Report for BIRS Workshop 22w5024

Specialisation and Effectiveness in Number Theory

August 28 – September 2, 2022

Names and affiliation of confirmed organizers

Alina Ostafe	University of New South Wales,	alina.ostafe@unsw.edu.au
Cameron Stewart	University of Waterloo,	cstewart@uwaterloo.ca
Robert Tichy	Graz University of Technology,	tichy@tugraz.at
Julie Tzu-Yueh Wang	Academia Sinica, Taiwan,	jwang@math.sinica.edu.tw

Overview

Understanding the arithmetic and geometric structure of algebraic functions is fundamental in essentially every area of mathematics and has been investigated for over a century, especially in number theory and arithmetic geometry. The workshop focused on establishing links between functional properties of rational and algebraic functions and similar properties of their specialisations. While in one direction these links are obvious, establishing them in the opposite direction presents significant challenges. Some of the most distinguished number theorists contributed to this legacy, including early seminal work of Faltings, Lang, Mahler, Siegel, Thue, and many others, about finiteness of integral solutions to certain Diophantine equations (Mahler, Siegel, Thue), followed by numerous other advances on problems about intersections of value sets of rational functions (or more generally of algebraic curves) with special sets of complex numbers, such as roots of unity (Mann, Conway, Jones, and others), finitely generated subgroups (Evertse, Schlickewei, Schmidt, Viada), squares and higher powers (Baker, Roth, Siegel, Thue), or, in the higher dimensional case, intersections with algebraic varieties (Faltings, Lang).

This workshop focused on various specialisation problems in number theory and Diophantine geometry, including links to complex analysis, dynamical systems, pseudorandomness, and other areas. One motivating example is the pivotal work of Lang, which made it clear that the existence of multiplicative relations between values of rational functions (or more generally, between coordinates of points on algebraic curves) is a very rare event, which may occur only if the functions themselves are multiplicatively related. In particular, the celebrated result conjectured by Lang in the 1960s and proved by Ihara, Serre and Tate asserts the finiteness of points on curves with all coordinates roots of unity. This has been extended, in various directions, from considering higher order multiplicative relations on curves (e.g., initially by Bombieri, Masser and Zannier, and later by others including Capuano, Habegger, Maurin, Ostafe, Pila, Sha, Shparlinski), to studying the distribution of points of small height on higher dimensional varieties in $\mathbb{G}_m^n$ (e.g. by Bombieri, Zannier, Zhang, and many others), and other similar problems. This phenomenon has turned out to be of great importance for many applications in number theory, Diophantine geometry, arithmetic dynamics, topology, and more.

Although this is a field with a substantial background, it is also rich in many (new and old) open problems, and it continues to attract a huge body of work from many distinguished researchers. For example, there is still a large **gap** between our knowledge of the structure of individual functions and of their joint properties. We illustrate this by a classical example of the equation $f(x) = y^2$ with a polynomial $f \in \mathbb{Z}[X]$ with at least 3 distinct roots which, thanks to Siegel's work, is known to have finitely many integer solutions. In contrast to this, much less is known about squares in products of specialisations of $s > 1$ polynomials $f_1, \dots, f_s \in \mathbb{Z}[X]$, that is, about the finiteness of integer solutions to $f_1(x_1) \dots f_s(x_s) = y^2$.

This area of research can also be seen as part of the so-called *Unlikely Intersections* area, where one typical problem is showing that any arithmetic correlations between the values of $s > 1$ rational functions (or more generally, between points on algebraic varieties) are unlikely, unless the functions (varieties) are special in some sense. The present exciting and challenging problems require deep mathematical tools coming from Diophantine approximation, algebraic and analytic number theory, arithmetic geometry and complex analysis. The workshop also focused on links (new and old) with various other research directions, such as, arithmetic dynamics (e.g., unlikely intersection problems for orbits of rational functions), pseudo-randomness (study of the distribution of elements in, and other arithmetic properties of, various recurrence sequences), as well as less known links to group theory, complex analysis, topology, graph theory, etc.

Abstracts of talks

The schedule of the workshop can be found on the BIRS website

`http://www.birs.ca/events/2022/5-day-workshops/22w5024/schedule`

The slides of many talks can also be found on

`http://www.birs.ca/workshops/2022/22w5024/files/`

The workshop talks centered on closely related and mutually fertilising research directions at the cross-roads of Number Theory (both algebraic and analytic) and Diophantine Geometry. We had a rich and broad schedule, including both on site and online talks. We include below the abstracts of the talks. All talks were 30 min long.

