Women in Numbers 4

Chantal David (Concordia University)
Michelle Manes (University of Hawaii at Manoa)
Jennifer Balakrishnan (Boston University)
Bianca Viray (University of Washington)

August 13-18, 2017

1 Conference at BIRS

1.1 Rationale and Goals

The first Women in Numbers workshop was held at BIRS in 2008, with the explicit goals of increasing the participation of women in number theory research and highlighting the contributions of women who were already doing high-quality research in the field. In their original proposal, the organizers cited the lack of representation of women in major institutions and at major international conferences.

Since that first workshop, 84 different women have participated in three WIN conferences at BIRS, with more than 60 other participants at the Women in Numbers – Europe conferences held at CIRM in Luminy and at the Lorentz Center. The number of women doing research in number theory is steadily growing. Though it is difficult to know exactly how much of this increase is due (directly or indirectly) to WIN, the visibility of the WIN conferences — due both to the community that has developed and the high quality of research output from these workshops — has helped to raise awareness in the broader community of the important contributions made by these researchers.

Another major indicator of the success of the WIN conferences is the publication output: three proceedings volumes containing a total of 36 papers (including some survey papers), as well as more than 10 journal articles published elsewhere. This far surpasses the output of a typical research workshop or graduate focused workshop such as the Arizona Winter School.

Less tangible but equally important outcomes include the lasting bonds formed between beginning researchers and their mentors, and the invigorating effect of the conferences on this mathematical community. WIN created a new model of working research conference designed to build supportive networks for women. Inspired by the success of WIN conferences, women in other fields have organized similar conferences at math institutes over the past few years, each focused on building collaboration groups consisting of senior and junior women in a given area. These include: Algebraic Combinatorixx and Women in Topology (WIT) at BIRS; Women in Shape (WiSh) at IPAM; and two Women in Applied Math conferences at IMA, Dynamical Systems with Applications to Biology and Medicine (WhAM!) and Numerical PDEs and Scientific Computing (WhAM2!). Each of these conferences has resulted in new, high-quality mathematics research as well as lasting collaborations among attendees.

These are positive changes, but our work is not done. Visibility of women at international number theory workshops and conferences, though increasing, continues to be low, with percentages of speakers who are women rarely exceeding 20%. Women are still underrepresented in major research universities, especially at the most prestigious institutions. Women receive disproportionately less grant money from the NSF than their peers. It is imperative that we continue to build on the success of the WIN and other research collaboration conferences for women, creating supportive networks for women at the early stage of their careers. The WIN4 workshop was the next step in this continuing story.

The specific goals of the workshop were:

- to generate research in significant topics in number theory;
- to broaden the research programs of women and gender minorities working in number theory, especially pre-tenure;
- to train graduate students and postdocs in number theory, by providing experience with collaborative research and the publication process;
- to strengthen and extend a research network of potential collaborators in number theory and related fields;
- to enable faculty at small colleges to participate actively in research activities including mentoring graduate students and postdocs; and
- to highlight research activities of women in number theory.

We would like to thank the following organizations for their support of this workshop: the Association for Women in Mathematics, BIRS, the Clay Mathematics Institute, Microsoft Research, the National Science Foundation, the Number Theory Foundation, and the Pacific Institute for the Mathematical Sciences.

1.2 Participants and Format

The focus of the workshop was on supporting new research collaborations within small groups. Before the workshop, each participant was assigned to a working group according to her research interests. Each group had two leaders chosen for their skill in both research and communication. These leaders designed projects and provided background reading and references for their groups. At the conference, there were a few talks, but most of the time was dedicated to working groups. Each group also submitted a short written progress report on their project. These reports, along with the project title and the names of the group members, are included in Section 2.

There were a total of forty-two participants (with sixteen of those project leaders[1]), all women or gender minorities. Of those, we had:

- 16 in tenured or tenure-track faculty positions,
- 12 early-career faculty or postdocs,
- 13 graduate students, and
- 1 industry mathematician.

Significant effort was made to enlarge the WIN community as much as possible: we had 4 project leaders who had never attended a WIN before and 24 out of 26 group members were first-time WIN-ers.

[1] 3 additional project leaders participated remotely.

1.3 Schedule

Sunday

16:00 – 17:30	Check-in begins
18:00 – 19:30	Dinner
20:00 – 22:00	Informal Gathering

Monday

07:00 – 08:45	Breakfast
08:45 – 09:00	Introduction and Welcome by BIRS Station Manager
09:00 – 10:00	Introduction and Welcome by Organizers
10:00 – 10:30	Coffee Break
10:30 – 12:00	Group Work
12:00 – 13:30	Lunch
13:30 – 14:30	Group Work
14:30 – 15:30	Coffee Break
15:30 – 16:30	Group Work
16:30 – 17:50	Project Introductions
18:00 – 19:30	Dinner

Tuesday

07:00 – 09:00	Breakfast
09:00 – 10:00	Group Work
10:00 – 11:00	Coffee Break
11:00 – 12:00	Group Work
12:00 – 13:30	Lunch
13:30 – 14:30	Group Work
14:30 – 15:30	Coffee Break
15:30 – 16:30	Group Work
16:30 – 17:50	Project Introductions
18:00 – 19:30	Dinner
20:30 – 21:30	Panel Discussion

Wednesday

07:00 – 09:00	Breakfast
09:00 – 10:00	Group Work
10:00 – 11:00	Coffee Break
11:00 – 12:00	Group Work
12:00 – 13:30	Lunch
13:30 – 17:30	Free Afternoon
18:00 – 19:30	Dinner
20:30 – 21:30	Panel Discussion

Thursday

07:00 – 09:00	Breakfast
09:00 – 10:00	Group Work
10:00 – 11:00	Coffee Break
11:00 – 12:00	Group Work
12:00 – 13:30	Lunch
13:30 – 14:30	Group Work
14:30 – 15:30	Coffee Break
15:30 – 16:30	Group Work
16:30 – 16:35	Group Photo
16:35 – 17:55	Project Introductions
18:00 – 19:30	Dinner

Friday

07:00 – 09:00	Breakfast
09:00 – 10:10	Project Presentations
10:15 – 10:45	Coffee Break
10:50 – 11:20	Project Presentations
11:30 – 12:00	Checkout by Noon
12:00 – 13:30	Lunch

1.3.1 Outcomes

The obvious outcomes of WIN4 are the research advances made by each of the nine working groups. As with the previous WIN workshops, these results will appear in peer-reviewed journals over the next few years. In addition, two of the organizers (Jennifer Balakrishnan and Michelle Manes) together with Amanda Folsom and Matilde Lalín will edit a Proceedings volume. We have recently signed a contract with Springer, and the *Proceedings* will appear in their AWM Series. We anticipate that each group will submit at least one paper — either a survey paper or a paper with new results — for peer review. We have announced a deadline of March 31, 2018 for submissions, with the Proceedings appearing in 2019.

