\mathbb{C}), \mathbb{C})$ can be represented as a sum of differential forms which are locally of the form

$$f(z_1, \cdots, z_n) dz_{i_1} \wedge \cdots \wedge dz_{i_p} \wedge d\overline{z}_{j_1} \wedge \cdots \wedge d\overline{z}_{j_q}$$

for local coordinates $z_1, \cdots, z_n$, a C^∞ function f and for some p and q with $p + q = k$. This actually induces a decomposition into subspaces

$$H^k(X(\mathbb{C}), \mathbb{C}) \ = \ \oplus_{p+q=k} H^{p,q}$$

and it is a fact that the cohomology class $[Z]$ associated to an algebraic subvariety of codimension k has the property that in the above decomposition, it has a non-zero component only in $H^{k,k}$, that is $[Z] \in H^{2k}(X(\mathbb{C}), \mathbb{Q}) \ \cap \ H^{k,k}$. By linearity, the same is true for algebraic cycles, that is, formal linear combinations of subvarieties Z. The famous Hodge conjecture asserts that the converse is true. By a well-known theorem of Lefschetz, this is known to be true for $k = 1$.

There is a vast literature on the Hodge conjecture and all the tools that people have developed to study it, but it still remains largely mysterious and was listed as one of the millennium problems of the Clay Foundation. In his thesis (also the article [38]), Kumar studied this problem for a class of Abelian varieties, including the Jacobians of modular curves and their quotients. He showed for these varieties that every Hodge class could be expressed in terms of Hodge classes in H^2 and therefore the Hodge conjecture follows from Lefschetz's theorem.

He then defined [39] what he called the Lefschetz group (generalizing two special cases that had been studied by Ribet [55]), which is the largest connected subgroup of $\mathrm{GL}(H^1(A(\mathbb{C}), \mathbb{Q})))$ which commutes with the endomorphisms of A. He computed this group explicitly and showed that its tensor invariants (in other words, the classes in the cohomology of all powers of A which it leaves fixed) are all in the subring of Hodge classes generated by those of type $(1, 1)$ except if A has a so-called factor of type III. If A did have a factor of type III, he found that the Lefschetz group leaves invariant a Hodge class which is not known to be algebraic, but which has the property that its square can be shown to be algebraic. This gave the first evidence of a question posed

by Weil [60] whether 'imposing a Hodge class' on an Abelian variety could be shown to 'impose an algebraic class on some power of A'.

The introduction of the Lefschetz group by Kumar has led to many insights and in particular, Milne [24] has defined a more abstract version of the Lefschetz group and subsequently used it to relate the Hodge and Tate conjectures for Abelian varieties.

2.2. **The Tate conjecture.** The ℓ-adic analogue of the Hodge conjecture is due to Tate and was formulated by him in the early sixties. In this case, one replaces the singular cohomology of the Hodge conjecture, with ℓ-adic (étale) cohomology $H^*_\ell(\overline{X})$ which is a finite dimensional vector space over $\mathbb{Q}_\ell$. Here, X is now a variety defined over a global field K (for example, K could be a number field or a finite extension of $\mathbb{F}(T)$ for some finite field $\mathbb{F}$) and $\overline{X}$ is the base change of K to an algebraic closure $\overline{K}$ of K. (In fact, Tate works with the more general case of a field that is finitely generated over its prime subfield, but we will mainly discuss the case of a number field.)

The ℓ-adic cohomology has the additional structure of a Galois action. Thus, there is a representation

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(H^k_\ell(\overline{X}))$$

for each prime ℓ. There is a finite set S of primes of K so that for prime ideals $\mathfrak{p}$ of K not in S, the characteristic polynomial of Frobenius $\mathrm{Frob}_\mathfrak{p}$ has coefficients in the rational integers and is independent of ℓ. Moreover, by the Weil conjectures proved by Deligne, the eigenvalues of $\mathrm{Frob}_\mathfrak{p}$ have complex absolute value $(\mathbb{N}\mathfrak{p})^{k/2}$. We can, therefore, consider the 'twist' $H^{2k}_\ell(\overline{X})(k)$ in which essentially the Galois action has been normalized so that the eigenvalues of Frobenius have absolute value 1. Then the ℓ-adic cycle class map associates to each subvariety Z of X of codimension k which is defined over K, a class

$$c_\ell(Z) \in H^{2k}_\ell(\overline{X})(k)^{\mathrm{Gal}(\overline{K}/K)}.$$

The Tate conjecture asserts that every element on the right hand side arises in this way, namely as a linear combination of classes of subvarieties with a representative defined over K.

In the case that X is an Abelian variety, Faltings proved it for $k = 1$. But unlike the Hodge conjecture, for general X, this is open even for $k = 1$. Kumar's thesis work also proves the Tate conjecture (in all codimensions) for a large class of Abelian varieties (including those that are quotients of the Jacobians of modular curves) assuming that we know it for $k = 1$ (and as stated above, Faltings' result assures us that we do know it in that case).

