Women in Numbers 3

Ling Long (Lousiana State University),
Rachel Pries (Colorado State University),
Kate Stange (University of Colorado)

April 21-25, 2014

1 Conference at BIRS

1.1 Rationale and Goals

There has been a recent surge of activity in number theory, with major results in the areas of algebraic, arithmetic and analytic number theory. This progress has impacted female number theorists in contradictory ways. Although the number of female number theorists has grown over the past fifteen years, women remain virtually invisible at high profile conferences and largely excluded from elite international workshops in number theory (data supporting this fact can be provided upon request). Moreover, there are not many tenured female number theorists at top research universities. This void — at conferences and at key institutions — has profound negative consequences on the recruitment and training of future female mathematicians. This workshop was meant to address these issues. The goals of the workshop were:

1. To train female graduate students and postdocs in number theory and related fields;
2. To generate new research of the highest caliber by female number theorists;
3. To increase the participation of women in research activities in number theory;
4. To build a research network of potential collaborators in number theory.

This workshop was a unique effort to combine strong broad impact with a top level technical research program. In order to help raise the profile of active female researchers in number theory and increase their participation in research activities in the field, this event brought together female senior and junior researchers in the field for collaboration. Emphasis was placed on on-site collaboration on open research problems as well as student training. Collaborative group projects introducing students to areas of active research were a key component of this workshop.

We would like to thank the following organizations for their support of this workshop: BIRS, Clay Institute, Microsoft Research, PIMS, and Number Theory Foundation.

1.2 Outcomes

Participant testimonials, comments from colleagues, and other feedback suggest that significant progress was made towards these goals. In particular, the conference gave greater exposure to the research programs of female researchers in number theory. Through collaborative projects, students participated in new research in the field, and faculty at small colleges were exposed to research topics of current interest. Many new

networking and mentorship connections were formed and plans were made for efforts to support the women in number theory community over the next few years.

Most of the group projects led to new research results. The conference organizers are currently submitting a proposal for publication of a conference proceedings volume, containing original research papers from each of the 9 groups as well as some additional survey papers. The organizers expect to publish this volume in 2015 or 2016.

1.3 Participants and Format

The participants were 42 female number theorists – approximately 15 senior and mid-level faculty, 15 junior faculty and postdocs, and 12 graduate students. About half of the participants, mostly faculty, were invited by the conference organizers. The remaining slots were filled through a formal application procedure.

Based on the participants' research interests and expertise, the organizers divided the participants up into 9 research groups of 4-6 members each; usually 2 senior members (group leaders) and 2-4 junior members. Research topics ranged from algebraic, analytic and arithmetic number theory to cryptography. Group leaders chose a project topic for collaborative research during and following the conference. They provided materials and references for background reading ahead of time. The group leaders also gave short talks during first three days of the meeting to introduce all participants to the projects. During the last day of the workshop, junior participants presented the progress made on the group projects.

All the groups made significant research progress during the week. Each group 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 below. Collaboration on the research projects is on-going via electronic communication.

1.4 Schedule

Monday

7:00–8:30	Breakfast
8:40–9:00	Introduction and Welcome by BIRS Station Manager, TCPL
9:00-9:30	Projects 3 and 2/4
9:30-10:00	30 second intros
10:00-10:30	Coffee Break, TCPL
10:30-12:00	Group Work
12:00-1:30	Lunch
1:00-2:00	Optional: Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall
1:30-2:00	Optional: Financial info
2:00-2:15	Group Photo; meet in foyer of TCPL (photograph will be taken outdoors).
2:15-2:45	Projects 7 and 10
2:45-3:15	Coffee Break, TCPL
3:15-5:30	Group work
5:30–7:30	Dinner

Tuesday

7:00–9:00	Breakfast
9:00-9:40	Talk - Wei Ho: Asymptotics for ranks of elliptic curves
9:45-10:00	Project 1
10-10:30	Coffee Break, TCPL
10:30-12:00	Group Work
12:00-1:30	Lunch
1:30-2:10	Talk - Ekin Ozman: Twisting Modular Curves
2:15-2:45	Projects 5 and 6
2:45-3:15	Coffee Break, TCPL
3:15-5:30	Group work
5:30–7:30	Dinner

Wednesday

7:00–8:30	Breakfast
8:45-9:25	Talk - Rachel Newton: The transcendental Brauer group of a product of CM elliptic curves
9:30-10:00	Projects 8 and 9
10-10:30	Coffee Break, TCPL
10:30-12:00	Group Work
12:00-1:30	Lunch
1:30-5:30	Free Afternoon
5:30–7:30	Dinner
8:00-9:00	Wine session

Thursday

7:00–9:00	Breakfast
9:00 - 9:40	Talk - Fang-Ting Tu: Automorphic Forms on Shimura Curves of Genus Zero
9:40 - 10:00	Financial info
10-10:30	Coffee Break, TCPL
10:30-12:00	Group Work
12:00-1:30	Lunch
1:30 - 2:00	Talk - Anna Haensch: My summer at NPR
2:15 - 2:45	Group work
2:45-3:15	Coffee Break, TCPL
3:15-5:30	Group work
5:30–7:30	Dinner

Friday

7:00–9:00	Breakfast
9:00 - 10:00	Wrap-up session (3 groups)
10-10:30	Coffee Break, TCPL
10:30-12:00	Group Work
12:00-1:30	Lunch

2 Project Reports

2.1 Automorphic forms and q-expansions

Ana Caraiani, Project Leader (Princeton University)
Ellen Eischen, Project Leader (The University of North Carolina at Chapel Hill)
Jessica Fintzen (Harvard University)
Bonita Graham (Wesleyan University)
Elena Mantovan (California Institute of Technology)
Ila Varma (Princeton University)

Our group studied *q-expansions*, an algebraic analogue of Fourier expansions, of certain functions called *automorphic forms*. Roughly speaking, we aimed to prove that congruences between values of certain automorphic forms can be completely described in terms of properties of their q-expansions.

