

# L-FUNCTIONS AND RANDOM MATRIX THEORY

The American Institute of Mathematics

This is a hard-copy version of a web page available through <http://www.aimath.org>  
Input on this material is welcomed and can be sent to [workshops@aimath.org](mailto:workshops@aimath.org)  
Version: Thu Jun 17 06:21:12 2004

The interplay between L-functions and random matrices seems to be a fertile ground for problems.

There are many analytical questions one can ask about the classical groups of matrices equipped with the Haar measure - notably about the distribution of eigenvalues and about the value distribution of characteristic polynomials.

There are many analytic questions that one can ask about families of L-functions; prominent among these are questions about the distribution of zeros, the distribution of values of the L-functions, and the connection with arithmetical questions (distribution of primes, the size of class groups, ranks of elliptic curves, etc.).

Using groups of matrices to model the behavior of families of L-functions has turned out to have remarkable predictive powers. For example, we now have fairly precise conjectures for moments of families of L-functions that seemed totally out of reach 5 years ago. It is hoped that this new insight will provide some clues to the proofs of these new conjectures.

The connections between L-functions and random matrices are appealing because they suggest the possibility of a spectral interpretation of the zeros and hint at the possible tools for establishing such a connection. In addition, the assignment of a “symmetry type” to a family of L-functions provides a tool for understanding the L-functions and has been found to be a useful guide<sup>128</sup> in proofs.

It is hoped that the problems listed here might serve as a starting point for discussions during the workshop. The list is by no means exhaustive - we want suggestions for things to include. Also, please let us know of any errors or misinformation.

Many of the problems seek to find or refine a model that random matrix theory gives for families of L-functions. For example, the problem about the distribution of zeros of  $\zeta'(s)$ <sup>71</sup> is asking to use random matrix theory to give a conjecture for the distribution of the horizontal parts of the zeros of  $\zeta'(s)$ , presumably based on an analogous calculation for the distribution of the zeros of the derivative of a characteristic polynomial from the group of

---

<sup>128</sup>page 17, *Mollified sums over a family of L-functions*

<sup>71</sup>page 7, *Horizontal distribution of the zeros of  $\zeta'(s)$*

unitary matrices. Note that the problem does not request a proof that the distribution one finds is correct (which would presumably imply that 100% of the zeros of  $\zeta(s)$  are on the critical line). However, it can be hoped that knowing the answer will lead to new insight and eventually to a proof of new results.

## Table of Contents

A. Distribution of zeros of L-functions . . . . .	5
1. The GUE hypothesis	
2. Correlations of zeros	
3. Neighbor spacing	
4. Zeros of derivatives	
a. Horizontal distribution of zeros of zeta prime	
b. Statistics of the zeros of the derivative of xi	
c. Relationship between symplectic and odd orthogonal	
5. The Alternative Hypothesis	
6. p-adic L-functions	
B. Zeros and primes . . . . .	9
1. The distribution of primes	
2. Gaps between primes	
3. Primes of a special form	
4. An exponential sum involving primes	
C. Mean-values . . . . .	12
1. The mean-value conjectures	
2. Shifted mean values	
3. Multiple Dirichlet series	
4. Ratios of zeta-functions	
5. Lower order terms	
a. Fractional moments	
6. Mollified mean values	
a. Mollifying a Family	
b. Long Mollifiers	
7. Moments of $S(T)$	
8. The integral of $\exp(i \lambda S(t))$	
9. High moments are not natural	
D. Critical values . . . . .	19
1. Ranks of elliptic curves	
a. The frequency of rank 2 curves in a family of quadratic twists	
b. The frequency of higher rank in a family of quadratic twists	
c. Connection with the class number problem	
E. Extremal problems . . . . .	21
1. Critical values	
a. The maximal order of $S(T)$	
b. The maximal order of the zeta-function on the critical line	
c. The maximal rank of an elliptic curve as a function of its conductor	
d. The distribution of Fourier coefficients of half-integral weight forms	
e. Omega results for twists	
2. Non-critical values	
a. The zeta-function on the 1-line	
b. The order of $\zeta'/\zeta$	
c. Class numbers of quadratic fields	
3. Difficult to classify	

a.	Large gaps between primes	
b.	Extreme gaps between consecutive zeros of the zeta-function	
c.	Maximal clusters of zeros of the zeta-function	
F.	Function field zeta-functions . . . . .	27
1.	Fixed $q$	
2.	Corrections for small degree	
3.	Effective computation of zeta-functions	
a.	Elliptic curves	
b.	Higher genus	
4.	More function field analogues	
5.	Distribution of $\text{sha}$	
G.	Random matrix questions . . . . .	30
1.	Derivatives of characteristic polynomials	
2.	Eigenvalues of high powers of a matrix	
3.	$p$ -adic random matrix theory	
H.	Miscellaneous topics . . . . .	31
1.	Explicit Formula	
2.	Value distribution	
3.	GOE and Graphs	

## CHAPTER A: DISTRIBUTION OF ZEROS OF L-FUNCTIONS

For ease of notation we will phrase everything in terms of the Riemann  $\zeta$ -function, with the understanding that all statements hold for general  $L$ -functions with the obvious modifications.

Assume the Riemann Hypothesis, let  $\frac{1}{2} + i\gamma$  denote a nontrivial zero of the  $\zeta$ -function with  $\gamma > 0$ , and write  $\gamma_j$  for the  $j$ th zero, ordered with increasing imaginary part and repeated according to their multiplicity. Let  $\tilde{\gamma} := \frac{1}{2\pi}\gamma \log(\gamma)$ , so that  $d_j := \tilde{\gamma}_{j+1} - \tilde{\gamma}_j$  has average value of 1. An important problem is establishing various statistical properties of the sequence of  $\tilde{\gamma}$ .

The pioneering work of Montgomery [49 #2590] on the pair correlation of zeros of the  $\zeta$ -function, work of Hejhal [96d:11093], and Rudnick and Sarnak [ 97f:11074 ], on higher correlations of zeros, and extensive numerical calculations of Odlyzko (see [MR 88d:11082] and unpublished work <http://www.research.att.com/~amo/> available on his web page), give persuasive evidence of the following:

**The GUE Conjecture** The (suitably rescaled) zeros of the Riemann  $\zeta$ -function are distributed like the eigenvalues of large random matrices from the Gaussian Unitary Ensemble.

The conjecture has yet to be stated in a precise form. See The GUE hypothesis<sup>124</sup> for a discussion. However, any reasonable form of the conjecture makes a prediction of the correlation functions<sup>115</sup> of the zeros and the distribution of the neighbor spacings<sup>116</sup> of the zeros, as well as various other statistics. Thus, the GUE conjecture is a powerful tool for making and testing conjectures about the  $\zeta$ -function, and for shedding new light on a variety of long-standing questions. See the discussions of mean values<sup>31</sup> and value distribution<sup>90</sup> for more examples of how this conjecture relates to classical objects studied in number theory.

### A.1 The GUE hypothesis

**Problem:** Formulate a precise and believable statement of the “GUE Hypothesis.”

Any reasonable form of the conjecture should predict that the correlation functions<sup>115</sup> of the zeros and the distribution of the neighbor spacings<sup>116</sup> of the zeros of any automorphic  $L$ -function should have the same statistics as the eigenvalues of some collection of matrices.

The question is: which statistics? what collection of matrices (which may be a function of how ‘high up’ the zeros are)? what is the rate of convergence, and how uniform is it in the various parameters?

Montgomery’s original pair correlation conjecture was that if  $\alpha > 1$  then  $F(\alpha, T) \sim 1$  as  $T \rightarrow \infty$ , uniformly for  $1 \leq \alpha \leq A$ . A weak version of the conjecture asserts that  $\int_{\alpha}^{\beta} F(x, T) dx \sim \beta - \alpha$ , uniformly for  $1 \leq \alpha < \beta < A$ . Such an “almost everywhere” version is usually all that is needed for applications. Goldston and Montgomery [90h:11084] show that it is equivalent to a statement about the variation of the distribution of primes in

---

<sup>124</sup>page 5, *The GUE hypothesis*

<sup>115</sup>page 6, *Correlations of zeros*

<sup>116</sup>page 6, *Neighbor spacing of zeros of L-functions*

<sup>31</sup>page 12, *Mean-values*

<sup>90</sup>page 31, *Distribution of critical values*

<sup>115</sup>page 6, *Correlations of zeros*

<sup>116</sup>page 6, *Neighbor spacing of zeros of L-functions*

short intervals, and Goldston, Gonek, and Montgomery (to appear in Crelle) show tht it is equivalent to a statement about the mean square of  $\zeta'/\zeta$  near the  $\frac{1}{2}$ -line.

It is possible that an acceptable formulation of the GUE conjecture can be made in terms of integrals of ratios of  $\zeta$ -functions<sup>92</sup>.

## A.2 Correlations of zeros

The  $n$ -correlation functions of the zeros of the Riemann  $\zeta$ -function have been determined for a restricted class of test functions. See [49 #2590][96d:11093][ 97f:11074 ]. These results are established by relating the correlation functions to a sum over the prime numbers, and at present it is possible to prove a rigorous result only in the range where the “diagonal terms” in the sum are dominant.

Extending to a larger range would require some sort of information on sums of the form  $\sum \Lambda(n)\Lambda(n+k)$ , where  $\Lambda$  is the Von Mangoldt function defined by  $\Lambda(n) = \log p$  if  $n = p^k$ ,  $p$  prime, and  $\Lambda(n) = 0$  otherwise. These sums appear to be closely related to the “twin prime” problem, because  $\Lambda(n)\Lambda(n+k)$  is nonzero only when  $n$  and  $n+k$  are both primes (or prime powers, which is not a significant contribution). Bogolmony and Keating see [Nonlinearity 8, 1115-1131] and [Nonlinearity 9, 911-935], derive all  $n$ -correlation functions by assuming the Hardy-Littlewood conjectures and ignoring error terms, and the result agrees with the GUE conjecture. The calculation involves some difficult combinatorics.

The Hardy-Littlewood twin prime conjectures are too strong of an input into this problem, because it is averages of sums of the form  $\sum \Lambda(n)\Lambda(n+k)$  which need to be evaluated, and the information about primes of a specific form is lost in the averaging. In particular, the GUE hypothesis does not imply the Hardy-Littlewood conjectures. Goldston, Gonek, and Montgomery have shown that the pair correlation conjecture is equivalent to a statement about the variation of the distribution of primes. This is not even strong enough to imply that there is a  $k$  for which  $p_{n+1} - p_n = k$  infinitely often. It appears that GUE hypothesis for  $n$ -correlation is equivalent to a statement about the variation in the distribution of  $n - 1$ -almost primes.

It would be a significant accomplishment to prove anything about the correlation functions outside the range in which they currently are known. Two results in this direction are Özlük’s work [92j:11091] on the  $Q$  aspect of pair correlation for Dirichlet L-functions, and recent work of Goldston, Gonek, Özlük and Snyder [2000k:11100] in which they prove a lower bound for  $F(\alpha; T)$  for  $1 < \alpha < \frac{3}{2}$ .

It also would be valuable to have an idea, assuming GUE, of the rate at which the  $n$ -correlation sums converge to their limiting behavior, and to have an idea of how that rate changes as  $n \rightarrow \infty$ . See ratios of zeta-functions<sup>92</sup> for some additional discussion.

## A.3 Neighbor spacing of zeros of L-functions

We use the notation from Distribution of zeros of L-functions<sup>114</sup>, and everything below assumes RH and is specialized to the case of the Riemann  $\zeta$ -function.