2.3. **Shimura varieties and period relations.** A few years later, Kumar started to collaborate with Dinakar Ramakrishnan on the Tate conjecture for some Shimura varieties. In particular, they considered the case of Hilbert modular surfaces. This had been studied by Oda [52] and by Harder, Langlands and Rapaport [16]. Thus, they were considering surfaces X which are obtained by taking a smooth compactification of quotients of the product of two upper half planes by a congruence subgroup of $\mathrm{SL}_2(\mathcal{O})$ where $\mathcal{O}$ is the ring of integers of a real quadratic field. Their work left open the case of so-called "complex multiplication cycles". Dinakar and Kumar were able to settle this

case [46] using period relations. It was also independently settled by Klingenberg using a different method involving L-indistinguishability. The approach of Kumar and Dinakar seems to be capable of proving the Tate conjecture in many other cases and we believe they are working on this project now.

2.4. **Reduction of Tate cycles modulo a prime.** In 2008, with his then doctoral student V. Patankar (currently a faculty member at Jawaharlal Nehru University, New Delhi), Kumar formulated a conjecture [47] for a simple or absolutely simple Abelian variety over a number field to remain simple when reduced modulo a density one set of primes (or a set of primes of positive density). This question of reductions of simple Abelian varieties is a very natural one but it seems not to have been considered before this paper. It can be viewed as the geometric analogue of the classical problem of how often an irreducible polynomial with integer coefficients remains irreducible modulo a prime p, which of course is the foundational question of algebraic number theory. This question can actually be interpreted in terms of the appearance of "extra" cycles on reduction modulo a prime, and in paper [48], Kumar and Patankar raised a related and more general question about Tate cycles on Abelian varieties, namely whether there is a set of primes of density one for which the ring of Tate cycles does not grow when the Abelian variety is reduced modulo a prime. In [48], they prove that this is the case for Abelian varieties with complex multiplication. And in [50] and [51] with postdoctoral fellow Y. Zong (currently at Shantou University in China), they related the original problem to one about monodromy and roots and weights.

3. L-functions

Another theme that Kumar has been very active in is various aspects of L-functions. These objects occupy a central position in number theory and seem to play the role of gatekeepers to secret knowledge.

3.1. **Sato-Tate conjecture.** As graduate students, both Kumar and Ram were interested in the Sato-Tate conjecture. In its original form, it was a conjecture about the "angles of Frobenius" associated to an elliptic curve over the rationals. To such a curve E and for any prime p where E has good reduction, one can count the number of points in $E(\mathbb{F}_p)$ and show that it has the form $p+1-(\alpha_p+\overline{\alpha}_p)$ where α_p is a complex number of absolute value $p^{\frac{1}{2}}$. Thus, we can write

$$\alpha_p = p^{\frac{1}{2}} e^{i\theta_p}$$

for some angle $\theta_p \in [0,\pi]$. The Sato-Tate conjecture predicted how the angles θ_p are distributed in the interval $[0,\pi]$. In particular, if E does not have complex multiplication, then the conjecture stated that for an interval $[a,b] \subseteq [0,\pi]$, we have

$$\#\{p \leq x,\ a \leq \theta_p \leq b\} \ \sim\ \left(\int_a^b \frac{2}{\pi}\sin^2\theta d\theta\right)\pi(x).$$

Interestingly, Tate arrived at this prediction as a result of his conjectures on algebraic cycles. Serre considered the family of L-functions $\{L_k\}$ given by an Euler product

$$L_k(s) \;=\; \prod_p L_{k,p}(s)$$

which for all but a finite number of p is given by

$$L_{p,k}(s) \;=\; \prod_{j=0}^{k} \left(1 - \frac{e^{i(2j-k)\theta_p}}{p^s}\right)^{-1}.$$

Then the L_k (for $0 \leq k \in \mathbb{Z}$) are defined, analytic and non-zero for $\Re(s) > 1$. Serre showed [57] that if all of the L_k have an analytic continuation as entire functions for all s (apart possibly for a pole at $s = 1$ for $L_0(s)$), and are non-vanishing on the line $\Re(s) = 1$, then the Sato-Tate conjecture follows. Kumar and Ram were fascinated by this because it was a new kind of prime number theorem which depended on the non-vanishing of infinitely many L-functions, unlike the classical prime number theorem which was essentially equivalent to the non-vanishing of the (single) Riemann zeta function on the line $\Re(s) = 1$.

Serre's result was later refined by Ogg [54] to show that continuation to the left of $\Re(s) = \frac{1}{2}$ would suffice and the non-vanishing would follow from this. As a graduate student, Kumar showed [37] that continuation to $\Re(s) = 1$ would suffice. Later, he showed [44] that if we just had continuation to the *point* $s = 1$ (in other words, if one can extend the functions $L_k(s)$ to a neighbourhood of $s = 1$, then the "weak Sato-Tate conjecture" would follow, namely that

$$\sum_{p \leq x, \theta_p \in [a,b]} \frac{\log p}{p} \;\sim\; \left(\int_a^b \frac{2}{\pi} \sin^2\theta d\theta\right) \log x.$$

The Sato-Tate conjecture is now a theorem thanks to the ground-breaking work of M. Harris, R. Taylor, L. Clozel, N. Shepherd-Barron, Barnet-Lamb and Geraghty. However, the question of the automorphy of the L_k remains. Interestingly, the conventional wisdom was that the Sato-Tate conjecture would be proved by establishing the automorphy of all of the L_k, but the published proof manages to avoid that. In recent joint work, Kumar and Ram showed [34] that the Sato-Tate conjecture, together with another hypothesis (namely the automorphy of $\pi \otimes \pi'$ where π is an arbitrary automorphic representation and π' is a $GL(2)$ automorphic representation), can actually be used to *deduce* the automorphy of the L_k.

