BIRS Workshop 11w5075: *WIN2 – Women in Numbers 2*,

C. David (Concordia University),
M. Lalín (Université de Montréal),
M. Manes (University of Hawai'i at Mānoa).

November 6–11, 2011

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, PIMS, Microsoft Research, and the Number Theory Foundation.

1 Rationale and Goals

Number theory is a fundamental subject with connections to a broad spectrum of mathematical areas including algebra, arithmetic, analysis, topology, cryptography, and geometry. This very active area naturally attracts many female mathematicians. Although the number of female number theorists is steadily growing, there are still relatively few women reaching high profile positions and visibility at international workshops and conferences. The lack of female leaders in the area is an issue that tends to perpetuate itself, since it has repercussions in attracting and training the next generation of female mathematicians.

In order to increase the number of active female researchers in number theory, a workshop on "Women in Numbers" (WIN 2008) was held at BIRS in November, 2008. This workshop was tremendously successful, surpassing even its stated goals. Several research collaborations—typically involving some senior and junior mathematicians, and in some cases advanced graduate students—began in the working groups of WIN 2008. Many of these collaborations have already proved fruitful in producing publishable research, and a few of the collaborations have continued long past the initial workshop.

For this momentum to continue, it is essential that WIN 2008 is not a single, isolated event, but rather the beginning of a long-term program to develop and support female number theorists. This workshop was designed continue and build upon the work started at WIN 2008. The specific goals were:

1. to highlight research activities of women in number theory;
2. to increase the participation of women in research activities in number theory;
3. to train female graduate students in number theory and related fields;
4. to strengthen the research network of potential collaborators in number theory and related fields started by the WIN 2008 conference;
5. to enable female faculty at small colleges to participate actively with research activities including the training of graduate students; and
6. to provide information on women in number theory with an inclusive approach.

Participant testimonials, comments from (male and female) colleagues, and other feedback suggest that significant progress was made toward goals 1 through 4. 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.

A Women in Numbers listserv, a website, and a Facebook page have all been established. These 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 goals 5 and 6 above, but only time will tell.

2 Participants and Format

The participants were 41 female number theorists — 12 senior and mid-level faculty, 14 junior faculty and postdocs, and 15 graduate students. About one-third of the participants, mostly faculty, were invited by the conference organizers. The remaining slots were intended for junior faculty, postdocs, and graduate students.

The organizers solicited applications, advertising via: the BIRS website, the *Association of Women in Mathematics* newsletter, and various mailing lists including the Number Theory listserv and the previous Women in Numbers 2008 participants.

Fifty-three applicants submitted a CV and a research statement (for postdocs and faculty) or a list of courses taken and letter of recommendation (for graduate 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 eight research groups of 4–6 members each; usually two senior members (group leaders) and 2–4 junior members. Group leaders chose a project 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 at some point during the conference.

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 4. 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

The official schedule for the workshop appears below. Note that most nights, the project groups reconvened and continued working after dinner.

Sunday:
4pm Check-in begins
5:30 – 7:30 dinner
8:00 informal gathering

Monday:
7:00 – 8:45 breakfast
8:45 – 9:00 intro & welcome (BIRS Station Manager & Organizers)
9:00 – 10:30 presentation by Group 1 leaders: Marie-José Bertin and Matilde Lalín
10:30 – 11:00 coffee
11:00 – 12:30 presentation by Group 2 leaders: Chantal David and Heekyoung Hahn
12:30 – 1:30 Lunch
1:30 – 2:30 BIRS tour
2:00 – 2:30 coffee
2:30 – 4:00 presentation by Group 3 leaders: Alina Bucur and Melanie Matchett Wood

4:00 – 6:30 work in project groups
6:30 dinner

Tuesday:
7:00 – 8:45 breakfast
8:45 – 9:00 announcements
9:00 – 10:30 presentation by Group 4 leaders: Alina Cojocaru and Alice Silverberg
10:30 – 11:00 coffee
11:00 – 12:30 presentation by Group 5 leaders: Wieslawa Niziol and Sujatha Ramdorai
12:30 – 1:30 Lunch
1:30 – 3:00 presentation by Group 6 leaders: Rachel Pries and Hui June Zhu
3:00 – 3:30 coffee
3:00 – 6:30 work in project groups
6:30pm dinner

Wednesday:
7:00 – 8:45 breakfast
8:45 – 9:00 announcements
9:00 – 10:30 presentation by Group 7 leaders: Ling Long and Gabriele Nebe
10:30 – 11:00 coffee
11:00 – 12:30 presentation by Group 8 leaders: Kristin Lauter and Bianca Viray
12:30 Lunch / Free afternoon

Thursday:
7:00 – 1:30pm breakfast / project groups / lunch
1:30 – 2:00 Group 1 report by team members
2:15 – 2:45 Group 2 report by team members
2:45 – 3:15 Coffee break
3:15 – 3:45 Group 3 report by team members
4:00 – 4:30 Group 4 report by team members
4:45 – 5:15 Group 5 report by team members
5:30 – 6:00 Group 6 report by team members
6:00 – 7:30 dinner
8:00 informal career discussion

Friday:
7:00 – 8:45 breakfast
8:45 – 9 announcements
9:00 – 9:30 Group 7 report by team members
9:45 – 10:15 Group 8 report by team members
10:15 – 10:45 Coffee
10:45 – 11:30 closing discussion / future plans
11:30 – 1:30 lunch
checkout by noon

4 Research Projects and Project Groups

4.1 Group 1: Elliptic Surfaces and Mahler measure

Participants: Marie-José Bertin (Université Paris VI), Amy Feaver (University of Colorado Boulder), Jenny Fuselier (High Point University), Matilde Lalín (Université de Montréal), and Michelle Manes (University of Hawai'i at Mānoa).