Write  $d_j = \tilde{\gamma}_{j+1} - \tilde{\gamma}_j$  for the normalized difference between consecutive zeros of the  $\zeta$ -function. The GUE conjectures imply that for all  $a, A > 0$  we have  $d_j < a$  for a positive

---

<sup>92</sup>page 15, *Ratios of zeta-functions*

<sup>92</sup>page 15, *Ratios of zeta-functions*

<sup>114</sup>page 5, *Distribution of zeros of L-functions*

proportion of  $j$ , and  $d_j > A$  for a positive proportion of  $j$ . There have been a number of efforts aimed at showing  $a < \frac{1}{2}$  because this would prove the nonexistence of Siegel zeros. (See [49 #2590] for a reference). At present the best results, which are due to Soundararajan [97i:11097], are  $a < 0.6878$  and  $A > 1.4843$ .

The GUE conjectures also imply that for all  $\mu, \lambda > 0$  we have  $d_j < \mu$  for infinitely many  $j$ , and  $d_j > \lambda$  for infinitely many  $j$ . At present the best results (which assume RH and GLH) are [88g:11057]  $\lambda > 2.68$  and [86i:11048]  $\mu < 0.5172$ . Unconditionally, Richard Hall (unpublished) has shown  $\lambda > \sqrt{\frac{11}{2}} = 2.345207\dots$

It has not been shown that  $\mu < \frac{1}{2}$  implies the nonexistence of Siegel zeros. However, Conrey and Iwaniec have recently shown that  $d_j < \frac{1}{2} - \delta$ , for  $\gg T/\log^A T$  zeros with  $0 < \gamma < T$ , implies the nonexistence of Siegel zeros.

As described in the article on The Alternative Hypothesis<sup>117</sup>, the possibility of  $d_j \geq \frac{1}{2}$ , for all  $j$ , is consistent with everything which is known about the correlation functions of the zeros of the  $\zeta$ -function. However, it is possible that there is a  $C > \frac{1}{2}$  such that  $d_j \geq C$ , for all  $j$ , is also consistent with current information on the correlation functions. It would be interesting to know the correct answer.

## A.4 Zeros of derivatives

Much attention focuses on zeros of L-functions, but there are also some interesting questions about zeros of the derivatives of these functions.

In some cases we know more about zeros of the derivatives. For example, Levinson's method [58 #27837][84g:10070] can be used to show that for any  $\epsilon > 0$  there is an  $N$  such that if  $n \geq N$  then more than  $(100 - \epsilon)\%$  the zeros of  $\xi^{(n)}(s)$  are on the critical line, where  $\xi(s)$  is the Riemann  $\xi$ -function.

In other cases we know almost nothing. For example, nobody has even made a plausible conjecture about the distribution of the zeros of the derivatives of the Riemann  $\zeta$ -function.

See the articles on derivatives of  $\xi(s)$ <sup>70</sup> and derivatives of  $\zeta(s)$ <sup>71</sup>.

**A.4.a Horizontal distribution of the zeros of  $\zeta'(s)$ .** Can one use random matrix theory to predict the horizontal distribution of the real parts of the zeros of  $\zeta'$ ? It is known that the Riemann Hypothesis is equivalent to the assertion that each non-real zero of  $\zeta'(s)$  has real part greater than or equal to  $1/2$ . Moreover, if such a zero of  $\zeta'(s)$  has real part  $1/2$ , then it is also a zero of  $\zeta(s)$  (and so a multiple zero of  $\zeta(s)$ ). These assertions are the point of departure for Levinson's work on zeros of the Riemann zeta-function on the critical line [MR 54 #5135]. It would be interesting to know the horizontal distribution of these zeros; in particular what proportion of them with ordinates between  $T$  and  $2T$  are within  $a/\log T$  of the  $1/2$ -line? See the paper [98k:11119] of Soundararajan for the best theoretical result in this direction.

**A.4.b Statistics of the zeros of  $\xi'(s)$ .** The Riemann  $\xi$ -function is real on the  $1/2$ -line and has all of its zeros there (assuming the Riemann Hypothesis). It is an entire function of order 1; because of its functional equation,  $\xi(1/2 + i\sqrt{z})$  is an entire function of order  $1/2$ .

---

<sup>117</sup>page 8, *The Alternative Hypothesis*

<sup>70</sup>page 7, *Statistics of the zeros of  $\xi'(s)$*

<sup>71</sup>page 7, *Horizontal distribution of the zeros of  $\zeta'(s)$*

It follows that the Riemann Hypothesis implies that all zeros of  $\xi'(s)$  are on the  $1/2$ -line. (See [MR 84g:10070] for proofs of these statements.) Assuming the Riemann Hypothesis to be true, one can ask about the vertical distribution of zeros of  $\xi'(s)$ , and more generally of  $\xi^{(m)}(s)$ . It seems that the zeros of higher derivatives will become more and more regularly spaced; can these distributions be expressed in a simple way using random matrix theory? See the unpublished paper Differentiation evens out zero spacings<sup>1</sup> of David Farmer.

### A.4.c Relationship between symplectic and odd orthogonal. A.5 The Alternative Hypothesis

The Alternative Hypothesis is the assertion that, asymptotically, the normalized neighbor spacings of the zeros of the  $\zeta$ -function,  $d_j = \tilde{\gamma}_{j+1} - \tilde{\gamma}_j$ , are all nonzero integers or half-integers. By work of Montgomery and Weinberger (see [49 #2590] for a reference) this distribution would hold if there were infinitely many Siegel zeros. Thus, it would be a significant result to prove that the Alternative Hypothesis (AH) is not true. Establishing consequences of AH will help focus attention on what sort of work might lead to a contradiction.

A simple consequence is that Montgomery's pair correlation function  $F(\alpha, T)$  is periodic of period 2 in  $\alpha$ . Since  $F(\alpha, T)$  is known for  $-1 \leq \alpha \leq 1$ , on AH we know  $F(\alpha, T)$  for all  $\alpha$ .

Similarly, the higher correlation functions are periodic with period 2 in each of their variables. However, these functions do not appear to be known on a sufficiently large region for AH to determine them completely. For example, the triple correlation function  $F(\alpha, \beta; t)$  is only known [96d:11093][ 97f:11074 ] for  $(\alpha, \beta)$  in the hexagon  $|\alpha| < 1$ ,  $|\beta| < 1$ ,  $|\alpha + \beta| < 1$ , and the translates by period two in both directions do not cover the plane.

**Question:** Does AH determine all correlations of the zeros?

It is possible that a positivity condition on the correlation functions will allow one to conclude that the functions vanish on the regions not covered by the translates.

A related question concerns neighbor spacings. Let  $p(d)$  be the probability that  $d_j = d$ , so on AH the only nonzero values are  $p(\frac{1}{2})$ ,  $p(1)$ ,  $p(\frac{3}{2})$ , .... It is possible to determine  $p(\frac{1}{2})$  and  $p(1)$ , and to give bounds on the rest. If AH determines all of the correlation functions, then AH determines all of the  $p(d)$ . Perhaps AH determines  $p(d)$  even if it does not determine the correlation functions?

Heath-Brown [84m:10029] proved that the existence of Siegel zeros implies that there are infinitely many twin primes. Can one give a new proof of this by showing that AH implies infinitely many twin primes? This may actually be a more natural way to prove such a result, because recent work of Sarnak and Zaharescu [to appear in Duke Math Journal] shows that the Siegel zeros required for Heath-Brown's proof are inconsistent with the (modified) Generalized Riemann Hypothesis<sup>†</sup><sup>0</sup>.

The connection between AH and twin primes is not as contrived as it may look. The current results on zero correlations are established exactly in the range where certain sums are dominated by their diagonal contributions. Extending to a larger range would require some sort of information on sums of the form  $\sum \Lambda(n)\Lambda(n+k)$ , where  $\Lambda$  is the Von Mangoldt function defined by  $\Lambda(n) = \log p$  if  $n = p^k$ ,  $p$  prime, and  $\Lambda(n) = 0$  otherwise. Thus, these sums are directly related to twin primes. And by the explicit formula this can be related to

<sup>1</sup><http://farmer.bucknell.edu/~farmer/papers.html#unpub>

<sup>0</sup><http://www.aimath.org/WWN/rh/articles/html/3a/>

sums of the form  $\sum_{\gamma < T} x^{i\gamma}$ . If the  $\gamma$  are contained in an arithmetic progression, then one can choose  $x$  so that the sum over zeros is very large or very small.

Montgomery's original work can be seen as being motivated by the desire to establish enough information about  $F(\alpha; T)$  to contradict AH. Proving Montgomery's conjecture for  $1 < \alpha < 1 + \epsilon$  would be sufficient. Recent work of Goldston, Gonek, Özlük, and Snyder [2000k:11100] makes some progress in this direction by proving that  $F(\alpha; T) \geq \frac{3}{2} - \alpha$  for  $1 < \alpha < \frac{3}{2}$ . This falls short of contradicting AH, for one would need a lower bound larger than  $2 - \alpha$  for some  $1 < \alpha < 2$  to obtain a contradiction. It would be interesting to see if their techniques could be modified to prove  $F(\alpha; T) \geq 2 - \alpha$  for  $1 < \alpha < 2$ . This would not disprove AH, but it would give yet another interesting example of a result which reaches the boundary of disproving the existence of Siegel zeros.

Siegel zeros are a subtle and elusive opponent, and many attempts to disprove their existence have fallen  $\epsilon$  short of success. It is as if there are two consistent universes, one in which there are Siegel zeros, and one in which there are not. At present we do not know in which universe we live. Perhaps by pursuing consequences of the Alternative Hypothesis we can find out.

## A.6 Zeros of $p$ -adic $L$ -functions

What can be said about the distribution of zeros of  $p$ -adic  $L$ -functions?

(Background information, results, and precise statements of problems are sought.)

### CHAPTER B: ZEROS AND PRIMES

The motivation for studying  $L$ -functions and their zeros is to gain information about the prime numbers. Thus, it is a fundamental problem to describe the precise connection between zeros of  $L$ -functions and various properties of the prime numbers.

At present, the connection is fully understood in only a few cases, such as the equivalence between the error term in the Prime Number Theorem and the real part of the zeros of  $\zeta(s)$ . Namely,  $\pi(x) = Li(x) + O(x^{\theta+\epsilon})$  is equivalent to  $\zeta(s) \neq 0$  for  $\sigma > \theta$ .

The connection between  $n$ -correlations of zeros of the Riemann  $\zeta$ -function and the distribution of the prime numbers appears to be close to being understood. See the article on the distribution of primes<sup>123</sup> for a discussion.

Most of the questions about the prime numbers of a special form (twin primes, etc) haven't been shown to be related to standard conjectures about the distribution of zeros of  $L$ -functions. See the articles on primes of a special form<sup>126</sup> and gaps between primes<sup>125</sup> for a further discussion.

The Riemann  $\zeta$ -function can be expressed as a product over the primes and also as a sum over its zeros. Thus, everything about the prime numbers can be determined from the zeros of the  $\zeta$ -function. However, not all information about the primes can be extracted from the zeros in a simple way. It is possible that some questions about the primes (eg, the variation of the distribution of primes in short intervals) are naturally related to the distribution of zeros of the Riemann  $\zeta$ -function, while other questions (twin primes?) may more naturally be related to the distribution of zeros of Dirichlet  $L$ -functions. Also, some of

---

<sup>123</sup>page 10, *The distribution of primes*

<sup>126</sup>page 11, *Primes of a special form*

<sup>125</sup>page 11, *Bounds on gaps between primes*

those questions may require information beyond the GUE Hypothesis<sup>124</sup>. It would be good to have some general principles describing which properties of the primes are most naturally related to which properties of particular  $L$ -functions.