In our minds, more important than the specific mathematical results that emerge from the conference are the collaborations and mentoring that happens there. In particular, we held two after-dinner mentoring panels in the lounge at BIRS. The first was primarily for early-career mathematicians, focused on job applications, interviews, publishing, and grant proposals. The second was focused on long-range career planning, relevant to both early- and mid-career participants.

Only time will prove the success of the WIN4 workshop, but the excitement and energy there were palpable. Besides plans for the Proceedings volume, plans are already in place for a third WINE (Women in Number-Europe) conference and potential organizers for a WIN5 workshop are being contacted. We had a number of WIN4 participants volunteer to help keep the WIN network active, whether it be through organizing special sessions at AMS or AWM meetings, leading projects at future WIN/WINE workshops, editing future WIN proceedings volumes, or even organizing a future WIN or WINE workshop. We take the enthusiasm of these volunteers as additional evidence of the benefits of the mentoring and collaboration of that occurs at WIN workshops.

2 Project Reports

2.1 Horizontal distribution questions for elliptic curves over $\mathbb{Q}$

Participants: Chantal David, Ayla Gafni, Amita Malik, Lillian Pierce, Neha Prabhu, Caroline Turnage-Butterbaugh

Let E denote an elliptic curve over $\mathbb{Q}$. There are many "horizontal distribution" questions about elliptic curves in the literature, that is, questions about the properties of the reduced curves modulo primes p on average over the primes. Most of them remain open questions, such as the Lang-Trotter conjecture, or the Koblitz conjecture, while some of were recently solved, as the Sato-Tate conjecture. The following conjecture for "extremal primes" was considered recently by [25] and [26] (where James and Pollack prove the conjecture for CM elliptic curves in the second paper). For a non-CM elliptic curve, it is conjectured that

$$\#\{p \leq x : a_p(E) = [2\sqrt{p}]\} \sim \frac{16}{3\pi} \frac{x^{1/4}}{\log x}. \tag{1}$$

This conjecture is completely open, and there are not even non-trivial upper bounds for the number of such primes.

Similar to Birch's take on the Sato-Tate conjecture [5], one can look at the "vertical distribution" to get evidence for conjecture (1). This means to consider the number of curves over $\mathbb{F}_p$ such that $a_p(E) = [2\sqrt{p}]$ on average over the primes. In a recent paper, David, Koukoulopoulos and Smith [13] presented a general framework to address such vertical distribution, which makes it possible to attack the vertical distribution for extremal primes.

Our first goal is then to use the axiomatic framework of [13] to prove the "vertical distribution"

$$\sum_{p \leq x} \frac{\#\{E/\mathbb{F}_p : a_p(E) = [2\sqrt{p}]\}'}{p} \sim \frac{16}{3\pi} \frac{x^{1/4}}{\log x},$$

where the dash in the numerator indicates that we are counting the number of curves E up to isogeny.

A key ingredient that is needed to apply the results of [13] is to know that $[2\sqrt{p}]$ and p are independently well distributed modulo ℓ, i.e., a result of the type

$$\#\{p \leq x : [2\sqrt{p}] \equiv a \bmod \ell,\, p \equiv b \bmod \ell\} \sim \frac{\pi(x)}{\ell(\ell-1)}, \tag{2}$$

with a good error term with sufficient uniformity in ℓ.

This leads to the distribution of the fractional part $\{\sqrt{p}\}$. Indeed, it is easy to see that

$$[2\sqrt{p}] = k\ell + a \iff \left\{\frac{2\sqrt{p}}{\ell}\right\} \in \left(\frac{a}{\ell}, \frac{a+1}{\ell}\right).$$

The distribution of $\{\sqrt{p}\}$ has been studied by Balog [4].

The first goal of our project was then to generalize Balog's result to include more general intervals for $\{\sqrt{p}\}$, to include a congruence condition on the primes p, and with sufficient uniformity in ℓ. We started to work on that specific problem during the week at BIRS, and have made very good progress: the approach of Balog generalizes to this case, with more work to control the various parameters involved. This should lead to a vertical distribution for champion primes, and we are currently writing the details of the argument.

After looking at the vertical distribution, we also want to address the problem of finding a non-trivial upper bound for (1), and this will lead to mixed distribution between the fractional parts $\{\sqrt{p}\}$ and primes splitting in the Galois extensions obtained by adding the ℓ-torsion point of E to $\mathbb{Q}$, i.e. a mix between the results of Balog and the Chebotarev Density Theorem. This is analogous to (2), which can be seen as the independence between Balog's result on the equidistribution of fractional parts and the equidistribution of primes in arithmetic progressions (which is the Chebotarev Density Theorem for the cyclotomic extensions).

2.2 Apollonian circle packings

Participants: Holley Friedlander, Elena Fuchs, Piper Harron, Catherine Hsu, Damaris Schindler, Katherine Stange

Apollonian circle packings are fractal sets in the plane which are obtained by repeatedly adding circles into an initial constellation of three mutually tangent circles. Starting from such a collection of three mutually tangent circles C_1, C_2, C_3 one adds all circles that are tangent to all three of those. By a theorem of Apollonius there are exactly two such circles (viewing a line as a circle with infinite radius). Given those five circles one can continue the process of adding circles that are tangent to three of the circles that are already in the picture. We repeat this process ad infinitum and let $\mathcal{P}$ be the union of all the circles obtained in this way.