3.2. **Artin L-functions.** A number of papers by Kumar deal with the analytic properties of Artin L-functions. Given a Galois extension K/F of number fields and a representation ρ of $\mathrm{Gal}(K/F)$ on a complex finite-dimensional vector space V, we can define the Artin L function $L(s, \rho, F)$ as an Euler product over primes of F. More precisely, it is given by

$$L(s, \rho, F) \;=\; \prod_{\mathfrak{p}} \det(I - (\mathrm{Frob}_{\mathfrak{p}} | V^{I_{\mathfrak{p}}})(N\mathfrak{p})^{-s})^{-1}$$

where $I_{\mathfrak{p}}$ denotes an inertia group of any prime of K above $\mathfrak{p}$ and $V^{I_{\mathfrak{p}}}$ denotes the subspace of V fixed by such an inertia group. This Euler product converges for $\Re(s) > 1$ and by theorems of Brauer, Hecke-Tate and class field theory, $L(s, \rho, F)$ has a meromorphic continuation for all s.

Artin's holomorphy conjecture (AC) asserts that in fact $L(s, \rho, F)$ is a holomorphic function of s apart from a possible pole at $s = 1$ of order equal to the multiplicity of the trivial representation in ρ. A result of Stark [59] asserts that $L(s, \rho.F)$ is analytic at any point $s = s_0$ at which the Dedekind zeta function $\zeta_K(s)$ of K has a zero of order ≤ 1. This was extended by Kumar and Richard Foote [12] to show that if K/F has odd degree, then $L(s, \rho, F)$ is analytic at any point $s = s_0$ where $\zeta_K(s)$ has a zero of order $\leq p_2 - 2$ where p_2 is the second largest prime divisor of $[K : F]$. This and other results are reviewed in the survey paper [11].

The Brauer-Siegel theorem asserts that as K runs through a sequence of number fields with the property that

$$\frac{1}{[K : \mathbb{Q}]} \log |d_K| \longrightarrow \infty$$

we have

$$\log \operatorname{res}_{s=1} \zeta_K(s) \longrightarrow 0$$

or equivalently,

$$\frac{\log h_K R_K}{\log |d_K|} \longrightarrow \frac{1}{2}.$$

Here, h_K and R_K denote the class number and regulator (respectively) of K. The Brauer-Siegel theorem is ineffective in general, and the original motivation of Stark's paper was to show that there are many cases in which it can be made effective. The ineffectivity occurs because of possible zeros of $\zeta_K(s)$ near $s = 1$. More precisely, if it can be shown that there are no zeros in the region

$$\Re(s) \geq 1 - \frac{1}{4 \log |d_K|}, \ |\Im(s)| \leq \frac{1}{4 \log |d_K|}$$

then, the theorem can be made effective. In particular, if K is a CM-field, and $\zeta_K(s)$ could be shown not to have zeros in this box, then Stark observed that one could get effective lower bounds for the class number of K. This technique was refined by Odlyzko in several papers.

In two beautiful papers [40], [41], Kumar showed that if we are working with CM fields which have solvable normal closure, then one can actually deal with the zeros near $s = 1$ and get good effective lower bounds for the minus part of the class number of the CM field.

3.3. **Chebotarev density theorem and its applications.** In his undergraduate thesis written at Carleton University, Kumar studied the distribution of primes in arithmetic progressions. He was able to improve a result of Turán on the least prime in an arithmetic progression. Turán had showed that if we assume the Lindelöf hypothesis for Dirichlet L-functions, then there is a prime in any arithmetic progression modulo q which is $\mathbf{O}(q^{4+\epsilon})$ for any $\epsilon > 0$. Kumar showed that in fact, unconditionally, this bound

could be improved to $\mathbf{O}(q^{2+\epsilon})$. This was never published but is mentioned (in a more general form) at the end of a long paper with Ram Murty [30].

The problem of distribution of primes in number fields has always been of great interest to both Kumar and Ram. The analogue of the prime number theorem for arithmetic progressions in a general number field is the Chebotarev density theorem. Ram was inspired by a course that Serre gave at Harvard on effective forms of the Chebotarev density theorem and told Kumar about it as well. A few years later, they were able to show [31] that Serre's estimates could be improved if one knew the Artin holomorphy conjecture AC. They then used this version to approach the Lang-Trotter conjecture and by some use of sieve methods and group theory, they were able to bypass the hypothesis of AC, and improve Serre's results on this problem.

The interplay between problems involving prime numbers and analytic aspects of L-functions together with their algebraic interrelationships is a recurrent theme in number theory that is still not understood very well. These questions bring to the foreground the importance of the study of this interplay.

