Number Theory Satellite Session
Session satellite en théorie des nombres
(Org: **Chantal David** (Concordia), **Eyal Goren** (McGill) and/et **Andrew Granville** (Montréal))

MOHAMMAD BARDESTANI, Université de Montréal
Product free sets in profinite groups

Inspired by Gowers' seminal paper on quasi-random finite groups, we will discuss quasi-randomness for profinite groups. We will obtain bounds for the minimal degree of non-trivial representations of $SL_k(\mathbb{Z}/(p^n\mathbb{Z})$ and $Sp_{2k}(\mathbb{Z}/(p^n\mathbb{Z})$. Our method also delivers a lower bound for the minimal degree of a faithful representation of these groups. Using the suitable machinery from functional analysis, we establish exponential lower and upper bounds for the supremal measure of a product-free measurable subset of the profinite groups $SL_k(\mathbb{Z}/(p^n\mathbb{Z})$ and $Sp_{2k}(\mathbb{Z}/(p^n\mathbb{Z})$. This is joint work with Keivan Mallahi-Karai.

SANDRO BETTIN, Universite de Montreal
Moments of derivatives of L-Functions

An important problem in analytic number theory is to understand the asymptotic behavior of mean values of L-functions. Keating and Snaith conjectured that these asymptotics can be predicted by computing mean values of characteristic polynomials of random matrices. In the same way one can also give conjectures for averages of derivatives of L-functions, but the process becomes computationally very expensive and we can compute the leading coefficients of only the first few moments. In the case of unitary families, Conrey, Rubinstein and Snaith showed that these coefficients can be expressed as the determinant of a matrix of I-Bessel functions, which allows a much faster computation. In this talk we extend their work to the case of symplectic families, expressing the coefficients as the determinant of certain hypergeometric functions. We also give a recursion formula for this determinant which speed up further the computations.

This work is joint with Ali Altug, Ian Petrow, Rishikesh and Ian Whitehead.

CE BIAN, University of Calgary
Introduction to the methods of computing GL(n) automorphic forms

During the last few years, mathimaticians have got some result in computational aspect of Maass cusp forms. Since after H.M.Stark and D.A.Hejhal gave a nice algorithem for computing $GL(2) = SL(2,\mathbb{Z})\backslash SL(2,\mathbb{R})/OL(2,\mathbb{R})$ form, a series of achievement was showed in Americian Institute of Mathematics (AIM) in 2008. In the workshop, three groups, who worked on computing $GL(3)$ forms, showed and confirmed there result with each other. I will introduce the methods they used together with the result we got at present. Also there are some "potential" method, which may give us other ways to compute those forms specially in higher rank.

CARMEN BRUNI, UBC
Twisted extensions of Fermat's Last Theorem

Let $x, y, z, p, n, \alpha \in \mathbb{Z}$ with $\alpha \geq 1$, p and $n \geq 5$ primes. In 2011, Michael Bennett, Florian Luca and Jamie Mulholland showed that the equation $x^3 + y^3 = p^\alpha z^n$ has no pairwise coprime nonzero integer solutions provided $p \geq 5$, $n \geq p^{2p}$ and $p \notin S$ where S is the set of primes q for which there exists an elliptic curve of conductor $N_E \in \{18q, 36q, 72q\}$ with at least one nontrivial rational 2-torsion point. I will present a solution that extends the result to include a subset of the primes in S; those $q \in S$ for which all curves with conductor $N_E \in \{18q, 36q, 72q\}$ with nontrivial rational 2-torsion have discriminants not of the form l^2 or $-3m^2$ with $l, m \in \mathbb{Z}$.

TIMOTHY CALEY, University of Waterloo
A new algorithm for the Prouhet-Tarry-Escott problem

Given natural numbers n and k with $k \leq n-1$, the Prouhet-Tarry-Escott problem (PTE) asks for distinct sets of integers $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ such that

$$\sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j$$

for $j = 1, \ldots, k$.

This problem has connections to combinatorics and theoretical computer science, as well as to other areas of number theory, such as Waring's problem.