In this section we write  $p$  for a prime and  $p'$  for the next larger prime. We also use the standard notation for the von Mangoldt function  $\Lambda(n) = \log p$  if  $n = p^j$  and  $\Lambda(n) = 0$  otherwise, and the Chebyshev function

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Note that the prime number theorem can be written as  $\psi(x) \sim x$ .

## B.1 The distribution of primes

There are many interesting questions concerning the statistical properties of the distribution of the primes. One would like to know such things as the distribution of gaps between primes, statistics for the number of primes in various sized intervals, etc.

All of those questions appear to be far out of reach (in terms of proving them), but for some of them we may be close to identifying the connection with the zeros of  $L$ -functions. For example, Goldston and Montgomery [90h:11084] prove an equivalence between the pair correlation conjecture for the  $\zeta$ -function and a statement about the variation of the distribution of primes in short intervals. Farmer and Gonek, in work in progress, extend this result to the case of  $n$ -correlation, and this time the equivalence is with the variation of the distribution of  $n - 1$  almost-primes in short intervals. These results suggest that it will require something beyond the correlation functions (or more than just the  $\zeta$ -function) in order to obtain more precise results about the distribution of primes.

The Cramèr model for the distribution of primes asserts that the primes are independently distributed and the gaps between primes obey Poisson statistics. In particular,

$$Prob\left(\frac{p' - p}{\log p} > \lambda\right) \sim e^{-\lambda},$$

for  $p \leq P$ , as  $P \rightarrow \infty$ . And more generally,

$$Prob((x, x + \lambda \log x) \text{ contains exactly } k \text{ primes}) \sim e^{-\lambda} \frac{\lambda^k}{k!},$$

for  $x \leq X$ , as  $X \rightarrow \infty$

Gallagher [MR 53 #13140] showed that the above prime gap distribution follows from a version of the Hardy–Littlewood conjectures.

The Cramèr model is only accurate for very crude measurements of the distribution of primes. For example, Goldston and Montgomery [90h:11084] have shown that the pair correlation conjecture is equivalent to

$$\int_1^X (\psi(x+h) - \psi(x) - h)^2 dx \sim hX \log \frac{X}{h},$$

for  $X^\epsilon < h < X^{1-\epsilon}$ . Montgomery and Soundararajan [arXiv:math/0003234] note that the above formula can be interpreted as suggesting that  $\psi(x+h) - \psi(x)$  is normally distributed with mean  $h$  and variance  $h \log(X/h)$ , for  $1 \leq x \leq X$  and  $X^\epsilon < h < X^{1-\epsilon}$ , while the Cramèr model predicts mean  $h$  and variance  $h \log X$ . They then use numerical and heuristic evidence

---

<sup>124</sup>page 5, *The GUE hypothesis*

to develop a more sophisticated probabilistic model for the distribution of primes in short intervals.

## B.2 Bounds on gaps between primes

It is a long-standing unsolved problem to prove that there is always a prime between  $n^2$  and  $(n+1)^2$ . This is equivalent to showing that  $p' - p \leq p^{1/2}$ . Since the average size of  $p' - p$  is  $\log p$ , and it is conjectured that  $p' - p \ll \log^2 p$ , current results seem to be very far from the final truth.

Goldston and Heath-Brown [85e:11064] have shown that the pair correlation conjecture implies  $p' - p = o(p^{1/2} \log^{1/2} p)$ .

**Problem:** Find a believable conjecture about the zeros of the  $\zeta$ -function which implies that  $p' - p \ll p^A$  for all  $A > 0$ . Even the case  $A = \frac{1}{2}$  would be significant.

For an example of a non-believable conjecture which may imply that there are small gaps between consecutive primes, see the article on the Alternative Hypothesis<sup>117</sup>.

Heath-Brown [83m:10078] showed that if Montgomery's conjecture on  $F(\alpha; T)$  holds in some neighborhood of  $\alpha = 1$  then  $\liminf \frac{p' - p}{\log p} = 0$ . The proof only requires the continuity of  $F(\alpha; T)$  at  $\alpha = 1$ . This continuity also follows from the alternative hypothesis<sup>117</sup>, so there may be hope of proving this unconditionally.

Erdős used sieve methods to show that there exists  $\delta > 0$  such that  $p' - p \leq (1 - \delta) \log p$  for a positive proportion of primes  $p$ . (It would be helpful if someone could provide details on the history of this problem and an up-to-date account of current results).

It has not yet been shown that there is a  $\lambda > 1$  such that  $p' - p \geq \lambda \log p$  for a positive proportion of  $p$ .

## B.3 Primes of a special form

There is a long history of interest in primes of a special form. Writing  $p$  for a prime and  $p'$  for the next larger prime, some of the famous examples are: twin primes ( $p' - p = 2$ ), primes represented by polynomials (the simplest case is  $p = n^2 + 1$ ), Sophie Germaine primes ( $2p + 1$  is prime), and many others.

None of these problems has been connected to the zeros of the Riemann  $\zeta$ -function in a satisfactory way. Turan [38 #127] related twin primes to zeros of  $L$ -functions near  $\frac{1}{2}$ , and it is possible that recent ideas on the distribution of low-lying zeros in a family will shed some light on that problem. Bogolmony and Keating [Nonlinearity 8, 1115-1131] [Nonlinearity 9, 911-935] derive all  $n$ -correlation functions by assuming the Hardy-Littlewood conjectures and ignoring error terms. However, one cannot deduce the Hardy-Littlewood conjectures from the correlation functions.

**Problem:** Devise a believable conjecture about the zeros of one or more  $L$ -functions which implies that there are infinitely many primes of one of the special forms described above.

---

<sup>117</sup>page 8, *The Alternative Hypothesis*

<sup>117</sup>page 8, *The Alternative Hypothesis*

## B.4 An exponential sum involving primes

Suppose

$$\sum_{p < X} e(2\sqrt{p}) \ll X^\alpha.$$

If that bound held for some  $\alpha < \frac{3}{4}$  then one could extend the current results on the 1-level density of low-lying zeros of cusp form  $L$ -functions. This would imply (assuming GRH for the critical zeros of these  $L$ -functions) that  $L(f, s)$  has no Siegel zeros in a strong sense. Namely, that there exists  $\delta > 0$  such that  $L(f, s)$  is nonzero for  $s > 1 - \delta$ .

(References and more details on the above are sought).

It is tempting to think that the above estimate must surely hold for any  $\alpha > \frac{1}{2}$ , because one naturally expects square-root cancellation in any “random looking” sum. However, the following example shows that nature is more subtle than that. Let  $\lambda_f(n)$  denote the (suitably normalized) Fourier coefficients of a holomorphic cusp form. Then [Conrey and Ghosh?, unpublished?] have shown that

$$\sum_{p < X} \log p \lambda_f(p) e(2\sqrt{p}) \sim cX^{3/4}.$$

The lack of cancellation in that sum is puzzling.

### CHAPTER C: MEAN-VALUES

There are so many results and conjectures having to do with the mean-values or moments of  $L$ -functions in families that it is difficult to mention all of them. So we will stick with some of the more familiar ones.

**Moments of  $\zeta(1/2 + it)$ .** Let

$$I_k(T) = \frac{1}{T} \int_0^T |\zeta(1/2 + it)|^{2k} dt.$$

Then asymptotic formulae are known for  $I_1$  and  $I_2$ . A good estimation for  $I_3$  seems to be far out of reach of today’s technology (maybe we need to know more about automorphic forms on  $GL_3$ ?) but would be a very important milestone. Conjectures based on number theory are known for  $k = 3, 4$ . Conjectures based on random matrix theory are known for all real  $k > -1/2$ .

**Moments of  $L(1/2, \chi_d)$ .** Let  $\chi_d$  be a real, primitive, quadratic character to the modulus  $|d|$  (i.e. a Kronecker symbol). Let

$$S(D) = \sum_{|d| \leq D} L(1/2, \chi_d)^k.$$

Then asymptotics are known for  $k = 1, 2, 3$ . A conjecture based on number theory is known for  $k = 4$ . Conjectures based on random matrix theory are known for all real  $k > -3/2$ . The fourth moment is just slightly out of reach of current technology.

**Moments of automorphic  $L$ -functions.** Let  $f$  be a normalized newform of weight  $k$  and level 1 and let  $L_f(s)$  be the associated  $L$ -function (with critical strip  $0 < \sigma < 1$ .) Let

$$O_\lambda(K) = \sum_{k \leq K} \sum_{f \in S_k} L_f(1/2)^\lambda.$$

Then asymptotic formulae are known for  $\lambda = 1, 2, 3, 4$ . Conjectures based on random matrix theory are known for all real  $\lambda > -1/2$ . Is the fifth moment doable?

**Quadratic twists of automorphic L-functions.** Let  $f$  be a fixed newform (for example the newform associated with a given elliptic curve). Let  $L_f(s)$  be the associated L-function and  $L_f(s, \chi_d)$  the twist by the primitive quadratic character  $\chi_d$ . It is possible to evaluate the first moment

$$\sum_{|d| \leq D} L(1/2, \chi_d)$$

but can one do the second moment

$$\sum_{|d| \leq D} L(1/2, \chi_d)^2?$$

Again, this is just at the edge of what can be done by today's techniques and is a problem worthy of study.

**Special families.** Recently the bound

$$\sum_{f \in S_k^*(q)} L_f(1/2, \chi_q)^3 \ll q^{1+\epsilon}$$

has been obtained, where  $S_k^*(q)$  denotes the set of newforms of weight  $k$  and level  $q$  (no character), and  $\chi_q$  is the real character to the modulus  $q$  where  $q$  is odd and squarefree. This estimate has been used to bound Fourier coefficients of half-integral weight forms and (its analogue for Maass forms has been used) to bound  $L(1/2 + it, \chi_q)$ . Can one strengthen this estimate to give an asymptotic formula (perhaps for  $q$  restricted to prime values)? Are there other situations where the underlying arithmetic is so fortuitous so as to give such a strong bound?

## C.1 The mean-value conjectures

For convenience we state examples of the three main conjectures for moments in families. There are no open questions in this article (except how to prove these conjectures!). For simplicity, we state the conjectures only for integral moments.

### Unitary

Let

$$I_k(T) = \frac{1}{T} \int_0^T |\zeta(1/2 + it)|^{2k} dt.$$

**Conjecture.**

$$I_k(t) \sim a_k \prod_{j=0}^{k-1} \frac{j!}{(j+k)!} (\log T)^{k^2}$$

where

$$a_k = \prod_p (1 - 1/p)^{(k-1)^2} \sum_{j=0}^{k-1} \binom{k-1}{j}^2 p^{-j}.$$

### Symplectic

Let  $\chi_d$  be a real, primitive, quadratic character to the modulus  $|d|$  (i.e. a Kronecker symbol) and let

$$S_k(D) = \frac{1}{D^*} \sum_{|d| \leq D} L(1/2, \chi_d)^k$$

where  $D^* = \sum_{|d| \leq D} 1$ .