3.4. **Non-vanishing of L-functions.** Starting with classical Dirichlet L-functions, it is a conjecture of Chowla that for a Dirichlet character (over the rationals), the associated L-function $L(s,\chi)$ does not vanish at $s=\frac{1}{2}$.

Note that if we look at the analogous question over number fields, then there are finite order Hecke characters ψ so that $L(\frac{1}{2},\psi)=0$. This happens because the vanishing is forced by a root number condition. So the general conjecture might be that the L function associated to a finite order Hecke character over any number field should not vanish unless forced to do so by the root number in the functional equation. We are far from being able to prove such an assertion.

Kumar and Balasubramanian looked at this question (over the rationals) and proved [2] that for any prime q, there is a positive proportion of characters χ modulo q so that $L(\frac{1}{2},\chi)\neq 0$. More recently, Iwaniec-Sarnak [20] (as part of a larger work) have obtained a better numerical value of the proportion. Moreover, Soundararajan [58] has proved that a large positive proportion of Dirichlet L-functions corresponding to real characters are non-vanishing at $s=\frac{1}{2}$.

Over the years, Kumar and Ram wrote more than 30 papers together. Their collaboration was (and is) effective on many levels. Perhaps their most intense collaboration was on the so-called Kolyvagin hypothesis. Kolyvagin had discovered a method to prove the finiteness of the Shafarevitch-Tate group of a modular elliptic curve E, provided the rank of $E(\mathbb{Q})$ is ≤ 1 and there is a quadratic twist E_D of E with the property that the L-function $L(E_D,s)$ has a simple zero at $s=1$ (the center of the critical strip). Assuming $L(E,1)\neq 0$, Kumar and Ram were able to prove [32] the existence of such a quadratic twist by showing that there is a constant $c\neq 0$ and a $\delta>0$ for which

$$\sum_{\substack{0<-D\leq x\\ D\equiv 1 \bmod 4N}} L'(E_D,1) \;=\; cx\log x + \mathbf{O}(x(\log x)^{1-\delta}).$$

In particular, we must have $L'(E_D,1)\neq 0$ for infinitely many D. This corollary was also proved by Bump, Friedberg and Hoffstein [3] by using other methods.

As was pointed out in [32], the theorem is really one about modular forms. Let f be a newform of weight 2 for $\Gamma_0(N)$ with the property that the L-function of f does not vanish at $s = 1$ (the center of the critical strip). Then one gets an asymptotic formula for the average of $L'(f, \chi_D, 1)$. Later, Kumar was able to refine the methods to get an asymptotic formula for the (weighted) average values of $L(f, \chi_D, 1)$ and thus deduce the existence of quadratic twists $f \otimes \chi_D$ for which $L(f \otimes \chi_D, 1) \neq 0$. In this work, f is allowed to be a form for $\Gamma_1(N)$ and in particular, have non-trivial Nebentypus character. Under these hypotheses, the asymptotic formula

$$\frac{1}{x}\int_1^x \sum_{\substack{|D|\leq t \\ D\equiv a \bmod 8N}} L(f, \chi_D, 1)dt \;=\; C(f)x + \mathbf{O}(x(\log x)^{-\delta})$$

is proved. Thus, the non-vanishing result extends a well-known result of Waldspurger which applies in the case of trivial Nebentypus character. This work appeared in the joint monograph [33]. This monograph was probably their second most intense collaboration. They wrote this monograph during one term when they were both at the Institute for Advanced Study. They were honoured and delighted when it was awarded the Balaguer Prize.

3.5. **Distribution of Euler-Kronecker constants.** There is a vast literature on the distribution of special values of L-functions. These values encode certain arithmetic and geometric features of related number fields and varieties. Notable examples are the Dirichlet class number formula and the Birch and Swinerton-Dyer conjectures which respectively deal with the values at 1 and 1/2 of the L-functions. For a number field K, Ihara [17] has introduced a new invariant γ_K, called the Euler-Kronecker constant, which is closely related to the values of the logarithmic derivative of L-functions at 1. More precisely,

$$\gamma_K = \lim_{s\to 1^+}\left(\frac{\zeta_K'(s)}{\zeta_K(s)} + \frac{1}{s-1}\right),$$

where $\zeta_K(s)$ is the Dedekind zeta function of K. In [17], Ihara relates the negativity of γ_K with the size of the set of primes with small norms of the number field K.

In past few years, Kumar has extensively investigated the size of γ_K for certain families of number fields. In [26], Mariam Mourtada and Kumar proved an Ω-result for the Euler-Kronecker constants of quadratic number fields. More precisely, they showed that as K varies over the family of quadratic fields $\mathbb{Q}(\sqrt{D})$, one gets

$$\gamma_K = \Omega(\log\log|D|).$$

This can be considered analogous to a classical Ω-result of Chowla [5] on the values of Dirichlet L-functions at 1. Further results on the distribution of γ_K for quadratic fields was obtained by Lamzouri [23]. For a quadratic field $\mathbb{Q}(\sqrt{D})$, we have

$$\gamma_K = \gamma + \frac{L'}{L}(1, \chi_D),$$

where γ is the Euler constant and $\chi_D(n) = (D/n)$ is the Kronecker symbol. In another joint work [27], Mariam Mourtada and Kumar established, under the assumption of GRH, the existence of a distribution function for the values of $\frac{L'}{L}(\sigma, \chi_D)$, where $\sigma > 1/2$ and D varies over the fundamental discriminants. This result should be compared with

a theorem of Chowla and Erdös [6] on the distribution of the values of $L(\sigma, \chi_D)$ for $\sigma > 3/4$ and a result of Elliott [9] on the value-distribution of $\log L(1, \chi_D)$.