The (logarithmic) Mahler measure of a nonzero multivariable Laurent polynomial $P \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ is defined by

$$\mathrm{m}(P) := \frac{1}{(2\pi i)^n} \int_{\mathbb{T}^n} \log|P(x_1, \dots, x_n)| \frac{dx_1}{x_1} \dots \frac{dx_n}{x_n}.$$

This object has interesting connections to heights of polynomials and numbers, transcendence theory, volumes in hyperbolic space, knot invariants, ergodic theory, among others.

For a one-variable polynomial, one obtains a simple expression in terms of the roots of the polynomial. For multivariable polynomials there is no general formula, but there exist several examples of polynomials that yield special values of zeta and L-functions that are often associated to the geometric object defined by the zero set of the polynomial. For example, there are several examples were the polynomials correspond to an elliptic curve and the Mahler measure is related to $L(E, 2)$. These formulas have been related to Beilinson's conjectures.

In this project, we considered a family of $K3$-surfaces Y_k (where k is a parameter) defined by the desingularization of $P_k = 0$ where

$$P_k(x, y, z) = x + \frac{1}{x} + y + \frac{1}{y} + z + \frac{1}{z} - k.$$

The Picard number $\rho(Y_k)$ is generically equal to 19, but for some special values of k, $\rho(Y_k) = 20$. In this case, the $K3$-surface is called singular and the transcendental lattice has dimension 2, analogous to the elliptic curve case. The cases of $k = 0, 2, 10$ fall into this category and were studied by Bertin [2, 3]. The goal of the project was to study the Mahler measures for the cases of $k = 3, 6, 18$ which are also known to correspond to singular $K3$-surfaces.

We were able to obtain

$$m(P_3) = \frac{15\sqrt{15}}{2\pi^3} L(f_{15}, 3) \overset{?}{=} \frac{|\det T(Y_3)|^{3/2}}{2\pi^3} L(Y_3, 3)$$

$$m(P_6) = \frac{24\sqrt{24}}{2\pi^3} L(f_{24}, 3) = \frac{|\det T(Y_6)|^{3/2}}{2\pi^3} L(Y_6, 3)$$

$$m(P_{18}) = \frac{120\sqrt{120}}{2\pi^3} L(f_{120}, 3) + \frac{21\sqrt{3}}{10\pi} L(\chi_{-3}, 2) \overset{?}{=} \frac{|\det T(Y_{18})|^{3/2}}{9\pi^3} L(Y_{18}, 3) + \frac{21\sqrt{3}}{10\pi} L(\chi_{-3}, 2),$$

where f_{15}, f_{24}, f_{120} denote newforms of levels 15, 24 and 120, and T denotes the transcendental lattice of Y_k. The question marks indicate conjectural formulas.

We used a formula of Bertin [1] to relate the Mahler measures to the L-functions of newforms. The other part of the proofs consists of relating the L-function of the newforms to the L-function of the surfaces. For this part, the main ingredient is Livné's modularity theorem. This was accomplished in the case of $k = 6$, but the $k = 3, 18$ cases are harder to attack because we use an elliptic fibration of the surface having an infinite section which requires the use of Néron's desingularization. We hope to complete theses proofs in the near future.

4.2 Group 2: Square-free values of sequences related to reductions of elliptic curves over finite fields

Participants: Shabnam Akhtari (CRM, Montreal), Chantal David (Concordia University), Heekyoung Hahn (McGill University), Min Lee (Columbia University), and Lola Thompson (Dartmouth College).

Let E be an elliptic curve over $\mathbb{Q}$. For each prime p of good reduction, E reduces to a curve E_p over the finite field $\mathbb{F}_p$ with $\#E_p(\mathbb{F}_p) = p + 1 - a_p(E)$ where $|a_p(E)| \leq 2\sqrt{p}$ (the Hasse bound).

There are many conjectures about properties of the various reductions as one varies over all the primes, for example, the Sato-Tate conjecture which was recently proven by Taylor, Harris and Shepherd-Barron. Or the Lang-Trotter conjecture about $\#\left\{p \leq x \ : \ a_p(E) = r\right\}$ for a given integer r, or the Koblitz conjecture about $\#\left\{p \leq x \ : \ \#E_p(\mathbb{F}_p) \text{ is prime}\right\}$. Those last two conjectures are mostly completely open. The most important result known is perhaps the work of Elkies [5] who showed that there are infinitively many supersingular primes (i.e. primes such that $a_p(E) = 0$) for any E over $\mathbb{Q}$. This is the only known lower bound for those questions.

Let $f_p(E)$ be a sequence associated with the reductions of E over $\mathbb{F}_p$. The two cases that we have in mind are $f_p(E) = p + 1 - a_p(E)$ and $f_p(E) = a_p(E)^2 - 4p$. The first sequence describes the order of the reduced groups $E_p(\mathbb{F}_p)$ and the second one is related to the ring of endomorphisms of the reduced curve E_p over $\mathbb{F}_p$. We concentrate on the case where E does not have CM.

We want to count
$$\pi_{f,E}^{\mathrm{SF}}(x) = \# \left\{ p \leq x \ : \ f_E(p) \ \text{ is squarefree} \right\}.$$
It is easy to make a conjecture

$$\pi_{f,E}^{\mathrm{SF}}(x) \quad \sim \quad C_{E,f}^{\mathrm{SF}} \pi(x) \tag{1}$$

where

$$C_{E,f}^{\mathrm{SF}} = \sum_{d=1}^{\infty} \frac{\mu(d) |C_{E,f}(d^2)|}{|G_E(d^2)|} \tag{2}$$

with $G_E(d^2)$ the Galois group of $\mathbb{Q}(E[d^2])/\mathbb{Q} \subseteq \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z})$ and $C_{E,f}(d^2) \subseteq G_E(d^2)$ a conjugacy class determined by $f_p(E)$.

There are some known results about the above conjecture. It was shown to hold under some standard conjectures in analytic number theory (namely the Generalized Riemann Hypothesis, the Artin Holomorphy Conjecture and the Pair Correlation Conjecture) by Cojocaru [4], and it as shown to hold on average by David and Jimenez Urroz [7].