The most interesting case is when $k = n-1$, which is called ideal. It is an open problem to determine whether ideal PTE solutions exist for a given n, as well as characterizing those that do exist. Computational techniques have been used to search for PTE solutions. In this talk, we present a new algorithm to find PTE solutions, and explain how the results yield additional information.

LUCA CANDELORI, McGill University
Harmonic weak Maass forms: a geometric approach.

In this talk we provide a geometric framework for the study of the Fourier coefficients of harmonic weak Maass forms of integral weight, a space of smooth modular forms first introduced by Bruinier and Funke in the context of singular theta lifts. In this geometric framework harmonic weak Maass forms arise from the construction of differentials whose classes are exact in certain de Rham cohomology groups attached to modular forms. We show how this new interpretation naturally leads to strengthenings of theorems of Bruinier,Ono and Rhoades, by answering in the affirmative conjectures about the field of definitions of Fourier coefficients of harmonic weak Maass forms. We also produce Eichler-Shimura-style isomorphisms for the de Rham cohomology attached to modular forms, generalizing results of Bringmann, Guerzhoy, Kent and Ono to any level and field of definition.

VORRAPAN CHANDEE, CRM
Simple zeros of primitive Dirichlet L-functions and the asymptotic large sieve

Assuming the Generalized Riemann Hypothesis, we show using the asymptotic large sieve that 91% of the zeros of primitive Dirichlet L-functions are simple. This improves on earlier work of Ozluk which gives a proportion of at most 82%. We further compute an q-analogue of the Pair Correlation Function $F(\alpha)$ averaged over all primitive Dirichlet L-functions in the range $|\alpha| < 2$. Previously such a result was available only when the average included all the characters χ. This is a joint work with Yoonbok Lee, Sheng-Chi Liu and Maksym Radziwill.

PETER CHO, University of Toronto
Logarithmic Derivatives of Artin L-functions

Let K be a number field of degree n, and d_K be its discriminant. Then under the Artin conjecture, GRH and certain zero density hypothesis, we show that the upper and lower bound of the logarithmic derivative of Artin L-functions attached to K at $s = 1$ are $\log\log|d_K|$ and $-(n-1)\log\log|d_K|$, resp. Unconditionally we show that there are infinitely many number fields with the extreme logarithmic derivative values. They are families of number fields whose Galois closures have the Galois group as C_n, $2 \leq n \leq 6$, D_n, $n = 3, 4, 5$, S_4, and A_5. This is a joint work with Henry H. Kim.

AARON CHRISTIE, University of Calgary
An Example of Geometrization in the Context of the Langlands Program

As work on the Langlands Program continues apace, it is useful to develop alternate perspectives that may prove important in furthering its progress, either as a means to new results or by shedding new light on what is already known. Geometrization offers one such alternate perspective. The notion will be briefly described by way of an example in the the case of p-adic $SL(2)$, which makes use of ℓ-adic local systems.

CHIH-YUN CHUANG, Mcgill university
Theta series of imaginary quadratic global function fields

Let $L/\mathbb{Q}$ be an imaginary quadratic extension. For an ideal class A of L one defines the partial zeta function ζ_A. Then ζ_A can be written as $\sum r_A(n)n^{-s}$ with certain well-defined integers $r_A(n)$. The theta series $\Theta_A(z) := \sum_{n\geq 0} r_A(n)\exp(2\pi inz)$ has a nice transformation law on certain congruence group. In this talk, we will give an analogue story in global function field with finite constant field $\mathbb{F}_q$ of characteristic $p \neq 2$. Similarly, the Fourier coefficients of the theta series in my case are also come from the cardinality of norm form. We will see that it is an automorphic form on GL_2.

BRIAN COOK, University of British Columbia
Many Variable Forms in the Primes

We will discuss the solubility of the equation $\mathcal{F}(x) = v$, where $\mathcal{F}$ is an symmetric integral form of fixed degree d in n variables $x = (x_1, \ldots, x_n)$, under the condition that x_i is prime for each $1 \leq i \leq n$.