In [18], Ihara studied the Euler-Kronecker constants $\gamma_m := \gamma_{\mathbb{Q}(\zeta_m)}$ for the family of cyclotomic fields $\mathbb{Q}(\zeta_m)$, and, based on numerical evidence, made several conjectures on the size of γ_m. Notably he conjectured that for q prime and given $\epsilon > 0$, the inequality

$$\left(\frac{1}{2} - \epsilon\right) \log q < \gamma_q < \left(\frac{3}{2} + \epsilon\right) \log q \tag{1}$$

holds for all sufficiently large primes q. Kumar obtained several results related to the above conjecture. In a joint work with Ihara and M. Shimura [19], they proved unconditionally that $|\gamma_q| = \mathbf{O}_\epsilon(q^\epsilon)$. Moreover, under the assumption of GRH they proved that the estimation can be improved to $|\gamma_q| = \mathbf{O}((\log q)^2)$. From (1) one predicts that $|\gamma_q|$ has order $\log q$. In [45], Kumar proved that this is the case on average over q. More precisely, he established that

$$\frac{1}{\pi^*(Q)} \sum_{\frac{1}{2}Q < q \leq Q} |\gamma_q| \ll \log Q,$$

where $\pi^*(Q)$ denotes the number of primes bigger than $\frac{1}{2}Q$ and not exceeding Q.

In [13], the authors showed that the lower bound in the conjectural inequality (1) is inconsistent with the prime k-tuple conjecture of Hardy and Littlewood. More precisely, they proved that the Hardy-Littlewood conjecture establishes the existence of infinitely many negative values of γ_q. In spite of possible negativity of γ_q, in [28], Mariam Mourtada and Kumar showed that $\gamma_q / \log q$ cannot be smaller than -11 for a positive proportion of primes, in other words they proved that $\gamma_q > -11 \log q$ on a set of primes of density 1.

3.6. **Spaces of L-functions.** Recently, Kumar has been thinking about spaces of L-functions. There is the well-known Selberg class introduced in [56] which captures most of the L-functions that 'arise in nature'. Ram had explained in [29] that Selberg's conjectures had many important consequences including Artin's holomorphy conjecture (AC) and in [36] it was shown that Selberg's conjectures could be seen as a pair correlation conjecture in the Selberg class.

However, as important as this class is, one often feels the need to go outside the class, especially when one has to perform algebraic operations on L-functions. For example, the sum of two elements in the Selberg class is in general not in the class. Kumar introduced in [43] a larger class which he called the Lindelöf class, which forms a natural ring. Elements of this class do not necessarily have a functional equation or an Euler product, but are defined in terms of certain growth requirements. The original definition was modified a little in Kumar's joint work with his student Anup Dixit [7] and properties of the new class were studied in Anup's thesis [8].

4. Cryptography and further applications

Starting in about 2001, Kumar has considered various ways in which number theory and algebraic geometry could be applied to problems that arise from Information Technology. This is the focus of the GANITA Lab that he started at that time. He has

published about 20 papers in data integrity, security and privacy and has two patents. Moreover, a number of his students (Nicolas Theriault, Vijay Patankar, Nataliya Laptyeva, Catalina Anghel, Robby Burko, Aaron Chow and William George) have written theses which explicitly or implicitly were motivated by problems that arise from one of these areas.

4.1. **Koblitz's conjecture.** His work with Ali Miri [25] uses the Selberg lower bound sieve method to address a conjecture of Koblitz. Given an elliptic curve E over the rationals, Koblitz had conjectured that the number of primes $p \leq x$ for which the number of points in $E(\mathbb{F}_p)$ is prime is asymptotic to

$$C_E x(\log x)^{-2}$$

for some non-zero constant C_E. Koblitz's conjecture has relevance for cryptography because one can build a public-key cryptosystem using the group of points $E(\mathbb{F}_p)$. However, the security of such a system is diminished when the order of the group is not prime, or nearly prime. Koblitz's conjecture would tell us that we can begin with an elliptic curve over the rationals and reduce it modulo many primes to get groups suitable for cryptography.

Kumar and Ali Miri considered the case where E does not have complex multiplication and showed assuming the GRH (Riemann Hypothesis for Dedekind zeta functions) that there are $\gg x(\log x)^{-2}$ primes $p \leq x$ for which the cardinality of $E(\mathbb{F}_p)$ has at most 16 prime divisors. This was the first result of its kind, and other authors have now reduced the number 16.