More precisely, our group focused on a problem concerning a p-adic q-expansion principle. In analogue with the q-expansion principle for modular forms (which describes properties of a modular form, in terms of its q-expansion coefficients), there is a q-expansion principle for Siegel modular forms, as well as a q-expansion principle for automorphic forms on unitary groups. There is also a p-adic q-expansion principle (over the Igusa tower, which parametrizes ordinary elliptic curves, or more generally, ordinary abelian varieties with additional structure). Roughly, this says that a p-adic modular form over the ordinary locus vanishes if its q-expansion coefficients vanish. Our group's goal was to give an analogue of the p-adic q-expansion principle for automorphic forms on unitary groups of signature (n, m).

The p-adic q-expansion principle for modular forms and for Hilbert modular forms has been used to construct p-adic families of modular forms (indexed by weight), which in turn can be used to p-adically interpolate special values of L-functions. (This is an approach taken by N. Katz in the 1970s, for instance [4].) For Siegel modular forms and unitary groups of signature (n, n), a p-adic q-expansion principle (in [3]) has similarly been used to construct p-adic families of automorphic forms (for instance, in [2]).

For unitary groups of signature (n, m), with $n \neq m$, an analogue of the q-expansion principle (using *Serre-Tate deformation coordinates*) has been conjectured to exist, but it is not yet in the literature. The ultimate goal of this project was to state and prove an analogue of the q-expansion principle for unitary groups of signature (n, m).

For unitary groups of signature (n, m), we stated and proved an analogue of the p-adic q-expansion principle, using Serre-Tate coordinates. This builds on work of H. Hida (see, e.g., [3]). We outlined a paper discussing these results, and we are now preparing a paper to submit for publication. For unitary groups of signature (n, n), we also outlined a proof of a p-adic q-expansion principle at cusps (which gives a different expansion from the one using Serre-Tate coordinates). Furthermore, we discussed how we might extend these results to give a p-adic analogue of the algebraic Fourier-Jacobi expansion principle for unitary groups (due to K.-W. Lan [5]); for unitary groups of signature (n, m) with $n \neq m$, this is still in progress, although we expect to continue to make progress on this case in the next few months.

The group generated many related questions for future study. Some of these problems concern the relationships between different approaches to p-adic automorphic forms, as well as how to express our results in the language of perfectoid spaces (a quickly developing area, made popular by Peter Scholze's recent advances in the field). Another problem on the list concerns the action of certain differential operators on p-adic automorphic forms, and in particular how they act on Serre-Tate expansions. These operators are a generalization of certain p-adic differential operators in [1], which generalizes [4]. They also are a generalization to the p-adic case of the C^∞ "Maass-Shimura" differential operators discussed extensively in works of G. Shimura (e.g. [6]).

2.2 Generalized Legendre Families

Aly Deines (University of Washington),
Jenny Fuselier (High Point University),
Ling Long, Project Leader (Louisiana State University and Iowa State University),
Holly Swisher (Oregon State University),
Fang-Ting Tu (National Chiao Tung University, Taiwan)

For the well-understood classical Legendre family of elliptic curves

$$E_\lambda : y^2 = x(1-x)(1-\lambda x),$$

several topics, including the Picard-Fuchs equations, the theory of modular forms and Galois representations, are nicely interlaced. In this project, we are interested in studying the generalized Legendre family of curves

$$C_\lambda^{(N;i,j,k)} : y^N = x^i(1-x)^j(1-\lambda x)^k,$$

where $1 \leq i, j, k \leq N$. The Picard-Fuchs equations for $C_\lambda^{(N;i,j,k)}$ have special solutions that are known as hypergeometric functions (HGF). Due to Schwarz, one can construct so-called Schwarz triangles, which define groups, out of HGFs. A special class of these, known as arithmetic triangle groups, include the classic modular curves which parameterize isomorphism classes of elliptic curves, and Shimura curves, which parameterize 2-dimensional abelian varities admiting quaternionic multiplication. In this project, we are investigating the periods of $C_\lambda^{(N;i,j,k)}$, the Jacobian of $C_\lambda^{(N;i,j,k)}$, automorphic forms (if there are any) for the monodromy groups of HGFs, determining CM values, and values of associated periods.

During WIN3, we began by studying the case when $N = 3$. We obtained a nearly complete analysis of this case, and began to study the cases $N = 4$ and $N = 6$ as well. Since WIN3, we have furthered our understanding of the cases $N = 3, 4, 6$, and have also worked on the $N = 5$ case. We analyze these curves (often of higher genus) based on a number of factors, and then group them into classes based on their attributes. The monodromy groups of suitable periods are triangle groups, which determine a tiling of either

the Euclidean plane, the Riemann sphere, or the hyperbolic plane. We have observed different patterns in these cases.