ZEBEDIAH ENGBERG, Dartmouth College
Sporadic balanced subgroups

Let $d > 2$ be an integer. Using the standard representatives, any unit mod d lies either in the interval $(0, d/2)$ or $(d/2, d)$. A subgroup H of the group of units mod d is called balanced if every coset of H intersects these two intervals equally. There are two nice families of such subgroups, and a balanced subgroup is called sporadic if it is not included in either family. For a fixed number g, we consider the distribution of $d > 2$ coprime to g for which $\langle g \bmod d\rangle$ is sporadic balanced. This relates to a conjecture of Carl Pomerance and Douglas Ulmer.

ADAM FELIX, Max-Planck-Institut für Mathematik/University of Lethbridge
Variations of Artin's conjecture

Let a be a fixed integer. We study $i_a(p) := [(\mathbb{Z}/p\mathbb{Z})^* : \langle a \mod p\rangle]$, the index of a modulo p. Particular attention will be given to Artin's conjecture. Time permitting, we will discuss some relations between $i_a(p)$ and the order of a modulo p.

ANDREW FIORI, McGill University
Characterization of Special Points on Orthogonal Shimura Varieties

We shall discuss a characterization of the special fields associated to the special points on the Shimura varieties attached to orthogonal groups O_q coming from quadratic forms q of signature (2,n). Shimura reciprocity tells us that the values of modular forms at special points will always be contained in the Hilbert class field of a field closely related to the special field of the point. The characterization we give is obtained by way of a characterization of the algebraic tori $T \subset O_q$.

DANIEL FIORILLI, University of Michigan
Elliptic curves of unbounded rank and Chebyshev's bias

We establish an equivalence between quantitative unboundedness of the analytic rank of rational elliptic curves and the existence of highly biased elliptic curve prime number races. For this purpose we study the bias in the count of local points of a rational

elliptic curve E created by its analytic rank. We show that conditionally on a Riemann Hypothesis and on a hypothesis on the multiplicity of the zeros of $L(E,s)$, large analytic ranks translate into extreme Chebyshev biases. Conversely, we show under a certain linear independence hypothesis on zeros of $L(E,s)$ that if highly biased elliptic curve prime number races do exist, then the Riemann Hypothesis holds for infinitely many elliptic curve L-functions and there exist elliptic curves of arbitrarily large rank.

AMIR GHADERMARZI, University of British Columbia
Integral points on Mordell's curves

Let $k \neq 0$ be an integer. The elliptic curve $y^2 = x^3 + k$ is known as the Mordell curve. A well known theorem by Mordell states that for a given $k \neq 0$, the equation $y^2 = x^3 + k$ has only finitely many integral solutions. We will follow Mordell (1965) giving an algorithmic approach to find all solutions for small values of k. The idea is to apply the theory of binary cubic forms and classical invariant theory. Then we will talk about the results on the number of integral points on Mordell curves with $|k| < 10^7$, based on the algorithm we implemented on Magma.

ADELA GHERGA, McMaster University
Brauer-Kuroda Relations for Higher Class Numbers

Arising from permutation representations of finite groups, Brauer-Kuroda relations are relations between Dedekind zeta functions of certain intermediate fields of a Galois extension of number fields. Taking $s = 0$, these relations then provide a correspondence between class numbers of the corresponding fields, whereas for totally real Galois extensions, $\zeta_F(1-n)$ at $n \geq 2$ instead gives relations between orders of certain motivic cohomology groups. In this talk, we consider Brauer-Kuroda relations at negative odd integer values of s, wherein we shall see that they can be used to compute these orders for fields of large degree, even outside the capabilities of SAGE.

NATHAN GRIEVE, Queen's University
Groups and line bundles associated to abelian varieties

A line bundle on an abelian variety is non-degenerate if its Euler characteristic is nonzero. By a theorem of Mumford, such a line bundle admits a single nonzero cohomology group. This cohomology group is the unique irreducible weight one representation of the theta-Heisenberg group of the line bundle.

This talk has three goals. The first is to discuss the nature of cup-product problems arising from pairs of non-degenerate line bundles with positive index; the second concerns the higher weight representation theory of non-degenerate theta groups; the third is to describe a relation amongst adelic theta groups arising from pairs of line bundles.