In a related theme, Kumar, along with Amir Akbary and Dragos Ghioca, studied the size of the reduction mod p of subgroups of the group of rational points $E(\mathbb{Q})$ as p varies. Under the assumption of GRH, they showed [1] that for a set of primes of density 1, the size is greater than $p/f(p)$ for any slowly increasing function f provided the Mordell-Weil rank of $E(\mathbb{Q})$ is greater than 18. If in addition the Artin holomorphy conjecture is assumed, the rank need only be greater than 10. They derive unconditional results for CM elliptic curves. In this case one needs the rank to be greater than 5. These results are the analogues for elliptic curves of results obtained by Erdös and Ram [10]. We should also mention the ground-breaking work of Rajiv Gupta and Ram [15].

The elliptic curve discrete logarithm problem is of great interest for those who work with public key cryptosystems involving elliptic curves. The problem says that given an elliptic curve E over a finite field $\mathbb{F}$ and given two points $P, Q \in E(\mathbb{F})$ with the property that Q is in the subgroup generated by P, we have to determine the integer h so that $Q = hP$. If the parameters of the curve are chosen correctly (for example, the cardinality of $\mathbb{F}$ has to be sufficiently large and E should avoid some properties, such as being supersingular or having 'trace 1', or having a group order which is not nearly prime), then we expect that the discrete logarithm will take approximately $\mathbf{O}(|\mathbb{F}|^{\frac{1}{2}})$ steps to solve. (See [53, 11.6.6 and 11.6.7, pp.396-397] for a discussion of this.)

4.2. **Factorization and modular forms.** Some years ago, Kumar considered what he called a variant of Lehmer's conjecture. There is a conjecture of Lehmer that asserts that $\tau(p) \neq 0$ for any prime p, where τ is the Ramanujan τ-function defined by

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} \;=\; \sum_{n=1}^{\infty}\tau(n)q^n.$$

Lehmer's conjecture is in fact equivalent to the assertion that $\tau(n) \neq 0$ for any integer $n \geq 1$.

A related conjecture is to ask whether we can have $\tau(p) \equiv 0 \bmod p$. In fact, this can happen and the list of known values of p is $\{2, 3, 5, 7, 2411\}$. It is not known if there are infinitely many such primes. The variant that Kumar studied is to ask about the greatest common divisor of n and $\tau(n)$. In [42] he showed that except for a set of n of density zero, there is always a common factor between n and $\tau(n)$. The estimate he obtained for the number of exceptional $n \leq x$ was $x/\log\log\log x$.

In these calculations, we can replace the τ function with the Fourier coefficients of a Hecke eigenform. Sanoli Gun and Kumar [14] considered the case of an eigenform f of weight 2 with Fourier expansion

$$f(z) = \sum_{n\geq 1} a_f(n)q^n$$

that has complex multiplication and showed that

$$\#\{n \leq x, (n, a_f(n)) = 1\} \;=\; (c_f + \mathbf{o}(1))\frac{x}{\sqrt{(\log x)(\log\log\log x)}},$$

where c_f is a positive constant. This result can be interpreted as meaning that with probability 1, n will have a factor in common with $a_f(n)$. Thus, we might look to the computation of Fourier coefficients as a way of factoring integers. However, the proof of the above results shows that it is generally only small factors that appear in the gcd of n and $a_f(n)$. The case of complex multiplication forms f of weight larger than 2 was considered in the thesis [21] of Kumar's student, Nataliya Laptyeva.

Another approach to the question of using modular forms for factorization was explored in the thesis of Kumar's student, Aaron Chow [4].

4.3. **Explicit arithmetic on Abelian varieties.** A public key cryptosystem can be built using the group of points on an Abelian variety over a finite field provided explicit arithmetic can be done efficiently and we have good point counting algorithms. Both of these have been extensively studied for elliptic curves, and also for Jacobians of curves. However, the situation for a general Abelian variety is different, in that we have to develop methods that don't rely so much on explicit equations.

Kumar and Pramath Sastry considered this problem, and they have developed an explicit method to do arithmetic on Abelian varieties over finite fields using an embedding of the Abelian variety into a Grassman variety (as opposed to a projective embedding). This work [49] is in the spirit of K. Khuri-Makdisi [22] who showed how to develop explicit arithmetic on the Jacobian of a curve using Grassmanians. The case of a general Abelian variety (that is, one which is not necessarily a Jacobian) is much more involved and relies

more on geometric tools, though the final result is expressed combinatorially. This work seems to be in its early stages and the calculations have still to be refined to make them more practical and efficient. On the other hand, it is not clear that discrete log based cryptosystems using Abelian varieties will be secure given the evolving knowledge about attacks on such varieties as described in various papers of G. Frey, as well as quantum attacks. However, it is possible that an isogeny-based cryptosystem might be secure.

Independently of the security, though, is that the methods developed by Kumar and Pramath seem to be of interest in the study of Abelian varieties even from a purely mathematical point of view. All of this is clearly something to be further investigated.

References

[1] A. Akbary, D. Ghioca, and V. Kumar Murty, Reductions of points on elliptic curves, *Math. Annalen,* **347**(2010), no. 2, 365–394.

[2] R. Balasubramanian and V. Kumar Murty, Zeros of Dirichlet L-functions, *Ann. Scient. Ecole Norm. Sup.*, **25**(1992), 567–615.