As a first project, we will concentrate on writing an unconditional upper bound for $\pi_{E,f}^{\mathrm{SF}}(x)$ of the type

$$\pi_{E,f}^{\mathrm{SF}}(x) \leq C_{E,f}^{\mathrm{SF}} \pi(x) \left(1 + \underline{o}(1)\right), \tag{3}$$

where $C_{E,f}^{\mathrm{SF}}$ is the conjectural constant of (2). In order to do so, we first write

$$\pi_{E,f}^{\mathrm{SF}}(x) \leq \# \left\{ p \leq x \ : \ \ell^2 \nmid f_p(E) \ \text{ for all } \ \ell \leq z \right\}, \tag{4}$$

and use the Cheboratev Density Theorem in the extension obtained by adjoining all ℓ^2-torsion for $\ell \leq z$. One needs to deal with the error term by choosing z appropriately, and presumably, this can be done without assuming the GRH.

In the paper [7], the authors considered the problem of evaluating $\pi_{E,f}^{\mathrm{SF}}(x)$ on average over a family of curves. The main result of the paper can be restated by saying that for most curves, $\left| \pi_{E,f}^{\mathrm{SF}}(x) - C_{E,f}^{\mathrm{SF}} \pi(x) \right|$ is very small, except possibly for a small exceptional set of curves. In a second project, we will concentrate on improving that result (i.e. improving the size of the exceptional set) by combining the use of the Cheboratev Density Theorem (for sieving small squares) and the average (for sieving large squares).

While in Banff, we wrote the details of the proof of (3), which involves only some straightforward applications of the Chebotarev Density Theorem, as a way to familiarise ourselves with the tools needed to study the conjecture (1). By using (4), and sieving for squares of primes up to $z = \log \log x$, we were able to get the correct upper bound, with the conjectural constant $C_{E,f}^{\mathrm{SF}}$.

We then began to study the second project. Among other things, we are led to averages of the type

$$\sum_{E \in \mathfrak{C}} C_{E,f}^{\mathrm{SF}},$$

where C_E^{SF} is the constant defined in (2). Such averages were considered by Jones [6], under some hypothesis on the size of exceptional Galois groups in Serre's theorem, and more recently by Zywina [8] who was able to prove the results of Jones in some cases with any hypothesis, by using an effective result of Masser and Wüstholz. We are now investigating the generalisation of the results of Jones and Zywina to our setting.

4.3 Group 3: Statistics for D_4 curves over finite fields

Participants: Alina Bucur (University of California at San Diego), Jing Hoelscher (University of Illinois at Chicago), Renate Scheidler (University of Calgary), and Melanie Matchett Wood (American Institute of Mathematics and University of Wisconsin-Madison).

Algebraic curves over finite fields are basic objects in number theory that also happen to come up in many applications, e.g. cryptography, error-correcting codes. One of the fundamental properties of a curve of a finite fields is its number of rational points over the field of definition, or more generally over extensions of said field. For example, these numbers determine the zeta function of the curve, which exhibits behavior similar to zeta functions of number fields, with the added bonus that in the case of finite fields, the Riemann Hypothesis is a theorem of Weil.

Besides looking at a single curve, it is also interesting to look at average properties of the number of points over a family of curves. Traditionally, this has been done in situations where the finite field was allowed to vary, as in this case one can use powerful methods of Deligne. But more recently, attention has been focused on families over a fixed finite field $\mathbb{F}_q$, where things behave quite differently. For instance, Kurlberg and Rudnick have studied the family of hyperelliptic curves [14]; Bucur, David, Feigon, Lalín looked at the families of cyclic p-fold covers of $\mathbb{P}^1$ [9, 11] and plane curves [10]; Bucur and Kedlaya computed the statistics for curves that are complete intersections of smooth quasi-projective subschemes of $\mathbb{P}^n$ [12]; Wood has answered the same question about degree 3 (not necessarily cyclic) covers of $\mathbb{P}^1$ [16]. In each of these cases, the statistics of the number of points on a curve in the given family turns out to be governed by a probabilistic model, i.e. they behave asymptotically like a sum of certain i.i.d. random variables. These random variables can be interpreted as the probabilities that the fiber over each point of the relevant projective space has a given number of points.

In the first three cases the average number of points on a curve in the family turns out to be exactly the same as the number of points on $\mathbb{P}^1$ itself, namely $q+1$. But in the case of complete intersections, the average number of points is $< q+1$, while in the last case it is $> q+1$.

A natural extension of the case studied by Kurlberg and Rudnick in [14] is the case of the double covers of hyperelliptic curves. While this is an easy question to formulate, one stumbles at the first step since not even the number of curves in this family is known. In all the previous cases, the objects in the families studied were parametrized by a rational moduli space. However, in the present case, the parameter space for our curves is more complicated.

Counting isomorphism classes of double covers of a scheme S is equivalent to counting isomorphism classes of pairs (s, L) where L is a line bundle on S and $s \in L^{\otimes -2}$ (e.g. see [15]). From Wood's previous work [15], we know that counting isomorphism classes of double covers of a scheme S with a line bundle on the double cover is equivalent to counting isomorphism classes of binary quadratic forms on S (as defined in [15]). These facts allow us to break the problem into two steps. First we will parametrize double covers $C \xrightarrow{2} \mathbb{P}^1_{\mathbb{F}_q}$ of fixed genus g_C with a line bundle L, and then we will parametrize double covers $D \xrightarrow{2} C$ of a specific hyperelliptic cover C with fixed genus g_D.