Apollonian circle packings are very interesting from a number theoretic point of view. By a theorem of Descartes, four mutually tangent circles C_1, C_2, C_3, C_4 with curvatures a, b, c, d fulfill the following quadratic equation

$$(a+b+c+d)^2 - 2(a^2+b^2+c^2+d^2) = 0.$$

From this equation one can deduce that if four mutually tangent circles C_1, C_2, C_3, C_4 in the starting configuration have integer curvatures, then all curvatures in the packing $\mathcal{P}$, as constructed above, are integers. This gives rise to a number of questions on arithmetic properties of the set of curvatures that appear in such a packing.

It is known that for a fixed primitive integral packing $\mathcal{P}$ not all integers $m \in \mathbf{N}$ can occur as the curvature of a circle in the packing. As Fuchs showed in [21], for every fixed packing $\mathcal{P}$ there is a non-trivial subset of residue classes modulo 24, say $\Sigma \subset \mathbf{Z}/24\mathbf{Z}$, to which the curvatures are restricted, and this is the only congruence obstruction. The local-global conjecture for Apollonian packings states that every sufficiently large integer m with $m \bmod 24 \in \Sigma$, also occurs as a curvature in $\mathcal{P}$. Building on work of Sarnak [35] and Bourgain and Fuchs [6], Bourgain and Kontorovich showed in [7] that the local-global conjecture holds for almost all positive integers $m \leq X$, with an exceptional set of size at most $O(X^{1-\epsilon})$ for some positive ϵ.

The goal of our project is to understand the local-global conjecture for certain subcomponents of a primitive integral packing $\mathcal{P}$. We start by constructing a "tree" $T_{\mathcal{P},r}$ (it isn't quite a tree) of tangent circles inside a primitive integral Apollonian packing $\mathcal{P}$. Fix a positive integer r and two tangent circles C_a, C_c in the packing of curvatures a and c, such that a and c are both r-almost primes (their existence follows from [35]). We begin drawing $T_{\mathcal{P},r}$ by drawing the (tangent) circles C_a, C_c of curvature a and c. Now, add into $T_{\mathcal{P},r}$ all those circles in $\mathcal{P}$ that are tangent to either C_a or C_c. Of those, let $W_{r,1}$ be the set of the circles in $T_{\mathcal{P},r}$ so far that have r-almost prime curvature, and add into $T_{\mathcal{P},r}$ all circles tangent to a circle in $W_{r,1}$. Of these new circles, let $W_{r,2}$ be the set of the circles that have r-almost prime curvature, and add into $T_{\mathcal{P},r}$ all circles tangent to a circle in $W_{r,2}$. Continue this process indefinitely (this process does indeed continue indefinitely as shown in [35]) to construct the tree $T_{\mathcal{P},r}$. Note that if $r = 1$, when we delete from $T_{\mathcal{P},r}(\mathbf{v})$ all of the circles whose curvatures are not prime we will get precisely a full prime component as described at the end of [35].

Our question is then, does there exist an r so that the resulting curvatures of circles in $T_{\mathcal{P},r}$ must satisfy a local-global principle?

During the workshop we worked on numerical experiments to test such a conjecture and we discussed ways to define Cayley-like graphs (which play an important role in [7]) for r-almost prime trees. Moreover, we worked on lower bounds on the number of curvatures less than X appearing in an r-almost prime component. Following the methods in Bourgain and Fuchs [6], we expect that we can show that the number $N(X)$ of curvatures of size at most X that appear in the r-almost prime tree $T_{\mathcal{P},r}$ is at least

$$N(X) \gg \frac{X}{(\log\log X)^{1/2}}.$$

We hope to improve this to a positive density result in the future.

2.3 Arithmetic dynamics and Galois representations

Participants: Jamie Juul, Holly Krieger, Nicole Looper, Michelle Manes, Bianca Thompson, Laura Walton

Let K be a number field and $f \in K(z)$ a rational function of degree $d \geq 2$. Let T_f be the infinite preimage tree rooted at 0, with absolute Galois group G_f acting as a subgroup of the automorphisms of T_f. There is a growing body of literature on these arboreal Galois representations. In particular, Joes [28] has a specific conjecture for quadratic functions:

Conjecture 1 *Let K be a number field, and $f(z) \in K(z)$ have degree 2. Then the index $[\mathrm{Aut}(T_f) : G_f]$ is finite unless one of the following holds:*

1. *f is post-critically finite*
2. *f commutes with a non-trivial Möbius transformation that fixes 0*
3. *the critical points c_1, c_2 of f satisfy $f^r(c_1) = f^r(c_2)$ for some $r \geq 2$*
4. *0 is a periodic point of f*

Cases of this conjecture have been dealt with by Jones [28], Jones-Manes [29], and others. It is known that if any of these conditions holds, then the arboreal Galois representation cannot be finite index. Our plan was to investigate this conjecture with an eye towards a very difficult question:

Question 1 *$\mathcal{F} = \{f_t\}$ be a one-parameter family of quadratic rational maps, defined over $\overline{\mathbb{Q}}$, and a_t a marked point defined over $\bar{\mathbb{Q}}$. Let T_t be the infinite preimage tree rooted at a_t and G_t the absolute Galois group, as a subgroup of* $\mathrm{Aut}(T_t)$. *When is*

$$S_{\mathcal{F}} := \{t : [\mathrm{Aut}(T_t) : G_t] = \infty\}$$

a set of bounded height?

It is known by Pink [33] that the set $S_{\mathcal{F}}$ will *not* have bounded height if any of the following conditions are met:

- if the family is a curve of quadratic rational maps defined by a specific critical orbit relation — specifically, there is some iterate $r > 0$ such that the critical points c_1, c_2 satisfy $f^r(c_1) = f^r(c_2)$ and $a_t \equiv 0$,
- if the family is a curve for which a_t is periodic, or
- if f commutes with a non-trivial Möbius transformation.

However, there is in all those cases a reasonable alternative to the full automorphism group (for example in the latter case, the centralizer of $\mathrm{Aut}(f)$ in $\mathrm{Aut}(T_f)$) in which the Galois group has finite index, and the question above can be modified accordingly. The set of post-crticially finite maps in the space of quadratic rational maps is known to have bounded height by work of Benedetto-Ingram-Jones-Levy. Hence the question can be viewed as a weaker version of the conjecture; however, the question could be refined to search for a subgroup for which the index is finite (as in the case of the centralizer for f with nontrivial automorphisms).