[3] D. Bump, S. Friedberg and J. Hoffstein, Non-vanishing theorems for L-functions of modular forms and their derivatives, *Invent. Math.*, **102**(1990), 543–618.

[4] A. Chow, Applications of Fourier coefficients of modular forms, PhD Thesis, University of Toronto, 2015.

[5] S. Chowla, Improvement of a theorem of Linnik and Walfisz, *Proc. London Math. Soc. (2)* **50**(1949), 423–429.

[6] S. Chowla and P. Erdös, A theorem on the distribution of the values of L-functions, *J. Indian Math. Soc. (N.S.)* **15**(1951), 11–18.

[7] A. Dixit and V. Kumar Murty, The Lindelöf class of L-functions II, *preprint* 2017.

[8] A. Dixit, On the Lindelöf class of L-functions, PhD Thesis, University of Toronto, 2018.

[9] P. D. T. A. Elliott, The distribution of the quadratic class number, *Litovsk. Mat. Sb.* **10**(1970), 189–197.

[10] P. Erdös and M. Ram Murty, *On the order of a* (*mod p*). Number theory (Ottawa, ON, 1996), 87–97, CRM Proc. Lecture Notes, 19, Amer. Math. Soc., Providence, RI, 1999.

[11] R. Foote, H. Ginsburg and V. Kumar Murty, On Heilbronn characters, *Bull. Amer. Math. Soc.*, **52**(2015), 465–496.

[12] R. Foote and V. Kumar Murty, Zeros and poles of Artin L-functions, *Math. Proc. Cambridge Phil. Soc.*, **105**(1989), 5–11.

[13] K. Ford, F. Luca, and P. Moree, Values of the Euler ϕ-function not divisible by a given odd prime, and the distribution of Euler-Kronecker constants for cyclotomic fields, *Math. Comp.* **83**(2014), 1447–1476.

[14] S. Gun and V. Kumar Murty, A variant of Lehmer's conjecture II: The CM case, *Canadian J. Math.*, **63**(2011), 298–326.

[15] R. Gupta and M. Ram Murty, Primitive points on elliptic curves, *Compositio Math.* **58**(1986), 13–44.

[16] G. Harder, R. Langlands and M. Rapaport, Algebraische Zyklen auf Hilbert-Blumenthal-Flchen. (German) [Algebraic cycles on Hilbert-Blumenthal surfaces] *J. Reine Angew. Math.*, **366**(1986), 53–120.

[17] Y. Ihara, On the Euler-Kronecker constants of global fields and primes with small norms, Algebraic geometry and number theory, *Progr. Math.* **253**(2006), 407–451.

[18] Y. Ihara,The Euler-Kronecker invariants in various families of global fields, Arithmetics, geometry, and coding theory (AGCT 2005), *Sémin. Congr.* **21**(2010), 79–102.

[19] Y. Ihara, V. Kumar Murty, M. Shimura, On the logarithmic derivatives of Dirichlet L-functions at $s = 1$, *Acta Arith.* **137**(2009), 253–276.

[20] H. Iwaniec and P. Sarnak, The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros, *Israel J. Math.*, **120**(2000), 155–177.