1. **Francesco Amoroso (Université de Caen, Laboratoire LMNO)**,

   Covolume, units, regulator [Joint work with S. David]

   Abstract: By a result of Zimmert (1981) the regulator of a number field K grows at least exponentially with the degree of K. The regulator is closely related to the (co)volume (of the image via the logarithmic embedding) of the full lattice of units of K. Thus a natural question concerns the (co)volume of subgroups of the group of units. For a one dimensional subgroup this question turns out to be equivalent to Lehmer's problem on the height of algebraic numbers. Bertrand and Rodriguez-Villegas independently formulate conjectures which interpolate between one dimensional and full dimensional subgroups. We discuss some recent results on these conjectures.

2. **Fabrizio Barroero (Roma Tre University)**,

   On the polynomial Pell equation

   Abstract: We call a complex polynomial D "pellian" if there are non-constant polynomials A and B such that $A^2 - DB^2 = 1$. While all non-square quadratic polynomials are

pellian, there are square-free polynomials of any even degree ≥ 4 that are not pellian. Masser and Zannier considered one-parameter families of polynomials which are non-identically pellian and studied the pellian specialisations. They gave a criterion for the existence of infinitely many pellian specialisation. In joint work with Laura Capuano and Umberto Zannier we consider the "moduli space" of monic polynomials of fixed even degree $2d \geq 4$ and prove, among other things, that the locus of pellian polynomials consists of a denumerable union of subvarieties of dimension at most $d+1$.

3. **Lior Bary-Soroker (Tel Aviv University)**,

   Rational points coming from ramified covers

   Abstract: The talk aims to present recent progress in the area Hilbert's irreducibility theorem. The theorem may be formulated as the statement there are "many" of rational points on the *line* not coming from rational points on a given cover. If one replaces the line by other variety, the situation becomes more complicated and, in particular, there are obstructions to the theorem coming from rational points of unramified covers (recall that the line has no nontrivial ramified covers).

   The first result, j/w Daniele Garzoni, deals with affine groups: We show that a random walk on a finitely generated Zariski dense subgroup almost surely misses rational points coming from a ramified cover. The second result, j/w Arno Fehm and Sebastian Petersen, deals with abelian varieties and with rational points over the maximal cyclotomic field (or more generally, the field obtained by adding the torsion points of an abelian variety).

4. **Attila Bérczes (University of Debrecen)**,

   Effective results for Diophantine equations over finitely generated domains

   Abstract: Let $A := \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be a finitely generated integral domain over $\mathbb{Z}$ and denote by K the quotient field of A. Finiteness results for several kinds of Diophantine equations over A date back to the middle of the last century. S. Lang generalized several earlier results on Diophantine equations over the integers to results over A, including results concerning unit equations, Thue-equations and integral points on curves. However, all his results were ineffective.

   The first effective results for Diophantine equations over finitely generated domains were published in the 1980's, when Győry developed his new effective specialization method. This enabled him to prove effective results over finitely generated domains of a special type.

   In 2011 Evertse and Győry refined the method of Győry such that they were able to prove effective results for unit equations $ax + by = 1$ in $x, y \in A^*$ over arbitrary finitely generated domains A of characteristic 0. Using this new general method Bérczes, Evertse and Győry obtained effective results for Thue equations, hyper- and superelliptic equations and for the Schinzel-Tijdeman equation over arbitrary finitely generated domains. Koymans generalized the effective result of Tijdeman on the Catalan equation for finitely geberated domains, while Evertse and Győry proved effective results for decomposable form equations in this generality. Bérczes proved effective results for equations $F(x, y) = 0$ in $x, y \in A^*$ for arbitrary finitely generated domains A, and for $F(x, y) = 0$ in $x, y \in \overline{\Gamma}$, where $F(X, Y)$ is a bivariate polynomial over A and $\overline{\Gamma}$ is the division group of a finitely generated subgroup Γ of K^*.

   In my talk I will focus mainly on these latter mentioned results, a short survey how the method of Evertse and Győry could be used in the proof of these results.

5. **Emmanuel Breuillard (University of Oxford)**,

Random character varieties

Abstract: Irreducibility of random polynomials of large degree has been studied recently in works by several authors (in particular by Bary-Soroker, Kozma, Koukoulopoulos and by Varju and myself). We study analogous problems in the setting of word maps in matrix groups, such as $\mathrm{SL}_2(\mathbb{C})$ or more general semisimple Lie groups. Conditionally on GRH, we are able to determine the dimension and number of components of word varieties with an exponentially small probability of exceptions. The proofs use effective Chebotarev type theorems and spectral gap bounds for Cayley graphs of finite simple groups. Joint work with Peter Varju and Oren Becker.

