BIRS Workshop 08w5112: *WIN – Women in Numbers*,

K. Lauter (Microsoft Research),
R. Pries (Colorado State University),
R. Scheidler (University of Calgary)

November 3-7, 2008

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, NSA, Fields Institute, PIMS, Microsoft Research, and University of Calgary.

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 in number theory and related fields;
2. To highlight research activities of women in number theory;
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;
5. To enable female faculty at small colleges to help advising graduate students.

Participant testimonials, comments from (male and female) colleagues, and other feedback suggest that significant progress was made toward goals 1, 2, 4 and 5. In particular, the conference gave greater exposure to the research programs of active female researchers in number theory. Through collaborative projects, students participated in new research in the field, and faculty at small colleges were exposed to supervision activities. Some of the group projects will lead to new results and publications, and the conference organizers are currently exploring venues for publication of a conference proceedings volume. Work has begun on a WiKi website that will serve as the basis for the **WIN Network**, a network for female researchers in number theory. It is the sincere hope of the workshop organizers that progress was also achieved toward goal 3 above, but only time will tell.

2 Participants and Format

In lieu of the goals of this workshop, participation was limited to women. The participants were 41 female number theorists – 15 senior and mid-level faculty, 16 junior faculty and postdocs, and 10 graduate students. About half of the participants, mostly faculty, were invited by the conference organizers. The remaining slots were intended for junior faculty, postdocs, and graduate students.

To that end, the organizers held an open competition involving a formal application procedure and a rigorous selection process. This was advertised in the *Association of Women in Mathematics* newsletter. Additionally, Math Departments of all PhD-granting institutions in Canada and many in the United States were contacted. 56 applicants submitted a CV and a research statement (for PDFs and junior faculty) or a list of courses taken (for grad students). After a careful and thorough review of these documents, the organizing committee selected what were deemed to be the strongest applicants for participation in the workshop.

Based on the participants' research interests and expertise, the organizers then divided the participants up into 8 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 algorithmic number theory to cryptography. In consultation with their group members, 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 talks during first three days of the meeting to introduce all participants to their respective group projects. During the last two days of the workshop, junior participants presented the progress made on the group projects. These presentations usually involved more than one presenter. As a result, essentially all workshop participants were able to give a talk, or a portion of one.

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 below. Collaboration on the research projects is on-going via electronic communication. Some of these projects will lead to new results and publications. The organizers also expect to publish a conference proceedings volume in the future.

3 Schedule

Sunday Afternoon: 4:00 pm Check-in begins (Front Desk Professional Development Center - open 24 hours) 5:30-7:30 Buffet Dinner 8:00 Informal gathering and introduction session, 2nd floor lounge, Corbett Hall

Monday: 7:00-8:45 Breakfast 8:45-9:00 Introduction and Welcome to BIRS by BIRS Station Manager, Max Bell 159 9:00-9:15 Introduction by organizers 9:15-10:00 Lecture: E) Renate Scheidler 10:00-10:30 Coffee 10:30-11:15 Lecture: C) Kirsten Eisentrager 11:15-12:00 Lecture: D) Katherine Stevenson 12:00-1:00 Lunch 1:00-2:00 Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall 2:00-2:45 Lecture: B) Audrey Terras 2:45-3:15 Coffee 3:15-4:00 Lecture: F) Helen Grundman 4:00-6:00 Introduction to project groups 6:00-7:30 Dinner

Tuesday: 7:00-9:00 Breakfast 9:00-9:15 Announcements 9:15-10:00 Lecture: A1) Stephanie Treneer 10:00-10:30 Coffee 10:30-11:15 Lecture: G) Mirela Ciperiani 11:15-12:00 Lecture: A2) Chantal David 12:00-1:00 Lunch 1:00-1:30 Group Photo; meet on the front steps of Corbett Hall 1:30-2:15 Lecture: F) Kristin Lauter 2:15-3:00 Lecture: E) Yoonjin Lee 3:00-3:30 Coffee 3:30-6:00 Project groups 6:00-7:30 Dinner

Wednesday: 7:00-9:00 Breakfast 9:15-10:00 Lecture: A2) Alina Cojocaru 10:00-10:30 Coffee 10:30-11:15 Lecture: B) Winnie Li 11:15-12:00 Lecture: D) Rachel Pries 12:00-1:30 Lunch Free afternoon 3:00-3:30 Coffee

Thursday: 7:00-8:30 Breakfast 8:30-9:15 Lecture: A1) Ling Long 9:15-10:00 Lecture: C) Edlyn Teske 10:00-10:30 Coffee 10:30-12:00 Project groups 12:00-1:30 Lunch 1:30-3:00 Project groups 3:00-3:30 Coffee 3:30-4:00 D) progress report 4:00-4:30 E) progress report 4:30-5:00 F) progress report 5:00-5:30 C) progress report 5:30-6:00 G) progress report 6:00-7:30 Dinner