BRANDON HANSON, University of Toronto
A Ramsey Theory Problem in Finite Fields

An open problem in arithmetic Ramsey theory asks if given a finite colouring $c : \mathbb{N} \to \{1, \ldots, r\}$ of the naturals, there exist $x, y \in \mathbb{N}$ such that $c(xy) = c(x+y)$. More generally, one could replace $x+y$ with a binary linear form and xy with a binary quadratic form. In this talk we discuss the analogous problem in a finite field $\mathbb{F}_q$. Specifically, given a linear form L and a quadratic from Q in two variables, we provide estimates on the necessary size of $A \subset \mathbb{F}_q$ to guarantee that $L(x,y)$ and $Q(x,y)$ are elements of A for some $x, y \in \mathbb{F}_q$.

ADAM HARPER, Centre de recherches mathematiques, Universite de Montreal
Inverse questions for the large sieve

The large sieve inequality implies that if one takes the integers less than x, and removes around half of the residue classes modulo each prime, then the resulting set must have size $\ll \sqrt{x}$. This bound is sharp in the case where one removes the

quadratic non-residues modulo each prime, in which case the set of squares is left behind. The *inverse conjecture for the large sieve* proposes, amongst other things, that there are no essentially different examples where this $\sqrt{x}$ bound is sharp.

In this talk I will outline how, by combining the large sieve, the larger sieve, and some basic ideas from additive combinatorics, one can prove some results in the direction of the inverse conjecture. This is joint work with Ben Green.

KEVIN HENRIOT, Université de Montréal et Université Paris 7

Arithmetic progressions in sumsets

We are concerned with quantitative statements about the additive structure of the set kA of sums of k elements of a subset A of $\{1,\dots,N\}$. For $k=2$, a result of Bourgain (1999) in this direction states that, provided A has density α at least $(\log N)^{-1/3+\varepsilon}$, the sumset $2A$ always contains a long arithmetic progression, of length $e^{c(\log N)^c}$. A recent result of Croot, Laba and Sisask (2011) shows that this result holds in the longer range $\alpha \geq (\log N)^{-1+\varepsilon}$. In this talk we discuss the analogue problem for $k=3$, in which case we expect the sumset $3A$ to possess more structure. Specifically, we show how methods developed by Sanders (2011) in the context of Roth's theorem may be applied to obtain an arithmetic progression of similar length in $3A$, in the longer range $\alpha \geq (\log N)^{-2+\varepsilon}$.

JING-JING HUANG, University of Toronto

Metric Diophantine approximation on planar curves

In 1998, Kleinbock and Margulis established the fundamental Baker-Sprindžuk conjecture concerning homogeneous Diophantine approximation on manifolds. Subsequently, the much stronger Khintchine-Jarník type theorem for non-degenerate planar curves has been established—thanks to Vaughan and Velani for the convergence theory and Beresnevich, Dodson and Velani for the divergence theory. Though, both approaches rely on estimates on the number of rational points with small denominators which are "close" to the curve, the two proofs differ quite significantly in nature. In this talk, I will try to describe a unified proof of the problem and some potential applications to the general case.

NATALIYA LAPTYEVA, University of Toronto

A Variant of Lehmers Conjecture in the CM Case

Lehmer's conjecture asserts that $\tau(p) \neq 0$, where τ is the Ramanujan τ-function. This is equivalent to the assertion that $\tau(n) \neq 0$ for any n. A related problem is to find the distribution of primes p for which $\tau(p) \equiv 0 \pmod{p}$. These are open problems. However, the variant of estimating the number of integers n for which n and $\tau(n)$ do not have a non-trivial common factor is more amenable to study. More generally, let f be a normalized eigenform for the Hecke operators of weight $k \geq 2$ and having rational integer Fourier coefficients $\{a(n)\}$. It is interesting to study the quantity $(n, a(n))$. It was proved by S. Gun and V. K. Murty (2009) that for Hecke eigenforms f of weight 2 with CM and integer coefficients $a(n)$

$$\{n \leq x \mid (n, a(n)) = 1\} = \frac{(1+o(1))U_f x}{\sqrt{\log x \log\log\log x}}$$

for some constant U_f. We extend this result to higher weight forms.
We also show that

$$\{n \leq x \mid (n, a(n)) \text{ is a prime}\} \ll \frac{x \log\log\log\log x}{\sqrt{\log x \log\log\log x}}.$$

SEYED LAVASANI, University of Calgary

The inside-out of cover attack

A cover attack is a method of decreasing the complexity of the discrete logarithm problem defined on the Jacobian of a curve by transferring it to the Jacobian of a new curve which admits a faster solution for this problem. The new curve shares a cover with the original curve.

