Alberta Number Theory Days – L-functions

Paul Buckingham (University of Alberta),
Matthew Greenberg (University of Calgary)

30th April 2010–2nd May 2010

1 Overview

Alberta Number Theory Days fell at the very start of the newly formed PIMS CRG in Number Theory, and was thus an excellent opportunity to kickstart interactions between three of the participating institutions, the universities of Alberta, Calgary and Lethbridge. A broad range of topics in number theory were featured, but almost all talks were in areas motivated by the understanding of L-functions. Indeed, two key frameworks in which L-functions are viewed were addressed during the weekend, each forming a core of talks.

The first framework is the analytic study of L-functions with the view to deriving properties of prime numbers. This included a reformulation of the generalized Riemann hypothesis by Brandon Fodden in terms of a decidable property of the natural numbers, thus giving a new insight into this most important of conjectures. In a related direction, Amir Akbary (discussing joint work with Brandon Fodden) gave improved bounds on the power moments of L-functions in the Selberg class, with applications to principal automorphic L-functions and Artin L-functions. Kaneenika Sinha's presentation also concerned bounds, but this time bounds on the analytic rank of Jacobians of modular curves, an area of study with links to the famous conjecture of Birch and Swinnerton-Dyer.

The second framework is the overarching Langlands programme, one of whose principal goals is to equate L-functions of Galois representations, important objects associated with the absolute Galois group of $\mathbb{Q}$, with L-functions of automorphic representations. The talks of Clifton Cunningham, Vinayak Vatsal and Jeremy Sylvestre can be viewed under the umbrella of the Langlands programme, and a particular highlight was Cunningham's criterion for when a certain L-packet arising from an elliptic curve was infinite, a criterion given in terms of the set of supersingular primes of the elliptic curve.

It was also a delight to observe Dustin Moody's talk on a novel way to count isogenies between elliptic curves over finite fields via isogeny volcanoes. The closing talk of the conference, by Matthew Greenberg, demonstrated the impressive contribution that Dembélé, Greenberg and Voight have made towards the verification of a conjecture of Gross, with only one case remaining.

The context for the talks will be described more fully in Section 2.

2 Conference themes in more detail

2.1 Analytic number theory

One of the main principles in studying the analytic behaviour of L-functions is to be able to infer properties of the prime numbers. For example, the biggest open problem in this direction is the Riemann hypothesis, whose assertion is that the non-trivial zeroes of the Riemann ζ-function should all have real part $1/2$. The most

important arithmetic consequence of this is a very precise description of the distribution of the primes in terms of the logarithmic integral Li. In the words of Enrico Bombieri, "In the opinion of many mathematicians, the Riemann hypothesis, and its extension to general classes of L-functions, is probably the most important open problem in pure mathematics today."

Related to the Riemann hypothesis (a consequence, in fact, in the case of the Riemann ζ-function) is the Lindelöf hypothesis, which makes a prediction concerning the clustering of the zeroes of the ζ-function around the line $\mathrm{Re}(s) = 1/2$. It implies, in particular, a bound on the difference between consecutive primes.

Both of the above conjectures were featured in Alberta Number Theory Days. In the first case, it is known that the Riemann hypothesis is equivalent to a statement of the form $\forall n, P(n)$, where $P(n)$ is a decidable property of the natural numbers; this goes back to Kreisel. A property $P(n)$ which is more amenable to study was found by Davis, Matiyasevich, Robinson and Shapiro in 1976. **Brandon Fodden** discussed work in which he generalized this idea to the Selberg class, a class of Dirichlet L-functions proposed by Selberg [9] which satisfy certain standard expected properties of L-functions that arise in arithmetic contexts. More precisely, if f is a member of the Selberg class, then Fodden gives an explicit property $P(n)$ for natural numbers n such that the generalized Riemann hypothesis for f holds if and only if $P(n)$ is true for all n. As an application, he showed that when f is the L-function of an elliptic curve over $\mathbb{Q}$ – an archetypal member of the Selberg class – the property $P(n)$ is indeed decidable. By the work of Davis, Matiysevich and Robinson on Hilbert's tenth problem, this therefore implies that the generalized Riemann hypothesis for f is equivalent to the insolvability of a Diophantine equation.