2.3 Shadow Lines in the Arithmetic of Elliptic Curves

Jennifer Balakrishnan, Project Leader (University of Oxford),
Mirela Çiperiani, Project Leader (University of Texas, Austin),
Jaclyn Lang (University of California, Los Angeles),
Bahare Mirza (McGill University),
Rachel Newton (University of Leiden)

We carried out the first computations of *shadow lines*: 1-dimensional vector spaces attached to triples (E, K, p), where E is an elliptic curve defined over $\mathbb{Q}$, K is an imaginary quadratic extension of $\mathbb{Q}$, and p is a prime. Our computations were motivated by questions posed by Mazur and Rubin at the 2002 ICM [10].

Fix an elliptic curve $E/\mathbb{Q}$ of analytic rank 2 and an odd prime p of good ordinary reduction. Assume that the p-primary Tate-Shafarevich group of $E/\mathbb{Q}$ is finite. Let K be a quadratic imaginary field such that the analytic rank of E/K is 3 and the Heegner hypothesis holds for E (that is, all primes dividing the conductor of $E/\mathbb{Q}$ split in K). Assume for simplicity that the p-torsion $E(K)[p]$ is trivial. Fix a choice c of complex conjugation. We are interested in computing a certain subspace of

$$V := E(K) \otimes \mathbb{Q}_p$$

defined by the anticyclotomic universal norms. To define this space, let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K, and let K_n denote the subfield of K_∞ whose Galois group over K is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. The module of *universal norms* is defined by

$$\mathcal{U} = \bigcap_{n \geq 0} N_{K_n/K}(E(K_n) \otimes \mathbb{Z}_p),$$

where $N_{K_n/K}$ is the norm map induced by $E(K_n) \to E(K)$ by $P \mapsto \sum_{\sigma \in \mathrm{Gal}(K_n/K)} P^\sigma$.

Consider

$$L_K := \mathcal{U} \otimes \mathbb{Q}_p.$$

Work of Bertolini [8], Cornut [9], and Vatsal [14] implies that L_K is a 1-dimensional $\mathbb{Q}_p$-vector space known as the *shadow line* [11]. The assumption on the finiteness of the p-primary Tate-Shafarevich group of $E/\mathbb{Q}$ implies that L_K is a line in the vector space V.

Our main motivating question is the following question of Mazur and Rubin: As K varies, we presumably get different shadow lines – what are these lines, and how are they distributed?

In order to study this question, we add the assumption that p splits in $K/\mathbb{Q}$ as $(p) = \pi\pi^c$ and figure out how to compute the *anticyclotomic p-adic height pairing* [12, §2.9] on $E(K)$. It is known that $\mathcal{U}$ is contained in the kernel of this pairing [13]. In fact, in our situation, the properties of this pairing together with the fact that the -1-eigenspace of $E(K) \otimes \mathbb{Q}_p$ with respect to the action of c is 1-dimensional implies that $\mathcal{U}$ is equal to the kernel. Thus computing the pairing allows us to determine the shadow line L_K.

Recently, the first two authors together with Stein worked out techniques to compute anticyclotomic Λ-adic regulators of elliptic curves [7], which involves working with universal norms and their cyclotomic p-adic heights. This work provides some crucial input in the computation of the anticyclotomic p-adic height pairing.

Let $\Gamma(K)$ be the Galois group of the maximal $\mathbb{Z}_p$-power extension of K and $I(K) = \Gamma(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Mazur, Stein, and Tate gave an explicit description [12, §2.6] of the universal p-adic height pairing

$$(\,,\,) : E(K) \times E(K) \to I(K).$$

One obtains various $\mathbb{Q}_p$-valued height pairings on E by composing this universal pairing with homomorphisms $I(K) \to \mathbb{Q}_p$. Such (non-zero) homomorphisms are in bijection with $\mathbb{Z}_p$-extensions of K. In particular, the anticyclotomic $\mathbb{Z}_p$-extension of K corresponds to a function $\rho : I(K) \to \mathbb{Q}_p$ such that $\rho \circ c = -\rho$. We denote the resulting anticyclotomic p-adic height pairing by $(\,,\,)_\rho$.

At the workshop we came up with an explicit description of ρ using the p-adic logarithm. With this explicit description of ρ, we implemented the following formula of [12] for the anticyclotomic p-adic height of a point $P \in E(K)$:

$$h_\rho(P) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(P)) + \sum_{w \nmid p} \rho_w(d_w(P)),$$

where ρ_v denotes the composition of ρ with the natural inclusion $K_v^\times \hookrightarrow \mathbb{A}^\times$, σ_π is the π-adic sigma function, and $d_w(P)$ is a local denominator for P at w. An algorithm for computing σ_π was given in [12], and we were able to use an argument in [7] to determine, for a given elliptic curve E, a finite set of places that includes all those w for which $\rho_w(d_w(P))$ is nonzero. Thus we are now able to compute anticyclotomic p-adic heights.