In this talk we carefully study the known algorithms for implementing the different steps of this attack while looking for possible generalizations. Furthermore we present new approaches for constructing the cover and finding new sub-curves with vulnerable Jacobians. We present an algorithm to compute a model for many potential covers using their automorphism group and their ramification structure.

SEBASTIEN LINDNER, Univerisity of Calgary
Divisor Arithmetic Over Low Genus Hyperelliptic Curves

Our main objective is to improve efficiency of low-genus hyperelliptic curve cryptosystems via alternative scalar multiplication algorithms and new explicit formulas. The basic operations in the divisor class group over a hyperelliptic curve are scalar multiplications, in other words adding a divisor to itself a fixed number of times. Divisor arithmetic on low-genus hyperelliptic curves is done by using explicit formulas described in terms of finite field operations. One way to increase efficiency is to use a double base algorithm for scalar multiplication where you represent the scalar as a sum of powers of two and three. The efficiency of using this algorithm over a single base algorithm becomes advantageous if you have fast explicit tripling formulas. We have produced explicit tripling formulas that are computationally faster than any other combination of doubling and adding, giving an increase in efficiency over all when using double base representation algorithms for scalar multiplication in the divisor class group.

MICHAEL LIPNOWSKI, Stanford University
On the asymptotic growth of torsion in the cohomology of arithmetic groups

We discuss new examples of towers of arithmetic groups where non-trivial lower bounds on the growth of torsion in their cohomology can be exhibited.

KARYN MCLELLAN, Dalhousie University
Two Growth Rates of Random Fibonacci Sequences

This talk will extend some ideas from both Viswanath's and Rittaud's work on random Fibonacci sequences. We can think of these sequences as forming a binary tree T. Viswanath has shown that almost all random Fibonacci sequences grow exponentially at the rate $1.13198824\ldots$. We will discuss a new computation of Viswanath's constant which uses a reduction R of the tree T developed by Rittaud. Further, we consider the growth rate of the expected value of the n^{th} term in a sequence, using the binary trees R and T, and a Pascal-like array of numbers.

NATHAN MCNEW, Dartmouth College
Radically weakening the Lehmer and Carmichael conditions

Lehmer's totient problem asks if there exist composite integers n satisfying the condition $\varphi(n)|n-1$, (where φ is the Euler-phi function) while Carmichael numbers satisfy the weaker condition $\lambda(n)|n-1$ (where λ is the Carmichael universal exponent function). We weaken the condition further, looking at those composite n where each prime divisor of $\varphi(n)$ also divides $n-1$. While these numbers appear to be far more numerous than the Carmichael numbers, we show that their distribution has the same rough upper bound as that of the Carmichael numbers, a bound which is heuristically tight.

ERIC NASLUND, University of British Columbia
Primitive Points in Polygons

A point $(a,b) \in \mathbb{Z}^2$ is called primitive if $\gcd(a,b) = 1$. Given a lattice polygon $\mathcal{P}$ in the plane, the number of primitive points inside a t-dilation of $\mathcal{P}$ as $t \to \infty$ is equal to $\frac{\text{Area}(\mathcal{P})}{\zeta(2)} t^2 + E(t)$ where $E(t) = O(t \log t)$. Our main result shows that this error term cannot be improved greatly, and that $E(t) = \Omega_{\pm}\left(t\sqrt{\log\log t}\right)$. To do this, we prove an independence result

over the rational numbers for the error term of the Totient summatory function. This expands on the lower bound results of Montgomery 1987. This is joint work with Imre Bárány, Greg Martin and Sinai Robins.

ROB NOBLE, Dalhousie University
Minimal polynomials of algebraic numbers with rational parameters

We describe the polynomials in the following three families: the family of minimal polynomials of algebraic numbers having rational real part, the family of minimal polynomials of algebraic numbers having rational imaginary part, and the family of minimal polynomials of algebraic numbers having rational modulus. Also, we show that no polynomial in the first family can be the minimal polynomial of two algebraic numbers having different rational real parts. Similar results are proved for each of the other two families. We also describe the polynomials in each of the intersections of the families.