Friday: 7:00-8:45 Breakfast 8:45-9:15 A1) progress report 9:15-9:45 A2) progress report 9:45-10:15 B) progress report 10:15-10:45 coffee 10:45-11:30 Concluding discussion 11:30-1:30 Lunch

Lectures (organized by project group):
A1 Speaker: Stephanie Treneer, Western Washington University
Title: Modular Forms I
Speaker: Ling Long, Iowa State University
Title: Modular Forms II

A2 Speaker: Chantal David, Concordia University
Title: Frobenius Distribution and L-functions
Speaker: Alina Cojocaru, University of Illinois at Chicago
Title: Koblitz's Conjecture on Average

B Speaker: Audrey Terras, University of California at San Diego
Title: Zeta Functions of Graphs Icharacteristic p I
Speaker: Winnie Li, Pennsylvania State University
Title: Zeta Functions of Graphs II

C Speaker: Kirsten Eisentraeger, Pennsylvania State University
Title: Computation of pairings on hyperelliptic curves I
Speaker: Edlyn Teske, University of Waterloo
Title: Computation of pairings on hyperelliptic curves II

D Speaker: Katherine Stevenson, California State University Northridge
Title: Towers of Galois covers in characteristic p I
Speaker: Rachel Pries, Colorado State University
Title: Towers of Galois covers in characteristic p II

E Speaker: Renate Scheidler, University of Calgary
Title: Class groups of function fields I
Speaker: Yoonjin Lee, Ehwa Womans University
Title: Class groups of function fields II

F Speaker: Helen Grundman, Bryn Mawr College
Title: Computations on Hilbert Modular Surfaces I
Speaker: Kristin Lauter, Microsoft Research
Title: Computations on Hilbert Modular Surfaces II

G Speaker: Mirela Ciperiani, Columbia University
Title: Galois representations I

4 Research Projects and Project Groups

4.1 Project A1: Modular forms – Zeros of a Class of Eisenstein Series

Participants: Sharon Garthwaite, Ling Long, Holly Swisher, Stephanie Treneer

The study of modular forms has been a central focus of number theory for more than one century. Modular forms are highly symmetric holomorphic functions defined on the Poincaré upper half plane, and the classical example of such a function is the Eisenstein series. In fact, Eisenstein series can be viewed as the building blocks of modular forms. To understand the properties of Eisenstein series is of fundamental importance to the study of modular forms and has many significant applications.

Work by R. A. Rankin, F.K.C. Rankin and H.P.F. Swinnerton-Dyer reveals that the zeros of the classical Eisenstein series $E_{2k}(z)$ for the full modular group $SL_2(\mathbb{Z})$ are all located on a particular arc of the unit circle. Equivalently, the j-values of these zeros are real and lie in the range $[0, 1728]$, where j is the classical

modular j-function. Despite the efforts these and many other mathematicians, Eisenstein series still remain an intriguing source of mysteries. For example, Nozaki recently proved that the (real) zeros of classical Eisenstein series $E_{2k}(z)$ interlace with the zeros of $E_{2k+12}(z)$.

In this project, we study a class of odd weight Eisenstein series $E_{2k+1,\chi}(z)$ for the principal level 2 subgroup $\Gamma(2)$ with a character χ. It is well-known that the modular curve $X_{\Gamma(2)} = (\mathfrak{H}/\Gamma(2))^*$ for $\Gamma(2)$ is a Riemann surface of genus zero, and that the field of meromorphic functions on $X_{\Gamma(2)}$ is generated by $\lambda(z)$, the classical λ function. The Eisenstein series $E_{2k+1,\chi}(z)$ in consideration have previously been used to obtain some nice formulae of Milnor involving the number of representations of natural numbers as sums of squares or sums of triangular numbers.

For our first investigation of this topic, we obtain a generating function $cn(u)$ of $E_{2k+1,\chi}(z)$, where $cn(u)$ is a Jacobi elliptic function and satisfies a non-linear differential equation. By using the inherited recursions, we are able to compute the polynomials $f_{2k+1}(\lambda)$ which encode the λ-values of the zeros of $E_{2k+1,\chi}(z)$. Numerical data suggests that the $f_{2k+1}(\lambda)$ have real λ-values which are within $(-\infty, 0)$, and these zeros of $f_{2k-1}(\lambda)$ interlace with the zeros of $f_{2k+1}(\lambda)$; this is parallel to the results in the classical case.

