Lectures
be presented at the final workshop
of HIM trimester on
Diophantine Equations

April 23–29, 2009

http://www.hausdorff-research-institute.uni-bonn.de/diophantine-equations

A semistable case of a generalization of the Shafarevich conjecture

Victor Abrashkin
victor.abrashkin@durham.ac.uk

Breuil's theory of semistable $\mathfrak{p}$-adic representations is applied to prove the following property: if X is a projective variety over $\mathbb{Q}$ with semistable reduction modulo 3 and good reduction in all $p \neq 3$ then its Hodge number $h^{2,0} = 0$.

Irreducibility criterion for elliptic Galois representations

Nicolas Billerey
billerey@math.jussieu.fr

Given a number field K and a non-CM elliptic curve E defined over K, the Galois representation on p-torsion points of E is irreducible for all prime numbers p outside a finite set of exceptional primes (depending on E and K). In this talk, we give an effective criterion for bounding this finite set of exceptional primes in an efficient way over quadratic fields. Numerical examples will be given.

On a sextenary cubic form

VALENTIN BLOMER
vblomer@math.toronto.edu

(joint work with JÖRG BRÜDERN)

Let $N(P)$ be the number of solutions to

$$x_1y_2y_3 + x_2y_1y_3 + x_3y_1y_2 = 0, \qquad y_1y_2y_3 \neq 0$$

inside the box $[-P, P]^6$. This cubic has an interesting geometry; for example, it contains infinitely many rational planes, but those contribute only $O(P^3)$ solutions to $N(P)$. We prove an asymptotic formula

$$N(P) = P^3Q(\log P) + O(P^{3-\delta})$$

for some polynomial Q of degree 4 and some $\delta > 0$. The method is a blend of elementary, real-analytic and complex-analytic arguments and can be generalized to certain higher degree forms.

Pairs of undenary cubic forms

JÖRG BRÜDERN
bruedern@mathematik.uni-stuttgart.de

In this short talk we describe recent joint work with T. D. WOOLEY on the system of equations

$$a_1x_1^3 + \ldots + a_sx_s^3 = b_1x_1^3 + \ldots + b_sx_s^3 = 0.$$

When $s \geq 13$, the Hasse principle for this system holds (BRÜDERN and WOOLEY, 2007), but we explore what can be said when $s = 12$ or (our main topic) $s = 11$. One would not hope to deal with this problem in full generality without proving the Hasse principle for a single additive cubic in six variables, but one can describe a certain class of systems where the Hasse principle can be established. On the more analytic pitch, within the framework of the circle method, note that $s = 12$ corresponds to the square root cancellation barrier, and $s = 11$ is below that! Still, we shall use the circle method.

Relative Lehmer problem for CM abelian varieties

Maria Carrizosa
carrizosa@math.jussieu.fr

We provide a lower bound for the canonical height of a point P in a CM abelian variety A/K, in terms of the degree of the field generated by P over $K(A_{\mathrm{tors}})$. We shall explain how this result can be used to prove some instances of the Zilber-Pink conjecture.

Quadrics over function fields in one variable over a $\mathfrak{p}$-adic field

Jean-Louis Colliot-Thélène
jean-louis.colliot-thelene@math.u-psud.fr

For p odd, there are by now three very different proofs that quadratic forms in at least 9 variables over such a function field have a nontrivial zero. I will review these proofs and discuss a local-global principle for quadratic forms in a smaller number of variables. Works of Parimala–Suresh, of Harbater–Hartmann–Krashen, and of Leep will be mentioned, as well as joint work of Parimala, Suresh and the speaker.

Recent results on integral points on surfaces

Pietro Corvaja
pietro.corvaja@dimi.uniud.it

About seven years ago, U. Zannier and the speaker introduced a new method to prove the degeneracy of integral points on certain open varieties, which led to the solution of some open cases of Vojta's conjecture.