6. **Yann Bugeaud (Université de Strasbourg)** – *Number Theory Web Seminar Talk*, B'

Abstract: Let $n \geq 1$ be an integer and $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers. Let $b_1, \ldots, b_n$ be integers with $b_n \neq 0$, and set $B = \max\{3, |b_1|, \ldots, |b_n|\}$. For $j = 1, \ldots, n$, set $h^*(\alpha_j) = \max\{h(\alpha_j), 2\}$, where h denotes the (logarithmic) Weil height. Assume that the quantity $\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$ is nonzero. A typical lower bound of $\log |\Lambda|$ given by Baker's theory of linear forms in logarithms takes the shape

$$-c(n, D)\, h^*(\alpha_1) \ldots h^*(\alpha_n) \log B,$$

where $c(n, D)$ is positive, effectively computable and depends only on n and on the degree D of the field generated by $\alpha_1, \ldots, \alpha_n$. However, in certain special cases and in particular when $|b_n| = 1$, this bound can be improved to

$$-c(n, D)\, h^*(\alpha_1) \ldots h^*(\alpha_n) \log \frac{B}{h^*(\alpha_n)}.$$

The term $B' := B/h^*(\alpha_n)$ in place of B originates in works of Feldman and of Baker. It is a key tool for improving, in an effective way, the upper bound for the irrationality exponent of a real algebraic number of degree at least 3 given by Liouville's theorem. We survey various applications of this B' to exponents of approximation evaluated at algebraic numbers, to the S-part of integer sequences, and to Diophantine equations.

7. **Laura Capuano (Roma Tre University)** – *suggested not to give a talk if we have enough*,

Multiplicative and linear dependence over finite fields and on elliptic curves modulo primes

Abstract: Given n multiplicatively independent rational functions $f_1, \ldots, f_n$ with rational coefficients, there are at most finitely many complex numbers a such that $f_1(a), \ldots, f_n(a)$ satisfy two independent multiplicative relations. This was proved independently by Maurin and by Bombieri, Habegger, Masser and Zannier, and it is an instance of more general conjectures of unlikely intersections over tori made by Bombieri, Masser and Zannier and independently by Zilber. We consider a positive characteristic variant of this problem, proving that, for sufficiently large primes, the cardinality of the set of $a \in \mathbb{F}_p$ such that $f_1(a), \ldots, f_n(a)$ satisfy two independent multiplicative relations with exponents bounded by a constant K is bounded independently of K and p. We prove also analogous results for products of elliptic curves and for split semiabelian varieties. This is a joint work with F. Barroero, L. Mérai, A. Ostafe and M. Sha.

8. **William Chen (IAS)**,

Hurwitz stacks and strong approximation for the Markoff equation

Abstract: The Markoff surface $X : x^2 + y^2 + z^2 - xyz = 0$ first appeared in the work of Markoff in 1879 as part of his study of Diophantine approximation and binary quadratic forms. Since then, questions about the integral solutions of X have been related to questions in numerous other settings, including the lengths of geodesics on hyperbolic tori, the monodromy of Painleve VI differential equations, and the derived categories of algebraic varieties. In this talk we will describe recent progress on a question of "abundance" of its integral solutions. Specifically, we will discuss a conjecture of Baragar (1991) and Bourgain, Gamburd, and Sarnak (2016) that the reduction map $X(\mathbb{Z}) \to X(\mathbb{F}_p)$ is surjective for every prime p (in this case we say that X satisfies "strong approximation"). In 2016, using analytic methods, Bourgain, Gamburd, and Sarnak were able to establish the conjecture for all but a thin (but possibly infinite) set of primes p. In this talk we will describe how to promote "all but a thin set" to "all but an explicit finite set", thus reducing the conjecture to a finite computation. The key ingredient is a new "rigidity" coming from algebraic geometry: we will relate $\mathbb{F}_p$-points of X to $\mathrm{SL}_2(\mathbb{F}_p)$-covers of elliptic curves branched over the origin. By studying the "Hurwitz" moduli stack of such covers, we will show that if the reduction map is not surjective, then the complement of its image must have size at least linear in p. Since asymptotic results of Bourgain, Gamburd, and Sarnak prohibit this latter possibility, we deduce surjectivity for large p. The connection with Hurwitz stacks uses the fact that X is a character variety for SL_2-representations of a free group of rank 2, and the method hints at an interesting relationship between the Diophantine properties of character varieties and the geometry of Hurwitz stacks.