On the theoretical side, we extend the approach of Rankin and Swinnerton-Dyer to show that at least 58 percent of the zeros of $f_{2k+1}(\lambda)$ are real and are within $(-\infty, 0)$. We also obtain formulas which relate the λ-values of the zeros of Eisenstein series on $\Gamma(2)$ to special values of certain L-series.

4.2 Project A2: Distributions of Traces of Cyclic Trigonal Curves over Finite Fields

Participants: Alina Bucur, Alina Cojocaru, Chantal David, Brooke Feigon, Matilde Lalín

The number of points of a hyperelliptic curve with affine model $y^2 = F(x)$ over the finite field $\mathbb{F}_q$ with q elements can be expressed as $q + S(F)$, where $S(F)$ denotes the character sum $\sum_{x\in\mathbb{F}_q} \chi(F(x))$. (Here F is a square-free monic polynomial of degree d and q is odd.) The character sum also expresses the trace of the Frobenius for this curve of genus $g = \left[\frac{d-1}{2}\right]$.

In their seminal work [12] Katz and Sarnak showed that for fixed genus g and $q \to \infty$, $S(F)/\sqrt{q}$ is distributed as the trace of a random $2g \times 2g$ unitary symplectic matrix. On the other hand, Kurlberg and Rudnick [11] showed that for fixed q and $g \to \infty$ the limiting distribution of $S(F)$ is that of a sum of q independent trinomial random variables taking the values ± 1 with probabilities $q/(2q+2)$ and the value 0 with probability $1/(q+1)$.

The natural question to ask is what happens when one works with higher degree curves, which means that one needs to study higher order characters. For instance, over a field with $q \equiv 1 \bmod 3$, cyclic trigonal curves

$$y^3 = F(x), \tag{1}$$

with $F \in \mathbb{F}_q[t]$ a monic cube free polynomial of degree d, correspond to cubic extensions, and thus to cubic characters. The number of affine points of the curve over $\mathbb{F}_q$ is given by $q + S_3(F) + \overline{S_3(F)}$, where $S_3(F) = \sum_{x\in\mathbb{F}_q} \chi_3(F(x))$ and χ_3 is a fixed cubic character of $\mathbb{F}_q$. The cyclic automorphism of the curve commutes with the Frobenius automorphism and splits the first cohomology group into two eigenspaces. The trace of the Frobenius on these subspaces is given by $S_3(F)$ and $\overline{S_3(F)}$, respectively.

One could restrict the investigation to curves for which the affine model (reftriell) is smooth, which corresponds to considering only square-free polynomials F. The genus of such a curve is $g = d - 2$. In this case, the limiting distribution of the character sum $S_3(F)$ as $g \to \infty$ is that of a sum of q i.i.d. random variables taking the values 0 with probability $1/(q+1)$ and $1, \rho, \bar{\rho}$ with probabilities $q/(3q+3)$. Here ρ denotes a primitive third root of unity.

Geometrically speaking the difference between this case and the case of hyperelliptic curves considered by Kurlberg and Rudnick is that, while the moduli space of hyperelliptic curves of fixed genus g is irreducible, this is no longer the case for higher degree curves. In the trigonal case, since F is cube-free it can be written as $F = F_1F_2^2$ where both F_1 and F_2 are square-free monic polynomials. The Riemann-Hurwitz formula tells us that the genus of (1) is $g = \deg F_1 + \deg F_2 - 2$. The moduli space $\mathcal{H}_{3,g}$ of cyclic trigonal curves of fixed genus g splits into irreducible subspaces indexed by pairs (d_1, d_2) with $d_1 + d_2 = g + 2$. (See [2] for further details.) We propose to investigate the limiting distribution of the character sum $S_3(F)$ in these irreducible components as either d_1 or d_2 grows, as well as over the whole moduli space $\mathcal{H}_{3,g}$ as $g \to \infty$.

4.3 Project B: Zeta functions of Graphs

Participants: Shabnam Akhtari, Habiba Kadiri, Winnie Li, Elisabeth Malmskog, Michelle Manes, Audrey Terras

Part I. The Analytic Part. We derived an analog of Weil's explicit formula for Dedekind zeta functions and plan to use it to study basic facts about the distribution of poles of the Ihara zeta function, for example. The result may also be viewed as a generalization to irregular graphs of the Selberg trace formula for a regular tree. We plan to plug in various kernels similar to those that work for the Selberg trace formula in the regular case.

Part II. Ramified Covers and Divisibility of Ihara Zetas. We investigated some examples of ramified covers in which there is divisibility of the zeta functions up to linear factors, and we plan to study connections with results for zeta functions of curves over finite fields. Here is a longer description.