During our week at BIRS, we investigated a particular family of quadratic rational functions. We proved some results related to height bounds on the parameter outside of which we had an attracting fixed point that would control much of the dynamics, and for several particular parameter choices we were able to prove that the image of Galois is the full automorphism group of the tree. We also proved that assuming Vojta's Conjecture, a similar set of conditions to those in Conjecture 1 characterizes the set of cubic polynomials $f \in K[x]$ such that $[\text{Aut}(T) : G_K(f)] < \infty$, where K is a number field. To do so, we make use of a result from [24]. Specifically, we have the following.

Theorem 1 *Let K be a number field, and let $f \in K[x]$ have degree $d \geq 2$, where d is prime. Suppose $f^n(x)$ has at most r irreducible factors over K as $n \to \infty$, so that*

$$f^{N+n}(x) = f_{N,1}(f^n(x))f_{N,2}(f^n(x)) \cdots f_{N,r}(f^n(x))$$

is the prime factorization of $f^{n+N}(x)$ in $K[x]$ for any sufficiently large N. Suppose that there is an M such that the following holds: for all $n \geq M$, and for all $1 \leq j \leq r$, there is a multiplicity one critical point γ_1 of f and a prime $\mathfrak{p}_n$ of K such that:

- $v_{\mathfrak{p}_n}(f_{N,j}(f^n(\gamma_1))) = 1$
- $v_{\mathfrak{p}_n}(f_{N,j}(f^n(\gamma_t))) = 0$ *for all* $t \neq 1$
- $v_{\mathfrak{p}_n}(f^m(\gamma_t)) = 0$ *for all critical points* γ_t*, and all* $m < N + n$
- $v_{\mathfrak{p}_n}(d) = 0$.

Then $[\text{Aut}(T) : G_K(f)] < \infty$.

2.4 Chabauty-Coleman experiments on genus three hyperelliptic curves

Participants: Jennifer Balakrishnan, Francesca Bianchi, Victoria Cantoral-Farfán, Mirela Çiperiani, Anastassia Etropolski

Let C be a hyperelliptic curve of genus $g = 3$ defined over $\mathbb{Q}$. An affine model for C can be written in the form $y^2 = f(x)$, where $f(x)$ is a polynomial with rational coefficients and $7 \leq \deg f(x) \leq 8$. As a special case of Faltings' theorem, we know that $C(\mathbb{Q})$, the set of rational points on C, is finite; moreover, by the Mordell-Weil theorem, the set of rational points of the Jacobian J of C forms a finitely generated abelian group, i.e., $J(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$.

When $r < g$, the Chabauty-Coleman method [12] can be used to help compute $C(\mathbb{Q})$. The method produces a finite set of p-adic points on C containing $C(\mathbb{Q})$, via the construction of p-adic integrals of *annihilating regular 1-forms*. In the case when $r = 1$ (and $g = 3$), the method produces two independent regular 1-forms α, β whose (p-adic) Coleman integrals can be used to compute $C(\mathbb{Q})$. It is of interest to see what other points on C the integrals of α and β cut out.

Indeed, under these hypotheses (hyperelliptic curves with $g = 3$ and $r = 1$), our goal is to produce algorithms that would allow us to use the Chabauty-Coleman method to compute the rational points of any such curve. One fully worked out example of this technique appears in the Ph.D. thesis of Wetherell [39] where he does various computations on the Jacobian of a genus 3 hyperelliptic curve to carry out Chabauty-Coleman; our goal is to automate this method, while replacing the computations on the Jacobian with computations directly on the curve.

We now also fix a prime p of good reduction and a naive height bound $B \in \mathbb{N}$. We first determine the set $S_B \subseteq C(\mathbb{Q})$ of points of naive height bounded by B. We proceed if S_B is non-empty. Suppose, for ease of exposition, that we have $\deg f(x) = 7$. Fix the embedding $C \hookrightarrow J$ that sends P to the class $[(P) - (\infty)]$ of the divisor $(P) - (\infty)$. If $P \in C(\mathbb{Q})$, then $Q := P - \infty$ gives us a rational point in the Jacobian of C, and if Q is non-torsion, by computing the three Coleman integrals $\int_\infty^P \omega_0$, $\int_\infty^P \omega_1$, $\int_\infty^P \omega_2$, where $\{\omega_i = \frac{x^i dx}{2y}\}$ forms a basis of $H^0(C, \Omega^1)$, we may determine α and β.

We then consider the indefinite Coleman integrals of α and β as p-adic power series over all residue disks of C. The zero locus of these integrals gives a set $C(\mathbb{Q}_p)_1 \subseteq C(\mathbb{Q}_p)$ such that $C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p)_1$. We want to determine, in practice, how much larger $C(\mathbb{Q}_p)_1$ is than $C(\mathbb{Q})$, and further, if we can describe $C(\mathbb{Q}_p)_1$ in terms of $C(\mathbb{Q})$ and other arithmetically relevant p-adic points on C.

During our week at BIRS, we implemented the algorithm described above to determine $C(\mathbb{Q}_p)_1$ and studied the data produced by a short list of curves pulled from the genus 3 database of hyperelliptic curves soon to be in the L-functions and Modular Forms DataBase (LMFDB) [37]. We plan on running these algorithms on further curves in the LMFDB and analyzing the resulting data.

2.5 Computational aspects of supersingular elliptic curves

Participants: Efrat Bank, Catalina Camacho, Kirsten Eisenträger, Jennifer Park

Project Goal: Our goal during the week at BIRS was to solve the following problem:

Problem: Given a supersingular elliptic curve, compute its endomorphism ring.

Setup and context: One of the methods for computing the endomorphism ring is to study the ℓ-isogeny graph of supersingular elliptic curves defined over a field of characteristic p, where p and ℓ are distinct primes. Kohel's thesis [30] outlines an algorithm to try to compute this endomorphism ring, but it is not completely explicit in the sense that some parts of the arguments are only sketched. Thus, we hope to make this algorithm more concrete, and prove the existence of some extra features in the ℓ-isogeny graph that could eventually aid in the efficiency of the algorithm to computing the endomorphism rings.