When we work out concretely what binary quadratic forms on $\mathbb{P}^1$ are, it turns out that we need to count orbits of the action of a certain group G on $\mathcal{O}(m-r)x^2 \oplus \mathcal{O}(m)xy \oplus \mathcal{O}(m+r)$ (where $\mathcal{O}(i)$ denotes the usual sheaf on $\mathbb{P}^1$, whose global sections are binary degree i forms). During the week of the workshop, we reduced the problem to the count of these orbits. We proved that the main term is given by the case $r = 0$. We used Dickson's work on equivalence classes of pairs of binary quadratic forms [13] to compute an asymptotic for the $r = 0$ term. Using this computation, we proved that the main term in the number of double covers of double covers $D \xrightarrow{2} C \xrightarrow{2} \mathbb{P}^1$ of a given genus g_D is given asymptotically as $g_D \to \infty$ by

$$q^{2g_D+5}\frac{(2-q^{-1})(1-q^{-(2g_D+4)/3})}{(1-q^{-1})(1-q^{-2})} + O\left(q^{5g_D/3}\left(1-q^{-(g_D-1)/6}\right)\right).$$

Note that the result is for double covers of double covers, and not for D_4 covers, which is our target. The next step is to sieve for the other possible Galois groups and get an asymptotic for all D_4 covers of $\mathbb{P}^1$. Then we will need to sieve for various covers that have various desirable geometric properties, like reduced, irreducible and smooth.

4.4 Group 4: Arithmetic Geometry

Participants: Alina Carmen Cojocaru (University of Illinois at Chicago), Rachel Davis (University of Wisconsin), Antonella Perucca (Katholieke Universiteit Leuven), Alice Silverberg (University of California, Irvine), Katherine E. Stange (Stanford University), and Diane Yap (University of Hawai'i at Mānoa).

The group explored some problems relating to abelian surfaces over the field of rational numbers and over finite fields.

We began by studying some of the background on abelian varieties, especially the arithmetic aspects of abelian surfaces, including classification of the endomorphism ring, structure of torsion modules, properties of the associated Galois representations, splitting (simple vs. non-simple), and properties of the reductions modulo primes for abelian varieties over the rationals. See [17-46] for some of the papers we looked at.

We also formulated some problems to consider, and discussed various approaches we would take to solve them. We did some exploratory work and achieved a better understanding of the problems, what is known, and what obstacles remain.

4.5 Group 5: K-theory and Algebraic Number Theory

Participants: Veronika Ertl (University of Utah), Wieslawa Niziol (University of Utah), Bregje Pauwels (University of California at Los Angeles), Sujatha Ramdorai (University of British Columbia), and Ila Varma (Princeton University).

One of the fundamental open problems in arithmetic is the description of the Galois group $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Class field theory affords a description of the Galois group G^{ab}maximal abelian extension of $\mathbb{Q}$ and the decomposition groups, namely the Galois groups G_p^{ab},of the maximal abelian extensions of the local fields $\mathbb{Q}_p$, as p varies over prime integer primes, are important constituents of the description of G^{ab}. Local class field theory affords a description of finite quotients of G_p^{ab} in terms of K^*, where K is a finite abelian extension of $\mathbb{Q}_p$, via the reciprocity map. Higher dimensional local fields of dimension > 1 have been studied by Kato, Saito, Vostokov, Fesenko and others. They have proved the existence of higher dimensional reciprocity maps which describes the Galois groups of abelian extensions of higher dimensional local fields F of dimension n, in terms of higher Milnor K-groups $K_n^M(F)$. Let F be any field. The Bloch-Kato conjecture asserts that there is an isomorphism

$$K_n^M(F)/p^n \simeq H^n(\mathrm{Gal}(F^{\mathrm{sep}}/F, A).$$

Here F^{sep} is a separable closure of F, p a prime and A is the Galois module $\mu_{p^m}^{\otimes m}$ if p is prime to the characteristic of F and the module of differentials $\nu_n(F))$ otherwise. Thus, for higher dimensional local fields F, the higher Milnor K-groups $K_n^M(F)$ occur as a common theme in studying higher dimensional reciprocity laws and the Milnor conjecture.

An important question in arithmetic geometry is the study of the Gersten sequence for Milnor K-theory which we describe below. Let X be a smooth (or more generally regular) scheme, over a local ring of mixed characteristic. Then the Gersten complex is the complex

$$0 \to K_n^M \to \oplus_{x \in X^0} i_x^* K_n^M(x) \to \oplus_{x \in X^1} i_x^* K_{n-1}^M(x) \to \dots$$

where X^k is the set of codimension k points on X, $i_x : x \to X$ is the inclusion map and one considers pull backs of the Milnor K-sheaves. The Gersten conjecture is the assertion that this sequence is exact. We would like to think about two concrete problems:

1. Determine the structure of $K_n^M(K)$ of complete discrete valuations fields of mixed characteristic. Check [49, 51] for what is known. Consult [52, 50] for basics on K-theory and Milnor K-theory.

2. Gersten's conjecture is open as stated, i.e., integrally. It is known mod-l, if l is different from the residue characteristic p. We will try to see whether we can prove it mod-p.

The problems as stated above are difficult problems and a review of literature on the questions was undertaken. Though no concrete progress was made towards the solution of the two problems, the possibility of using the existing techniques in describing the Milnor K-groups $K_i^M(F)$ for special higher dimensional local fields, to understand the Milnor K-group $K_1^M(R)$ for total quotient rings of noncommutative, Auslander regular Iwasawa algebras was explored. This would have implications for the study of p-adic L-functions arising in noncommutative Iwasawa theory.

4.6 Group 6: Zeta functions of Artin-Schreier varieties and Hodge polygons of exponential sums

Participants: Rebecca Bellovin (Stanford University), Sharon Anne Garthwaite (Bucknell University), Ekin Ozman (University of Texas-Austin), Rachel Pries (Colorado State University), Cassandra Williams (Colorado State University), and Hui June Zhu (State University New York at Buffalo).

Let q be a power of a prime p. Given a variety V over the finite field $\mathbb{F}_q$, an important problem is to count the number of rational points of V over finite extensions of $\mathbb{F}_q$. This information is encoded in the zeta function of V. By works of Dwork [56] and Deligne [55] on the Weil conjectures [60], the zeta function of a smooth projective variety V is a rational function in $\mathbb{Q}[T]$. When V is a hypersurface of dimension n, the non-trivial information about the zeta function is encoded in an L-function $L(V/\mathbb{F}_q;T)$, whose roots are algebraic integers with complex absolute values equal to $q^{n/2}$, and ℓ-adic absolute values equal to 1 for each prime $\ell \neq p$. It remains to know the distribution of the p-adic absolute values of these roots. This question is equivalent to determining the slopes of the p-adic Newton polygon $\mathrm{NP}(V)$ of the L-function.