The Ihara zeta function of a graph was defined by Yatsutaka Ihara in the 1960s. It was modeled on other zeta functions in its form, an infinite product over primes in the graph, and has some analogous properties, for example convergence to a rational function. Emile Artin defined the zeta function of a curve over a finite field in his 1921 thesis. Serre proved that the Artin zeta function of a covered curve divides that of the covering curve as long as the covering is defined over the base field of the zeta function.

Audrey Terras and Harold Stark have outlined a notion of unramified coverings of connected graphs, and have found that if G and H are connected graphs such that there exists an unramified covering map $H \to G$, then the reciprocal of the Ihara zeta function of G divides the reciprocal of the Ihara zeta function of H. In an attempt to extend the theory of Ihara zeta functions and draw further parallels with Artin's zeta function, we sought a notion of ramified coverings of graphs for which some divisibility relations between Ihara zeta functions could be found.

In 2007, Matthew Baker and Serguei Norine outlined a definition of covering maps of graphs and ramification in these coverings, and proved a graph theoretic analogue of the Riemann-Hurwitz formula for curves using their definitions. Adapting this notion of ramification, we found an "almost" divisibility relationship between the Ihara zeta functions of some simple ramified covers of graphs.

In particular we found a formula for the zeta function of a complete graph on k vertices, and of a graph consisting of n copies of a complete graph on k vertices all sharing a single vertex. We considered the latter as a ramified cover of the complete graph. All terms except a cubic of the zeta function of the complete graph divide the zeta function of the covering graph. If $k = 3$ we have true divisibility, as the cubic term has a particularly simple form which divides the zeta function of the covering graph.

4.4 Project C: Elliptic Curve Cryptography

Participants: Jennifer Balakrishnan, Juliana Belding, Sarah Chisholm, Kirsten Eisenträger, Katherine Stange, Edlyn Teske

Since 2000, there has been much interest in the explicit computation of pairings on elliptic curves, as these can be used in tripartite key exchange, ID-based encryption and other cryptographic protocols. More recently, there has been heightened interest in computation of pairings on hyperelliptic curves. While hyperelliptic curves require more involved computations, they provide security comparable to that of elliptic curves while working with a smaller finite field. For example, a genus two hyperelliptic curve requires a field of only half the bit size for the same security level.

The focus of our group at WIN 2008 was to bring everyone up to speed on the current state of pairings on hyperelliptic curves. Our starting point was the 2007 survey paper by Galbraith, Hess and Vercauteren on this topic [8]. We spent the week surveying the current literature, learning the computational issues, and brainstorming questions we could explore.

We focused on the Tate pairing, as it is more efficient than the Weil pairing and more universally applicable than the eta or ate pairings, for example. We also focused on curves of genus two, as these are of primary interest for cryptographic and computational reasons. Let r be a prime dividing the order of the Jacobian of the curve C over $\mathbb{F}_q$ and let k be the smallest integer such that r divides $q^k - 1$, known as the *embedding degree* of C. Then the Tate pairing $e_r(D_1, D_2)$ maps a pair of points of the r-torsion subgroup of $\mathrm{Jac}(C)(\mathbb{F}_{q^k})$ to an element of $\mathbb{F}_{q^k}$. The curve C and field $\mathbb{F}_q$ are carefully chosen to balance the difficulty

of the discrete logarithm problem (DLP) in the r-torsion subgroup of $\mathrm{Jac}(C)(\mathbb{F}_{q^k})$ with the difficulty of the DLP in $\mathbb{F}_q^*$. Such curves are called *pairing-friendly* (for a precise definition, see [7]).

The input to the pairing is two divisors, the first defining a function f_{D_1} on $\mathrm{Jac}(C)$ and the second encoding the points where the function is evaluated: $e(D_1, D_2) = f_{D_1}(D_2)$. Miller's algorithm for computing the Weil pairing has been adapted to the Tate pairing, and computes the pairing recursively [13].

The main approach to speeding up the computation of pairings is straightforward: reduce the number of computations, specifically expensive ones like field inversions. The techniques to do this, however, are varied and often apply to only special cases. During our work together, we encountered two situations which lead to some interesting questions (both open to our knowledge).

- In the case of even embedding degree k, it is "traditional" to exploit the degree two subfield, essentially replacing field inversion by conjugation. For this reason, much of the work on computation of pairings restricts to this case. As the case of odd embedding degree is neglected in the literature, it is natural to ask:

  > What computational improvements can be made in the case of $k \equiv 0 \mathrm{mod} 3$ by using arithmetic in a degree 3 sub-field? Similarly, what about $k = 5$?