This method, unlike the previously known ones by Faltings and Vojta, avoids any recourse to semi-abelian varieties, so it may apply sometimes even in case the (generalised) Albanese variety is trivial.

In this talk we shall outline the proof of a general statement concerning surfaces, and provide some concrete applications to rational quasi projective surfaces. In particular, we shall provide an example of a simply connected surface whose integral points are degenerate (whatever ring of S-integers is considered).

Linear spaces on rational algebraic hypersurfaces

RAINER DIETMANN
dietmarr@mathematik.uni-stuttgart.de

By a result of BIRCH, for given positive integers d and m, where d is odd, there is a $s_0(d, m)$ such that any rational form F of degree d in at least $s_0(d, m)$ variables admits a rational linear space V of zeros of F, such that V has dimension m. Known bounds for $s_0(d, m)$ grow rapidly in d and m. By an application of the circle method we will show that for fixed d, and F restricted to be non-singular, the growth is polynomial in m.

The proof of Serre's conjecture
The ubiquity of modular forms

LUIS DIEULEFAIT
ldieulefait@ub.edu

I will present some of the key ideas developed by KHARE, WINTENBERGER, and the speaker that allow to propagate modularity and establish Serre's modularity conjecture. In particular I will discuss "existence of compatible families" (DIEULEFAIT–TAYLOR), "existence of minimal lifts" (DIEULEFAIT, KHARE–WINTENBERGER), "existence of Galois conjugates" (DIEULEFAIT), and two methods of "weight reduction" (KHARE/DIEULEFAIT). Modularity Lifting Theorems (from TAYLOR–WILES to KISIN) and the potential modularity result of TAYLOR will be our main tools.

Effective results on points of certain subvarieties of tori

JAN-HENDRIK EVERTSE
evertse@math.leidenuniv.nl

(joint work with ATTILA BERCZES, KÁLMÁN GYÖRY and CORENTIN PONTREAU)

Let X be an algebraic subvariety of the n-dimensional torus $\mathbb{G}_m^n$, and Γ a subgroup of finite rank of $\mathbb{G}(\overline{\mathbb{Q}})$. In the 1980's Laurent proved that $X \cap \Gamma$ is contained in the union of a finite number of translates of algebraic subgroups of $\mathbb{G}(\overline{\mathbb{Q}})$. His method of proof is ineffective in the sense that it does not give a method to determine the translates. In 1998, POONEN proved a generalization of this, where instead of Γ he considered a thickening consisting of all points of $\mathbb{G}(\overline{\mathbb{Q}})$ that are very close to Γ. In 2002, EVERTSE extended this further, by taking the set of points that have in some sense a very small angle with Γ. Both their results are ineffective. In this lecture we present some effective versions of the results of LAURENT, POONEN and EVERTSE, valid for a very specific class of varieties X.

Additive equations over $\mathfrak{p}$-adic fields

HEMAR GODINHO
hemar@unv.br

Consider a system of R diagonal forms of degree k in N variables over a $\mathfrak{p}$-adic field K. Write $k = p^\tau m$ where p is the residue field characteristic and $(m,p) = 1$. We prove that this system has a nontrivial $\mathfrak{p}$-adic solution if N exceeds $(Rk)^{2\tau+5}$, a bound independent of the field K. We prove the same if N exceeds $4nR^2k^2$ where $n = [K : \mathbb{Q}_p]$. Both results improve previously known bounds.