9. **Gabriel Dill (Leibniz Universität Hannover)**,

On the support problem for Hilbert class polynomials

Abstract: In 1988, Erdös asked in Banff: let x and y be positive integers such that for all n, the set of primes dividing $x^n - 1$ is equal to the set of primes dividing $y^n - 1$. Is $x = y$? Corrales-Rodrigáñez and Schoof answered this question in the affirmative and showed more generally that, if every prime dividing $x^n - 1$ also divides $y^n - 1$, then y is a power of x. In joint work with Francesco Campagna, we have studied this so-called support problem with the Hilbert class polynomials $H_D(T)$ instead of the polynomials $T^n - 1$, replacing roots of unity by singular moduli. In my talk, I will state the result we obtained, sketch its proof, and tell you about a surprising property of the two singular moduli of discriminant -15 that we discovered.

10. **Jan-Hendrik Evertse (Universiteit Leiden)**,

Effective results for Diophantine equations over finitely generated domains (I)

Abstract: We consider Diophantine equations with unknowns taken from finitely generated domains of characteristic 0. Up to isomorphism, such a domain is of the shape $\mathbb{Z}[X_1, \ldots, X_r]/\mathcal{I}$, where $\mathcal{I}$ is a prime ideal of $\mathbb{Z}[X_1, \ldots, X_r]$ with $\mathcal{I} \cap \mathbb{Z} = (0)$. Special cases of such domains are rings of $(S-)$-integers in number fields and polynomial rings over $\mathbb{Z}$.

Lang (1960) was the first to prove finiteness results over arbitrary finitely generated domains of characteristic 0 for various classes of Diophantine equations, by combining Roth's theorem over number fields, Roth's theorem over function fields, and specialization arguments. His finiteness results were ineffective, in that their proofs did not provide methods to determine all solutions. Győry (1983/84) proved *effective* finiteness results for certain classes of Diophantine equations, valid for a restricted class of finitely generated

domains. Later, Győry and E. (2013) managed to generalize Győry's effective method to arbitrary finitely generated domains of characteristic 0. The idea is to map the equation over the finitely generated domain under consideration to various related equations over rings of S-integers in number fields by means of specializations and use effective height estimates for the solutions of the equations over the S-integers, e.g., obtained by means of Baker's method. Which specializations to use is controlled by height estimates for the solutions of related equations over function fields. In 2013, Győry and E. obtained in this manner an effective finiteness result for unit equations $ax + by = c$ in $x, y \in A^*$, with A any finitely genereated domain of characteristic 0. This was extended later to various other classes of Diophantine equartions over finitely generated domains.

In my talk I would like to give an idea how the method of Győry and E. works and give some applications. This is a prequel to the talk of Attila Bérczes.

Reference:
J.-H. Evertse, K. Győry: *Effective results and methods for Diophantine equations over finitely generated domains,* London Math. Soc. Lecture Note Ser. 475.

11. **Christopher Frei (TU Graz)**,

Average genus number of abelian extensions

Abstract: The genus group of an extension K/k of number fields is a certain natural quotient of the class group of K. We discuss the average cardinality of the genus group, as K ranges over Galois extensions of k with fixed abelian Galois group, ordered by conductor. This is joint work with Dan Loughran and Rachel Newton.

12. **Clemens Fuchs (University of Salzburg)** – *virtual*,

A Hilbert irreducibility type result for polynomials over the ring of power sums

Abstract: Let K be a number field and let $\mathcal{E} = \mathcal{E}_K$ be the ring of K-power sums (i.e. functions of the shape $n \mapsto a_1\alpha_1^n + \cdots + a_t\alpha_t^n$ with coefficients $a_1, \ldots, a_t$ and characteristic roots $\alpha_1, \ldots, \alpha_t$ belonging to K). Moreover, let $f(n, X)$ be a polynomial in X with coefficients in $\mathcal{E}$. In this talk we discuss the question, what can be said if f specializes to a reducible polynomial in $K[X]$ for infinitely many n. Under suitable, but restrictive, assumptions we show that this happens if and only if f is reducible as a polynomial in $\mathcal{E}[X]$, which can be checked effectively. This is joint work with Sebastian Heintze (TU Graz).

13. **Nathan Grieve (Royal Military College of Canada, Carleton University, L'Université du Québec à Montréal)** – *sugested not to give talk if we have enough*,

About approximation sets for properly intersecting divisors and effective techniques for local Weil and height functions

Abstract: My plan is to give a more detailed construction of Diophantine approximation sets for properly intersecting nonzero and effective Cartier divisors on a given polarized projective variety. I will then outline a proof of compactness of such approximation sets. This will expand on what I recently described, briefly, at BIRS this past June 2022. Also, I intend to survey some key concepts that allow for effective approaches for working with local Weil and logarithmic height functions.