**Conjecture.**

$$S_k(D) \sim a_k \prod_{j=1}^k \frac{j!}{(2j)!} (\log D)^{k(k+1)/2}$$

where

$$a_k = \prod_p \frac{(1 - 1/p)^{k(k+1)/2}}{(1 + 1/p)} \left( \frac{(1 - 1/\sqrt{p})^{-k} + (1 + 1/\sqrt{p})^{-k}}{2} + \frac{1}{p} \right)$$

### Orthogonal

Let  $f$  be a normalized newform of weight 2 and level  $q$  (where  $q$  is prime) (we write  $f \in F(q)$ ) and let  $L_f(s)$  be the associated  $L$ -function (with critical strip  $0 < \sigma < 1$ .) Let

$$O_k(q) = \frac{1}{q^*} \sum_{f \in F(q)} L_f(1/2)^k$$

where  $q^* = \sum_{f \in F(q)} 1$ .

**Conjecture.**

$$O_k(q) \sim a_k 2^{k-1} \prod_{j=1}^{k-1} \frac{j!}{(2j)!} (\log q)^{k(k-1)/2}$$

where  $a_k$  is a product over primes (which can be worked out for any  $k$ , but for which we don't have a simple closed form expression);

$$a_1 = \zeta(2),$$

$$a_2 = \zeta(2)^2 \prod_p (1 + 1/p)^2,$$

$$a_3 = \zeta(2)^3 \prod_p (1 - 1/p)(1 + 1/p + 4/p^2 + 1/p^3 + 1/p^4),$$

and so on.

## C.2 Mean values of shifted zeta-functions

Recently Conrey, Farmer, Keating, and Snaith have conjectured mean values for products of zeta functions shifted off the  $\frac{1}{2}$ -line. The integrals they consider are of the form

$$\int_0^T \prod_{j=1}^J \zeta\left(\frac{1}{2} + a_j + \epsilon_j t\right) dt,$$

where  $\epsilon_j = \pm 1$ . They have shown that it is possible to use Dirichlet polynomial techniques to conjecture the full main term for the above mean value, and it is also possible to exactly

evaluate the analogous expression involving characteristic polynomials of matrices from the CUE. The two calculations agree in every term, apart from arithmetic factors which are not incorporated into the random matrix model.

These techniques extend to the case of ratios of zeta functions<sup>92</sup>, and also are applicable to mean values of  $L$ -functions with other symmetry types.

(A more extensive description is in preparation).

### C.3 Multiple Dirichlet series

Recently Diaconu, Goldfeld, and Hoffstein [arXiv:math.NT/0110092] have considered mean values similar to those described in the article on shifted zeta functions<sup>138</sup>. They refer to these as “Multiple Dirichlet Series.”

These mean values are viewed as functions of several complex variables, and they make a precise conjecture about the polar divisors of the function. Furthermore, they prove that their conjecture on the polar divisors implies the truth of the conjectured mean values which have been obtained from random matrix theory.

These techniques extend to the case of ratios of zeta functions<sup>92</sup>, and also are applicable to mean values of  $L$ -functions with other symmetry types.

(A more extensive description is in preparation).

### C.4 Ratios of zeta-functions

A possible route to understanding the correlation functions of zeros of  $L$ -functions is via integrals of ratios of  $L$ -functions near the critical line. The simplest nontrivial case is the following formula conjectured by Farmer [95a:11076]. Suppose  $u, v, a, b$  are of size  $1/\log(T)$  and  $a, b$  have positive real part. It was conjectured that

$$\int_1^T \frac{\zeta(\frac{1}{2} + u + it)\zeta(\frac{1}{2} + v - it)}{\zeta(\frac{1}{2} + a + it)\zeta(\frac{1}{2} + b - it)} dt \sim T \left( 1 + (1 - T^{-(u+v)}) \frac{(u-a)(v-b)}{(u+v)(a+b)} \right),$$

as  $T \rightarrow \infty$ .

The above formula was obtained from a mollified mean value<sup>127</sup> of the  $\zeta$ -function. This formula can be differentiated with respect to any of  $u, v, a, b$ , leading to other conjectures, such as for the mean 2nd and 4th moments of  $\zeta'/\zeta$  near the critical line. This is useful because those moments are relevant in the study of the distribution of the prime numbers<sup>73</sup>.

Combining the 2nd moment of  $\zeta'/\zeta$  with work of Goldston, Gonek, and Montgomery, shows that the above formula implies Montgomery’s pair correlation conjecture almost everywhere. This is interesting because the above formula was not explicitly based on any conjectures about the primes, nor did it obviously rely on any strong assumptions about the distribution of the zeros.

If the  $\zeta$ -functions in the above expression are replaced by the characteristic polynomial of a matrix from the Circular Unitary Ensemble and then averaged over the ensemble, the result agrees with the formula conjectured above. This suggests a way to conjecture more

---

<sup>92</sup>page 15, *Ratios of zeta-functions*

<sup>138</sup>page 14, *Mean values of shifted zeta-functions*

<sup>92</sup>page 15, *Ratios of zeta-functions*

<sup>127</sup>page 17, *Long Mollifiers*

<sup>73</sup>page 9, *Zeros and primes*

complicated versions if this formula, and may give a framework for a better understanding of which aspects of the zeros of  $\zeta$ -function should be governed by random matrix theory.

Recently Conrey, Farmer, Keating, and Snaith have shown that it is possible to use Dirichlet series techniques to conjecture generalizations of the above formula, both in terms of having more  $\zeta$ -functions and relaxing the restriction that  $u, v, a, b$  be of size  $1/\log T$ . The results agree with the formulas obtained from random matrix theory. This could lead to a conjecture for the full main term<sup>75</sup> in the  $2k$ th moment of the  $\zeta$ -function on the critical line.

It would be useful to fully understand the consequences of formulas like the one conjectured above, to find more formulas which give a clear connection with the GUE hypothesis, and to have a unified picture of the connection between various integrals of L-functions and the distribution of zeros. And, of course, it would be good to identify an approach which could lead to a proof of these formulas.

There is a formal similarity between the integrals of ratios of  $\zeta$ -functions and the ratios of  $\Gamma$ -functions in Barnes' type integrals. It may be that a natural object to study is an integral of ratios Riemann  $\xi$ -functions, which would include both  $\Gamma$ -factors and  $\zeta$ -function factors.

## C.5 Lower order terms

*Full moment conjecture.* What are the lower order terms in the moment formulae for  $|\zeta(1/2 + it)|^{2k}$  and for  $L(1/2)^k$ ? These are known in a few instances (see [MR 88c:11049] Theorem 7.4 and [MR 97e:11096] for the second and fourth moments of  $\zeta(s)$ ) but not in general. The difficulty is that random matrix theory does not “see” the contribution of the arithmetic factor  $a_k$ . Lower order terms will likely involve a mix of derivatives of  $a_k$  and secondary terms from the moments of the characteristic polynomials of matrices. In general, a better understanding of how  $\zeta(s)$  is modeled by a characteristic polynomial of a certain type of matrix is needed; how do the primes come into play? Perhaps we should think of  $\zeta(1/2 + it)$  as a partial Hadamard product over zeros multiplied by a partial Euler product. Perhaps these two parts behave independently, and the Hadamard product part can be modeled by random matrix theory. See the article on Explicit Formula<sup>113</sup> for more discussion of this point.

Recently, Conrey, Farmer, Keating, Rubinstein, and Snaith and, independently by another method, Diaconu, Goldfeld, and Hoffstein, have developed a conjecture for these lower order terms.

**C.5.a Fractional moments.** There is now a preliminary conjecture for the lower order terms of the above article in the case of integral moments. However, it would be interesting to have the lower order terms for fractional moments as well. For example, we expect that

$$\frac{1}{T} \int_0^T |\zeta(1/2 + it)| dt \sim c(\log T)^{1/4}.$$

What would be the expected error term here? Are there more main terms? It may not be unreasonable to guess that for this example there will be an (infinite) asymptotic series of

---

<sup>75</sup>page 16, *Lower order terms*

<sup>113</sup>page 31, *Explicit Formula*

powers of  $\log T$  so that

$$\frac{1}{T} \int_0^T |\zeta(1/2 + it)| dt = \sum_{n=0}^N c_n (\log T)^{1/4-n} + O((\log T)^{-3/4-N})$$

holds for any  $N$  with some sequence of  $c_n$ . Is there some way to guess this answer? A good conjecture could easily be tested numerically.

## C.6 Mollified mean values

**C.6.a Mollified sums over a family of L-functions.** Article not submitted yet.

**C.6.b Long Mollifiers.** Let  $h(x)$  be a real polynomial with  $h(0) = 0$ , let  $y = T^\theta$  for some  $\theta > 0$ , and let

$$M(s) = M(s, h(x)) = \sum_{n \leq y} \frac{\mu(n) h\left(\frac{\log y/n}{\log y}\right)}{n^s}.$$

The Dirichlet polynomial  $M(s)$  is called a ‘‘mollifier’’ of the Riemann  $\zeta$ -function because it is an approximation to  $1/\zeta(s)$ , and so  $\zeta(s)M(s)$  should be much better behaved than  $\zeta(s)$  near the  $\frac{1}{2}$ -line.

The mean value of  $\zeta(s)M(s)$  near the  $\frac{1}{2}$ -line is a fundamental tools for studying zeros of the  $\zeta$ -function. The most general version currently used is the following formula of Conrey, Ghosh, and Gonek [MR 90h:11077]

$$\int_1^T \zeta\left(\frac{1}{2} + u + it\right) \zeta\left(\frac{1}{2} + v - it\right) M\left(\frac{1}{2} + a + it, h(x)\right) M\left(\frac{1}{2} + b - it, g(x)\right) dt \\ \sim T \left( h(1)g(1) + \frac{1}{\theta} \int_0^1 T^{-\xi(u+v)} d\xi \frac{d}{d\alpha} \frac{d}{d\beta} T^{-\theta(\alpha u + \beta v)} \int_0^1 h_a(x + \alpha) g_b(x + \beta) dx \right) \Big|_{\alpha=\beta=0},$$

where  $h_a(x) = T^{\theta a(x-1)} h(x)$ , uniformly for  $|u| + |v| + |a| + |b| \ll 1/\log T$ . This formula is used in Levinson’s method [MR 58 #27837], and is known to be valid [90g:11120] for  $0 < \theta < \frac{4}{7}$ . Showing that the formula is valid for large  $\theta$  is key to having good results.

Farmer [95a:11076] conjectured that the above formula should remain valid for all  $\theta > 0$ . This leads to a conjecture for an integral involving ratios of zeta-functions<sup>92</sup>, which implies the pair-correlation conjecture. See the original paper [95a:11076] for some additional consequences.

It would be a significant result to prove that the above formula holds for some  $\theta > \frac{4}{7}$ . Establishing it for  $\theta > 0.7631$  would prove that more than half of the zeros of the  $\zeta$ -function are on the  $\frac{1}{2}$ -line. Proving that it holds for all  $\theta > 0$  is more-or-less equivalent to the GUE conjecture, because it can be deduced from the formulas for ratios of zeta-functions<sup>92</sup>.