Perfect powers in products with terms from arithmetic progression

KÁLMÁN GYÖRY
gyory@math.klte.hu

A celebrated theorem of ERDÖS and SELFRIDGE states that the product of consecutive positive integers is never a power. It is an old conjecture that even the equation

$$m(m+d)\cdots(m+(k-1)d) = y^n \qquad (*)$$

has no solution in positive integers m, d, k, y, n with $\gcd(m,d) = 1$, $k \geq 3$, $n \geq 2$ and $(k,n) \neq (3,2)$. This equation has been investigated by many people. In the last ten years the conjecture was confirmed for $k \leq 11$ (Gy, $k = 3$; GY, HAJDU, SARADHA, $k = 4,5$; BENNETT, BRUIN, GY, HAJDU, $6 \leq k \leq 11$). Recently these results have been extended to the case $k < 35$ by HAJDU, PINTÉR and the speaker. As in the earlier proofs, we reduced $(*)$ to systems of ternary equations. However, our proof required fundamentally new ideas. For $k > 11$, a great number of new ternary equations arose that we solved by combining the modular method with local and cyclotomic considerations. Furthermore, the number of systems of equations grows so rapidly with k that, in contrast with the previous proofs, it was practically impossible to handle the different cases in the earlier way. We algorithmized our proof which enabled us to employ a computer. We applied an efficient, iterated combination of our procedure for solving the arising new ternary equations with several sieves based on the ternary equations already solved. Our algorithm seems to work for larger k as well, but there is of course a computational time limit.

Some Poitou–Tate exact sequences

DAVID HARARI
David.Harari@math.u-psud.fr

We discuss miscellaneous Poitou–Tate exact sequences. In particular we deal with the case of 1-motives (due to T. SZAMUELY and myself for number fields and to C. GONZALEZ for function fields) and with the case of 2-term complexes of tori (due to C. DEMARCHE).

On cubic forms in seven variables

MICHAEL P. HARVEY
Mike.Harvey@bristol.ac.uk

In this talk we consider a family of cubic hypersurfaces in $\mathbb{P}^6$ and report on recent progress concerning an asymptotic formula for the number of rational points of bounded height on these varieties. The proof is based on the Hardy–Littlewood circle method and is on the boundary of what can be achieved using this method, and it also requires some key exponential sum moment estimates.

Zeros of systems of $\mathfrak{p}$-adic forms

ROGER HEATH-BROWN
rhb@maths.ox.ac.uk

As a special case of a conjecture of Artin, any r $\mathfrak{p}$-adic quadratic forms should have a common zero as soon as the number of variables is at least $4r+1$. It is known that Artin's conjecture is false in general, but this case is still open. The Ax–Kochen Theorem shows that the conjecture is true if the residue class field has cardinality $q = p^e$ with $p > p(r, e)$. This latter bound can be made explicit, but one such result gives an exponential tower of height 8 as a function of r.

The talk will describe a new approach, requiring only $q > q(r)$, with a first order exponential function $q(r)$.

Serre curves in one-parameter families

Nathan Jones
jones@dms.umontreal.ca

(joint work with A. Cojocaru and D. Grant)

A Serre curve is an elliptic curve defined over the rational numbers whose torsion subgroup has "as much Galois symmetry as possible." In this talk, I will discuss a theorem which says that, in appropriately chosen one-parameter families of elliptic curves, almost all specializations are Serre curves.

Manin's Conjecture for a singular sextic Del Pezzo surface

Daniel Loughran
daniel.loughran@bristol.ac.uk

A natural problem in Diophantine Geometry is to count the number of rational points of bounded height on an algebraic variety. In this talk, I will present recent progress on this problem for a certain singular del Pezzo surface of degree six.

Schanuels conjecture and systems of exponential equations over the reals and the complexes

Angus Macintyre
angus@dcs.qmul.ac.uk

I work in the category of characteristic zero fields with exponentiation, with the formalism of exponential polynomials and exponential algebra. There are three main examples, the reals, the complexes, and a field (Zilbers field) constructed by Zilber. For all three Schanuels Conjecture (SC) makes sense. It is unproved for the reals or complexes, but holds by model-theoretic construction for Zilbers field. The latter satisfies a subtle analogue of Hilberts Nullstellensatz.

Wilkie and I showed that the decision problem for the real case (and in particular for deciding solvability of systems of exponential equations) is solvable provided Schanuels Conjecture is true. It is not very hard to show, unconditionally, that the problem of testing solvability in the complex or Zilber cases is undecidable (encoding Hilberts 10th Problem).