[21] N. Laptyeva, A variant of Lehmer's conjecture in the CM case, Ph. D Thesis, University of Toronto, 2013.
[22] K. Khuri-Makdisi, Linear algebra algorithms for divisors on an algebraic cuve, *Math. Comp.*, **73**(2003), 333–357.
[23] Y. Lamzouri, The distribution of Euler-Kronecker constants of quadratic fields, *J. Math. Anal. Appl.* **432**(2015), 632–653.
[24] J. Milne, Lefschetz classes on abelian varieties, *Duke Math. J.*, **96**(1999), 639–675.
[25] S. Ali Miri and V. Kumar Murty, An application of sieve methods to elliptic curves, in: INDOCRYPT 2001, eds. C. Pandu Rangan and C. Ding, pp. 91–98, *Lecture Notes in Computer Science* 2247, Springer, Berlin, 2001.
[26] M. Mourtada and V. Kumar Murty, Omega theorems for $\frac{L'}{L}(1, \chi_D)$, *Int. J. Number Theory* **9**(2013), 561–581.
[27] M. Mourtada and V. Kumar Murty, Distribution of values of $L'/L(\sigma, \chi_D)$, *Mosc. Math. J.* **15**(2015) 497–509.
[28] M. Mourtada and Kumar Murty, On the Euler Kronecker constant of a cyclotomic field, II, SCHOLAR—a scientific celebration highlighting open lines of arithmetic research, *Contemp. Math.* **655** (2015), 143–151.
[29] M. Ram Murty, Selberg's conjectures and Artin L-functions, *Bull. Amer. Math. Soc.*, **31**(1994), 1–14.
[30] M. Ram Murty and V. Kumar Murty, A variant of the Bombieri-Vinogradov theorem, in: *Number Theory*, Volume 7, CMS Conference Proceedings, ed. H. Kisilevsky et. al., pp 243–272, Amer. Math. Soc, Providence, 1987.
[31] M. Ram Murty, V. Kumar Murty and N. Saradha, Modular forms and the Chebotarev density theorem, *Amer. J. Math.*, **110**(1988), 253–281.
[32] M. Ram Murty and V. Kumar Murty, Mean values of derivatives of modular L-series, *Annals of Math.*, **133**(1991), 447–475.
[33] M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and applications*, Progress in Mathematics Volume 157, Birkhauser, Basel, 1997.
[34] M. Ram Murty and V. Kumar Murty, Some remarks on automorphy and the Sato-Tate conjecture, in: Advances in the theory of numbers, eds. A. Alaca et. al., pp. 159–168, Fields Institute Communications Volume 77, Springer, New York, 2015.
[35] M. Ram Murty, V. Kumar Murty and P. J. Wong, Pair correlation and the Chebotarev density theorem, *J. Ramanujan Math. Soc.*, to appear.
[36] M. Ram Murty and A. Perelli, The pair correlation of zeros of functions in the Selberg class, *Internat. Math. Res. Notices*, 1999, pp. 531–545.
[37] V. Kumar Murty, On the Sato-Tate conjecture, in: *Number Theory related to Fermat's Last Theorem*, ed. N. Koblitz, pp. 195-205, Birkhauser-Verlag, Boston, 1982.
[38] V. Kumar Murty, Algebraic cycles on Abelian varieties, *Duke Math. J.*, **50**(1983), 487–504.
[39] V. Kumar Murty, Exceptional Hodge classes on certain Abelian varieties, *Math. Annalen*, **268**(1984), 197–206.
[40] V. Kumar Murty, Stark zeros in certain towers of fields, *Math. Res. Letters*, **6**(1999), 511–520.
[41] V. Kumar Murty, Class numbers of CM-fields with solvable normal closure, *Compositio Math.*, **127**(2001), 273–287.
[42] V. Kumar Murty, A variant of Lehmer's conjecture, *J. Number Theory*, **123**(2007), 80–91.
[43] V. Kumar Murty, The Lindelöf class of L-functions, in: *L-functions*, eds. L. Weng and M. Kaneko, pp. 165–174, World Scientific, 2007.
[44] V. Kumar Murty, On the Sato-Tate conjecture II, in: *On Certain L-functions: A volume in honour of F. Shahidi*, Clay Mathematics Proceedings Volume 43, pp. 471–482, Amer. Math. Soc., Providence,, 2011.
[45] V. Kumar Murty, The Euler-Kronecker constant of a cyclotomic field, *Ann. Sci. Math. Québec* **35**(2011), 239–247.
[46] V. Kumar Murty and D. Ramakrishnan, Period relations and the Tate conjecture for Hilbert modular surfaces, *Invent. Math.*, **89**(1987), 319–345.

[47] V. Kumar Murty and V. Patankar, Splitting of Abelian varieties, *Intl. Math. Res. Not.*, **2008**(2008), 27 pages, doi: 10.1093/imrn/rnn033, published May 6, 2008.
[48] V. Kumar Murty and V. Patankar, Tate cycles on Abelian varieties with complex multiplication, *Canadian J. Math.*, **67**(2015), 198–213.
[49] V. Kumar Murty and Pramathanath Sastry, Explicit arithmetic on Abelian varieties, *this volume.*
[50] V. Kumar Murty and Y. Zong, Splitting of Abelian varieties, *Math. of Communication*, **8**(2014), 511–519.
[51] V. Kumar Murty and Y. Zong, Elliptic minuscule pairs and splitting of Abelian varieties, *Asian J. Math.*, **21**(2017), 287–336.
[52] T. Oda, Periods of Hilbert modular surfaces, Progress in Mathematics Volume 19, Birkahauser, Boston, 1982.
[53] A. Odlyzko, *Discrete logarithms over finite fields*, in: Handbook of Finite Fields, eds. G. L. Mullen and D. Panario, pp. 393-401, CRC Press, Boca Raton, USA, 2013
[54] A. Ogg, A remark on the Sato-Tate conjecture, *Invent. Math.*, **9**(1969/1970), 198–200.
[55] K. Ribet, Hodge classes on certain types of abelian varieties, *Amer. J. Math.*, **105**(1983), 523–538.
[56] A. Selberg, Old and new conjectures and results about a class of Dirichlet series, in: *Collected Papers Volume 2*, pp. 57–63, Springer, New York, 1991.
[57] J. -P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, New York-Amsterdam, 1968.
[58] K. Soundararajan, Nonvanishing of quadratic Dirichlet L-functions at $s = 1/2$, *Annals of Math.*, **152**(2000), 447–488.
[59] H. M. Stark, Some effective cases of the Brauer-Siegel theorem, *Invent. Math.*, **23**(1974), 135–152.
[60] A. Weil, Abelian varieties and the Hodge ring, in: *Collected Papers*, Volume III, pp. 421–429, Springer, Berlin, 1980.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, Canada
E-mail address: amir.akbary@uleth.ca

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada
E-mail address: murty@mast.queensu.ca

Institute for Mathematical Sciences, Chennai, India
E-mail address: sanoli@imsc.res.in