  These are not vacuous questions, as there exist supersingular curves with such embedding degrees. Currently, the main source for pairing-friendly genus two hyperelliptic curves is *supersingular* curves, which have embedding degree divisible by 2, 3 or 5 (see [17]).

- For many pairing-based algorithms, the technique of *denominator elimination* reduces field inversions by using an evaluation point which lies in a subfield of $\mathbb{F}_{q^k}$. Furthermore, we may often use *degenerate* divisors (divisors which involve a single non-infinite point of C) as the evaluation point. For example, in the elliptic curve case, all divisors are degenerate and the technique in [3] is to transform the divisor to one lying in a trace-zero subgroup of $E(\mathbb{F}_{q^k})$.

  However, in the genus two case, this technique transforms a degenerate divisor into a non-degenerate one. As we must now evaluate f_{D_1} at two points, this offsets the computational gain from denominator elimination. The paper [14] proposes two work-arounds in this situation; however, we would like to address the issue itself: can one find degenerate divisors lying over a subfield?

  > What is the intersection of the set of degenerate divisors and the trace-zero subgroup of $Jac(C)(\mathbb{F}_{q^k})$? If it is non-empty, how can we efficiently compute elements of it (to use as evaluation points)?

Our current plan is to examine the two questions outlined above (and any related implementation questions which may arise) and incorporate our findings into a survey paper on the state of hyperelliptic pairings, thus updating the 2007 survey paper, [8].

4.5 Project D: Galois Covers of Curves in Characteristic p

Participants: Linda Gruendken, Laura Hall-Seelig, Bo-Hae Im, Ekin Ozman, Rachel Pries, Katherine Stevenson

In this group, we discussed known results and open questions about fundamental groups of curves in characteristic p and completed a project about this topic.

New phenomena in characteristic p: This project is about phenomena that occur for curves in characteristic p but not in characteristic 0. Here are some of the basic properties of complex curves that are false for k-curves if k is an algebraically closed field of characteristic $p > 0$.

A. If $\mathcal{X}$ is a complex curve and $\emptyset \neq \mathcal{B} \subset \mathcal{X}$ is a finite set, then the fundamental group $\pi_1(\mathcal{X} - \mathcal{B})$ is a free group of rank $2g_{\mathcal{X}} + |\mathcal{B}| - 1$. There exists a G-Galois cover $\varphi : \mathcal{Y} \to \mathcal{X}$ branched only at $\mathcal{B}$ if and only if G can be generated by $2g_{\mathcal{X}} + |\mathcal{B}| - 1$ elements. Given $\mathcal{X}$, $\mathcal{B}$, and G, the number of G-Galois covers $\varphi : \mathcal{Y} \to \mathcal{X}$ which are branched only at $\mathcal{B}$ is finite. These statements are false in characteristic

p. For any affine k-curve $X - B$, the algebraic fundamental group $\pi_1(X - B)$ is infinitely profinitely generated.

B. The inertia groups of a cover $\varphi : \mathcal{Y} \to \mathcal{X}$ of complex curves are cyclic. By the Riemann-Hurwitz formula, the genus of $\mathcal{Y}$ is determined by $|G|$, $g_{\mathcal{X}}$, $|\mathcal{B}|$ and the orders of the inertia groups. In particular, there are no nontrivial Galois covers of $\mathbb{A}^1_{\mathbb{C}}$ since the complex plane is simply connected.

The situation is more complicated for covers of k-curves due to the presence of *wild ramification* which occurs when p divides the order of an inertia group. The inertia groups of a wildly ramified cover are usually not cyclic. Furthermore, the inertia group I carries extra information, including a filtration of I called the ramification filtration, [18, IV]. The genus of Y now depends on this filtration.

C. If $\mathcal{X}$ is a complex curve of genus g, then there are p^{2g} points of order p on its Jacobian $J_{\mathcal{X}}$. This property is false for the Jacobian J_X of a k-curve X of genus g. In characteristic p, the number of points of order p in $J_X(k)$ equals p^f for some integer f such that $0 \leq f \leq g$. Here f is called the *p-rank* of X. The p-rank equals the maximum rank of an elementary abelian p-group which occurs as the Galois group of an unramified cover of X.

D. A cover of complex curves can only be deformed by changing the base curve $\mathcal{X}$ or the branch locus $\mathcal{B}$. In contrast, a wildly ramified cover of k-curves can almost always be deformed without varying X or B.