## C.7 Moments of $S(T)$

$S(T)$  is defined by

$$S(T) = \frac{1}{\pi} \arg \zeta(1/2 + iT)$$

<sup>92</sup>page 15, *Ratios of zeta-functions*

<sup>92</sup>page 15, *Ratios of zeta-functions*

where the argument is obtained by continuous variation from  $s = 2$  where the argument is 0, to  $s = 2 + iT$  to  $s = 1/2 + iT$ , circumventing zeros of  $\zeta(s)$  by small semicircular detours above the zeros. Selberg [MR 8,567e] proved an asymptotic formula for

$$\frac{1}{T} \int_0^T S(t)^{2k} dt \sim c_k (\log \log T)^k$$

for positive integral values of  $k$  and an appropriate  $c_k$ . Goldston [MR 89a:11086], assuming the Riemann Hypothesis, was able to give a second main term in the case that  $k = 1$ . Keating and Snaith's conjectures for moments of  $|\zeta(1/2 + it)|$  imply formula for the above moments of  $S(T)$ , including lower order terms all the way to a constant, i.e. they conjecture that

$$\frac{1}{T} \int_0^T S(t)^{2k} dt = \sum_{n=0}^k c_n (\log \log T)^n + o(1)$$

for some explicit constants  $c_n = c_n(k)$ .

It seems like further work should allow one to obtain the lower order terms in the moments of  $S(T)$ ; it's possible that the assumption of the Riemann Hypothesis will allow for the evaluation of some of the lower order terms, and the assumption of GUE will allow for the rest.

## C.8 The integral of $\exp(i\lambda S(t))$

In the paper [CMP 1 794 265] by Keating and Snaith, the authors conjecture (see equation (100)) that

$$\int_0^T e(2\lambda S(t)) dt \sim T(\log T)^{-\lambda^2} G(1 - \lambda)G(1 + \lambda)b(\lambda)$$

where  $b(\lambda)$  may be expressed as an absolutely convergent product over primes and  $G$  is the Barnes double gamma function.

If  $\lambda$  is an integer, then the main term is 0. If  $\lambda$  is not an integer, then no instance of this remarkable formula has been proven (or even conjectured) before.

## C.9 Mean values are not the natural object to study

Moments of the Riemann  $\zeta$ -function were introduced as a tool to attack the Lindelöf Hypothesis, which asserts that  $\zeta(\frac{1}{2} + it) \ll t^\epsilon$  for any  $\epsilon > 0$ . This is equivalent to

$$I_k(T) = \int_0^T |\zeta(\frac{1}{2} + it)|^{2k} dt \ll T^{1+\epsilon}$$

for any  $\epsilon > 0$ , where the implied constant depends on  $k$ .

The above bound has only been established for  $k = 1$  and 2, and for those values an asymptotic formula is known for the more general integral

$$\mathcal{I}_k(a_1, \dots, a_{2k}; w; T) = \int_0^\infty g(t/T) \prod_{j=1}^{2k} \zeta(\frac{1}{2} + a_j + \epsilon_j t) t^w dt,$$

where  $\epsilon_j = \pm 1$  and  $g$  is a function which decreases rapidly at  $\infty$ .

When  $k = 1$  or 2, the function  $\mathcal{I}_k$  can be continued to a meromorphic function. But if  $k$  is larger, then  $\mathcal{I}_k$  is (conjecturally) not continuable to a meromorphic function, and in

fact it has a natural boundary. Diaconu, Goldfeld, and Hoffstein<sup>139</sup> have shown that the function continues to a sufficiently large region that standard conjectures for the moments of  $L$ -functions should be able to be recovered from the polar divisors of  $\mathcal{I}_k$ . However, the fact that the function under consideration is not entire suggests that it may not be the correct object to study.

**Problem:** Find a natural way to modify  $\mathcal{I}_k$  so that it becomes an entire (meromorphic) function.

The fact that  $\mathcal{I}_k$  is not a nice function for  $k \geq 3$  is an aspect of the “Estermann Phenomonon.” Consider the Dirichlet series

$$F_k(s) = \sum_{n=1}^{\infty} \frac{d(n)^k}{n^s},$$

where  $d(n) = \sum_{ab=n} 1$  is the number of divisors of  $n$ . We have

$$\begin{aligned} F_0(s) &= 1 \\ F_1(s) &= \zeta(s)^2 \\ F_2(s) &= \frac{\zeta(s)^4}{\zeta(2s)} \end{aligned}$$

But if  $k \geq 3$  then  $F_k(s)$  can only be expressed as an infinite product of  $\zeta$ -functions, and it has a natural boundary at  $\sigma = 0$ .

An example which may be more closely related to the situation at hand is

$$F(s) = \sum_{n=1}^{\infty} \frac{d_3(n)^2}{n^s},$$

where  $d_3(n) = \sum_{abc=n} 1$ . Again  $F(s)$  has a natural boundary at  $\sigma = 0$ , but it is possible to modify the coefficients of  $F(s)$ , only involving the terms divisible by a cube, so that the function has an analytic continuation. This is promising because a partial sum of  $F(s)$  is the diagonal contribution to the integrand of  $I_3(T)$ .

See Titchmarsh [MR 88c:11049] for more background information.

## CHAPTER D: CRITICAL VALUES

The critical value of an  $L$ -function (the first nonzero Taylor coefficient at the symmetry point of the functional equation) contains significant arithmetic information. The most famous example is the case of an  $L$ -function associated with an elliptic curve. The Birch and Swinnerton–Dyer conjecture states that the order of vanishing at the critical point gives the rank of the group of rational points on the curve, and the critical value gives a combination of other important arithmetic information about the curve.

Random matrix theory can be used to study critical values by using an analogy between the  $L$ -function and the characteristic polynomial. In this case the behavior of the  $L$ -function at the critical point corresponds to the behavior at  $x = 1$  for the characteristic polynomial  $f(x)$ .

---

<sup>139</sup>page 15, *Multiple Dirichlet series*

At present the most extensive work has been done on the study of ranks of elliptic curves<sup>23</sup>, but it is likely that random matrix methods will soon be employed to study other questions related to critical values.

## D.1 Ranks of elliptic curves

The Birch and Swinnerton–Dyer conjecture relates the rank of an elliptic curve (and other arithmetic information) to the order of vanishing (and the first nonzero coefficient) of the associated  $L$ -function at the critical point.

Thus, results and conjectures about the critical values of various families of  $L$ -function will give information about the ranks of elliptic curves.

(more details and some good references are sought.)

**D.1.a The frequency of rank 2 curves in a family of quadratic twists.** Let  $E$  be an elliptic curve over the rationals. Then its associated modular form  $f$  is a newform of weight 2 with integral coefficients; let  $L_f(s)$  be its associated  $L$ -function. Suppose that the  $L$ -function is scaled so that its functional equation relates the values of  $L$  at  $s$  and  $1 - s$ . Suppose that the sign of the functional equation is  $\epsilon = \epsilon_f$  and the level is  $N$ . Let  $\chi_p$  be a real, primitive, Dirichlet character to the modulus  $p$ ,  $p$  prime, for which  $\chi_p(-N) = \epsilon$  so that the sign of the functional equation of  $L_f(s, \chi_p)$  is  $+1$ . We are interested in the number  $V_E(P)$  of  $p \leq P$  for which  $L_f(1/2, \chi_p) = 0$ . By the Birch and Swinnerton-Dyer conjecture, this will be the number of quadratic twists of  $E$  with even rank at least 2. Goldfeld has conjectured that  $V_E(Q) = o(Q/\log Q)$  for any  $E$ .

In recent work of Conrey, Keating, Rubinstein, and Snaith [arXiv:math/0012043] it was conjectured that there is a constant  $c_E > 0$  such that

$$V_E(P) \sim c_E P^{3/4} / (\log P)^{11/8}.$$

The heuristics behind the conjecture involve applying random matrix theory to try to understand the value distribution of the  $L$ -functions  $L_E(1/2, \chi_p)$  and using the conjectural formula of Birch and Swinnerton-Dyer for this special value to determine how often the value is 0.

The method does not appear to give a value for  $c_E$ . The reason seems to be that it is difficult to include in the reasoning the fact that one of the factors in the formula of Birch and Swinnerton-Dyer involves the order of a (finite) group, namely the Tate-Shafarevich group. The orders of “random” groups of size  $\leq X$ , say, are not uniformly distributed over the interval  $[1, X]$ , but instead depend on extra information, such as the automorphisms of the groups, as was observed in the work [MR 85j:11144] of Cohen and Lenstra. It would be interesting to extend the Cohen-Lenstra heuristics to the present situation.

The problem, then, is to determine (heuristically) the constants  $c_E$ . The method described above involves using a continuous distribution to conjecture how often a discrete quantity is zero. It is desirable to have a well-formulated approach for deciding in general how to turn a continuous distribution into a “cut off” function.

It would also be nice to have a geometric explanation for the exponents occurring in the above conjecture.

The above is inconsistent with a conjecture of Zagier and Kramarz [90d:11072]. They conjecture that a positive proportion of the curves  $x^3 + y^3 = m$  have rank 2 or more, and they give both heuristic and numerical evidence for their conjecture. It can be argued that

---

<sup>23</sup>page 20, *Ranks of elliptic curves*

current numerical calculations are not able to distinguish between a constant and a power of the logarithm, rendering the numerics inconclusive. It is also possible that there is an interesting explanation (perhaps relating to small height points?) for why an excess of high rank seems to occur experimentally.

**D.1.b The frequency of higher rank in a family of quadratic twists.** Random matrix theory can be used to predict the frequency of rank 2 curves in a family of quadratic twists<sup>52</sup>, but it does not seem to be able to tell us what the prediction is for quadratic twists of rank 3 or higher.

The reason that the RMT approach fails is that the height of a generating point is a factor in the formula for the central value of the derivative of the L-function of a rank 1 curve. We don't have a prediction for the distribution of the heights of the generating points, and so can't predict (within the collection of curves of odd rank) the distribution the critical derivatives of the  $L$ -functions. Since the frequency of vanishing is determined by analyzing the tail of that distribution, we are unable to predict how often the derivative of the L-series is 0.

In [arXiv:math/0010056] (to appear in *Exp. Math.*), Rubin and Silverberg show that for several infinite families of elliptic curves  $E$ , the number of quadratic twists  $E_d$ ,  $|d| < X$ , with rank at least 3 is  $\gg X^{1/6}$ . (Assuming the Parity Conjecture, the same result holds with 3 replaced by 4.) Some of these examples were previously obtained by Stewart and Top [MR 95m:11055].

Rubin and Silverberg ask whether it is possible to find a hyperelliptic curve over  $Q$  whose jacobian contains  $r \geq 4$  copies of a fixed elliptic curve  $E$ . This would give a lower bound for the frequency of quadratic twists of  $E$  of rank at least  $r$ .

**D.1.c Ranks of elliptic curves and the class number problem.** Goldfeld [MR 56 #8529] showed that if there is an elliptic curve  $E$  whose  $L$ -function vanishes to order  $g \geq 2$  at the critical point, then we can obtain a lower bound for the class number:

$$h(D) \gg_E (\log D)^{g-2}.$$

At present,  $g = 3$  is the largest value for which this has been shown to hold. See the paper by Oesterlé [86k:11064] for a readable account with the explicit calculation of the relevant constants, and the survey by Goldfeld [86k:11065] for background information.

In the article on the maximal rank of an elliptic curve as a function of its conductor<sup>51</sup> it is suggested that there are elliptic curves  $E$  with rank as large as  $\log N / \log \log N$ , where  $N$  is the conductor of  $E$ . Might this lead to the lower bound

$$h(D) \gg \frac{\sqrt{D}}{\log D}?$$

Is it possible to use a family of elliptic curves of high rank to improve Goldfeld's result?