We computed the following example of a shadow line at the workshop. Let $E : y^2 + y = x^3 + x^2 - 2x$. Note that $E/\mathbb{Q}$ has analytic rank 2 and $P_1 = (-1, 1), P_2 = (0, 0) \in E(\mathbb{Q})$ are linearly independent generators of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

Fix $p = 5$ and $K = \mathbb{Q}(\sqrt{-11})$. Note that the class number of K is 1 and E/K had analytic rank 3. In addition, $P_1 = (-1, 1), P_2 = (0, 0) \in E(\mathbb{Q})$ and $Q = \left(\frac{1}{4}, \frac{1}{8}\sqrt{-11} - \frac{1}{2}\right) \in E(K)$ are linearly independent generators of $E(K)/E(K)_{tors}$. Computing the shadow line in this example amounts to finding $a, b \in \mathbb{Q}_5$ for which

$$a(P_1, Q)_\rho + b(P_2, Q)_\rho = 0.$$

We are able to compute $(P_i, Q)_\rho$ by computing $h_\rho(P_i + Q)$. Using this, we found that

$$[a : b] = [2 + 2 \cdot 5 + 4 \cdot 5^3 + 4 \cdot 5^4 + 2 \cdot 5^5 + O(5^6) : 3 + 3 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^4 + 4 \cdot 5^5 + O(5^6)].$$

Hence, the shadow line for the triple $(E, K, 5)$ is $(aP_1 + bP_2)\mathbb{Q}_5 \subset E(\mathbb{Q}) \otimes \mathbb{Q}_5$.

2.4 Curves in positive characteristic with many automorphisms

Irene Bouw, Project Leader (Ulm University),
Wei Ho (Columbia University),
Beth Malmskog (Colorado College),
Renate Scheidler (University of Calgary),
Padmavati Srivivasan (Massachuchets Institute of Technology),
Christelle Vincent (Stanford University).

Let q be a power of a prime p. We consider a family of smooth projective curves C_R defined by

$$y^p - y = xR(x),$$

where $R(x) \in \mathbb{F}_q[x]$ is an additive polynomial, i.e., for indeterminates x and y we have $R(x + y) = R(x) + R(y)$. These curves have many interesting properties; for example, they have many rational points and many automorphisms. These properties seem to be closely related. A key to the description of both the $\mathbb{F}_q$-rational points and the automorphism group of C_R is the $\mathbb{F}_q$-vector space

$$W(\mathbb{F}_{q^s}) := \{x \in \mathbb{F}_{q^s} \mid \mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(xR(y) + yR(x)) = 0 \quad \forall y \in \mathbb{F}_{q^s}\}.$$

It can be shown that there exists a polynomial $E_R(x) \in \mathbb{F}_q[x]$ such that W is the zero set of E. After replacing $\mathbb{F}_q$ by a finite extension, we may assume that $\mathbb{F}_q$ is the splitting field of E_R.

Van der Geer and Van der Vlugt [15] study the curves C_R in characteristic $p = 2$. In particular, they determine the group of automorphisms that fix the unique point of C_R at infinity. Its Sylow p-subgroup P is an extraspecial group, which is a central extension of W by the Artin–Schreier automorphism $\rho(x, y) = (x, y + 1)$. Using suitable elementary abelian subgroups A of P, Van der Geer and Van der Vlugt show that the Jacobian J_R of C_R is isogenous over $\mathbb{F}_q$ to a product of supersingular elliptic curves E_A, where $E_A = C_R/A$ is the quotient curve. The description of the group P of automorphisms in terms of the vector space W allows them to make this construction completely explicit and determine the zeta function of C_R over $\mathbb{F}_q$.

The goal of the project is to extend the results of Van der Geer and Van der Vlugt to odd characteristic. In particular, we aim to determine the zeta function of C_R over the splitting field $\mathbb{F}_q$ of E_R. Van der Geer and Van der Vlugt sketch the generalization of some of their statements to odd characteristic in Section 13 of [15]. As a first step of the project, we worked out the details of these statements, supplying missing proofs and correcting mistakes.

The description of the group P of automorphisms of C_R is a rather straightforward generalization of that in characteristic 2. This group is also described in [16] without the assumption that R is additive. An important role is played by the maximal elementary abelian subgroups A of P which intersect the center $Z(P) = \langle \rho \rangle$ trivially. A careful analysis of the combinatorics of these subgroups yields a decomposition

$$J_R \sim_{\mathbb{F}_q} \prod J(X_A)$$

of the Jacobian J_R of C_R. Here the product is taken over a suitable collection of subgroups A and $X_A = C_R/A$ is the quotient curve. The key step to compute the zeta function of C_R over $\mathbb{F}_q$ is to determine an $\mathbb{F}_q$-model of the curves X_A. Van der Geer–Van der Vlugt already state an equation of these curves over the algebraic closure.

2.5 π_1-obstructions to Rational Points on Fermat Curves

Rachel Davis (Purdue University),
Rachel Pries (Colorado State University),
Vesna Stojanoska, Project Leader (MIT),
Kirsten Wickelgren, Project Leader (Georgia Tech)

Grothendieck's section conjecture gives a natural map from the rational points $X(k)$ of a k-scheme X to the Galois cohomology pointed set $H^1(G_k, \pi_1(X_{k^s}))$, where G_k is the absolute Galois group $\mathrm{Gal}(k^s/k)$. The Abel-Jacobi map from a pointed curve X to its Jacobian gives rise to a commutative diagram

$$\begin{array}{ccc} X(k) & \longrightarrow & \mathrm{Jac}(k) \\ \downarrow & & \downarrow \\ H^1(G_k, \pi_1(X_{k^s})) & \longrightarrow & H^1(G_k, \pi_1(\mathrm{Jac}(X)_{k^s})). \end{array}$$

It is a consequence of Poincare duality that $\pi_1(\mathrm{Jac}(X)_{k^s})$ is naturally the abelianization of $\pi_1 := \pi_1(X_{k^s})$ at least away from the characteristic of k. Jordan Ellenberg suggested using the lower central series filtration of π_1 to make an obstruction for a rational point p in $\mathrm{Jac}X(k)$ to be in $X(k)$ by obstructing p's image in $H^1(G_k, \pi_1(\mathrm{Jac}(X)_{k^s}))$ from being in the image of the bottom horizontal map. The first of these obstructions goes as follows.