One can illustrate these phenomena for the group $G = \mathbb{Z}/p$. Let $h(x) \in k[x]$ have degree σ where $p \nmid \sigma$. Consider the $\mathbb{Z}/p$-Galois cover $\phi : Y \to \mathbb{P}^1_k$ branched only at ∞ given by the Artin-Schreier equation $y^p - y = h(x)$. The p-rank of Y is $f = 0$. The ramification filtration ends at index σ. The genus of Y equals $(\sigma - 1)(p - 1)/2$ and thus can be arbitrarily large. There are non-trivial families of such covers given by deforming $h(x)$. Similar results are true for G-Galois covers of a fixed affine k-curve as long as p divides $|G|$ but their proofs require advanced techniques when G is not an abelian p-group.

Open questions Let X be a smooth projective connected k-curve defined over an algebraically closed field k of characteristic $p > 0$. Let B be a non-empty finite set of points of X. Raynaud and Harbater made a crucial contribution to Galois theory [16] [10] by proving Abhyankar's Conjecture [1] which classifies the finite quotients of the algebraic fundamental group $\pi_1(X - B)$, i.e., the finite groups which occur as Galois groups for covers of X ramified only above B.

At this time, there is still no affine k-curve whose fundamental group is known. The structure of the fundamental group depends on towers of covers of curves and on the geometry of the curves in these towers. The goal of understanding fundamental groups provides a strong motivation to answer new questions about towers of covers of k-curves. Towards this goal, it is necessary to determine which inertia groups and ramification filtrations actually occur for wildly ramified covers of k-curves.

Given X, B, G, only in special cases is it known which inertia groups and ramification filtrations occur for G-Galois covers $\phi : Y \to X$ branched at B. One result is that, for any finite quotient G of $\pi_1(X - B)$ with p dividing $|G|$, then there exists a G-Galois cover $\phi : Y \to X$ branched only at B such that the genus of Y is arbitrarily large, [15]. An open problem, for a non-abelian p-group G, is to determine the smallest genus that can occur for a G-Galois cover of X branched only at B.

A crux case is to understand Galois covers of the affine line, and specifically those with small genus. By Abhyankar's Conjecture, there exists a G-Galois cover of the affine line if and only if G is quasi-p, which means that G is generated by p-groups. There are many quasi-p groups, including all simple groups with order divisible by p.

An example of a quasi-p group is $G = (\mathbb{Z}/\ell)^a \rtimes \mathbb{Z}/p$ where ℓ and p are distinct primes and a is the order of ℓ modulo p. As a group project, we calculated the minimal genus that can occur for a Galois cover of the affine line in characteristic p with this group G. We proved that there are only finitely many curves of this minimal genus which are Galois covers of the affine line with group G. The proof involved studying the action of an automorphism of order p on the ℓ-torsion of the Jacobian of an Artin-Schreier curve.

4.6 Project E: Class Groups of Function Fields

Participants: Lisa Berger, Jing Long Hoelscher, Yoonjin Lee, Jennifer Paulhus, Renate Scheidler

Let $C/\mathbb{F}_q$ denote a hyperelliptic curve of genus g over the finite field $\mathbb{F}_q$, q a prime power. For a prime ℓ consider the ℓ-rank of $\mathrm{Jac}(C)$. Over $\bar{\mathbb{F}}_q$ this rank is $2g$, and it is obtained over a finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. In [4] Bauer et. al. provide an algorithm to determine an upper bound on n and give conditions for which their bound is exact. The authors then prove a theorem which determines a minimum base field extension that guarantees that the ℓ-rank of $\mathrm{Jac}(C)$ over $\mathbb{F}_{q^n}$ exceeds its ℓ-rank over $\mathbb{F}_q$. Our project focused on extending the theoretical results and improving the algorithm.

Consider the injection $\rho : Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \hookrightarrow GL_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, and let π denote the Frobenius element restricted to $\mathbb{F}_{q^n}$, the generator of $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$. For a fixed basis let A_π denote the matrix representation of $\rho(\pi)$ in $GL_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. Since the homomorphism is injective, we have $\mathrm{ord}(A_\pi) = \mathrm{ord}(\pi) = n$. One would like to compute n by computing the order of A_π in $GL_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, but this image is not known. Setting $t = q^{-s}$, the zeta function of a variety $X/\mathbb{F}_q$ may be expressed as the rational function

$$\zeta(X, s) = Z(X, t) = \frac{L(t)}{(1-t)(1-qt)} .$$

In [4] Bauer et. al. compute the L-polynomial $L(t)$ of $C/\mathbb{F}_q$ to determine the characteristic polynomial of the Frobenius element: $F(t) = t^{2g}L(t^{-1}) \pmod{\ell}$. Then, considering each possible elementary divisor decomposition and associated matrix, they determine an upper bound on the order of A_π, and hence on n. As a first step toward improving the algorithm we proved a linear algebra result which allows us to obtain the same bound on the order of the Frobenius element by computing the order of the companion matrix of its characteristic polynomial. This proves the first proposition below, a revision of Theorem 5.2 from [4]. We then considered the question of the minimum field extension of $\mathbb{F}_{q^n}/\mathbb{F}_q$ necessary to guarantee an increase in the ℓ-rank. In our project we modified this result, eliminating one of the assumptions in Theorem 5.6 of [4], proving the second proposition.