## CHAPTER E: EXTREMAL PROBLEMS

There are a collection of problems that go under this heading: the most basic is the question of the maximal size of the zeta-function on the critical line. There are basically two

---

<sup>52</sup>page 20, *The frequency of rank 2 curves in a family of quadratic twists*

<sup>51</sup>page 23, *The maximal rank of an elliptic curve as a function of its conductor*

guesses for the answer - the larger or O-bound which follows from the Riemann Hypothesis and the smaller or omega result which in some cases can actually be proven. By “omega result” we mean an assertion of the form  $f(t) = \Omega(g(t))$  as  $t \rightarrow \infty$ , which means that  $\limsup_{t \rightarrow \infty} f(t)/g(t) > 0$ .

For the case of the  $\zeta$ -function, on RH we have

$$\zeta\left(\frac{1}{2} + it\right) = O\left(\exp(c \log t / \log \log t)\right)$$

for some  $c > 0$ , and

$$\zeta\left(\frac{1}{2} + it\right) = \Omega\left(\exp(c_1(\log t / \log \log t)^{1/2})\right)$$

for some  $c_1 > 0$

Traditional wisdom has favored the smaller bound. It seems to be the bound that is suggested by probability arguments. For example, one might think of  $\log \zeta(\sigma + it)$  as being approximated by a sum  $-\sum_{p \leq x} p^{-\sigma - it}$  for an appropriate choice of  $x$ . How large can this sum be? It seems to depend on how well one can “line up” the small primes so that the  $p^{it}$  are “pointing” in roughly the same direction. One can prove (Kronecker’s theorem) that there exist  $t$  for which the primes  $p < \log t$  all have  $\Re p^{it} > 1/2$ . But

$$\sum_{p \leq x} p^{-1/2} \approx x^{1/2} / \log x.$$

With  $x = \log t$  this bound is near the smaller bound.

On the other hand, the new conjectures for moments<sup>74</sup> of the zeta-function may suggest that  $\zeta(1/2 + it)$  can be as big as the larger bound. One has

$$\max_{0 \leq t \leq T} |\zeta(1/2 + it)| \geq \left( \frac{1}{T} \int_0^T |\zeta(1/2 + it)|^{2k} dt \right)^{1/2k}.$$

If we substitute the conjectural asymptotic formula for the  $2k$ -th moment here and optimize over  $k$  one is led to the bigger bound.

A seemingly related problem is the order of the  $\zeta$ -function on the 1-line. On RH we have

$$e^\gamma \leq \limsup_{t \rightarrow \infty} \frac{\zeta(1 + it)}{\log \log t} \leq 2e^\gamma.$$

Again, it would be interesting to determine which number, the larger or the smaller value, is correct.

Similar results (or conjectures) concern ranks of elliptic curves<sup>51</sup>, Fourier coefficients of modular forms<sup>28</sup>, and many other problems.

For each of these cases there is a similar paradigm: a larger and a smaller guess, and (properly interpreted) those two guesses differ by a factor of two. These problems are all based on the size of the value of an L-function, and it is possible that they naturally fall into one of two categories, depending on whether the quantity in question naturally relates to a critical value<sup>130</sup> of an L-function, or a non-critical value<sup>131</sup> of an L-function. It is possible

<sup>74</sup>page 13, *The mean-value conjectures*

<sup>51</sup>page 23, *The maximal rank of an elliptic curve as a function of its conductor*

<sup>28</sup>page 24, *The distribution of Fourier coefficients of half-integral weight forms*

<sup>130</sup>page 23, *Maximal size of an L-function: critical values*

<sup>131</sup>page 25, *Maximal size of an L-function: non-critical values*

that for the problems related to critical values the larger guess is correct, while for non-critical values the smaller guess is correct. This change in behavior at the critical line was first suggested by Littlewood.

If there is indeed a fundamental distinction between the maximal size of critical<sup>130</sup> vs. non-critical<sup>131</sup> values, then it would also be important to understand the transition between those behaviors.

## E.1 Maximal size of an $L$ -function: critical values

The problems in this section can be directly related to a critical value (or the behavior on the critical line) of an  $L$ -function. In each case there are proven or conjectured upper and lower bounds, with those bounds differing by a factor of two. It may be that for these problems the larger value is the truth.

**E.1.a The maximal order of  $S(T)$ .** How big can  $S(T) := \frac{1}{\pi} \arg \zeta(1/2 + iT)$  be? Assuming the Riemann Hypothesis, it is known that  $S(T) \ll \log T / \log \log T$  but that infinitely often it is bigger than  $c(\log T / \log \log T)^{1/2}$  for some  $c > 0$ . Which is closer to the truth?

**E.1.b The maximal order of the zeta-function on the critical line.** How large is the maximum value of  $|\zeta(1/2 + it)|$  for  $T < t < 2T$ ? It is known that the Riemann Hypothesis implies that the maximum is at most  $\exp(c \log T / \log \log T)$  for some  $c > 0$ . It is also known that the maximum gets as big as  $\exp(c_1 (\log T / \log \log T)^{1/2})$  for a sequence of  $T \rightarrow \infty$  for some  $c_1 > 0$ . It has been conjectured that the smaller bound (the one that is known to occur) is closer to the truth. However, the new conjectures about moments<sup>74</sup> suggest that it may be the larger.

**E.1.c The maximal rank of an elliptic curve as a function of its conductor.** Many people believe that ranks of elliptic curves are unbounded. If so, what is the maximal rank of an elliptic curve as a function of its conductor? This question is related to the maximal size of the argument of  $L_E(1/2)$  for the (normalized)  $L$ -function associated with an elliptic curve  $E$ . (See the article on the maximal size of  $S(T)$ <sup>27</sup>.)

If one were to make a guess, the two possibilities which may seem most natural are that the maximal rank of a curve of conductor  $N$  is  $\log N / \log \log N$  (an upper bound which is implied by the Riemann Hypothesis) or  $\sqrt{\log N / \log \log N}$  (inspired by omega-results for  $S(T)$ ).

In the function field case the answer is the larger of these two as recent work of Ulmer [arXiv:math.NT/0109163] shows. Ulmer conjectures that the larger bound is occasionally achieved for elliptic curves over  $\mathbb{Q}$ .

An elementary version of this problem was formulated by Penney and Pomerance ([MR 51 #12862] and [MR 51 #12861]) for curves of the form

$$E : y^2 = x^3 + ax^2 + bx.$$

Define

$$A = \{n : n \mid b \text{ and } n + b/n + a \text{ is a square}\}.$$

---

<sup>130</sup>page 23, *Maximal size of an  $L$ -function: critical values*

<sup>131</sup>page 25, *Maximal size of an  $L$ -function: non-critical values*

<sup>74</sup>page 13, *The mean-value conjectures*

<sup>27</sup>page 23, *The maximal order of  $S(T)$*

Then the rank of  $E$  is  $\gg \log |A|$ . For example, if  $a = 17$  and  $b = -105$ , then

$$A = \{-21, -15, -7, -3, -1, 5, 7, 15, 35, 105\}.$$

Let  $d(b)$  be the number of divisors of  $b$ . Then

$$\limsup \frac{d(b)}{2^{\log b / \log \log b}} = 1,$$

so that  $\log |A| \ll \log b / \log \log b$ . Can  $\log |A|$  be as large as this?

Nick Katz suggests the following problem:

**Prove or Disprove:**  $\text{rank}(E) \leq C \sum e_i$ , where the conductor of  $E$  is  $\prod p_i^{e_i}$ , and  $C$  is the maximal rank of an elliptic curve with prime conductor.

It is conjectured by Brumer and Silverman [97e:11062] that the number of elliptic curves of prime conductor is infinite. So it is not clear that the constant “ $C$ ” in the above problem is finite.

**E.1.d The distribution of Fourier coefficients of half-integral weight forms.** Let

$$f(z) = \sum_{n=1}^{\infty} a(n) n^{(k-1)/2} e(nz)$$

be a newform of weight  $k$  for the full modular group, and let

$$g(z) = \sum_{n=1}^{\infty} c(n) n^{(k-1)/4} e(nz)$$

be a cusp form of weight  $(k+1)/4$  and level 4 which is associated to  $f(z)$  by the Shimura map. We normalize  $f$  by requiring that  $a(1) = 1$  and we normalize  $g$  by requiring that

$$\frac{1}{6} \int_{\Gamma_0(4) \backslash H} |g(z)|^2 y^{(k+1)/2} d\mu z = 1.$$

Then for squarefree  $q$  with  $\chi_q(-1) = (-1)^k$  we have, by the formula of Kohnen and Zagier,

$$c(q)^2 = \pi^{-\frac{k}{2}} \Gamma\left(\frac{k}{2}\right) L_f(1/2, \chi_q) \langle f, f \rangle^{-1}$$

where

$$\langle f, f \rangle = \int_{\Gamma_0(1) \backslash H} |f(z)|^2 y^k d\mu z.$$

In particular, the Riemann Hypothesis for  $L_f(s, \chi_q)$  implies that

$$c(q) \ll \exp(c \log q / \log \log q)$$

for an appropriate choice of  $c$ . If the bound

$$L_f(1/2, \chi_q) \ll \exp(c_1 \sqrt{\log q / \log \log q})$$

holds, then a similar bound for  $c(q)$  will hold (but with  $c_1$  replaced by  $c_1/2$ ). The question here is to decide which (if either) of these bounds represents the true state of affairs.

If  $q$  has a square factor, then  $c_q$  can be determined from values of  $a_p$  where  $p^2 \mid q$ . It is known, by Deligne’s theorem, that

$$|a_n| \leq d(n)$$

where  $d(n)$  is the number of divisors of  $n$ . Of course,  $d(p) = 2$  so that we can write

$$a_p = 2 \cos \theta_p$$

where  $\theta_p$  is real. The conjecture of Sato and Tate about the distribution of the  $\theta_p$  asserts that

$$\lim_{x \rightarrow \infty} x^{-1} \sum p \leq x\alpha < \theta_p < \beta \log p = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \theta \, d\theta$$

for  $0 \leq \alpha < \beta \leq \pi$ . A consequence of the Sato-Tate conjecture is that there are infinitely many  $p$  (actually a positive proportion of  $p$ ) for which

$$2 - \epsilon < a_p < 2$$

for any given  $\epsilon > 0$ . The maximum order of  $d(n)$  is given by

$$\limsup_{n \rightarrow \infty} \frac{\exp(\log 2 \log n / \log \log n)}{d(n)} = 1.$$

The Sato-Tate conjecture implies the same assertion with  $d(n)$  replaced by  $a_n$ .

Thus, in particular, we find that

$$c(p^2) = a(p) \ll \exp(\log 2 \log p / \log \log p)$$

and we expect this bound to be sharp in the sense that the  $\log 2$  cannot be replaced by anything smaller.

Thus, if the “smaller” bound is true for  $L_f(1/2, \chi_q)$  then there is a great variation between the distribution of the Fourier coefficients  $c(n)$  according to whether  $n$  is square or squarefree.

**E.1.e Omega results for twists.** We write  $f(x) = \Omega(g(x))$  to mean  $\limsup_{x \rightarrow \infty} f(x)/g(x) > 0$ .

Hoffstein and Lockhart [2000j:11071] prove an  $\Omega$ -result for quadratic twists of the  $L$ -function associated to a holomorphic newform on  $\Gamma_0(N)$ :

$$L\left(\frac{1}{2}, f, \chi_d\right) = \Omega(\exp(c\sqrt{\log d}/\log \log d))$$

for squarefree  $d \rightarrow \infty$ , for some  $c > 0$ .