On the other hand, it is a classical question in number theory to study the exponential sum of a Laurent polynomial $f(x_1,\ldots,x_n)$ in $\mathbb{F}_q[x_1^{\pm 1},\ldots,x_n^{\pm 1}]$ by its L-function $L(f/\mathbb{F}_q;T)$. Write its normalized p-adic Newton polygon by $\mathrm{NP}(f)$. These two questions are related in the following way: Consider the affine toric Artin-Schreier variety V_f in $\mathbb{A}^{n+1}$ defined by the affine equation $y^p - y = f(x_1,\ldots x_n)$. The p-adic Newton polygon of $L(f/\mathbb{F}_q;T)$ and the p-adic Newton polygon of $L(V_f/\mathbb{F}_q;T)$ are the same after scaling by a factor of $p-1$, denoted by $\mathrm{NP}(V_f) = (p-1)\mathrm{NP}(f)$.

Until recently the task of determining the p-adic Newton polygon of an Artin-Schreier variety or exponential sum was anything but easy; they were only accessible in very special cases, and estimation results of the Newton polygons were often case-by-case. However things have changed due to the work of [57, 54, 59].

For a Laurent polynomial f, the Hodge polygon $\mathrm{HP}(f)$ of the L-function of the exponential sum of f is defined using weightings of lattice points in a polytope Δ_f determined by the monomials in f. This combinatorial object encodes the essential topological (cohomological) data for the toric Artin-Schreier variety V_f. In this way $\mathrm{HP}(f)$ guards the p-adic valuations of the roots of $L(f/\mathbb{F}_q;T)$, and hence it gives a lower bound of $\mathrm{NP}(f)$ (see [59, 54]). This is analogous to the fact that the Hodge numbers of an algebraic variety over a finite field determine a Hodge polygon which is a lower bound for the Newton polygon [58]. For a prescribed Newton polytope Δ in $\mathbb{R}^n$, and a Laurent polynomial $f(x_1,\ldots,x_n)$ in $\mathbb{F}_q[x_1^{\pm 1},\ldots,x_n^{\pm 1}]$ with $\Delta_f = \Delta$, there are necessary and sufficient conditions for when $\mathrm{NP}(f)$ coincides with the lower bound $\mathrm{HP}(\Delta_f)$ (see [54, 59]).

The starting point of our group project was computing the L-function of $f = x_1^m + \cdots + x_n^m$ over $\mathbb{F}_q$. This classical case has been studied in the literature, and the Newton polygon of f can be computed using Gauss sums and the Stickelberger theorem. The goal of our project is to study deformations of the classical diagonal case to cases closely related to the important Kloosterman forms. First, we found closed form formulae for the Hodge polygons of Laurent polynomials of the form

$$f = x_1^m + \cdots + x_n^m + x_1^{-m} + \cdots + x_j^{-m}.$$

Second, we found closed form formulae for the Hodge polygons of the generalized Kloosterman family given by

$$f = x_1^m + \cdots + x_n^m + t(x_1 \cdots x_n)^{-1},$$

with parameter t varying in $\mathbb{Q}^*$. For each reduction modulo p of f, one arrives at a special fibre of a motive over the torus $\mathbb{G}_m(\mathbb{F}_p)$. In addition, we proved some original asymptotic results about the variation of the Newton polygon for fixed dimension n and $m >> 0$.

4.7 Group 7: Project Title: Ramanujan supercongruences and complex multiplications

Participants: Sarah Chisholm (University of Calgary), Alyson Deines (University of Washington), Ling Long (Iowa State University), Gabriele Nebe (RWTH Aachen University), and Holly Swisher (Oregon State University).

Ramanujan discovered 17 series of the form

$$\sum_{k\geq 0} \frac{(1/2)_k^3}{k!^3}(6k+1)\frac{1}{4^k} = \frac{4}{\pi},\ (1/2)_k = 1/2\cdot(1/2+1)\cdots(1/2+k-1)$$

which is related to elliptic curves with complex multiplications. These expansions of $\frac{1}{\pi}$ admit p-adic analogues, called Ramanujan supercongruences, of the following form: for any prime $p>3$

$$\sum_{k=0}^{(p-1)/2} \frac{(1/2)_k^3}{k!^3}(6k+1)\frac{1}{4^k} \equiv (-1)^{(p-1)/2}p \mod p^3.$$

The goal of the project is to give a geometric proof of Ramanujan supercongruences. To be more precise, for $\lambda \in \overline{\mathbb{Q}}$ such that $E_\lambda : y^2 = (x-1)(x^2 - \frac{1}{1+\lambda})$ admits complex multiplications, following Ramanujan's idea, there exist numbers $a, b, \delta \in \mathbb{Q}(\lambda)$ such that

$$\sum_{k\geq 0} \frac{(1/2)_k^3}{k!^3}(ak+b)\lambda^k = \frac{\delta}{\pi}.$$

Correspondingly, we will like to prove that for any prime $p>7$ such that $\lambda \in \mathbb{Q}_p$ the following congruence hold

$$\sum_{k=0}^{(p-1)/2} \frac{(1/2)_k^3}{k!^3}(ak+b)\lambda^k = u(p)\cdot b\cdot p \mod p^2,$$

where $u(p)$ is a root of unity depending on p that can be embedded in $\mathbb{Q}_p$.