Now to turn to another problem associated with the Selberg class. The Lindelöf hypothesis for a member of the Selberg class can be reformulated in terms of the power moments of that series, which are integrals of powers of the given series along partial segments of a vertical line in the critical strip. Ramachandra showed that in the case of the Riemann ζ-function, the kth power moment is bounded below in terms of $T(\log T)^{k^2}$ under the assumption of the Riemann hypothesis, with Heath-Brown [5] removing that assumption a year later in 1981, at the cost of restricting attention to rational k rather than real k.

In the past five years, Laurincikas et al have succeeded in obtaining similar results for power moments of other Dirichlet series, inspired by Heath-Brown's method. Principally they dealt with kth power moments where k is the reciprocal of an integer greater than 2. As discussed in his talk, **Amir Akbary**, together with Brandon Fodden, has obtained a quite general result on a class of Dirichlet L-series that can be specialized to include principal automorphic L-functions and Artin L-functions. In the former case, Akbary and Fodden's result generalizes the aforementioned result of Laurincikas et al to rational k. In the Artin case, the lower bound given by Akbary and Fodden is $T(\log T)^{(\|\chi\|k)^2}$, where $\|\chi\|$ is the norm of the given character χ. This specializes, in the case of the Dedekind ζ-function of a Galois extension of $\mathbb{Q}$ of degree n, to the lower bound $T(\log T)^{nk^2}$, improving on a lower bound of Ramachandra.

A particular kind of L-function that is at the forefront of the geometric side of number theory is the L-function associated to some arithmetically defined abelian variety. Such an L-function is expected to hold important information about the arithmetic of the variety. For example, the order of vanishing of the L-function at 1, called the analytic rank, is conjectured by Birch and Swinnerton-Dyer (original form found in [1]) to be the rank of the group of rational points on the variety, also known as the algebraic rank. This conjecture on the analytic and algebraic ranks of an abelian variety over a number field is still only known in restricted cases.

In her talk, **Kaneenika Sinha** described how one can obtain upper bounds on the analytic rank of the new part of the Jacobian of the modular curve $X_0(N)$, at least when averaging over a sequence of consecutive values of N. More precisely, this bound is given in terms of the average of the dimensions of the spaces of new forms of level N and weight 2 for the same consecutive integers N.

2.2 The Langlands programme

Class field theory, the framework in which one aims to survey all abelian extensions of a given number field, could be said to have had its origins in the Kronecker–Weber Theorem, which asserts that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. One way to prove this theorem is via the information which goes into constructing L-functions associated with $\mathbb{Q}$. On the one hand, there are Artin L-functions for abelian Artin representations of $\mathbb{Q}$, and on the other hand there are Dirichlet L-functions for Dirichlet characters arising from the Artin representations. It turns out that the information that the latter gives about

the former says enough about the splitting of primes in a given abelian extension of $\mathbb{Q}$ to establish that it must lie in a cyclotomic field.

The Langlands programme can be seen as a large-scale generalization of this phenomenon. Dirichlet characters are replaced by automorphic representations of the adelic points of a connected reductive algebraic group, and Artin representations by Galois representations into the Langlands "dual group" ${}^LG$. The philosophy is that there should be a way of assigning the latter to the former in a precise way, but in particular so that L-functions are preserved. If the programme is successful, the applications to L-functions, and number theory more generally, will be significant. Indeed, L-functions of Galois representations are in themselves difficult to study, but if we knew that they were equal to L-functions of automorphic representations, which are simpler to understand, a host of expected properties of the Galois L-functions would be confirmed.

When the algebraic group in question is GL_n, this assignment is expected to be bijective. However, in general this need not be the case, and the potential failure of injectivity gave rise to the notion of L-packets. These are defined to be the fibres of the assignment taking automorphic representations of G to Galois representations into ${}^LG$. In the local version of the conjectures, L-packets are finite, but this is not always the case in the global setting.

The infinitude of L-packets in the global setting was a point of commonality of the talks of **Clifton Cunningham** and **Vinayak Vatsal**. A highlight of Cunningham's talk was a characterisation of when a particular L-packet arising naturally from an arithmetic situation would be infinite. More precisely, if one considers the automorphic representation of GL_2 arising from an elliptic curve, then although the corresponding L-packet is a singleton, the L-packet once we pass by functoriality to SL_2 need not be. Indeed, as described by Cunningham, the L-packet of SL_2 is infinite if and only if the elliptic curve admits infinitely many supersingular primes. Note that this L-packet is therefore necessarily infinite for elliptic curves defined over a number field of odd absolute degree, thanks to Elkies' proof of the infinitude of the set of supersingular primes of such an elliptic curve [3]. Vatsal's talk also addressed differences between representations of GL_2 and SL_2, with emphasis on the effects on the non-vanishing of L-functions.

