Alberta Number Theory Days 2013

Brandon Fodden (University of Lethbridge),
David Roe (University of Calgary)

May 10–May 12, 2013

1 Overview

After a hiatus of a year due to the University of Lethbridge hosting the CNTA meeting in June 2012, we resumed the annual Alberta Number Theory Days workshop, once again hosted by BIRS. The workshop achieved its goals of bringing together number theorists from across Alberta, though we had only a few attendees from the University of Alberta due to the larger number theory groups at Calgary and Lethbridge. Moreover, we had a substantial attendance from younger mathematicians: the 29 participants included 14 faculty, 2 postdoctoral fellows, 12 graduate students and 1 undergraduate. For the undergraduates and some of the graduate students, Alberta Number Theory Days was their first conference.

In addition to the participants from Alberta, we were happy to be able to have Noam Elkies from Harvard give a talk. His participation was made possible by his attendance at a BIRS 5-day workshop the previous week.

The workshop extended all day Saturday and into Sunday morning, with eight 50 minute talks and two 25 minute talks. Thematically, the talks ranged widely, demonstrating the diversity of the number theoretic research within Alberta. Elliptic curves arose in various contexts through many of the talks, both algebraic and analytic.

2 Summary of Talks

Number Theory and Physics

Charles Doran kicked off the workshop with a discussion of mirror symmetry, elliptic curves, K3 surfaces and Calabi-Yau threefolds. In particular, he discussed recent work [3] on variations of Hodge structure (the fourteenth case from [5]). This variation can be realized either as a family of Calabi-Yau threefolds or a family of elliptic surfaces.

Combinatorial Number Theory

Richard Guy described three unsolved problems in combinatorial number theory. Barrycades are a collection of permutations of $1, 2, \ldots, n$ in which every partial sum between 1 and $n(n+1)/2 - 1$ arises exactly once (e.g. $1+2+3+4$ and $2+3+4+1$ and $4+3+1+2$). It is unknown whether a Barrycade exists for every even n. In the cookie monster game, the cookie monster is confronted by a collection of jars with different numbers of cookies in each; on each move it may pick a subset of the jars and eat the same number of cookies from each. There is no known universal algorithm that minimizes the number of moves required to eat all

the cookies. In the third problem, Richard presented a modification of the classic Fibonacci sequence. A subfibonacci sequence is defined by the same recurrence, but whenever a composite is reached you divide by the smallest prime factor $(1, 1, 2, 3, 5, 4, 3, \ldots)$. What cycles can occur for different starting values? Richard finished by presenting a conjecture on continued fractions and class numbers of quadratic fields related to a theorem of Don Zagier.

Arithmetic Geometry

Colin Weir discussed recent work on the p-torsion group schemes of Jacobians of Suzuki curves [9]. For $m \in \mathbb{N}$, $q = 2^{2m+1}$ and $q_0 = 2^m$, the Suzuki curve $S_m/\mathbb{F}_q$ is defined by the equation $W^{q_0}(Z^q + ZW^{q-1}) = Y^{q_0}(Y^q + YW^{q-1})$. Some of the interest in these curves arises since they have the maximal number of rational points allowed by their genus. The a-number of $\mathrm{Jac}(S_m)$ is an invariant that gives partial information about its decomposition into indecomposible principally polarized abelian varieties; Colin showed that

$$a(m) = q_0(q_0 + 1)(2q_0 + 1)/6.$$

Soroosh Yazdani reported on a conjecture related to the Szpiro conjecture [2]. The local Szpiro conjecture asserts that for an elliptic curve $E/\mathbb{Q}$ with discriminant Δ_E and conductor N_E, there is a prime p with

$$0 < v_p(\Delta_E) \leq 6v_p(N_E).$$

He discussed the relationship between this conjecture and the classical Szpiro conjecture and gave some computational evidence for the local conjecture, focusing on the special case of a semistable elliptic curve with $\Delta_E = p^v M^n$.

Noam Elkies also discussed conjectures on discriminants and conductors of elliptic curves, including Hall's conjecture and the ABC conjecture. He explained why we can find large numbers of curves with the same composite conductor, giving a family of examples where the number grows without bound. Finally, he discussed the open case of prime conductor, and described the algorithms used to find prime conductors with many curves as well as the record result of 24 curves with discriminant 998820191314747.