Proposition 4.1 *Let $L(t)$ denote the L-polynomial of $C/\mathbb{F}_q$, set $F(t) \equiv t^{2g}L(t^{-1})$ mod ℓ, so $F(t) \in \mathbb{F}_\ell[t]$. Let A_F denote the companion matrix of $F(t)$. Then $b = ord(A_F)$ is an upper bound on n and is equal to n if $F(t)$ is square free. Furthermore, let $F = P_1^{m_1} \cdots P_s^{m_s}$ be the factorization of F into distinct monic irreducibles in $\mathbb{F}_\ell[t]$, and let A_{P_i} denote the companion matrix of P_i, then $b = lcm_{1\le i\le s}\{\ell^{m_{0,i}} ord(A_{P_i})\}$, where $m_{0,i} = \lceil \log_\ell m_i \rceil$.*

Proposition 4.2 *Let $L(t)$ be the L-polynomial of $C/\mathbb{F}_q$, and set $F(t) \equiv t^{2g}L(t^{-1})$ mod ℓ, $F(t) \in \mathbb{F}_\ell[t]$. Suppose $F(t)$ has an irreducible factor $P(t) \in \mathbb{F}_\ell[t]$. Let A_p be the companion matrix of P and $n = ord(A_p)$. Suppose $P^k(t)$ is the elementary divisor of π_{q,n_l} with the smallest power of $P(t)$. Then the ℓ-rank of Jac(C) over $\mathbb{F}_q^{n\ell^m}$ exceeds its ℓ-rank over any proper subfield by at least $\deg(P)$, where $m = \lceil \log_\ell k \rceil$.*

Corollary 4.3 *Let $F(t) = P_1^{m_1}(t) \cdots P_s^{m_s}(t)$ be the prime decomposition of the characteristic polynomial $F(t)$, and let $P_i^{m_{ij}}$ be the elementary divisors, where $1 \le i \le s, 1 \le j \le r_i, m_{i1} \le \cdots \le m_{ir_i}$ and $\sum_j m_{ij} = m_i$. Suppose $\ell^{\lceil \log_\ell m_{11} \rceil} ord(A_{P_1}) = \min_i\{\ell^{\lceil \log_\ell m_{i1} \rceil} ord(A_{P_i})\}$, denoted by γ. Then the ℓ-rank of $Jac(\mathbb{F}_{q^\gamma})$ is at least $\deg P_1$, and the ℓ-rank of $Jac(E)$ for any subfield $E \subset \mathbb{F}_{q^\gamma}$ is zero.*

4.7 Project F: Hilbert Modular Surfaces

Participants: Helen Grundman, Jennifer Johnson-Leung, Kristin Lauter, Adriana Salerno, Bianca Viray, Erica Wittenborn

Explicit class field theory of imaginary quadratic fields is intimately connected with the geometry of elliptic curves with complex multiplication. One posits that the same should hold for explicit class field theory of quartic CM fields and abelian surfaces with complex multiplication. Unsurprisingly, the case of curves turns out to be much simpler than that of surfaces, and progress in this direction has been elusive. The goal of this project is to explore more deeply the relationship between certain class invariants of quartic CM fields studied by Goren and Lauter in [9] and the intersection numbers of special cycles on Hilbert modular surfaces conjectured by Brunier and Yang [5] by focusing on specific examples.

Igusa defined three Siegel modular functions which generate the space of modular functions on the Siegel upper half space of degree four. The class invariants that we are interested in were introduced by deShalit and Goren [6] and are closely related to the Igusa polynomials. Although these polynomials are non-canonical, one choice of j_1, j_2, j_3 is given as a quotient of Siegel modular forms where the denominator is a power of χ_{10}. This modular form has a specific geometric interpretation. For a CM abelian surface, A, we have that $\chi_{10}(A) = 0$ if and only if, A is a product of elliptic curves with the product polarization. Hence, $p \mid \chi_{10}(A)$ if and only if the reduction of A modulo p is a product of elliptic curves with the product polarization [9]. The class invariants introduced by deShalit and Goren also have the property that the primes in the denominator are exactly the primes dividing $\chi_{10}(A)$ where A has CM by K.