The setup that we will consider is as follows: For distinct primes p and ℓ, we can define the ℓ-isogeny graph $G(p, \ell)$ as follows:

1. The vertex set V is the set of isomorphism classes of supersingular elliptic curves over the finite field $\mathbf{F}_{p^2}$. (This gives us, up to isomorphism, all supersingular elliptic curves in characteristic p because every supersingular elliptic curve has a model defined over $\mathbf{F}_{p^2}$.) We can think of the vertices labeled by the j-invariants of the supersingular elliptic curves. The number of vertices is roughly $p/12$ and depends on the congruence class of p modulo 12 (see [36]).

2. The edge set can be described as follows: given a supersingular j-invariant j, write down an elliptic curve E in Weierstrass form with $j(E) = j$. This can be done explicitly.

   Choose a subgroup H of E of order ℓ, and let E' be the elliptic curve $E' = E/H$. Now connect the vertices $j = j(E)$ and $j' = j(E')$ by an edge, which represents the ℓ-isogeny with torsion H. Since the ℓ-torsion on the elliptic curve E is isomorphic to $\mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}$, there are $\ell + 1$ subgroups of order ℓ. Hence, with this construction, we get an $\ell + 1$-regular directed graph, and the edges leaving a vertex $j(E)$ are labelled by subgroups of E of order ℓ. The graph is a multigraph, which means that two vertices can be connected by more than one edge, and allows self-loops.

In this setup, a loop beginning and ending at a vertex j can be interpreted as an element of the endomorphism ring of the supersingular elliptic curve E with $j(E) = j$.

By Deuring's theorem, each endomorphism ring corresponds to a maximal order in the unique quaternion algebra ramified at p and ∞. When one can identify the maximal order corresponding to the endomorphism ring of a particular elliptic curve, we say that the endomorphism ring has been computed.

By identifying the elements of the quaternion algebra corresponding to these loops, one has a chance of finding the generators of the maximal order, according to Kohel's thesis [30, Chapter 7].

Parts of the project that were finished during the week at BIRS: During the week, we were able to:

1. Find a short list of at most eight elements of the quaternion algebra that could correspond to a given loop;

2. For certain primes ($p = 31, 101, 103$), identify the maximal orders attached to all of the supersingular elliptic curves over $\mathbf{F}_p$ by using the above short list;

3. Identify some criteria for when two given loops generate an order of rank < 4;

4. Identify some criteria for when two given loops generate a non-maximal order;

5. Conjecturally identify some criteria for when two given loops generate an order of rank 4.

2.6 Quantum modular forms and singular combinatorial series

Participants: Amanda Folsom, Min-Joo Jang, Susie Kimport, Holly Swisher

Mock modular forms are complex-valued functions which share similar transformation properties to ordinary modular forms with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper-half complex plane $\mathbb{H}$, but gain their modular transformation properties on $\mathbb{H}$ at the expense of losing their holomorphic properties there. The theory of mock modular forms, and the more overarching theory of harmonic Maass forms, has largely developed during this century [9]; however, their origins trace back to both the original Maass forms and Ramanujan's mock theta functions from the early-to-mid 1900s. The development of the theory of harmonic Maass and mock modular forms has been of great importance within the theory of modular forms, itself a major area of research in Number Theory related to the Langlands Program, the BSD Conjecture, and Fermat's Last Theorem, for example. Applications of harmonic Maass and mock modular forms have also emerged in the diverse areas of Mathematical Physics, Representation Theory, Topology, and more.

Quantum modular forms were defined by Zagier in 2010 [40]; they are similar to mock modular forms in that they feign modularity in some way, with the notable exception that their domain is not $\mathbb{H}$, but rather $\mathbb{Q}$. More precisely, a *weight k quantum modular form* ($k \in \frac{1}{2}\mathbb{Z}$) is a complex-valued function f on $\mathbb{P}^1(\mathbb{Q}) \setminus S$, for some appropriate S, such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, the functions $h_\gamma(x) = h_{f,\gamma}(x) := f(x) - \epsilon^{-1}(\gamma)(cx+d)^{-k} f\left(\frac{ax+b}{cx+d}\right)$ satisfy a 'suitable' property of continuity or analyticity in $\mathbb{R}$ (such as real analyticity). Here, the $\epsilon(\gamma) \in \mathbb{C}$ satisfy $|\epsilon(\gamma)| = 1$.

Questions of interest to many (see for example [9, 18, 19, 22, 23, 27, 40]) have been to understand spaces of quantum modular forms, determine explicit examples of and sources of quantum modular forms, and to understand the relationship, if any, between quantum modular and mock modular forms. Rational cusps are a natural boundary to the fundamental domain of a mock modular form, so on one hand, the latter problem is a natural one to study. On the other hand, a relationship is not immediate as the domains and analytic properties of mock and quantum modular forms are a priori different.

In this project, we address the above questions in our study of a $(k+1)$-variable combinatorial generating function $R_k(w_1, w_2; \ldots, w_k; q)$, $k \geq 1$, for k-marked Durfee symbols introduced by Andrews [3]. Historically, combinatorial functions are known to occasionally be a source of automorphic functions; likewise, such automorphic properties can sometimes be used to prove combinatorial theorems. Andrews' celebrated $(k+1)$-variable function R_k is a vast generalization of the one-variable combinatorial generating function for integer partitions, an ordinary modular form whose automorphic properties were famously studied and developed along with the Circle Method by Hardy and Ramanujan. The automorphic properties of R_k when viewed as a function of $\tau \in \mathbb{H}$ with $q = e^{2\pi i \tau}$ and fixed w_j have slowly been uncovered in a series of papers [8, 10, 17], the last of which was authored by participants Folsom and Kimport. R_k indeed exhibits "mock" behavior, though the exact type of transformations it exhibits on $\mathbb{H}$ depend on k, and also the w_j. Our project seeks to understand the quantum properties of R_k, if any, on $\mathbb{Q}$.