14. **Kálmán Győry (University of Debrecen)** – *virtual*,

Bounds for the solutions of S-unit equations in two unknowns over number fields

Abstract: The S-unit equations in two unknowns, equations of the form

$$\alpha x + \beta y = 1,$$

where the unknowns x, y are S-units in a number field K containing α, β, are very important in the solution of many other families of Diophantine equations. For their application to obtaining the complete solution of Diophantine equations, an upper bound on the (height of) solutions of associated S-unit equations is required.

The speaker (1974,79) gave explicit upper bounds for (slightly more general) solutions of S-unit equations, and used them to get various applications. Later several authors, including Evertse, Stewart, Tijdeman and Gy (1988), Bombieri (1993), Bugeaud and Gy (1996), Bugeaud (1998), Yu and Gy (2006) and Evertse and Gy (2015) improved upon or modified the previous bounds. Their bounds depend among others on the cardinality $|S|$ of S and the largest norm P of the prime ideals in S.

In Yu and Gy (2006) we obtained two different, considerably improved bounds for the solutions. Le Fourn (2020) combined the proof of the first bound with his variant of Runge's method to replace P in the first bound by the third largest norm P' of the prime ideals in S. In Gy (2020) we refined the second, more complicated proof and combined it with Le Fourn's idea to replace P in the second bound by P'. Further, we improved also the dependence on $|S|$ and, in terms of S, derived the best known bound to date for the solutions.

In our talk we formulate the bounds from Gy (1979), Bugeaud and Gy (1996), Yu and Gy (2006), Le Fourn (2020), and Gy (2020), compare the bounds, emphasize the main tool and outline the main steps in the proof of Gy (2020). Further, we present some recent applications of our latest bound, giving improved upper bound on the S-integral solutions of Thue equations and some more general decomposable form equations over number fields, and providing the best Masser's type ABC inequality to date towards Masser's ABC conjecture over number fields; Gy (2022).

15. **Lajos Hajdu (University of Debrecen)**,

The proof of Skolem's conjecture for certain three term equations

Abstract: Skolem's conjecture (roughly speaking) says that if an exponential Diophantine equation has no solution, than the equation has already no solution modulo m, with an appropriate m. In the talk we summarize some recent results justifying the conjecture for certain three term equations. The handled cases include Catalan's equation and Fermat's equation, for arbitrary, fixed bases. Note that previously Skolem's conjecture (in the integral case) was proved only for equations of the shape $a_1^{x_1} \cdots a_n^{x_n} = k$ by Schinzel.

The presented new results are joint with A. Bérczes, F. Luca, R. Tijdeman.

16. **Peter Koymans (University of Michigan)**,

The negative Pell equation and applications

Abstract: In this talk we will study the negative Pell equation, which is the conic $C_D : x^2 - Dy^2 = -1$ to be solved in integers $x, y \in \mathbb{Z}$. We shall be concerned with the following question: as we vary over squarefree integers D, how often is C_D soluble? Stevenhagen conjectured an asymptotic formula for such D. Fouvry and Kluners gave upper and lower bounds of the correct order of magnitude. We will discuss a proof of Stevenhagen's conjecture, and potential applications of the new proof techniques. This is joint work with Carlo Pagano.

17. **Florian Luca (Wits, MPI-SWS)**,

Recent progress on the Skolem problem

Abstract: The celebrated Skolem-Mahler-Lech Theorem states that the set of zeros of a linear recurrence sequence is the union of a finite set and finitely many arithmetic progressions. The corresponding computational question, the Skolem Problem, asks to determine whether a given linear recurrence sequence has a zero term. Although the Skolem-Mahler-Lech Theorem is almost 90 years old, decidability of the Skolem Problem remains open. The main contribution of this talk is to present an algorithm to solve the Skolem Problem for simple linear recurrence sequences (those with simple characteristic roots). Whenever the algorithm terminates, it produces a stand-alone certificate that its output is correct – a set of zeros together with a collection of witnesses that no further zeros exist. We give a proof that the algorithm always terminates assuming two classical number-theoretic conjectures: the Skolem Conjecture (also known as the Exponential Local-Global Principle) and the p-adic Schanuel Conjecture. Preliminary experiments with an implementation of this algorithm within the tool SKOLEM point to the practical applicability of this method.