Let $[\pi_1]_2$ denote the closed subgroup of π_1 generated by all the commutators, and let $[\pi_1]_3$ denote the closure of the subgroup generated by elements in $[[\pi_1]_2, \pi_1]$. The short exact sequence

$$1 \longrightarrow [\pi_1]_2/[\pi_1]_3 \longrightarrow \pi_1/[\pi_1]_3 \longrightarrow \pi_1/[\pi_1]_2 = \pi_1(\mathrm{Jac}(X)_{k^s}) \longrightarrow 1$$

gives rise to a map $H^1(G_k, \pi_1(\mathrm{Jac}(X)_{k^s})) \to H^2(G_k, [\pi_1]_2/[\pi_1]_3)$. Any p which is in the image of $X(k)$ must vanish under this map, so having a non-zero image is an obstruction.

The goal of the project is to use Anderson ([17]) and Ihara's ([18]) results about the fundamental group and Jacobians of Fermat curves to compute or partially compute this obstruction when X is a Fermat curve. Let N be odd and let $\overline{U} : x^N + y^N = z^N$, $U : X^N + Y^N = 1$; then $Z = \overline{U} \backslash U = \{[-\zeta_N^i : 1 : 0]\}$. Let $Y \subset U$ be the closed subset $Y = \{(\zeta_N^i, 0), (0, \zeta_N^i)\}$. The genus of the Fermat curve $\overline{U}$ is $\binom{N-1}{2}$ and we have that the following homology groups with coefficients in $\mathbb{Z}/N\mathbb{Z}$ have the listed ranks.

$$\begin{array}{ccccc} H_1(\overline{U}) & \longleftarrow & H_1(U) & \hookrightarrow & H_1(U, Y) \\ \text{ranks} \quad 2g = (N-1)(N-2) & & 2g + (N-1) = (N-1)^2 & & N^2. \end{array}$$

Anderson ([17]) largely computes $H_1(U,Y)$ (up to a factor of dlog that we determined) as a $G_{\mathbb{Q}}$-module in the following way. As a $\Lambda_1 = \mathbb{Z}/N\mathbb{Z}[\mu_N \times \mu_N]$-module, $H_1(U,Y)$ is free of rank 1 and is generated by an element β. The action of $\sigma \in G_{\mathbb{Q}}$ on $H_1(U,Y)$ is determined by the action of σ on β

$$\sigma(\beta) = B_{\sigma,N}\beta,$$

where $B_{\sigma,N} \in \Lambda_1^{\times}$. We are working to explicitly compute $B_{\sigma,N}$ in terms of the classical Kummer map, which we will then use in computing the obstructions described above.

To compute $H_1(\overline{U})$ and $H_1(U)$ as $G_{\mathbb{Q}}$-modules (given $H_1(U,Y)$), we use the exact sequence to find $\ker(\delta)$

$$0 = H_1(Y) \longrightarrow H_1(U) \longrightarrow H_1(U,Y) \xrightarrow{\delta} H_0(Y) \longrightarrow H_0(U) \longrightarrow 0.$$

Further, we find that $H_1(\overline{U}) \simeq \frac{H_1(U)}{\mathrm{Stab}(\epsilon_0\epsilon_1)}$ where $\epsilon_0\epsilon_1$ is a diagonal element in the group ring Λ_1.

A further result of Anderson [loc.cit] is helpful in computing the Galois cohomology groups we need. To explain, define L_f to be the splitting field of $f(x) = 1 - (1-x^N)^N$. Let S be the generalized Jacobian of (U,Y), and fix b to be the base point of S given by the difference of the points $(0,1)$ and $(1,0)$ of U. Anderson's theorem is that the field of definition of the coordinates of the set of points $\{P \in S | nP = b\}$ contains L_f; he also shows that these fields are equal if N is prime. When N is prime, $H^1(U,Y)$ (and therefore $H^1(\overline{U})$) is a trivial G_{L_f}-module. For this reason, we need to compute $H^1(\overline{U})$ as a module over the finite Galois group of L_f over $\mathbb{Q}$.

2.6 Computing the Transcendental Brauer Set for a 3-parameter Family of Enriques Surfaces

Francesca Balestrieri (University of Oxford),
Jennifer Berg (University of Texas at Austin),
Michelle Manes, Project Leader (University of Hawaii at Manoa),
Jennifer Park (MIT),
Bianca Viray, Project Leader (Brown University)

Given a smooth, projective, geometrically integral variety X over $\mathbb{Q}$, one may ask whether X has a $\mathbb{Q}$-rational point, i.e. whether $X(\mathbb{Q})$ is nonempty. Since $\mathbb{Q}$ embeds into each of its completions, it is always the case that $X(\mathbb{Q})$ is a subset of the set of adelic points $X(\mathbb{A}_{\mathbb{Q}})$. However, it is possible for $X(\mathbb{Q})$ to be empty even when $X(\mathbb{A}_{\mathbb{Q}})$ is nonempty, and such varieties X are said to fail the Hasse principle.