In Zilbers model there is a beautiful condition implying solvability of very general systems. It may well be that Zilbers field is isomorphic to the complex exponential field, but for now only some very special cases of the Zilber systems are known to be solvable in the complexes, and the proofs typically involve hard complex analysis (I will give examples).

On the other hand, one knows for the complexes a result, Schanuels Nullstellensatz (proved by Henson and Rubel using Nevanlinna Theory), which provides a criterion for a single exponential polynomial to have no complex root. It is not obvious that this holds for Zilbers field. I sketch the proof that it does (a result joint with DÁquino and Terzo). I will also show the connection to the still-open Shapiro Conjecture in complex analysis.

If time permits, I will explain the notion of exponential-algebraic, and discuss the issue of automorphisms of the complex exponential.

Mordell–Weil problem for cubic surfaces
In search of a model-theoretic approach

Yuri I. Manin
manin@mpim-bonn.mpg.de

Mordell–Weil theorem for elliptic curves establishes that over a field K which is finitely generated, say, over $\mathbb{Q}$, such a curve C has a finitely generated abelian group $C(K)$ of rational points. The proof allows also to get an asymptotic formula for the number of points of bounded height. If $C(K)$ is nonempty, C can be embedded as a cubic curve in the projective plane, and finite generation can be restated in terms of projective geometry: all points of $C(K)$ can be obtained from an initial finite subset by drawing secants (and tangents) L through initial/already constructed points of C and adding their (K-rational) intersection points with C to the previously constructed subset. In this form, conjecture of finite generation can be extended to higher-dimensional cubic hypersurfaces. The crucial two-dimensional case still resists solution since 1970s.

In this talk, I will discuss theoretical approaches and computer experiments motivated by the two-dimensional Mordell–Weil type conjecture, and stress the emerging model-theoretic framework which might provide a key to this elusive problem.

Almost prime roots of ternary quadratic forms

Gihan Marasingha
gihan.marasingha@gmail.com

Let Q be an isotropic ternary quadratic form over the integers. Under suitable local conditions, we show that there exist infinitely many solutions x, y, z to $Q(x, y, z) = 0$ such that the product xyz has at most 15 prime factors. By careful consideration of the parametrization, this can, in special cases, be improved to at most 8 prime factors. This relates to work of J. Liu and P. Sarnak on the equivalent problem for anisotropic ternary quadratic forms.

The Erdös–Moser equation $1^k + 2^k + ... + (m-1)^k = m^k$ revisited using continued fractions

Pieter Moree
moree@mpim-bonn.mpg.de

(joint work with Yves Gallot (computer calculation) and Wadim Zudilin)

Leo Moser in 1953 gave a beautiful proof that if the equation of the title has a solution with $k \geq 2$, then $m > 10^{1000000}$. We improve on this bound by showing that $2k/(2m-3)$ is a convergent of $\log 2$ and making an extensive continued fraction digits calculation of $(\log 2)/N$, with N an appropriate integer. The N comes from a result published 15 years ago by the speaker, H. te Riele and J. Urbanowicz.

An asymptotic formula for the number of S-integral points of bounded height in $\mathbb{P}^n$ with respect to a quadric

Nic Niedermowwe
niedermo@maths.ox.ac.uk

We consider a conjecture by Tschinkel regarding the asymptotic distribution of (D, S)-integral points in projective space in the case where $D \in \mathbb{Z}[\underline{x}]$ is a smooth hypersurface of degree two.

Rational points of definable sets and Diophantine problems

Jonathan Pila
J.Pila@bristol.ac.uk

(joint work with Alex Wilkie and Umberto Zannier)

I will describe a result (joint with Alex Wilkie) concerning the distribution of rational points on certain real non-algebraic sets. More specifically, definable sets in o-minimal structures, and I will explain this notion. I will give some applications to Diophantine problems, including a new proof (joint with Umberto Zannier) of the Manin–Mumford conjecture, and some further results of Andre–Oort–Manin–Mumford type.