18. **FLászló Mérai (Austrian Academy of Sciences, Linz, Austria)**,

Divisors of sums of polynomials

Abstract: In a series of papers, Sárközy and Stewart studied the prime divisors of sum-sets $\mathcal{A}+\mathcal{B}$. Among others, they showed that if $\mathcal{A},\mathcal{B}\subset\{1,\dots,N\}$ are not too small, then there are $a\in\mathcal{A}$ and $b\in\mathcal{B}$ such that $a+b$ has large prime divisors.

In this talk we explore this problem for polynomials over finite fields. In particular, we show that if $\mathcal{A},\mathcal{B}\subset\mathbb{F}_q[x]$ are sets of polynomials of degree n, then $a+b$ has large degree irreducible divisors for some $a\in\mathcal{A},b\in\mathcal{B}$. In particular, if $\mathcal{A},\mathcal{B}$ have positive relative densities, then $a+b$ has an irreducible divisor of degree $n+O(1)$ for some $a\in\mathcal{A},b\in\mathcal{B}$.

19. **Carlo Pagano (Concordia University)**,

Field counting and arboreal degrees

Abstract: I will present new results on Malle's conjecture for nilpotent groups, a joint work with Koymans. I will relate this work to the problem of lower bounding arboreal degrees, and report ongoing work in progress with Mello, Ostafe and Shparlinski, along with past work of mine on the subject. I will finally relate these works with joint work with Ferraguti on (abelian) arboreal Galois representations.

20. **Fedor Pakovich (Ben Gurion University of the Negev)**,

Invariant curves for endomorphisms of $\mathbb{P}^1\times\mathbb{P}^1$

Abstract: Let $A_1,A_2\in\mathbb{C}(z)$ be rational functions of degree at least two that are neither Lattès maps nor conjugate to $z^{\pm n}$ or $\pm T_n$. In the talk, we describe invariant, periodic, and preperiodic algebraic curves for endomorphisms of $\mathbb{P}^1\times\mathbb{P}^1$ of the form $(z_1,z_2)\to(A_1(z_1),A_2(z_2))$. In particular, we show that if $A\in\mathbb{C}(z)$ is not a "generalized Lattès map", then any (A,A)-invariant curve has genus zero and can be parametrized by rational functions commuting with A. As an application, for A defined over a number field we give a criterion for a point of $\mathbb{P}^1\times\mathbb{P}^1$ to have a Zariski dense (A,A)-orbit in terms of canonical heights, and deduce from this criterion a version of a conjecture of Zhang.

21. **Laura Paladino (University of Calabria)** – *virtual*,

Division fields and an effective version of the local-global principle for divisibility

Abstract: Let K be a number field with $\mathrm{char}(K) \neq 2, 3$ and let $\mathcal{E}$ be an elliptic curve defined over K. For every positive integer m, the m-division field $K(\mathcal{E}[m])$ is the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. In the study of the arithmetic of elliptic curves, the fields $K(\mathcal{E}[m])$ have played an important rôle. The investigation of the Galois representations on the total Tate module, Iwasawa theory, modularity and even the proof of the Mordell-Weil theorem are related to the properties of $K(\mathcal{E}[m])/K$. When $m = p^r$, with $p \geq 5$ a prime and r a positive integer, we prove $K(\mathcal{E}[p^r]) = K(x_1, \zeta_p, y_2)$, where $\{(x_1, y_1), (x_2, y_2)\}$ is a generating system of $\mathcal{E}[p^r]$ and ζ_p is a primitive p-th root of unity. In addition we produce an upper bound to the logarithmic height of the discriminant of the extension $K(\mathcal{E}[m])/K$, for all $m \geq 3$. As a consequence, we give an effective version of the hypothesis of the following local-global divisibility problem in elliptic curves over number fields, where the local conditions are known only for finitely many places.

Problem (Dvornicich, Zannier, 2001). Let M_K be the set of places $v \in K$ and let K_v be the completion of K at the valuation v. Suppose that for all but finitely many $v \in M_K$, there exists $D_v \in \mathcal{E}(K_v)$ such that $P = mD_v$, where P is a fixed K-rational point of $\mathcal{E}$. Is it possible to conclude that there exists $D \in \mathcal{E}(K)$ such that $P = mD$?

This is a joint work with Roberto Dvornicich.

22. **Hector Pasten (PUC Chile)**,

p-adic counting of rational points on surfaces

Abstract: The classical Chabauty-Coleman theorem gives an explicit upper bound for the number of rational points on a hyperbolic curve by p-adic means. I'll explain an analogous result for surfaces. While the statement is completely analogous to the case of curves, the proof is rather different and it is based on the theory of ω-integral curves and overdetermined systems of ODEs. This is joint work with Jerson Caro.