To explain counterexamples to the Hasse principle, Manin defined an intermediate Brauer set

$$X(\mathbb{Q}) \subset X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset X(\mathbb{A}_{\mathbb{Q}})$$

and a variety X is said to have the Brauer-Manin obstruction to the Hasse principle when $X(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ but $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. Skorobogatov later refined this by defining the étale Brauer set $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{et,\,Br}}$, and provided an example of a surface X such that $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{et,Br}} = \emptyset$, but $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$, thereby showing that the étale-Brauer obstruction is stronger than the Brauer-Manin obstruction. In practice, however, it is often easier to compute the larger algebraic Brauer-Manin set $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_1}$, and this can still cause an obstruction to the existence of rational points.

In [19], Várilly-Alvarado and Viray constructed a 3-parameter family of Enriques surfaces $X_{a,b,c}/\mathbb{Q}$ such that

$$\emptyset = X_{a,b,c}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{et,Br}} \subset X_{a,b,c}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset X_{a,b,c}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}_1} \neq \emptyset$$

thereby showing that the algebraic Brauer-Manin obstruction is insufficient to explain the lack of rational points on Enriques surfaces. The goal of the present project is to determine whether $X_{a,b,c}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

In general, it is difficult to determine transcendental Brauer classes, i.e. those surviving in $\mathrm{Br}(X)/\mathrm{Br}_1(X)$. However, in [21] Creutz and Viray were able to obtain a presentation of the 2-torsion Brauer classes on double covers of ruled surfaces. In particular, since every Enriques surface (over a separably closed field) is birational to a double cover of a ruled surface whose branch locus has at worst simple singularities, we may employ their method.

We consider the K3 surfaces $Y := Y_{a,b,c}$ defined as the complete intersection of the following three quadrics in $\mathbb{P}^5 = \text{Proj } \mathbb{Q}[s,t,u,x,y,z]$:

$$\begin{aligned} xy + 5z^2 &= s^2 \\ (x+y)(x+2y) &= s^2 - 5t^2 \\ ax^2 + by^2 + cz^2 &= u^2 \end{aligned}$$

and the Enriques surface $X = Y/\sigma$, where σ is the fixed point free involution $[s:t:u:x:y:z] \mapsto [-s:-t:-u:x:y:z]$. We focus initially on the case $(a,b,c) = (12, 111, 13)$.

There exist nine pairs of fibrations $Y \to \mathbb{P}^1$ which descend to X. This yields $2 \cdot 2 \cdot \binom{9}{2}$ ways of presenting Y as a double cover of the ruled surface $\mathbb{P}^1 \times \mathbb{P}^1$ branched over a $(4,4)$-curve, B. We explicitly computed these branch loci and, in many cases, determined that B has four singularities and the normalization of B has genus at most 5.

The methods in [21] give conditions to determine which functions in the function field $\mathbf{k}(B)$ give rise to central simple algebras in $\text{Br}(\mathbf{k}(Y))$ that are in fact in the subgroup $\text{Br}(Y)$. This can be described via an exact sequence that relates the Picard group of Y, these candidate functions in $\mathbf{k}(B)$, and $\text{Br}(Y)[2]$. The computations on the K3 surface should allow us to compute an explicit presentation of $\text{Br}(X)[2]$ over some number field. We hope to then descend this to $\mathbb{Q}$ and compute the obstruction. Once this is complete, we would like to compute the obstruction more generally for tuples (a,b,c) satisfying the hypotheses in [19].

2.7 On the hardness of the Ring-LWE problem

Yara Elias (McGill University)
Kristin Lauter, Project Leader (Microsoft Research)
Ekin Ozman (University of Texas at Austin)
Kate Stange, Project Leader (University of Colorado at Boulder)

Cryptography is rightfully the most celebrated application of Number Theory, as information security relies on it to preserve data confidentiality, data integrity, authentication, and non-repudiation. Lattice-based cryptography has allowed for efficient cryptographic schemes [26] and applications in fully homomorphic encryption [24, 25]. Both rely on hard problems in lattices. Recently, the *ring learning with errors problem* (Ring-LWE) was introduced, and reductions to hard lattice problems were proved. We define next the RLWE hardness assumption: Given a ring $R = \mathbb{Z}[x]/(f(x))$, and integer $q > 0$, where

- $f(x) \in \mathbb{Z}[x]$ is a monic, irreducible polynomial of degree n,

the *ring-LWE problem* is to distinguish a set of pairs

$$(a_i, b_i = a_i s + e_i) \in R/qR \times R/qR \text{ where}$$

- a_i are uniformly random and independent,
- e_i are independent and 'short',
- $s \in R/qR$ is a random secret

from a set of uniformly random pairs. For practical purposes, security estimates in [22, Figure 4] suggest that n and q should be at least 320 and 4093 respectively, with a Gaussian distribution for the error vector of width 8.

On the one hand, Regev [27] showed that the LWE problem is as hard to solve as several worst-case lattice problems. In addition, Lyubashevsky, Peikert, and Regev [23] proved that the hardness of a discrete version of *ring-LWE* follows from the hardness of the original problem for a wide family of appropriate distributions. They also developed efficient algorithms for cryptographic operations over arbitrary cyclotomic fields hence obtaining efficient cryptosystems relying on the hardness assumption for *ring-LWE*. On the other hand, Eisentraeger, Hallgren and Lauter elaborated an attack of *ring-LWE* under some assumptions on f, which distinguishes random pairs with non-negligible probability.