On the density of rational points on curves and Fermat hypersurfaces

Per Salberger
salberg@math.chalmers.se

We report on new uniform bounds for the number of rational points of bounded height on curves and Fermat hypersurfaces. The latter estimates have applications for mean values of Weyl sums, which will be presented by Trevor Wooley at this conference.

The collection of metric Mahler measures

Charles Samuels
csamuels@mpim-bonn.mpg.de

Let $M(\alpha)$ denote the Mahler measure of the algebraic number α. Several recent papers construct Archimedean and non-Archimedean versions of M on $\bar{\mathbb{Q}}^{\times}$, denoted M_1 and M_∞, respectively. We extend these constructions in a natural way in order to assign, to each $x \in (0, \infty]$, a metric version M_x of the Mahler measure. We are able to identify a function $\bar{M}$ that is, in some sense, minimal with respect to the collection $\{M_x\}$. We further examine some basic properties of the map $x \mapsto M_x(\alpha)$ for fixed α.

Equal values of trinomials

Andrzej Schinzel
schinzel@impan.pl

(joint work with Gy. Peter and A. Pintér)

Theorem 1. The Diophantine equation

$$ax^m + bx^n + c = dy^p + ey^q$$

where $m > n > 0,\ m + 1 > p > q > 0,\ (m, n) = 1,\ ab \neq 0 \neq de$ and $p > 2$ has only finitely many solutions x, y with a bounded denominator, unless either $m < 5$, or $m = p,\ n = q,\ a = dt^m,\ b = dt^n,\ t$ in $\mathbb{Q}$.

Theorem 2. Suppose that $m > 2,\ m > n > 0,\ abd \neq 0,\ m \neq 2n$ and $(m, n) \neq (3, 1), (3, 2), (4, 1), (4, 3), (6, 2), (6, 4)$, further, if $4dc + e^2 = 0$ then assume that $m - n > 2$, or $m - n = 2$ and n is odd. The Diophantine equation

$$ax^m + bx^n + c = dy^2 + ey$$

in integers x, y implies $\max\{|x|, |y|\} < C$, where C is an effectively computable constant depending only on $H = \max\{|a|, ..., |e|\}$.

The Brauer group of Kummer surfaces and torsion of elliptic curves

ALEXEI SKOROBOGATOV
a.skorobogatov@imperial.ac.uk

(joint work with YURI ZARHIN)

A theorem of ZARHIN and the speaker says that if X is a $K3$ surface over a field k finitely generated over $\mathbb{Q}$, then $\mathrm{Br}(X)/\mathrm{Br}(k)$ is finite. However, this group was not known for a single $K3$ surface over a number field. We give a formula for the Brauer group of the Kummer surface X constructed from the product of two elliptic curves. It turns out that for almost all such surfaces over $\mathbb{Q}$ we have $\mathrm{Br}(X) = \mathrm{Br}(\mathbb{Q})$. This raises the question of weak approximation on these surfaces, and also the unexpected question of whether the size of $\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q})$ can take only finitely many values for $K3$ surfaces X over $\mathbb{Q}$.

On the distribution of Frobenius numbers

ALEXEY USTINOV
ustinov.alexey@gmail.com

For given relatively prime positive integers $a_1, \ldots, a_n$, Frobenius number $g(a_1, \ldots, a_n)$ is the largest natural number that is not representable as a non-negative integer combination of $a_1, \ldots, a_n$.

It is more natural to consider the function $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n) + a_1 + \ldots + a_n$, which gives the largest integer number that is not representable as a positive integer combination of $a_1, \ldots, a_n$. For example $f(a, b) = ab$ as $g(a, b) = ab - a - b$ (SYLVESTER, 1884).