The Picard-Fuchs equation of the family of elliptic curves $E_\lambda : y^2 = (x-1)(x^2 - \frac{1}{1+\lambda})$ is an order 2 hypergeometric differential equation, whose symmetric square is the Picard Fuchs equation for the family of K3 surfaces $X_\lambda : z^2 = xy(x+1)(y+1)(x+\lambda y)$. We counted the $\mathbb{F}_p$ points on X_λ modulo p^3 for arbitrary λ over $\mathbb{F}_p$ by using results of Ahlgren, Kilbourn, Ono, Pennisten and hope this will give insights for accomplishing our project.

4.8 Group 8: Arithmetic Intersection Formulas

Participants: Jackie Anderson (Brown University, Jennifer Balakrishnan (Harvard University, Kristin Lauter (Microsoft Research), Jennier Park (Massachusetts Institute of Technology), and Bianca Viray (Brown University).

The goal of our project was to prove equality between two arithmetic intersection formulas when the assumptions for both formulas are satisfied. We begin with some motivation. The *absolute Igusa invariants* i_1, i_2, i_3 of a genus 2 curve can be defined by values of modular functions on the Siegel moduli space. They determine the isomorphism class of a genus 2 curve over $\mathbb{C}$ when $i_1 \neq 0$. The *Igusa class polynomials* $H_{j,K}$ of a primitive quartic CM field K are the minimal polynomials of Igusa invariants: for each $j = 1, 2, 3$, $H_{j,K} = \prod(x - i_j(C))$, where the product ranges over isomorphism classes of genus 2 curves C with CM by K (i.e. with an embedding of $\mathcal{O}_K$ into $\mathrm{End}(\mathrm{Jac(C)})$), and the modular function is evaluated at the point in the Siegel upper half plane corresponding to the canonically polarized Jacobian of the curve C. The coefficients of these polynomials are rational but not necessarily integral. To compute them efficiently, it is important to understand the denominators appearing in the coefficients.

The first Igusa invariant can be defined by the following ratio of modular forms: $i_1 := 2\cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}$. A prime ℓ appearing in the denominator of i_1 corresponds to a pole of i_1 at a CM-point over $\overline{\mathbb{F}}_\ell$. Since the numerators are modular forms, there is a pole of i_1 at a point P only if P is a zero of χ_{10}. Away from 2, $\operatorname{div}(\chi_{10}) = 2G_1$, so $12\,(G_1.CM(K))_\ell$ gives a formula for the ℓ-valuation of the denominators, up to cancellation.

Bruinier and Yang [61] gave a conjectural formula for this intersection number for primitive quartic CM fields K, under the assumption that the discriminant of K is $D^2\widetilde{D}$, where D and $\widetilde{D}$ are primes $\equiv 1 \pmod 4$. Let K be a totally imaginary quadratic extension of $F = \mathbb{Q}(\sqrt{D})$, $D \equiv 1 \pmod 4$ and prime, A and B such that $K = F(\sqrt{A + B\sqrt{D}})$.

Theorem 1 (Bruinier-Yang Conjecture)**.** *Let $\widetilde{K}$ be the reflex field of K and $\widetilde{F}$ be the quadratic subfield of $\widetilde{K}$. Then*

$$\frac{(CM(K).G_1)_\ell}{\log(\ell)} = \sum_{\delta = \frac{D - x^2}{4} \in \mathbb{Z}_{\geq 0}} \quad \sum_{\substack{n \text{ s.t. } \frac{n + \delta\sqrt{\widetilde{D}}}{2D} \in \mathrm{Disc}_{\widetilde{K}/\widetilde{F}} \\ |n| < \delta\sqrt{\widetilde{D}}}} B_{\frac{n+\delta\sqrt{\widetilde{D}}}{2D}}(\ell),$$

where

$$B_t(l) = \begin{cases} 0, \text{ if } \mathfrak{l} \text{ splits in } \widetilde{K} \\ (v_{\mathfrak{l}}(t) + 1)\mathfrak{A}(t\mathcal{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1})f(\mathfrak{l}/l), \text{ otherwise} \end{cases},$$

where $\mathfrak{A}(t\mathcal{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1})$ denotes the number of ideals in $\mathcal{O}_{\widetilde{K}}$ whose relative norm in $\widetilde{F}$ is $t\mathcal{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}$. It has been proved by Yang [64] when $A^2 - DB^2 \equiv 1 \pmod 4$ is prime and $\mathcal{O}_K$ is generated over $\mathcal{O}_F$ by an element of a special form.

More recently, Lauter and Viray [63] gave a formula for the intersection number that holds, away from a few primes, for all primitive quartic CM fields such that $\mathcal{O}_K$ is principally generated over $\mathcal{O}_F$. We state it here in a simple case to emphasize its formal likeness to the formula given by Bruinier-Yang. Assume that $\mathcal{O}_K$ is generated over $\mathcal{O}_F$ by one element, say η, so $\mathcal{O}_K = \mathcal{O}_F[\eta]$. Let $\widetilde{D}$ denote $\mathrm{Norm}_{F/\mathbb{Q}}\left(\mathrm{Disc}_{K/F}(\mathcal{O}_K)\right)$ and let $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{Z}$ be such that

$$\mathrm{Tr}_{K/F}(\eta) = \alpha_0 + \alpha_1\frac{\mathrm{D} + \sqrt{\mathrm{D}}}{2}, \quad \mathrm{Norm}_{K/F}(\eta) = \beta_0 + \beta_1\frac{\mathrm{D} + \sqrt{\mathrm{D}}}{2}.$$