The goal of our project is two-fold; we aim to look at specific number fields that do not satisfy the hardness assumption, and to construct families of number fields for which cryptographic schemes based on the ideal lattice problem *ring-LWE* are efficient.

During our stay at BIRS, we elaborated a probabilistic argument that we hope will extend the attack on *ring-LWE* by Eisentraeger, Hallgren and Lauter for certain ranges of parameters. We also implemented a concrete attack for a certain number field, where the algorithm returned the secret when the given pair was not random. Currently, we are working on relaxing the assumptions in [23] using number-theoretic tools like Mahler measure, monogenic families of Galois extensions, and others.

2.8 Sieve methods in geometry

Alina Bucur (University of California at San Diego),
Alina Carmen Cojocaru, Project Leader (University of Illinois at Chicago),
Matilde Lalin (Université de Montréal),
Lillian Pierce, Project Leader (Duke University)

Around 200 BC, Eratosthenes developed an ingenious, yet simple method of detecting prime numbers. This is still one of the most effective methods of finding relatively small primes. Around two millennia later, Legendre reformulated the sieve of Eratosthenes in combinatorial terms, giving rise to the simplest method in what is now called sieve theory. It was Brun, at the beginning of the 20th century, who brought in profound new ideas to the sieve concept, his work marking the birth of sieve theory.

Over the following decades and through the new millennium, sieve methods have been vastly refined and expanded: combinatorial and non-combinatorial sieves alike are frequently utilized towards advances in the theory of numbers, with results as astonishing as the current ones on the twin prime conjecture. At WIN 3, our team focused on a better understanding and applications of non-combinatorial sieve methods in geometric contexts. Our work will be described in detail in an upcoming research article.

2.9 Kneser-Hecke-operators for quaternary codes

Gabi Nebe, Project Leader (RWTH Aachen University)
Amy Feaver (University of Colorado at Boulder)
Anna Haensch (Duquesne University/Max Planck Institute for Mathematics)
Jingbo Liu (Wesleyan University)

Defining $R := \mathbb{Z}/4\mathbb{Z}$ and $S := \mathbb{Z}/2\mathbb{Z}$, a quaternary codes C of length N is a R^N-submodule, where $N \in \mathbb{N}$. Using the standard inner product, the dual of a code C is defined

$$C^\perp = \{x \in R^N : (x, c) = 0 \ \forall c \in C\},$$

and we call C self-dual if and only if $C = C^\perp$. Define $\mathcal{F} := \{C = C^\perp \leq R^N\}$, the set of all self-dual codes of length N. Two codes $C, D \in \mathcal{F}$ are equivalent, denoted $C \simeq D$ if there exists some permutation $\pi \in S_N$ such that $C = \pi(D)$. Let $\mathcal{V}$ denote the $\mathbb{C}$-vector space spanned by the equivalence classes $[C]$ where $C \in \mathcal{F}$. Then $\mathcal{B} := \{[C] : C \in \mathcal{F}\}$ is a $\mathbb{C}$-basis for $\mathcal{V}$.

For any $C \in \mathcal{F}$, if follows from the Krull-Schmidt Theorem that there exist unique integers a and b such that $C \cong R^a \oplus S^b$, as R-modules. In this way, each code has a unique isomorphism type as an R-module, and we define the set of all codes of a certain isomorphism class by

$$\mathcal{F}_{a,b} := \{C = C^\perp \leq R^N : C \cong R^a \oplus S^b\} \subseteq \mathcal{F}.$$

For any $C \in \mathcal{F}_{a,b}$, we have $\mid C \mid \cdot \mid C^\perp \mid = \mid R \mid^N$, and consequently for a self-dual code of length N we have $2a + b = N$, meaning that the choice of a completely determines the isomorphism type. We note that equivalent codes are always isomorphic as modules, but two codes of the same module type need not be equivalent as codes.

For codes $C, D \in \mathcal{F}$, we call C and D neighbors if and only if

$$C/C \cap D \cong D/C \cap D \cong S.$$

We define a graph Γ by taking the set of equivalence classes in $\mathcal{B}$ as the set of vertices, and placing an edge between two vertices $[C]$ and $[D]$ if there exist $C' \in [C]$ and $D' \in [D]$ such that $C' \sim D'$. Then Γ is a connected graph, as shown by Meyer in [28].

We define a linear operator T on $\mathcal{V}$ by $T([C]) = \sum_{D \sim C} [D]$. Viewed as a matrix, T is just the adjacency matrix for the graph Γ. By arranging the basis elements in $\mathcal{B}$ according to module isomorphism type, we have

$$T = \begin{bmatrix} T_0 & \cdots & & \\ \vdots & T_1 & & \\ & & \ddots & \vdots \\ & & \cdots & T_{\frac{N}{2}} \end{bmatrix},$$

where T_a denotes the adjacency matrix obtained by restricting the vertex set to $\mathcal{F}_{a,b}$. We immediately observe that for any choice of $\mathcal{F}$, $T_0 = [0]$, since there is only one code in $\mathcal{F}$ of isomorphism type S^N.

The eventual goal of this project is to describe the eigenvalues of the T_a and compute the corresponding eigenspaces to obtain a result analogous to that given by Gabi Nebe for binary codes. To understand these eigenspaces we must understand the shape of neighboring codes and their possible overcodes and subcodes. To that end, we have proved the following result: for $C \in \mathcal{F}_{a,b}$, let E be a maximal submodule in C. If $C \cap 2R^N \leq E$ then there exist two neighbors G and F of C, with $G \cong R^a \oplus S^b$ and $F \cong R^{a-1} \oplus S^{b+2}$.