Our first example is the quartic CM field $K = \mathbb{Q}(i\sqrt{61 - 6\sqrt{61}})$ of discriminant 61. This field has several nice properties; in particular, $K/\mathbb{Q}$ is Galois and has class number 1. Van Wamelen has computed the Igusa class polynomials for all isomorphism classes of smooth genus two curves over $\mathbb{Q}$ whose Jacobians have complex multiplication [19]. For our example, 3, 5, and 41 divide $\chi_{10}(A)$, so we know from [9] that there exist embeddings with certain properties

$$\mathcal{O}_K \hookrightarrow \mathrm{M}_2(B_{p,\infty})$$

where $p = 3$, 5, and 41, and $B_{p,\infty}$ is the unique quaternion algebra ramified at p and ∞. The first aim of our project is to construct these embeddings.

The second aim of our project involves the intersection numbers of Hirzebruch-Zagier divisors on Hilbert modular surfaces. To make the connection to these intersection numbers, we first note that there is a strong relationship between Hilbert and Siegel modular forms. Indeed, the Siegel modular form χ_{10} yields a divisor on the Hilbert modular surface that is a sum of Hirzebruch-Zagier divisors, $\sum T_m$ where $m = \frac{d_F - x^2}{4}$ is a positive integer. So, taking $d_F = 61$, we see that the possibilities for m are 3, 9, 13, 15.

Brunier and Yang [5] give a conjectural formula for the arithmetic intersection numbers of the divisors T_M with the CM points associated to K on the Hilbert modular surface for any quartic CM field K. We calculate that, for $\sum T_m$ with the m as above, the conjectural intersection formula at the primes 3, 5, and 41 matches the power to which those primes divide χ_{10}, and attempt to find the corresponding embeddings.

References

[1] S. Abhyankar. Coverings of algebraic curves. *Amer. J. Math.*, 79:825–856, 1957.

[2] J. Achter and R. Pries, The integral monodromy of hyperelliptic and trielliptic curves. *Math. Ann.* 338 (2007), no. 1, 187–206.

[3] P. Barreto, H. Kim, B. Lynn and M. Scott, Efficient algorithms for pairing-based cryptography, *CRYPTO 2002*, *LNCS* **2442** (2002), 354-369.

[4] M. Bauer, M.J. Jacobson, Jr., Y. Lee and R. Scheidler, Construction of hyperelliptic function fields of high three-rank, *Math. Comp.* **77** (2008), 503–530.

[5] J. Brunier and T. Yang, CM-values of Hilbert modular functions, *Invent. Math.* **163** (2006), 229–288.

[6] E. DeShalit and E. Goren, On special values of theta functions of genus two, *Ann. Inst. Fourier* **47** (1997), 775–799.

[7] D. Freeman, M. Scott and E. Teske, A taxonomy of pairing-friendly elliptic eurves, Cryptology, *ePrint Archive*, Report 2006/372, 2006.

[8] S. Galbraith, F., Hess and F. Vercauteren, Hyperelliptic Pairings, *Pairings 2007*, *LNCS* **4575** (2007), 108–131. *Crypto 2002*, *LNCS* **2442** (2002), 336–353.

[9] E. Goren andn K. Lauter, Class invariants for quartic CM fields, *Ann. Inst. Fourier* **57** (2007), 457–480.

[10] D. Harbater. Abhyankar's conjecture on Galois groups over curves. *Invent. Math.*, 117(1):1–25, 1994.

[11] P. Kurlberg and Z. Rudnick; The fluctuations in the number of points on a hyperelliptic curve over a finite field, to appear in *J. Number Theory.*

[12] N. Katz and P. Sarnak; *Random matrices, Frobenius eigenvalues, and monodromy,* American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999.

[13] V. Miller, The Weil Pairing and its Efficient Computation, *J. Cryptology* **17** (2004), 235–261.

[14] C. Ó hÉigeartaigh, M. Scott, Pairing Calculuation on Supersingular Genus 2 Curves, *SAC 2006*, *LNCS* **4356** (2007), 302–316.

[15] R. Pries. Wildly ramified covers with large genus. *Journal of Number Theory*, 119(2):194–209, 2006. math.AG/0507274.

[16] M. Raynaud. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar. *Invent. Math.*, 116(1-3):425–462, 1994.

[17] K. Rubin and A. Silverberg, Supersingular abelian Varieties in cryptology,

[18] J.-P. Serre. *Corps Locaux*. Hermann, 1968.

[19] P. van Wamelen, Examples of genus 2 cm curves defined over the rationals, *Math. Comp.* textbf68 (1999), 307–320.