23. **Gerold Schefer (University of Basel)**,

Counting torsion points on algebraic subvarieties of the algebraic torus

Abstract: We estimate the growth rate of the function which counts the number of torsion points of order at most T on an algebraic subvariety of the algebraic torus $\mathbb{G}_m^n$ over some algebraically closed field. We will see that there is a general upper bound which is sharp, and characterize the subvarieties for which the growth rate is maximal. For all other subvarieties there is a better bound which is power saving compared to the general one.

24. **Harry Schmidt (University of Basel)**,

Specialisations of families of rational maps

Abstract: Iterations of rational maps on the projective line are ubiquitous in mathematics and appear in number theory as well as numerical analysis, for example in the Newton method. I will talk mainly about joint work with Mavraki in which we study families of rational maps and their specialisation maps. Our main goal is to understand properties that hold uniformly for all specialisations. Our investigations have connections to a relative Bogomolov conjecture for dynamical systems and use tools such as heights and equi-distribution.

25. **Igor Shparlinski (UNSW Sydney)**,

Dynamical irreducibility of polynomials modulo primes

Abstract: For a large class of integer polynomials, we link irreducibility of their iterates modulo a prime p (also known as dynamical irreducibility) to the distribution of quadratic residue and non-residues in certain specialisations of their iterates. This allows us to use bounds of character sums to study dynamical irreducibility for almost all p.

There are however some Diophantine obstacles related to the possible existence of many squares in the above specialisations when considered over $\mathbb{Q}$. We will explain this obstacle and discuss possible ways to overcome it (which also work for quadratic polynomials and some special trinomials).

Joint work with Laszlo Merai and Alina Ostafe

26. **Ilya Shkredov (Steklov Institute of Mathematics)**,

On Korobov bound concerning Zaremba's conjecture

Abstract: We prove in particular that for any sufficiently large prime p there is $1 \le a < p$ such that all partial quotients of a/p are bounded by $O(\log p/ \log\log p)$. This improves the well–known Korobov bound concerning Zaremba's conjecture from the theory of continued fractions.

27. **Niclas Technau (California Institute of Technology)**,

The gap distribution of $(\sqrt{n} \bmod 1)_{n\ge1}$ and the circle method

Abstract: The (renormalized) gap distribution is a popular statistic for studying how random a deterministic sequence really is. While the gap distribution of many classical sequences is conjectured to be a Poisson distribution, there are hardly any examples known for which this can be (dis)proven!

One such exception is $(\sqrt{n} \bmod 1)_{n\ge1}$. In the 2000's, Elkies and Mcmullen showed that the gap distribution of $(\sqrt{n} \bmod 1)_{n\ge1}$ exists and is *not* a Poisson distribution. Their (ineffective) proof relies Teichmüller theory and homogeneous dynamics, in particular on Ratner's theorem. Some years ago, Browning and Vinogradov made the proof of Elkies and Mcmullen effective.

In a recent work with Maksym Radziwiłł we give a rather different (effective) proof, relying on purely analytic methods, which one could even describe as elementary. We shall discuss the basic strategy of this new approach.

28. **Robert Tijdeman (Leiden University)** – *virtual*,

Diophantine equations $f(x) = g(y)$ with infinitely many rational solutions

Abstract: A theorem of Bilu and Tichy (2000) gives deep insight into the structure of polynomials f, g with rational coefficients such that the equation $f(x) = g(y)$ has infinitely many rational solutions x, y. Lajos Hajdu and I have worked out the consequences in case f has only simple rational roots, a case often considered in the literature. We describe the pairs $(deg(f), deg(g))$ which are possible, also in case both f and g have only simple rational roots. There is a connection with the classical Prouhet-Tarry-Escott problem to find two disjoint sets of n integers such that the sums of the k-th powers are equal for $k < n$.

29. **Evelina Viada (University of Göttingen)** – *virtual*,

Rational points on curves embedded in a product of elliptic curves

Abstract: I would like to give some new examples of curves in E^n, with E an elliptic curve, for which we can give all rational points. These examples are interesting because the rank of the elliptic curve is larger than in other methods. These examples are related to a diophantine approximation method in the context of anomalous intersections.