It is known that the maximal eigenvalue of T_a counts the number of neighbors of isomorphism type $R^a \oplus S^b$. It is clear that when C and D are neighbors then $C \cap 2R^N \leq C \cap D$, therefore in view of the result in the preceding paragraph, it is clear that counting neighbors of the same type is equivalent to counting the number of $a-1$ dimensional subspaces of $\mathbb{F}_2^a$, which is precisely $2^a - 1$. Therefore, we have also shown the following: The maximal eigenvalue of T_a is $2^a - 1$.

Finally, knowing the structure of subcodes and overcodes for neighboring codes, we are able to say the following: If $[C] \cong R^a \oplus S^b \cong [D]$ and C and D are in the same connected component, then $C \mod 2 = D \mod 2$. This result is particularly advantageous, since binary codes are very well-studied, and lifting a quaternary code C into this binary setting will allow us to have many more tools at our disposal.

References

[1] Ellen E. Eischen. p-adic differential operators on automorphic forms on unitary groups. Ann. Inst. Fourier (Grenoble) 62 (2012), no. 1, 177–243.

[2] Ellen E. Eischen. A p-adic Eisenstein measure for unitary groups, Accepted for publication in the Journal für die reine und angewandte Mathematik (Crelles Journal). 32 pages. DOI 10.1515/ crelle-2013-0008.

[3] Haruzo Hida. p-adic automorphic forms on reductive groups, Astérisque (2005), no. 298, 147254, Automorphic forms. I.

[4] Nicholas M. Katz. p-adic L-functions for CM fields, Invent. Math. 49 (1978), no. 3, 199-297.

[5] Kai-Wen Lan. Arithmetic compactifications of PEL-type shimura varieties, London Mathematical Society Monographs, vol. 36, Princeton University Press, 2013.

[6] Goro Shimura. Arithmeticity in the theory of automorphic forms, Mathematical Surveys and Monographs, vol. 82, American Mathematical Society, Providence, RI, 2000.

[7] J. S. Balakrishnan, M. Çiperiani, and W. A. Stein, p-adic heights of Heegner points and anticyclotomic Λ-adic regulators, *Math. Comp.* to appear.

[8] M. Bertolini, Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions, *Compos. Math.* **99** (1995), 153-182.

[9] C. Cornut, Mazur's conjecture on higher Heegner points, *Invent. Math.* **148(3)** (2002), 495-523.

[10] B. Mazur and K. Rubin, Elliptic curves and class field theory, *Proceedings of the International Congress of Mathematicians* **II**, 185-195, Higher Ed. Press, Beijing, 2002.

[11] B. Mazur and K. Rubin, Studying the growth of Mordell-Weil, *Doc. Math.* (Extra Vol.) (2003), 585-607.

[12] B. Mazur, W. A. Stein, and J. Tate, Computation of p-Adic Heights and Log Convergence, *Doc. Math.* (Extra Vol.) (2006), 577-614.

[13] B. Mazur and J. Tate, Canonical height pairings via biextensions, Arithmetic and Geometry, Progr. Math. 35, Birkhauser, Boston (1983) 195-237.

[14] V. Vatsal, Special values of anticyclotomic L-functions, *Duke Math. J.* **116(2)** (2003), 219-261.

[15] G. van der Geer and M. van der Vlugt, Reed–Muller codes and supersingular curves, *Compos. Math.* **84** (1992), 333–367.

[16] C. Lehr and M. Matignon, Automorphism groups for p-cyclic covers of the affine line, *Compos. Math.* **141** (2005), 1213–1237.

[17] Greg W. Anderson. Torsion points on Jacobians of quotients of Fermat curves and p-adic soliton theory. *Invent. Math.*, 118(3):475–492, 1994.

[18] Yasutaka Ihara. Profinite braid groups, Galois representations and complex multiplications. *Ann. of Math. (2)*, 123(1):43–106, 1986.

[19] A. Varilly-Alvarado and B. Viray, *Failure of the Hasse Principle for Enriques Surfaces*, Adv. Math. **226** (2011), no. 6, 48844901.

[20] W. Barth, K. Hulek, C. Peters, A. Van de Ven, *Compact Complex Surfaces*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics **4**, Springer Verlag, Berlin 2004.

[21] B. Creutz and B. Viray, *On Brauer Groups of Double Covers of Ruled Surfaces*, Preprint, arXiv: 1306.3251.

[22] Richard Lindner, Chris Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption, CT-RSA 2011.

[23] Lyubashevsky, Peikert, Regev, A Toolkit for Ring-LWE Cryptography. *Advances in Cryptology*, 2013

[24] Gentry, A fully homomorphic encryption scheme. *Ph.D. thesis, Stanford University*, 2009

[25] Gentry, Fully homomorphic encryption using ideal lattices. *In STOC, pages 169178.*, 2009

[26] Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity, 16(4):365411, 2007. Preliminary version in FOCS 2002.*

[27] Regev, On lattices, learning with errors, random linear codes, and cryptography. *J. ACM, 56(6):140, 2009. Preliminary version in STOC 2005.*

[28] A. Meyer, Automorphism groups of self-dual codes, PhD thesis, RWTH Aachen University, 2009.