A number of complications arose in our study. First, it is unclear that R_k is even defined when viewed as a function on $\mathbb{Q}$. Second, the automorphic properties of R_k on $\mathbb{H}$ depend on k and the w_j. Third, showing errors to modularity extend to analytic functions on $\mathbb{R}$ is non-trivial. Barring these obstacles, our strategy is to ultimately make use of the mock-automorphic transformation properties possessed by R_k on $\mathbb{H}$, and to use analytic continuation to obtain quantum transformation properties on $\mathbb{Q}$.

To this end, our first result establishes a quantum set of rationals on which R_k is defined; this involves working with a $(k+1)$-fold q-hypergeometric series related to R_k by work of Andrews [3]. We then work with general automorphic transformation properties on $\mathbb{H}$ established by Folsom and Kimport in [17] to produce explicit errors to modularity exhibited by R_k. The errors which emerge are in terms of the non-holomorphic function

$$S(z;\tau) := \sum_{n \in \frac{1}{2}+\mathbb{Z}} \left(\mathrm{sgn}(n) - E\left(\left(n + \tfrac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}\right)\sqrt{2\,\mathrm{Im}(\tau)}\right) (-1)^{n-\frac{1}{2}}\, e^{-2\pi i n z} q^{-\frac{n^2}{2}} \right),$$

where $E(z) := 2\int_0^z e^{-\pi t^2}\,dt$. In certain settings, our errors to modularity in fact involve limiting versions of S, further complicating their understanding. We next transform our errors to modularity from functions involving the non-holomorphic S to period integrals $\int_{a/b}^{i\infty} g(\rho)(-i(\tau+\rho))^{-\frac{1}{2}}\,d\rho$, where the g are ordinary modular forms, and $\frac{a}{b} \in \mathbb{Q}$. We are also able to turn the limiting versions of S which appear into derivatives of period integrals after working with properties of S as proved in [41], among other things. We then employ delicate analytic arguments to deduce that the errors to modularity indeed extend to analytic functions in $\mathbb{R}$, and use analytic continuation to establish that the R_k is a quantum modular form. As corollaries to our results, we also obtain – non-trivially – exact formulas for period integrals of modular forms and their derivatives as evaluations of simple finite q-hypergeometric multi-sums when parameters are specialized to roots of unity.

2.7 Newton polygons of cyclic covers of the projective line

Participants: Wanlin Li, Elena Mantovan, Rachel Pries, Yunqing Tang

A fundamental problem in arithmetic geometry is understanding which abelian varieties arise as Jacobians of (smooth) curves. This question is equivalent to studying (the interior of) the Torelli locus in Siegel varieties.

In positive characteristic p, there are an abundance of discrete invariants associated with abelian varieties, e.g., the p-rank, the Newton polygon, and the Ekedahl–Oort type. These invariants give information about the Frobenius morphism and the number of points of the abelian variety defined over finite fields. It is a natural question to ask which of these invariants are realized by Jacobians. As each type of discrete invariant yields a stratification of the reduction modulo p of the Siegel variety, this problem is equivalent to understanding which strata intersect the Torelli locus, and its interior.

Ultimately, one would like to understand the geometry of the induced stratifications of the Torelli locus (e.g., the connected components of each stratum and their closure), in the same way that the geometry of the corresponding stratifications of Siegel varieties is understood. For example, in [16], Faber and van der Geer prove that for any genus g and prime p, the p-rank strata are non-empty and have the appropriate codimension. See also [1] and [2].

In the case of the Newton polygon, more precisely the Newton polygon of the characteristic polynomial of Frobenius, much less is known beyond genus 3. Most interestingly, in 2005, Oort observed that for genus $g \geq 9$, a dimension count suggests that it is unlikely for all Newton polygons to occur for Jacobians.

This project focuses on understanding the Newton polygons of cyclic covers of the project line. In [15], for any family T of cyclic covers of the projective line, Deligne and Mostow construct a PEL-type Shimura variety containing T. In [31], Moonen shows that there are precisely twenty families of cyclic covers of the projective line which give rise to special subvarieties of Siegel varieties, and each of these twenty special families agrees with the associated Shimura variety constructed in [15]. The Newton polygon and Ekedahl–Oort stratifications of PEL-type Shimura varieties are well understood by the work of Viehmann and Wedhorn [38]. Combining these results thus enables us to compile the list of all Newton polygons and Ekedahl–Oort types of Jacobians in each of the twenty special families in [31]. (Some of the necessary computations were carried out using MAGMA.)

Given this list, we proceed to investigate which invariants arise for smooth curves in the families. For the Newton polygon corresponding to the open stratum (i.e., the μ-ordinary polygon) the answer is always affirmative. Beyond that it is less clear. In the cases when the closed stratum (which corresponds to the Newton polygon called basic) has codimension 1, a count of the number of connected components of the boundary implies that the answer is affirmative for sufficiently large primes. These two results yield several new examples of Newton polygons of Jacobians of smooth curves for low genera for infinitely many p.

Finally, to attack the same questions for arbitrarily large genera, we develop a new induction argument, similar in flavor to the one initially used in [16] for p-ranks and its most recent refinement for Newton polygons in [34]. The value of the induction argument is that it yields information about the geometry of the Newton polygon strata for higher genus, starting from geometric information for the strata in low genus. This yields new occurrences for Newton polygons of smooth cyclic covers of the projective line varying in non-special families. Unfortunately, one hypothesis is in general not stable under the inductive argument, and so far our result only yields finitely many new Newton polygons. As we have not yet exhausted all possible settings, there is still hope to construct new examples for arbitrary large genera. Either way, we expect to establish the non-emptiness of many/most/all Newton polygon strata for genera $g \leq 8$ under certain congruence conditions on the prime p.