It would be interesting to prove  $\Omega$ -results for the collection of all Dirichlet  $L$ -functions  $L(\frac{1}{2}, \chi)$ ,  $\chi \pmod{d}$ , and for twists by all characters of  $L(\frac{1}{2}, f, \chi)$ , for  $f$  a cusp form.

## E.2 Maximal size of an $L$ -function: non-critical values

The problems in this section can be directly related to a non-critical value (or the behavior off the critical line) of an  $L$ -function. In each case there are proven or conjectured upper and lower bounds, with those bounds differing by a factor of two. It may be that for these problems the smaller value is the truth.

**E.2.a The order of the  $\zeta$ -function on the 1-line.** On RH we have

$$e^\gamma \leq \limsup_{t \rightarrow \infty} \frac{\zeta(1+it)}{\log \log t} \leq 2e^\gamma,$$

and

$$\frac{6}{\pi^2} e^\gamma \leq \limsup_{t \rightarrow \infty} \frac{1/\zeta(1+it)}{\log \log t} \leq \frac{12}{\pi^2} e^\gamma,$$

where  $\gamma$  is Euler's constant. See Titchmarsh [ 88c:11049] for proofs.

Since these estimates concern non-critical values of an  $L$ -function, one might suspect that the smaller of each of the above results is the true answer.

**E.2.b The order of  $\zeta'/\zeta$ .** Assume the Riemann Hypothesis. Define  $\nu(\sigma)$  for  $\sigma > 1/2$  to be the greatest lower bound of the numbers  $\nu$  for which

$$\frac{\zeta'}{\zeta}(\sigma + it) \ll_{\epsilon} (\log t)^{\nu+\epsilon}$$

holds as  $t \rightarrow \infty$  for all  $\epsilon > 0$ . It is a theorem that  $\nu(\sigma)$  is a convex function of  $\sigma$  which is continuous and decreasing for  $\sigma > 1/2$  with  $\nu(\sigma) = 0$  for all  $\sigma \geq 1$ . It can be shown that

$$1 - \sigma \leq \nu(\sigma) \leq 2 - 2\sigma$$

for  $1/2 < \sigma < 1$ . There is an analogous function which can be defined for  $\log |\zeta(\sigma + it)|$  and it can be shown that this analogous function is, in fact, equal to  $\nu(\sigma)$ . See Titchmarsh for all of these facts. Which bound is correct?

If the smaller bound is the correct one, then near the half-line we see that

$$\frac{\zeta'}{\zeta}(1/2 + a + it) \ll_{\epsilon} (\log t)^{1/2-a+\epsilon}$$

for  $a > 0$ . On the other hand,

$$\Re \frac{\zeta'}{\zeta}(1/2 + it) = \frac{1}{2} \frac{\chi'}{\chi}(1/2 + it) = -\frac{1}{2} \log t + O(1).$$

Thus, if the smaller bound holds, then there is a jump at  $1/2$ . It could be that the smaller bound holds to the right of the critical-line but that there is radically different behavior on the critical line.

**E.2.c The maximal size of  $h(D)$ .** By the class number formula,  $h(d) = \frac{\sqrt{D}}{\pi} L(1, \chi_d)$ . Thus, the maximal size of the class number of an imaginary quadratic field should be governed by the same considerations as the maximal order of the  $\zeta$ -function on the 1-line<sup>136</sup>.

### E.3 Difficult to classify

The extremal problems in this section are not easily identified as being related to values of an  $L$ -function. Thus, it is not clear if they fall under the categories of critical vs. non-critical values.

**E.3.a Large gaps between primes.** Is it true that

$$\limsup_{p \rightarrow \infty} \frac{p' - p}{\log^2 p} = 2e^{-\gamma} ?$$

---

<sup>136</sup>page 25, *The order of the  $\zeta$ -function on the 1-line*

**E.3.b Extreme gaps between consecutive zeros of the zeta-function.** The number of zeros of  $\zeta(s)$  with imaginary parts smaller than  $T$  is given by

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi e} + O(1/T) + S(T)$$

where

$$S(T) = \frac{1}{\pi} \arg \zeta(1/2 + iT).$$

It is known that  $S(T) \ll \log T$  and, conditional on the Riemann Hypothesis that

$$S(T) \ll \frac{\log T}{\log \log T}.$$

Thus, the average gap between zeros of  $\zeta(s)$  at height  $T$  is  $\frac{2\pi}{\log T}$  and  $S(T)$  measures the local fluctuations in the zero spacings. (If not for  $S(T)$  the zeros of  $\zeta(s)$  would have a ‘picket fence’ spacing.)

Clearly, a large gap between consecutive zeros of  $\zeta(s)$  implies that  $S(T)$  is correspondingly large. It seems not unreasonable to speculate that the largest gaps between consecutive zeros of  $\zeta(s)$  will ‘match’ with the largest values of values of  $S(T)$ :

$$\lim_{T \rightarrow \infty} \frac{(\log T) \max_{\gamma < T} (\gamma^+ - \gamma)}{2\pi \max_{t < T} S(t)} = 1$$

Thus, if  $2\pi S(T)$  is occasionally as large as  $c \log T / \log \log T$  see the article on  $S(T)$ <sup>27</sup> then we would expect the maximal gaps between zeros of  $\zeta$  to be as large as  $c / \log \log T$ .

**E.3.c Maximal clusters of zeros of the zeta-function.** Random matrix theory predicts that at a height  $T$ , the closest that two zeros of  $\zeta(s)$  could be is about  $T^{-1/3}$ . (Unlike the situation of large gaps, where the primes enter into the picture in a critical way, the random matrix prediction is expected to give the right answer here.) Now the question is, how many zeros could be clustered together in a small region? Clearly, this question is related to large values of  $S(T)$ . Let  $M_S(T) = \max_{t < T} S(t)$ . Is it reasonable to believe that for certain  $T$  there will be  $\gg M_S(T)$  zeros clustered together in an interval  $(T, T + T^{-1/3+\epsilon})$ ?

## CHAPTER F: FUNCTION FIELD ZETA-FUNCTIONS

Much of our understanding about the connection between  $L$ -functions and random matrix theory comes from analogies with function fields, for in the function fields case it is possible to prove many of the results which are only conjectured for number fields. This is described in the book of Katz and Sarnak [2000b:11070].

The analogy between the two cases is not perfect (or at least, not perfectly understood). For example, it is not known what should play the role of monodromy in the number field case. Another example is the proof of the Riemann hypothesis. In the function field case the proof makes use of high tensor powers, so it would be desirable to understand the analogue of this in the number field case.

In this section we address questions relating to function fields, as well as the analogy between function fields and number fields.

---

<sup>27</sup>page 23, *The maximal order of  $S(T)$*

## F.1 Fixed $q$

The results of Katz and Sarnak [2000b:11070] concern curves of genus  $g$  over  $\mathbb{F}_q$  with both  $g \rightarrow \infty$  and  $q \rightarrow \infty$ .

It would be interesting to have results in the case of fixed  $q$ . Does one still get random matrix statistics?

A particular case that it worth investigating is the set of all quadratics over  $\mathbb{F}_q$ .

## F.2 Corrections for small degree

The available numerical data does not agree well with the theoretical results. Find a model (with  $d \rightarrow \infty$  slowly?) which explains the discrepancy.

(Help is sought in making the above more precise).

## F.3 Effective computation of zeta-functions

The Weil conjectures (proved by Dwork, Grothendieck, Deligne et al.) assert that for any algebraic variety  $X$  over a finite field  $F_q$ , the power series

$$\zeta_X(T) = \exp \left( \sum_{i=1}^{\infty} \frac{\#X(F_{q^i})}{i} T^i \right)$$

is a rational function of  $T$ ; giving explicit methods for computing  $\zeta_X(T)$  is a fundamental problem in computational number theory. In principle, one can do this by simply giving bounds on the degrees of the numerator and denominator, then explicitly computing  $\#X(F_{q^i})$  for enough values of  $i$ . (E.g., if  $X$  is projective, one can choose a projective embedding of  $X$ , defined by certain equations, then count the number of points in projective space satisfying those equations.) In practice, this enumeration gives an algorithm which requires time exponential in the “complexity” of  $X$  (e.g., the logarithm of the base field size  $q$ , and the degrees of the equations defining  $X$ ) and thus can only be completed for relatively small examples.

Below we describe the current state of knowledge regarding subexponential methods for computing zeta functions. We omit mention of methods which improve on pure exhaustion but are still exponential, such as Mestre’s “baby step-giant step” method for computing the zeta function of an elliptic curve.

**F.3.a Computing the local factors of an elliptic curve.** The simplest nontrivial case of a zeta function is for  $X$  an elliptic curve; in this case

$$\zeta_X(T) = (1 - aT + qT^2)/(1 - T)(1 - qT)$$

for some integer  $a$ , and the problem is simply to determine  $a$ . Moreover, by the Weil conjectures,  $|a| \leq 2\sqrt{q}$ .

Schoof [86e:11122] [97i:11070] introduced an algorithm for computing the zeta function of an elliptic curve over a finite field  $F_q$  which is polynomial time in  $\log q$ . His strategy is to compute  $a$  modulo enough small primes that the Chinese remainder theorem plus the Weil bound on  $a$  together determine  $a$  uniquely. Practical improvements to the algorithm were later introduced by Atkin and Elkies. The result is fairly efficient in practice, and many implementations are available (e.g., in the computer algebra package Magma).

In small characteristic, even more efficient methods are available. The algorithm of Satoh [2001j:11049] computes the zeta function of an ordinary elliptic curve over  $F_{p^n}$ , for

$p$  prime, in time polynomial in  $p$  and  $n$ , essentially by computing  $a$  modulo a suitably high power of  $p$ . (The restriction to ordinary elliptic curves is not a big problem, as the supersingular case is quite easy to handle, even by hand.) Thus it is not useful for fields of large characteristic. However, it is more efficient than Schoof’s algorithm for fields of small characteristic. Satoh’s algorithm was originally limited to  $p \neq 2, 3$ ; later authors have removed this restriction, e.g. Fouquet, Gaudry and Mestre [1 801 223] and Skjernaas [B. Skjernaas, Satoh point counting in characteristic 2, preprint].

Satoh’s algorithm involves iteratively computing the Serre-Tate canonical lift of the given elliptic curve. It may be possible to streamline the calculation by retaining the iteration while omitting some irrelevant data about the canonical lift. An example of is the AGM method of Gaudry, Harley and Mestre (Eurocrypt 2001 rump session), which is limited to characteristic 2 but outperforms all known algorithms in that case.

**F.3.b Computing the local factors of higher genus curve.** Not much is known about computing zeta functions of curves of genus greater than 1; all known methods involve computing  $p$ -adic approximations of the zeta function, so are limited to small characteristic. Attempts to generalize the methods of the previous section have mostly been unsuccessful. A generalization “in principle” of Schoof’s algorithm to higher genus was given by Pila [91a:11071], but it requires explicit equations for the Jacobian of the curve. It is possible this could be carried out in genus 2, but seems hopeless for higher genus. Satoh’s method hinges on the existence of the canonical lift; in higher genus, the Jacobian of an ordinary curve admits a Serre-Tate lift as a principally polarized abelian variety, but the lift need not be a Jacobian, making working with it difficult. In genus 2, this problem does not arise, and Harley (Midwest Algebraic Geometry in Cryptography 2001 talk) has proposed a genus 2 version of the AGM method that will probably be quite efficient in practice.