Theorem 2 (Lauter-Viray)**.** *Assume that $\ell \neq 2$, $D = 5$ and that $\mathrm{d}_u(n)$ (defined below) is an odd fundamental quadratic discriminant prime to ℓ, for every n that appears below.*

$$\frac{(CM(K).G_1)_\ell}{\log(\ell)} = \sum_{\delta = \frac{D - \square}{4} > 0} \quad \sum_{\substack{n \text{ such that} \\ \frac{\delta^2\widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0} \\ n \equiv -c(K) \pmod{2D}}} B(\delta, n)$$

$$B(\delta, n) = \frac{1}{2}\left(v_\ell\left(N\right) + 2\right)\mathfrak{A}_{d_u(n)}\left(N\right)\rho_{d_u(n)}\left(N\right),$$

where

$$\mathfrak{A}_d(N) := \#\left\{\mathfrak{b} \subseteq \mathbb{Z}\left[\frac{d + \sqrt{d}}{2}\right] : \mathrm{Norm}(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible}\right\}$$

$$\rho_d(N) := \begin{cases} 0 & \text{if } \left(\frac{d^*}{p}\right)^{a_p}\left(\frac{-\ell e_p}{p}\right) = -1 \text{ for some } p|d, \\ & \text{where } N = p^{a_p}e_p \text{ and } d^* = (-1)^{\frac{p-1}{2}}\frac{d}{p} \\ 2^{\#\{p : p|N \text{ and } p|d\}} & \text{otherwise} \end{cases}$$

$$c(K) := \delta\left(\alpha_0^2 + \alpha_0\alpha_1 D + \alpha_1^2\frac{D^2 - D}{4} - 4\beta_0 - 2\beta_1 D\right)$$

$$d_u(n) := (\alpha_1\delta)^2 - 4\frac{(n + c(K))\delta}{-2D}.$$

Since the Lauter-Viray and Bruinier-Yang formulas both hold for primitive quartic CM fields under certain assumptions, we considered the fields where both hypotheses were satisfied and sought to prove a direct correspondence between the two statements. As a first step, we split the work into cases according to the form of the generator η (see [62]). During the WIN2 Workshop, we worked on the case where $\eta = \frac{1+\sqrt{A+B\sqrt{D}}}{2}$. This gives simplified formulas for $\alpha_i, \beta_i, c(K), d_u(n)$. Using this, we were able to prove that the Bruinier-Yang and Lauter-Viray formulas are equal and match term-by-term:

Theorem 3 (ABLPV). *Assume that* $\left(\frac{\delta^2\widetilde{D}-n^2}{4Dl}\right)$ *is coprime to* $(2\delta\ell d_u)$*, that* $\rho_{d_u(n)}\left(\frac{\delta^2\widetilde{D}-n^2}{4Dl}\right) \neq 0$ *and that all the assumptions for BY and LV are satisfied (in particular, assume that* $(\ell, 2\delta d_u) = 1$*). Then*

$$\mathfrak{A}_{d_u(n)}\left(\frac{\delta^2\widetilde{D}-n^2}{4Dl}\right)\rho_{d_u(n)}\left(\frac{\delta^2\widetilde{D}-n^2}{4Dl}\right) = \mathfrak{A}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathcal{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}\right).$$

References

[1] M.-J. Bertin, Mesure de Mahler d'hypersurfaces K3. *J. Number Theory* **128** (2008), 2890–2913.

[2] M.-J. Bertin, Mahler's measure and L-series of K3 hypersurfaces. *Mirror symmetry.* V, 3–18, AMS/IP Stud. Adv. Math., 38, Amer. Math. Soc., Providence, RI, 2006.

[3] M.-J. Bertin, Measure de Mahler et série L d'une surface K3 singulière. *Actes de la Conférence "Fonctions L et Arithmétique"*, 5–28, Publ. Math. Besançon Algèbre Théorie Nr., Lab. Math. Besançon, Besançon, 2010.

[4] A. C. Cojocaru, Cyclicity of Elliptic Curves modulo p, Ph.D. thesis, Queen's University, 2002.

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

[6] N. Jones, Averages of elliptic curve constants, *Math. Ann.* **345** (2009), 685–710.

[7] C. David and J. Jimenez Urroz, Square-free discriminants of Frobenius rings, *International Journal of Number Theory* **6** (2010), 1391–1412.

[8] D. Zywina, Bounds for Serre's open image theorem, preprint.

[9] A. Bucur, C. David, B. Feigon and M. Lalín, Statistics for traces of cyclic trigonal curves over finite fields, *Int. Math. Res. Not. IMRN* 2010, no. 5, 932–967.

[10] A. Bucur, C. David, B. Feigon and M. Lalín, The fluctuations in the number of points of smooth plane curves over finite fields, *J. Number Theory* **103**, Issue 11 (2010), 2528–2541.

[11] A. Bucur, C. David, B. Feigon and M. Lalín, Biased statistics for traces of cyclic p-fold covers over finite fields. In *WIN—Women in Numbers*, Fields Institute Communications, **60**, 121–143, American Mathematical Society, 2011.

[12] A. Bucur and K.S. Kedlaya, The probability that a complete intersection is smooth. *J. Théor. Nombres Bordeaux*, to appear; arXiv:1003.5222v2.

[13] L.E. Dickson, Rational Reduction of a Pair of Binary Quadratic Forms; Their Modular Invariants, *Amer. J. Math.* **31** (1909), no. 2, 103–146.

[14] P. Kurlberg and Z. Rudnick, The fluctuations in the number of points on a hyperelliptic curve over a finite field, *J. Number Theory* **129** (2009), no. 3, 580–587.

[15] M.M. Wood, Gauss composition over an arbitrary base, *Adv. Math.* **226** (2011), no. 2, 1756–1771.

[16] M.M. Wood, The distribution of the number of points on trigonal curves over $\mathbb{F}_q$, preprint, arXiv:1108.2526.

[17] J. Achter. Split reductions of simple abelian varieties. *Math. Res. Lett.* , 12(2): 199–213, 2009.

[18] P. Bayer and J. González. On the Hasse-Witt invariants of modular curves. *Experiment. Math.*, 6(1): 57–76, 1997.

[19] C-L. Chai, B. Conrad, and F. Oort. CM Liftings. Available at `http://math.stanford.edu/∼conrad/papers/CMbook.pdf`.

[20] N. Chavdarov. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke. Math. J.*, 87(1): 151–180, 1997.

[21] K-M Chou and E. Kani. Simple geometrically split abelian surfaces over finite fields. Available at `http://www.mast.queensu.ca/∼kani/papers/simpleAS3.pdf`.