Also viewable in the context of the Langland's programme, the talk by **Jeremy Sylvestre** discussed depth-zero representations of GL_n of a local field, and θ-twists of these. The main aims of the talk were to show that the character of the twist satisfies a Harish-Chandra type integral formula, and to provide an equation for the character in terms of characters of depth-zero supercuspidal representations.

2.3 Volcanoes

in 1985, René Schoof [8] proposed an algorithm, later improved by Elkies and Atkin, for computing the number of points on an elliptic curve over a finite field, a key ingredient in the definition of the L-function of an elliptic curve over a global field. Some variations of this algorithm, known as the SEA algorithm after the principal contributers, employ so-called *isogeny volcanoes* as a way of organising the information about isogenies between elliptic curves. Constructing isogeny volcanoes is something of an ad hoc process. In his very illuminative talk, **Dustin Moody** outlined some improvements on algorithms for constructing isogeny volcanoes, with the aim of improving the efficiency. Applications of the method include identifying m-isogenies with m a prime or a product of two primes (not necessarily distinct).

2.4 Positive solutions to cases of a conjecture of Gross

Controlling ramification in extensions of number fields is not a straightforward process. In particular, the number of primes that ramify can be large, and demanding that only one prime ramify imposes significant restrictions. For abelian extensions of $\mathbb{Q}$, finding examples where only one prime ramifies is classical: one can just take cyclotomic extensions obtained by adjoining a root of unity of prime-power order, taking the maximal real subfield if one further wishes the infinite place to split completely. However, for non-solvable Galois extensions of $\mathbb{Q}$, the problem is still not entirely complete.

In [4], Gross conjectured that for each prime p, there should be a real non-solvable Galois extension of $\mathbb{Q}$ ramified only at p. (Note: In our present formulation of the conjecture, we opt to use Neukirch's convention on the terminology for the splitting of infinite primes [7, p.184]. Namely, infinite primes are always declared unramified, but are either split completely or not split completely. Thus in the above formulation of the conjecture, it is necessary under this convention to include the word "real", since "unramified outside p" does

not capture this.) For $p \geq 11$, Gross' Conjecture is a consequence of the work of Khare and Wintenberger [6] on Serre's Modularity Conjecture, but for the primes 2, 3, 5 and 7, Gross' Conjecture saw no further progress until Dembélé's discovery [2] of a real non-solvable Galois extension of $\mathbb{Q}$ ramified only at 2.

In a very interesting talk discussing joint work with Dembélé and Voight, **Matthew Greenberg** revealed examples giving a positive solution to the conjecture for the primes 3 and 5. Building on the method of Dembélé for $p = 2$, the strategy of Dembélé, Greenberg and Voight used Hilbert modular forms to obtain systems of Hecke eigenvalues in the cohomology of a Shimura curve. The computations themselves are also impressive, exhibiting examples of fields with approximate absolute degrees of as much as $3 \cdot 10^{52}$. The case $p = 7$ of Gross' Conjecture is now the remaining unsolved case.

3 Concluding remarks

A number of participants commented on how much they enjoyed the conference, with particular reference to the high quality of the talks. The success of the weekend increases the likelihood that Alberta Number Theory Days, previously a one-day meeting, will remain a two-day event in subsequent years.

The organizers would like to thank BIRS and the Banff Centre for their hospitality and helpful staff, greatly adding to the enjoyment of the weekend. We would also like to thank the speakers for their hard work, and to acknowledge the generous support from PIMS and the universities of Alberta and Calgary.

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[2] Lassina Dembélé. A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only. *C. R. Math. Acad. Sci. Paris*, 347(3-4):111–116, 2009.

[3] Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[4] Benedict H. Gross. Modular forms $(\mathrm{mod}\ p)$ and Galois representations. *Internat. Math. Res. Notices*, (16):865–875, 1998.

[5] D. R. Heath-Brown. Fractional moments of the Riemann zeta function. *J. London Math. Soc. (2)*, 24(1):65–78, 1981.

[6] Chandrashekhar Khare and Jean-Pierre Wintenberger. On Serre's conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Ann. of Math. (2)*, 169(1):229–253, 2009.

[7] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[8] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[9] Atle Selberg. Old and new conjectures and results about a class of Dirichlet series. In *Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989)*, pages 367–385, Salerno, 1992. Univ. Salerno.