JENNIFER PARK, Massachusetts Institute of Technology
A symmetric version of Chabauty's method on families of hyperelliptic curves

It is known since Faltings that hyperelliptic curves have finitely many rational points, and several heuristics suggest that 100% of them have no rational points apart from ∞. Using similar heuristics, we expect 100% of the hyperelliptic curves to have no nontrivial degree-d points. We will discuss how Chabauty's method could be applied to families of hyperelliptic curves to obtain a bound on the number of non-trivial degree-d points on a certain family of hyperelliptic curves. This can be combined with the recent result of Bhargava and Gross on the distribution of 2-Selmer elements of hyperelliptic curves, allowing one to take the first steps towards describing the statistics of non-trivial degree-d points.

JIM PARKS, Concordia University
An upper bound for the average number of amicable pairs

Let E be an elliptic curve over $\mathbb{Q}$. Silverman and Stange defined a pair (p, q) of rational primes to be an *amicable pair* for E if E has good reduction at these primes and the number of points on the reductions $\widetilde{E}_p$ and $\widetilde{E}_q$ satisfy $\#\widetilde{E}_p(\mathbb{F}_p) = q$ and $\#\widetilde{E}_q(\mathbb{F}_q) = p$. Let $Q_E(X)$ denote the number of amicable pairs (p, q) for $E/\mathbb{Q}$ with $p \leq X$. They conjectured that $Q_E(X) \asymp X/(\log X)^2$ if E does not have complex multiplication. This conjecture was refined by Jones by specifying the appropriate constants. In this talk I will show that the conjectured upper bound holds for $Q_E(X)$ on average over the family of all elliptic curves.

DONG QUAN NGOC NGUYEN, University of British Columbia
Generalized Mordell curves, generalized Fermat curves, and the Hasse principle

We show that for each prime p congruent to 1 (mod 8), there exists a threefold $\mathcal{X}_p$ in $\mathbb{P}^6$ such that the existence of certain rational points on $\mathcal{X}_p$ produces families of generalized Mordell curves and of generalized Fermat curves that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction. We also introduce a notion of the descending chain condition (DCC) for sequences of curves, and prove that there are sequences of generalized Mordell curves and of generalized Fermat curves satisfying DCC.

MAKSYM RADZIWILL, Stanford University
The distribution of the zeros of $\zeta(s)$, of $\zeta'(s)$ and the non-existence of Siegel zeros

Denote by ζ the Riemann zeta-function. All the non-trivial zeros of ζ' lie to the right of the half-line if and only if the Riemann Hypothesis is true. Assuming the Riemann Hypothesis, the finer distribution of the zeros of ζ' is not chaotic and seems to depend, on average, on spacings between the consecutive zeros of ζ. We establish a conjecture of Farmer and Ki asserting this finer relation. Farmer and Ki's conjecture is interesting because of its relevance to the class number problem, and the non-existence of Siegel zeros. Time permitting we will also discuss some recent related probabilistic results.

MATT ROGERS, University of Montreal
Spanning trees and Mahler measure

I will discuss several integrals that arise in statistical mechanics, which are related to Mahler measures of multivariable polynomials. I will show that these integrals reduce to 5F4 hypergeometric functions. This is joint work with Tony Guttmann.

SIMON RUBINSTEIN-SALZEDO, Dartmouth College
The Cohen-Lenstra heuristics and roots of unity

The Cohen-Lenstra heuristics are a collection of conjectures on the distribution of the Sylow p-subgroups of class groups of number fields. While these conjectures are usually very well-supported by numerical data, there are several primes at which they do not appear to hold. In this talk, we will discuss the case of $p = 2$ for cyclic cubic fields, and we propose a correction term that fits the data more closely.

MAJID SHAHABI, University of Lethbridge
Limiting Distributions

In this talk, we establish theorems about the existence of a limiting distribution for certain arithmetic functions which possess a nice explicit formula. Furthermore, we mention some results concerning large deviations of infinite sums of independent random variables.