[22] A. Cojocaru. Questions about the reductions modulo primes of an elliptic curve. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 61–79. Amer. Math. Soc., Providence, RI, 2004.

[23] A. Cojocaru and C. David. Frobenius fields for elliptic curves. *Amer. J. Math.*, 130(6): 1535–1560, 2008.

[24] A. Cojocaru, E. Fouvry, and M.R. Murty. The square sieve and the Lang-Trotter conjecture. *Canad. J. Math.*, 57(6): 1155–1177, 2005.

[25] L. Dieulefait. Explicit determinaion of the images of the Galois representations attached to abelian surfaces with End$(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4): 503–512 (2003), 2002.

[26] L. Dieulefait and V. Rotger. The arithmetic of QM-abelian surfaces through their Galois representations. *J. Algebra*, 281(1): 124–143, 2004.

[27] F. Fité, K. Kedlya, V. Rotger, and A. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. Available at `http://arxiv.org/abs/1110.6638`.

[28] S. Galbraith. Supersingular curves in cryptography (full version). Available at `http://www.math.auckland.ac.nz/∼sgal018/ss.pdf`.

[29] J. González. On the p-rank of an abelian variety and its endomorphism algebra. *Publ. Mat.*, 42(1): 119–130, 1998.

[30] S. Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *J. Number Theory*, 130(12): 2745–2752, 2010.

[31] S. Haloui. The minimum and maximum number of rational points on Jacobian surfaces over finite fields, 2010. Available at `http://arxiv.org/abs/1002.3683`.

[32] S. Haloui and V. Singh. The characteristic polynomials of abelian varieties of dimension 4 over finite fields. 2011. Available at `http://www.arxiv.org/pdf/1101.5070`.

[33] E. Howe, D. Maisner, E. Nart, and C. Ritzenthaler. Principally polarizable isogeny classes of abelian surfaces over finite fields. *Math. Res. Lett.*, 15(1): 121–127, 2008.

[34] E. Howe, E. Nart, and C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier (Grenoble)*, 59(1): 239–289, 2009.

[35] S. Lang and H. Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distributions of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[36] D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3): 321–337, 2002.

[37] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[38] D. Mumford. Abelian varieties. *Oxford Univ. Press*, 1970.

[39] F. Oort. Abelian varieties over finite fields. In *Higher-dimensional geometry over finite fields*, volume 16 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 123–188. IOS, Amsterdam, 2008.

[40] H-G Rück. Abelian surfaces and Jacobian varieties over finite fields. *Composito Math.*, 76(3): 351—366, 1990.

[41] W. M. Ruppert. Two-dimensional complex tori with multiplication by $\sqrt{d}$. *Arch. Math. (Basel)*, 72(4): 278–281, 1999.

[42] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[43] W. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[44] W.C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y.*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[45] D. Zywina. The splitting of reductions of an abelian variety. Available at `http://arxiv.org/pdf/1111.0624v1`.

[46] D. Zywina. The Lang-Trotter Conjecture and Mixed Representations. 2009. Available at `http://www.math.upenn.edu/ zywina/papers/LangTrotter.pdf`.

[47] Th. Geisser, Motivic cohomology over Dedekind rings. *Math. Z.* **248** (2004), no. 4, 773–794.

[48] M. Kerz, The Gersten conjecture for Milnor K-theory. *Invent. Math.* **175** (2009), no. 1, 1–33.

[49] M. Kurihara, On the structure of Milnor K-groups of certain complete discrete valuation fields. *J. Théor. Nombres Bordeaux* **16** (2004), no. 2, 377–401.

[50] J. Milnor, Introduction to algebraic K-theory. *Annals of Mathematics Studies*, No. 72. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971.

[51] J. Nakamura, On the structure of the Milnor K-groups of complete discrete valuation fields. Invitation to higher local fields (Münster, 1999), 123–135 (electronic), Geom. Topol. Monogr., 3, Geom. Topol. Publ., Coventry, 2000.

[52] D. Quillen, Higher algebraic K-theory. I. Algebraic K-theory, I: Higher K-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972), pp. 85–147. Lecture Notes in Math., Vol. 341, Springer, Berlin 1973.

[53] W. Raskind, Abelian class field theory of arithmetic schemes. K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), 85–187, Proc. Sympos. Pure Math., 58, Part 1, Amer. Math. Soc., Providence, RI, 1995.

[54] A. Adolphson and S. Sperber, Exponential sums and Newton polyhedra: Cohomology and estimates, *Ann. of Math.* **130** (1989), 367–406.

[55] P. Deligne, La conjecture de Weil. I, *Publications Mathematiques de l'IHES* **43** (1974), 273–307.

[56] B. Dwork, On the rationality of the zeta function of an algebraic variety, *American Journal of Mathematics* **82** (1960), 3:631–648.

[57] N. Katz, Sommes exponentielles, *Astérisque* **79** (1980).

[58] B. Mazur, Frobenius and the Hodge filtration (estimates). Ann. of Math. **98** (1973), 2:58–95.

[59] D. Wan, Variation of p-adic Newton polygons of L-functions for exponential sums, *Asian J. Math.*, **8** (2004), 3:427–474.

[60] A. Weil, Numbers of solutions of equations in finite fields, *Bulletin of the American Mathematical Society*. **55** (1949), 5:497–508.

[61] Jan Hendrik Bruinier, Tonghai Yang, CM-values of Hilbert modular functions, *Invent. Math.*, vol. 163, no. 2, (2006) pp. 229–288.

[62] B. K. Spearman and K. S. Williams. Relative integral bases for quartic fields over quadratic subfields. *Acta Math. Hungar.*, 70(3):185–192, 1996.

[63] Kristin Lauter, Bianca Viray, An arithmetic intersection formula for denominators of Igusa class polynomials, Preprint, 2011.

[64] Tonghai Yang, Arithmetic intersection on a Hilbert modular surface and the Faltings height, Preprint, 2007.