2.8 Ramanujan graphs in Cryptography

Participants: Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, Anna Puskás

Our WIN4 group studied the security of a new proposal for Post-Quantum Cryptography (PQC) from both a number theoretic and cryptographic perspective. National Institute of Standards and Technology (NIST) will be running an international competition over the next few years to select a new system for PQC. One of the possible candidates is based on the hardness of finding isogenies between supersingular elliptic curves. This hard problem was first proposed by Charles-Goren-Lauter in 2006 ([11]) as the basis for a new cryptographic hash function construction. A Pizer graph is the isogeny graph of supersingular elliptic curves, $SS(\ell, p)$, which can be interpreted in terms of Brandt matrices representing Hecke operators acting on spaces of modular forms. The idea behind the cryptographic applications is to use the hardness of finding paths in these Ramanujan graphs (or inverting random walks) as a way to construct a one-way function. The hard problem is then to find paths in the graph, given the starting and ending point. In the same paper, Charles-Goren-Lauter also proposed a PQC system based on another family of Ramanujan graphs, those of Lubotzky-Phillips-Sarnak (LPS). A 2008 paper by Petit-Lauter-Quisquater ([32]) breaks the hash function based on LPS graphs, whereas recent work has built on the hardness of finding isogenies between supersingular elliptic curves. In particular, in [14] De Feo-Jao-Plût proposed a cryptographic system based on supersingular isogeny Diffie-Hellman as well as a set of five hard problems.

Our group had two goals related to the crypto-systems on these Ramanujan graphs. On the one side we wanted to study the weaknesses and reductions in the problems proposed by De Feo-Jao-Plût. On the other side we wanted to study the relation between the Pizer and LPS graphs by viewing both from a number theoretic perspective.

For the first goal, we started to understand the relationships between the 5 problems posed by De Feo-Jao-Plût and to relate them to the hardness of the Supersingular Isogeny Graph problem which is the foundation for the CGL hash function.

For the second goal, we started explicating the relation between LPS graphs and Pizer graphs. The vertex set of both of these graphs can be viewed as a set of double cosets obtained from the adelic points of the multiplicative group of a particular quaternion algebra, B, acted on by an order of the algebra. The particular algebra and the order one must choose depend on the graphs. For LPS graphs we must fix $B = B_{2,\infty}$, the quaternion algebra over $\mathbb{Q}$ that is ramified at 2 and ∞, and choose a non-maximal order that will depend on a prime p. Whereas for the Pizer graphs we choose $B = B_{p,\infty}$, the quaternion algebra over $\mathbb{Q}$ that is ramified at p and infinity, and take the maximal order in B. Thus we were able to see that the Pizer and LPS considered in [11] are not isomorphic. However, there are generalizations of both of these graphs that we believe do come from the same choices of quaternion algebras and orders. We are continuing to explore how explicit we can make this isomorphism and whether or not this can provide any insight into why the hash-function for LPS graphs has been broken, but the one for Pizer graphs has not been.

2.9 Torsion structures on elliptic curves

Participants: Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, Bianca Viray

A result of Frey, which relies on Faltings's theorem about rational points on subvarieties of abelian varieties, states that a curve $C_{/\mathbb{Q}}$ has infinitely many points of degree at most d only if $2d$ is at least the $\mathbb{Q}$-gonality of C [20]. Moreover, the proof shows that if C has infinitely many points of degree at most d and $d < \operatorname{gon}_{\mathbb{Q}}(C)$, then the image of $\operatorname{Sym}^d(C)$ in $\operatorname{Jac}(C)$ contains a translate of a positive rank subabelian variety. One can think of Frey's result as saying that there are infinitely many points of degree at most d only when there is an infinite family parametrizing them (e.g., a $\mathbb{P}^1$ or a positive rank abelian variety).

Degree d points that are *not* parametrized by an infinite family are less understood. Such points are called **sporadic**; precisely, a closed point x on a curve C is sporadic if C has only finitely many closed points of degree at most $\deg(x)$. In our project, we study sporadic points on the modular curves $\{X_1(N)\}_{N\geq 1}$, whose non-cuspidal points correspond to isomorphism classes of pairs of elliptic curves with a marked point of order N. In particular, we seek to better understand the properties of elliptic curves that can give rise to sporadic points on $X_1(N)$.

Let $E_{/\mathbb{Q}}$ be an elliptic curve and let ℓ be a prime. If there is a sporadic point $x \in X_1(\ell)$ with $j(x) = j(E)$, then E must achieve a rational point of order ℓ in unusually low degree. This in turn implies that the image of the mod ℓ Galois representation must be unusually small. Thus one may anticipate that elliptic curves with complex multiplication (CM) are good candidates for producing sporadic points, and indeed any CM elliptic curve will give rise to infinitely many sporadic points in $\bigcup_\ell X_1(\ell)$. In contrast, if $E_{/\mathbb{Q}}$ is a non-CM elliptic curve, Serre's Uniformity Conjecture states that the image of the mod ℓ Galois representation associated E is surjective for all primes $\ell > C$, where C is a constant that does not depend on E (a standard guess is that $C = 37$). If true, this would imply there are only finitely many non-CM non-cuspidal sporadic points on $\cup_\ell X_1(\ell)$ that correspond to elliptic curves E with $j(E) \in \mathbb{Q}$. This observation inspires the following question:

Question 2 *Does there exist an absolute constant C such that if $N > C$, there are no non-CM non-cuspidal sporadic points on $X_1(N)$ corresponding to elliptic curves with rational j-invariant?*

More generally, one may ask:

Question 3 *Fix a positive integer d. Does there exist a constant $C = C(d)$ such that if $N > C$, there are no non-CM non-cuspidal sporadic points x on $X_1(N)$ with $[\mathbf{k}(j(x)) : \mathbb{Q}] \leq d$, where $j\colon X_1(N) \to X(1)$ denotes the natural map to $X(1) = \mathbb{P}^1_j$?*

During our week at BIRS, our group succeeding in proving the following partial affirmative answer to this question. We write $\mathrm{Spor}(N)$ for the closed subset of $X_1(N)$ consisting of all sporadic points on $X_1(N)$.

Theorem 2 *Fix a number field k and assume Serre's Uniformity Conjecture for k. Then there exists a positive integer $A = A(k)$ such that*

$$j\left(\bigcup_{N\in\mathbb{N}} \mathrm{Spor}(N)\right) \cap \mathbb{P}^1_j(k) \subset j\left(\bigcup_{N|A} \mathrm{Spor}(N)\right).$$

In particular, the set of k-rational j-invariants of sporadic points is finite.