30. **Robert Wilms (University of Basel)** – *virtual*,

    A quantitative Bogomolov-type result for curves over function fields

    Abstract: We will discuss a quantitative bound for the number of points of small Néron-Tate height in the embedding of a curve over a function field into its Jacobian. The proof uses Zhang's admissible pairing on curves, the arithmetic Hodge index theorem over function fields, and the metrized graph analogue of Elkies' lower bound for the Green function. As a special case, we will show that the number of torsion points on the curve is bounded by $16g^2+32g+124$, where g denotes the genus. This is joint work with Nicole Looper and Joseph Silverman.

31. **Trevor Wooley (Purdue University)** – *virtual*,

    Subconvexity in twisted mean values of exponential sums

    Abstract: In most circumstances, proving estimates better than those tantamount to square-root cancellation for mean values of exponential sums remains a distant prospect. It is classical that this is possible for small moments of quadratic Weyl sums. In this talk, we describe progress for higher degree exponential sums associated with Vinogradov's mean value theorem. It transpires that a natural extension of the Main Conjecture in Vinogradov's mean value theorem delivers subconvex estimates for twisted moments at the critical exponent, and that such conclusions may be proved unconditionally in the cubic case.

Besides reporting via regular talks on new advances that have already been achieved, the program encouraged participants to work on current open problems of interest.

List of Participants

We brought together researchers of different number theoretic backgrounds (algebraic, analytic and geometric) so that they can combine their techniques (and of course, intellectual efforts) to address many of the problems outlined above. We had a total of 54 actively attending participants, with 34 attending on site and 20 online.

1. Amoroso, Francesco (Université de Caen, Laboratoire LMNO)
2. Barroero, Fabrizio (Università degli studi Roma 3)
3. Bary-Soroker, Lior (Tel Aviv University)
4. Bell, Jason (University of Waterloo) – online
5. Bennett, Michael (University of British Columbia)
6. Bérczes, Attila (University of Debrecen)
7. Breuillard, Emmanuel (University of Oxford)

8. Bugeaud, Yann (Université de Strasbourg) – online
9. Capuano, Laura (University Roma Tre)
10. Checcoli, Sara (Université Grenoble-Alpes) – online
11. Chen, William (Institute for Advanced Study)
12. Destagnol, Kevin (Université Paris-Saclay, Orsay)
13. Dill, Gabriel (Leibniz Universität Hannover)
14. Evertse, Jan-Hendrik (Universiteit Leiden) – online
15. Ferraguti, Andrea (Scuola Normale Superiore Pisa) – online
16. Frei, Christopher (TU Graz)
17. Fuchs, Clemens (University of Salzburg) – online
18. Garcia-Fritz, Natalia (Pontificia Universidad Católica de Chile)
19. Grieve, Nathan (Royal Military College of Canada, Carleton University and L'Université du Québec à Montréal)
20. György, Kálmán (University of Debrecen) – online
21. Hajdu, Lajos (University of Debrecen)
22. Holmes, Erik (University of Calgary)
23. Ingram, Patrick (York University)
24. Jones, Gareth (University of Manchester) – online
25. Konyagin, Sergey (Steklov Institute, Russian Academy of Sciences) – online
26. Koymans, Peter (University of Michigan)
27. Kühne, Lars (University of Hannover) – online
28. Levin, Aaron (Michigan State University) – online
29. Luca, Florian University of the Witwatersrand
30. Mello, Jorge (IMPA) – online
31. Mérai, László (Austrian Academy of Science)
32. Nguyen, Dang Khoa (University of Calgary)
33. Ostafe, Alina (University of New South Wales)
34. Pagano, Carlo (Concordia University)
35. Pakovich, Fedor (Ben Gurion University of the Negev)
36. Paladino, Laura (University of Calabria) – online
37. Pasten, Hector (PUC Chile)

38. Schefer, Gerold (University of Basel)
39. Schmidt, Harry (University of Basel) – online
40. Sha, Min (South China Normal University) – online
41. Shkredov, Il'ya Steklov (Institute of Mathematics) – online
42. Shparlinski, Igor (University of New South Wales)
43. Stewart, Cameron (University of Waterloo)
44. Technau, Niclas (California Institute of Technology)
45. Tichy, Robert (Graz University of Technology)
46. Tijdeman, Robert (Leiden University) – online
47. Turchet, Amos (Roma Tre University)
48. Viada, Evelina (University of Göttingen) – online
49. Voloch, Felipe (University of Canterbury)
50. Wang, Julie Tzu-Yueh (Academia Sinica)
51. Widmer, Martin (Royal Holloway, University of London)
52. Wilms, Robert (University of Basel) – online
53. Wooley, Trevor (Purdue University) – online
54. Yasufuku, Yu (Nihon University)