A very general algorithm of Lauder and Wan [A.G.B. Lauder and D. Wan, Counting points on varieties over finite fields of small characteristic, preprint], based on Dwork’s proof of the rationality of the zeta function, gives an algorithm for computing the zeta function of a genus  $g$  curve over  $\mathbb{F}_{p^n}$  in time polynomial in  $p$ ,  $n$  and  $g$ . However, the algorithm seems difficult to implement in practice. Lauder and Wan also have a simplified version [A.G.B. Lauder and D. Wan, Computing zeta functions of Artin-Schreier curves over finite fields, preprint] of their algorithm in the special case of Artin-Schreier curves of  $p$ -rank 0, and it is likely that other special cases can be handled efficiently.

A related distinct approach is used in an algorithm of Kedlaya [arxiv:math.AG/0105031](K.S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, J. Ramanujan Math. Soc. 16,(2001), 323–338), which computes the zeta function of a genus  $g$  hyperelliptic curve over  $\mathbb{F}_{p^n}$  ( $p$  odd) in time polynomial in  $p$ ,  $n$  and  $g$ . This algorithm uses the Lefschetz trace formula for Monsky-Washnitzer cohomology. This technique has been extended by Gaudry and Gurel [An extension of Kedlaya’s algorithm to superelliptic curves, to appear in Advances in Cryptology–ASIACRYPT 2001, Springer-Verlag Lecture Notes in Computer Science] to handle superelliptic curves, and by Denef and Vercauteren [J. Denef and F. Vercauteren, An extension of Kedlaya’s algorithm to Artin-Schreier curves in characteristic 2, preprint] to handle Artin-Schreier curves of  $p$ -rank 0 or 1; again, it is likely that other cases can be handled efficiently. (Denef and Vercauteren, in their paper, indicate that they can handle general Artin-Schreier curves, and in fact arbitrary curves, but details are not yet available.)

Remaining questions include:

- developing efficient implementations of the above algorithms;
- developing algorithms for more general curves;
- developing algorithms for higher dimensional varieties.

Once efficient implementations are available, it will be possible to conduct some new experiments, e.g., determine experimentally the distribution of the zeroes of the zeta function over all hyperelliptic curves of a given large genus over a given small field.

## F.4 More function field analogues are needed

There are several families of  $L$ -functions over a number field for which we don't currently know the correct analogue in the function field case. Two of these are:

A. The family of all Dirichlet  $L$ -functions  $L(s, \chi)$ .

B. The family of  $L$ -functions  $L(f, s)$  associated to  $S_k(N)$ , with  $k$  fixed and  $N \rightarrow \infty$ . Here  $S_k(N)$  is the space of weight  $k$  cusp forms for the Hecke congruence group  $\Gamma_0(N)$ .

## F.5 Distribution of sha in quadratic twists

We seek someone to write on this topic.

## CHAPTER G: RANDOM MATRIX QUESTIONS

The topics below are phrased in terms of random matrix theory, although many of them are motivated by the analogous questions concerning  $L$ -functions.

### G.1 Distribution of zeros of derivatives of characteristic polynomials

The eigenvalues of a unitary matrix lie on the unit circle. Therefore the zeros of the derivative of the characteristic polynomial of the matrix lie strictly inside the unit circle (apart from those coming from multiple zeros).

How are the zeros of the derivative distributed? What is the distribution of the absolute value of those zeros?

This question is related to the question of zeros of the derivative of the zeta-function<sup>71</sup>, where one would like to know how far the zeros of  $\zeta'(s)$  lie to the right of the  $\frac{1}{2}$ -line.

### G.2 The distribution of eigenvalues of high powers of a matrix

Let  $CL(N)$  denote a classical group of unitary  $N \times N$  matrices. Andrew Granville asks for a simple proof of the fact that if  $M > N$  then the eigenvalues of  $A^M$  for  $A \in CL(N)$  are uniformly distributed on the  $N$ -torus.

### G.3 $p$ -adic random matrix theory

Can  $p$ -adic random matrix theory explain the arithmetic factors that appear in the asymptotic formulas for the mean values<sup>74</sup> of  $L$ -functions?

It would be interesting to evaluate moments of the  $p$ -adic absolute value of the characteristic polynomial of matrices averaged over the classical groups (over  $\mathbb{Z}_p$ ). In other words,

---

<sup>71</sup>page 7, *Horizontal distribution of the zeros of  $\zeta'(s)$*

<sup>74</sup>page 13, *The mean-value conjectures*

evaluate

$$\int_{GL_n(\mathbb{Z}_p)} |\det(1 - u)|_p^s du.$$

(More information is sought. It was suggested that these calculations may have already been done by Anderson(?) or they may be in Macdonald's book?)

## CHAPTER H: MISCELLANEOUS TOPICS

It is hoped that these topics will eventually be expanded or incorporated into the main sections of this web page.

### H.1 Explicit Formula

In the conjectures for mean-values<sup>31</sup> there are two factors to notice: one is the arithmetical function  $a_k$ , which arises in a quite natural way from the techniques of Dirichlet polynomials. The other is the factor  $g_k$  which arises from Random Matrix theory.

These conjectures are a kind of pasting together of random matrix theory techniques and Dirichlet polynomial techniques.

An explanation for this phenomenon of disparate pieces is that the random matrix theory explains behavior of zeros clustered together in a spacing of approximately the inverse of the logarithm of the conductor, whereas it is quite likely that the arithmetical  $a_k$  arises from considerations of longer range correlations of the zeros of the family. The fact that the  $a_k$  do not appear from random matrix theory pose no problem from the point of view of the highest order main term of the asymptotic formula. However, we know that for the second and fourth moments of  $\zeta$  the main terms are actually polynomials of degrees 1 and 4, all terms of which can be expressed in closed form (See "Lower Order terms")<sup>75</sup>. These terms seem to involve derivatives of  $a_k$  at  $k = 1$  and  $2$  as well as mysterious geometric factors that should be explainable from random matrix theory.

In order to really understand the mechanism connecting prime numbers, random matrices, and mean-value formulas, we will likely need to proceed via the explicit formula of Weil [MR 14,727e] (see also Guinand [MR 10,104g]). This formula is the explicit link between zero sums and prime number sums which will be needed to rigorously explain the connection between short and long range correlations.

Thus, we want a model of the Riemann zeta-function as a product of two factors: one of which is a kind of Euler product and the other is a kind of Hadamard product (whose behavior is like that of the characteristic polynomial of a random unitary matrix).

A related problem is to find a model for the distribution of zeros which works for both short and long range correlations. This would presumably include a random matrix model for the short range behavior, and some other model (somehow based on the prime numbers?) for the long range behavior.

---

<sup>31</sup>page 12, *Mean-values*

<sup>75</sup>page 16, *Lower order terms*

## H.2 Distribution of critical values

By considering the moments of  $\log \zeta(1/2 + it)$ , Selberg (in unpublished work) proved that for Borel measurable sets  $B$ ,

$$\lim_{T \rightarrow \infty} \frac{1}{T} \text{meas} \left\{ t \in [0, T] : \frac{\log \zeta(1/2 + it)}{\sqrt{1/2 \log \log T}} \in B \right\} = \frac{1}{2\pi} \iint_B e^{-(x^2+y^2)/2} dx dy$$

which roughly speaking says that, high up the critical line, the real and imaginary parts of  $\log \zeta(1/2 + it)$  behave like independent Gaussian random variables with mean zero and variance  $\frac{1}{2} \log \log T$ .

It is also of interest to look at the tails of this distribution, for example the probability that  $\log |\zeta(1/2 + it)|$  takes very large negative values (which will be when  $|\zeta(1/2 + it)|$  is very small). One can make plausible conjectures about the behaviour of

$$P(T, x) = \frac{1}{T} \text{meas} \{ t \in [0, T] : \log |\zeta(1/2 + it)| < -x \}$$

when  $x$  is very large, using methods of random matrix theory. In particular, Hughes, Keating and O'Connell [Proc. R. Soc. Lond. 456, 2611–2627] and Keating and Snaith [Comm. Math. Phys 214, 57–89] have conjectured that for large  $T$ ,

$$\lim_{x \rightarrow \infty} e^x P(T, x) \sim G^2(1/2) a(-1/2) (\log T)^{1/4}$$

where  $G$  is the Barnes  $G$ -function, and  $a(k)$  is a certain product over primes, coming from mean values<sup>74</sup> of the  $\zeta$ -function.

But much more is true (Hughes, PhD thesis). Writing  $x = y \log \log T$ , then it is conjectured that for large  $T$ ,

$$P(T, y \log \log T) \sim G^2(1/2) a(-1/2) (\log T)^{1/4-y}$$

uniformly for any  $y > 1/2$ . The fact that  $y$  is restricted to being greater than  $1/2$  is important, since there is a phase transition there:

$$\lim_{T \rightarrow \infty} \frac{\log P(T, y \log \log T)}{\log \log T} = \begin{cases} -y^2 & \text{for } 0 < y < 1/2 \\ 1/4 - y & \text{for } y > 1/2 \end{cases}.$$

And thus we see a change in the behaviour of the left tail of the distribution of  $\log |\zeta(1/2 + it)|$  from the Gaussian decay (anticipated from Selberg's result) to exponential decay.

## H.3 GOE and Graphs

To a graph one can associate a combinatorial Laplacian, which operates on functions on the vertices by giving the sum of the differences between the values of a function  $f$  at the vertex and its neighbors:

$$\Delta f(x) = \sum_{y \sim x} (f(x) - f(y)),$$

the sum being over all neighbours of the vertex  $x$ . There are  $|V|$  eigenvalues. If we take a sequence of graphs such that the number of edges tends to infinity, then under certain conditions there is a limiting density of states analogous to Weyl's law. This gives a mean counting function  $\tilde{N}(E)$ , the expected number of levels below  $E$ . If, as usual, we unfold the

---

<sup>74</sup>page 13, *The mean-value conjectures*

sequence, then we get a sequence  $\tilde{E}_j$  with mean spacing unity. Put  $s_j := \tilde{E}_{j+1} - \tilde{E}_j$ . Then  $P_N(s) = \frac{1}{N} \sum \delta(s - s_i)$  is the distribution function of the spacings and is called the level spacing distribution of the graph.

A question that arises is to study the level spacing distribution of certain families of graphs. One such family is the family of  $k$ -regular graphs. A graph is  $k$ -regular if each vertex has exactly  $k$  neighbours. For this family numerical evidence [1] indicates that the resulting family of graphs have GOE spacings. Indeed in [1] the authors conjecture that for fixed degree  $k \geq 3$ , the eigenvalues of the generic  $k$ -regular graph on a large number of vertices have fluctuations which tend to those of GOE.

On the other hand certain classes of graphs are known (for example 4-regular Cayley graphs on  $SL_2(F_p)$ ,  $S_{10}$ , and large cyclic groups) where numerics suggest that the eigenvalue distribution is Poisson [2000g:05072]. Cayley graphs on  $SL_2(F_p)$  are naturally thought of as discrete approximations to the spectral behaviour in the continuous setting of  $SL_2(Z) \backslash H$ , where computations indicate that the spacing distribution should be also Poisson. In all cases where the distribution seems to be Poisson, there are symmetries or degeneracies (eigenvalues occurring with a high multiplicity).

[1] D. Jakobson, S.D. Miller, I. Rivin and Z. Rudnick, Eigenvalue spacings for regular graphs, in Emerging applications of number theory.