Moreover if the constant in Serre's Uniformity conjecture can be taken to depend only on the degree d of k for all number fields k of degree d, then the same is true for A. In particular, then there are only finitely many j-invariants corresponding to sporadic points x with $[\mathbf{k}(j(x)) : \mathbb{Q}]$ bounded.

References

[1] J. Achter and R. Pries. Monodromy of the p-rank strata of the moduli space of curves. *Int. Math. Res. Not. IMRN*, (15):Art. ID rnn053, 25, 2008.

[2] J. Achter and R. Pries. The p-rank strata of the moduli space of hyperelliptic curves. *Adv. Math.*, 227(5):1846–1872, 2011.

[3] G.E. Andrews, *Partitions, Durfee symbols, and the Atkin-Garvan moments of ranks,* Invent. Math. 169 (2007), no. 1, 37–73.

[4] A. Balog, *On the fractional parts of p^θ*, Arch. Math. (Basel) 40 (1983), no. 5, 434–440.

[5] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies.* J. London Math. Soc. 43 (1968) 5760.

[6] J. Bourgain, E. Fuchs, *A proof of the positive density conjecture for integer Apollonian circle packings*, Journal of the AMS, **24**, (4), pp. 945–967, 2011.

[7] J. Bourgain, A. Kontorovich, *On the local-global conjecture for integral Apollonian gaskets*, Invent. Math., **196** (3), pp. 589-650, 2014

[8] K. Bringmann, *On the explicit construction of higher deformations of partition statistics*, Duke Math. J., 144 (2008), 195–233.

[9] K. Bringmann, A. Folsom, K. Ono, and L. Rolen, *Harmonic Maass forms and mock modular forms: theory and applications,* American Mathematical Society Colloquium Publications, Providence, R.I., to appear.

[10] K. Bringmann, F. Garvan, and K. Mahlburg, *Partition statistics and quasiweak Maass forms*, Int. Math. Res. Notices, 1 (2009), 63–97.

[11] D. Charles, K. Lauter and E. Goren, Cryptographic hash functions from expander graphs, *Journal of Cryptology. The Journal of the International Association for Cryptologic Research* **22** (2009), 93–113.

[12] R. F. Coleman, Effective Chabauty, Duke Mathematical Journal 52 (1985), No. 3, 765–770.

[13] C. David, D. Koukoulopoulos and E. Smith, *Sums of Euler products and statistics of elliptic curves*, to appear in Mathematische Annalen.

[14] L. De Feo, D. Jao and J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *Journal of Mathematical Cryptology* **8** (2014), 209–247.

[15] P. Deligne and G. D. Mostow. Monodromy of hypergeometric functions and nonlattice integral monodromy. *Inst. Hautes Études Sci. Publ. Math.*, (63):5–89, 1986.

[16] C. Faber and G. van der Geer. Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.*, 573:117–137, 2004.

[17] A. Folsom and S. Kimport, *Mock modular forms and singular combinatorial series,* Acta Arith. 159 (2013), no. 3, 257–297.

[18] A. Folsom, S. Garthwaite, S-Y Kang, H. Swisher, and S. Treneer, *Quantum mock modular forms arising from eta-theta functions*, Research in Number Theory 2:14 (2016), 41pp.

[19] A. Folsom, K. Ono, and R.C. Rhoades, *Mock theta functions and quantum modular forms,* Forum Math. Pi 1 (2013), e2, 27 pp.

[20] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1–3, 79–83.

[21] E. Fuchs, *Strong approximation in the Apollonian group*, J. Number Theory, **131** (12), pp. 2282–2302, 2011.

[22] S. Garoufalidis and T.T.Q. Le, *Nahm sums, stability and the colored Jones polynomial,* Res. Math. Sci. 2 (2015), Art. 1, 55 pp.

[23] K. Hikami, *Quantum invariant for torus link and modular forms,* Comm. Math. Phys. 246 (2004), no. 2, 403–426.

[24] K. Huang. Generalized Greatest Common Divisors for the Orbits under Rational Functions. Preprint available at arxiv: 1702.03881.

[25] K. James, B. Tran, M.-T. Trinh, P. Wertheimer, and D. Zantout, Extremal primes for elliptic curves, J. Number Theory 164 (2016), 282–298.

[26] K. James and P. Pollack, Extremal primes for elliptic curves with complex multiplication, J. Number Theory 172 (2017), 383–391

[27] M-J Jang and S. Lobrich, *Radial limits of the universal mock theta function g_3,* Proc. Amer. Math. Soc. 145 (2017), no. 3, 925–935.

[28] R. Jones. Galois representations from pre-image trees: an arboreal survey. *Pub. Math. Besanon.* (2013) 107-136.

[29] R. Jones and M. Manes. Galois theory of quadratic rational functions. *Comment. Math. Helv.* 89(1) (2014), 173-213.

[30] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Ph.D. thesis, University of California at Berkeley, 1996.

[31] B. Moonen. Special subvarieties arising from families of cyclic covers of the projective line. *Doc. Math.*, 15:793–819, 2010.

[32] C. Petit, K. Lauter, J. Quisquater, Full cryptanalysis of LPS and Morgenstern hash functions, *Security and Cryptography for Networks* (2008), 263-277.

[33] R. Pink. Profinite iterated monodromy groups arising from quadratic morphisms with infinite postcritical orbits. arXiv:1309.5804.

[34] R. Pries. Current results on Newton polygons of curves. Submitted.

[35] P. Sarnak, *Letter to Lagarias on Apollonian circle packings*, `http://web.math.princeton.edu/sarnak/AppolonianPackings.pdf`

[36] J. H. Silverman. *The arithmetic of elliptic curves*. Springer, New York, 2 edition, 2009.

[37] A. Sutherland, personal communication, August 2017.

[38] E. Viehmann and T. Wedhorn. Ekedahl-Oort and Newton strata for Shimura varieties of PEL type. *Math. Ann.*, 356(4):1493–1550, 2013.

[39] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, Ph.D. thesis, University of California at Berkeley, 1997.

[40] D. Zagier, *Quantum modular forms,* Quanta of maths, 659–675, Clay Math. Proc., 11, Amer. Math. Soc., Providence, RI, 2010.

[41] S. Zwegers, *Mock theta functions*, Ph.D. Thesis, Universiteit Utrecht, 2002.