TATCHAI TITICHETRAKUN, UBC
Corners in dense subset of $\mathbb{P}^d$

Furstenberg-Katnelson's Theorem states that if A is a subset of $\mathbb{Z}^d$ with positive upper density then for any finite subset F of $\mathbb{Z}^d$, A contains an affine image of F. We wish to prove analogue theorem in prime tuples $\mathbb{P}^d$ where positive upper density is replaced by positive relative upper density in $\mathbb{P}^d$. This is partially done by Magyar and Cook in the case that no two points in F have the same orthogonal projection to any coordianate axis ; when we count such configurations in that case, $\mathbb{P}^d$ behaves like a random subset of $\mathbb{Z}^d$ but this is not true in general since $\mathbb{P}^d$ has direct product structure and the natural majorant of $\mathbb{P}^d$ cannot be pseudorandom. In this talk, we will discuss how to use hypergraph approach, Green-Tao measure and Gowers's Transference Principle to deal with the case that F is the corner i.e., simplex of the form

$$\{(x_1, .., x_d), (x_1 + s, x_2, .., x_d), ..., (x_1, ..., x_d + s)\}, s \neq 0.$$

We expect that the same method should also work for any finite set F. This is a joint work with Akos Magyar.

NGOC AI VAN NGUYEN, University of Ottawa
A new small value estimate on $\mathbb{C} \times \mathbb{C}^*$

Typical constructions of auxiliary functions from transcendental number theory yield polynomials with integers coefficients taking small values at many points of a finitely generated subgroup of an algebraic group. For future progress in Algebraic independence, it is desirable to study the cases where these values are not small enough so that we can apply Philippon's criterion of algebraic independence. In this talk, we present such a new situation where we achieve an almost optimal result. More precisely, we assume the existence of a sequence of polynomials in $\mathbb{Z}[X_1, X_2]$ of controlled degree and height taking small values at points of the form $(\xi + ir, \eta s^i)$ $(i = 0, 1, 2, \dots)$ for fixed non-zero rational numbers r and $s \neq \pm 1$ and show that this is possible if and only if both ξ and η are algebraic.

PATRICK WALLS, University of Toronto
The Theta Correspondence and Periods of Automorphic Forms

I will describe my work on relations between periods of automorphic forms on groups related by the theta correspondence. These relations can be interpreted as a comparison of relative trace formulas. One trace formula is standard however the other is novel in that it involves a kernel function built from theta functions. The result is a spectral identity relating the Fourier coefficients of automorphic forms on symplectic groups to periods over orthogonal subgroups of automorphic forms on orthogonal groups. Finally, I will describe work in progress where these ideas are applied to the arithmetic geometry of an integral model of a Shimura curve by considering a kernel built from the arithmetic theta functions, with values in arithmetic Chow groups, constructed by Kudla, Rapoport and Yang.

COLIN WEIR, University of Calgary
Constructing and Tabulating Function Fields

We present a Kummer theoretic algorithm for constructing degree ℓ dihedral function fields over a finite field $\mathbb{F}_q$ with prescribed ramification. We then use this in a tabulation algorithm to construct all non-Galois cubic function fields over $\mathbb{F}_q$ up to a given discriminant bound and compare the data to known asymptotics. We will also survey other applications where these techniques can be made useful, such as constructing curves with many points, or in implementing cover attacks on hyperelliptic curve cryptography. Moreover, we show how our construction techniques can be extended to characteristic zero to construct interesting curves over number fields.

ASIF ZAMAN, Toronto
Escape of Mass on Hilbert Modular Varieties

Let F be a number field, $G = PGL(2, F_\infty)$, and K be a maximal compact subgroup of G. We discuss eliminating the possibility of escape of mass for measures associated to Hecke-Maass cusp forms on Hilbert modular varieties, and more generally on congruence locally symmetric spaces covered by G/K, hence enabling its application to the non-compact case of the Arithmetic Quantum Unique Ergodicity Conjecture. This generalizes a result of Soundararajan in 2010 eliminating escape of mass for congruence surfaces, including the classical modular surface $SL(2, \mathbb{Z})\backslash\mathbb{H}^2$, and follows his approach closely.

This talk is based on joint work with Lior Silberman.