Clifton Cunningham continued the focus on elliptic curves, but also brought automorphic representations into the picture. A theorem of Elkies shows that elliptic curves over $\mathbb{Q}$ without complex multiplication have infinitely many primes of supersingular reduction. Clifton described how to reinterpret this result as a statement about the infinitude of a certain global L-packet of automorphic representations of SL_2. He then proceeded to discuss generalizations to abelian varieties, and relate the infinitude of supersingular primes to the infinitude of L-packets for other reductive groups.

David Roe described a project to geometrize characters of tori over non-Archimedian local fields [4]. The theory of character sheaves for connected groups over finite fields is due to Lusztig [10]. In geometrizing characters of tori, non-connected groups naturally arise through the Néron model. David described how to generalize character sheaves to the non-connected setting for abelian groups, and applied this theory to geometrizing characters of tori.

Analytic Number Theory

Adam Felix discussed generalizations to Artin's conjecture [6, 7, 8]. Let $N_a(x)$ be the number of primes p at most x with a a primitive root modulo p. Under GRH, Hooley showed that

$$N_a(x) = A(a)\pi(x) + O_a\left(\frac{x \log\log x}{(\log x)^2}\right),$$

where $A(a)$ is a constant depending on a. Adam gave an alternate proof of this fact, then proceeded to talk about analogues for elliptic curves, where the role of $N_a(x)$ is taken on by $N_E(x)$: the number of primes p at most x that do not divide the conductor of E for which $E(\mathbb{F}_p)$ is cyclic.

Amir Akbary gave an introduction to the theory of limiting distributions and to error terms in analytic number theory which are known to have limiting distributions. A function $\phi\colon [0, \infty) \to \mathbb{R}^n$ has a limiting distribution μ if μ is a probability measure on $\mathbb{R}^n$ and

$$\lim_{Y\to\infty} \frac{1}{Y} \int_0^Y f(\phi(y))dy = \int_{\mathbb{R}^n} f d\mu$$

for bounded continuous $f\colon \mathbb{R}^n \to \mathbb{R}$. In the second half of his talk, Amir described recent work [1] on a theorem that generalizes various classical results on which error terms have limiting distributions.

Algebraic Number Theory

Michael Jacobson's talk was more algorithmic in nature than any of the others: he described methods for computing class groups of number fields and function fields. In computing class groups, the Minkowski bound provides a ready set of generating ideals; the hard work is finding the relations among them. Michael showed us how to use sieving methods to generate these relations, and provided applications to the elliptic curve discrete log problem, which is relevant in cryptographic contexts.

3 Concluding remarks

The organizers received a number of comments from participants expressing their appreciation of the talks as well as the setting of the workshop. We would like to thank BIRS and the Banff Centre for their hospitality and helpfulness. We feel that the two day weekend format fits the aims of this workshop very well, and hope to be able to continue to use the BIRS facilities in future years.

Finally, we want to thank the speakers for their hard work as well as PIMS for their financial support, without which this conference would not have been possible.

References

[1] A. Akbary, N. Ng and M. Shahabi, Limiting distributions of the classical error terms of prime number theory, arXiv:1306.1657.

[2] M. Bennett and S. Yazdani, A local version of Szpiro's conjecture, *Experiment. Math.* **21** (2012) no. 2, 103-116.

[3] A. Clingher, C. F. Doran, J. Lewis, A. Y. Novoseltsev and A. Thompson, The 14th case VHS via K3 fibrations (in preparation).

[4] C. Cunningham and D. Roe, Geometrization of characters of tori over non-Archimedean local fields (in preparation).

[5] C. F. Doran and J. W. Morgan, Mirror symmetry and integral variations of Hodge structure underlying one-parameter families of Calabi-Yau threefolds, Mirror Symmetry. *V, AMS/IP Stud. Adv. Math.* vol. 38, Amer. Math. Soc., Providence, RI (2006), 517-537.

[6] A. Felix, A problem of Fomenko's related to Artin's conjecture, *Int. J. of Number Theory* **8** (2012) no. 7, 1687-1723.

[7] A. Felix, Higher rank generalizations of Fomenko's conjecture, *J. Number Theory* **133** (2013), 1738-1751.

[8] A. Felix and M. R. Murty, On a conjecture of Erdős, *Mathematika* **58** (2012) no. 2, 290-304.

[9] H. Friedlander, D. Garton, B. Malmskog, R. Pries and C. Weir, The a-numbers of Jacobians of Suzuki curves, *Proceedings of the AMS* (to appear). arXiv:1110.6898.

[10] J. G. M. Mars and T. A. Springer, Character Sheaves, *Orbites unipotentes at représentations III, Astérisque* **173-174** (1989), 111-198.