DAVISON (1994) conjectured that the value of $f(a, b, c)$ for a "random" triple is likely to be of the order $\sqrt{abc}$. More formally, if

$$X_N = \{(a, b, c) : 1 \leq a, b, c \leq N; (a, b, c) = 1\}$$

then

$$\lim_{N\to\infty} \frac{1}{|X_N|} \sum_{(a,b,c)\in X_N} \frac{f(a, b, c)}{\sqrt{abc}}$$

exists and is finite. ARNOLD (1999) conjectured that for all $n \geq 2$ function $f(a_1, \ldots, a_n)$ has weak asymptotic of the form $c_n \sqrt[n-1]{a_1 \ldots a_n}$.

Case of $n = 3$ can be studied using continued fractions and Kloosterman sums.

Theorem 1 (weak asymptotic). *Let a be positive integer, $x_1, x_2, \varepsilon > 0$ and*

$$M_a(x_1, x_2) = \{(b, c) : 1 \leq b \leq x_1 a, 1 \leq c \leq x_2 a, (a, b, c) = 1\}.$$

Then

$$\frac{1}{|M_a(x_1, x_2)|} \sum_{(a,b,c)\in M_a(x_1,x_2)} \left(f(a, b, c) - \frac{8}{\pi}\sqrt{abc} \right) = O_{x_1,x_2,\varepsilon}(a^{4/3+\varepsilon}).$$

Theorem 2 (strong form of Davison's cojecture). For all $a \geq 1$, $\varepsilon > 0$

$$\frac{1}{|M_a(1,1)|} \sum_{(b,c)\in M_a(1,1)} \frac{f(a,b,c)}{\sqrt{abc}} = \frac{8}{\pi} + O_\varepsilon(a^{-1/12+\varepsilon}).$$

Theorem 3 (density function for normalized Frobenius numbers). *For all* $a \geq 1$, $x_1, x_2, \varepsilon > 0$

$$\frac{1}{|M_a(x_1,x_2)|} \sum_{\substack{(a,b,c)\in M_a(x_1,x_2)\\ f(a,b,c)\leq \tau\sqrt{abc}}} 1 = \int_0^\tau p(t)\,dt + O_{\varepsilon,x_1,x_2,\tau}(a^{-1/6+\varepsilon}),$$

with

$$p(t) = \begin{cases} 0, & \text{for } t \in [0,\sqrt{3}];\\ \frac{12}{\pi}\left(\frac{t}{\sqrt{3}} - \sqrt{4-t^2}\right), & \text{for } t\in[\sqrt{3},2];\\ \frac{12}{\pi^2}\left(t\sqrt{3}\arccos\frac{t+3\sqrt{t^2-4}}{4\sqrt{t^2-3}} + \frac{3}{2}\sqrt{t^2-4}\log\frac{t^2-4}{t^2-3}\right), & \text{for } t\in[2,+\infty).\end{cases}$$

such that

$$\int_0^\infty p(t)\,dt = 1, \qquad \int_0^\infty tp(t)\,dt = \frac{8}{\pi}, \qquad p(t) = \frac{3}{2}\cdot\frac{1}{t^3} + O\left(\frac{1}{t^5}\right) \quad (t\to\infty).$$

Cox rings of big rational surfaces

Anthony Várilly-Alvarado
varilly@math.berkeley.edu

(joint work with D. Testa and M. Velasco)

Cox rings of del Pezzo surfaces have been used by several authors to count points of bounded height and thus verify instances of Manin's conjecture on the subject. We will show that the more general class of smooth projective rational surfaces with big anticanonical class has a finitely generated Cox ring. We will also present some systematic collections of examples of these surfaces.

Failure of the Hasse principle for Enriques surfaces

Bianca Viray
bviray@math.berkeley.edu

Most counterexamples to the Hasse principle can be explained by an algebraic Brauer–Manin obstruction. We define some of the other possible obstructions and exhibit an Enriques surface where the failure of the Hasse principle is not explained by an algebraic Brauer–Manin obstruction.

Rational points on complete intersections, and mean values of Weyl sums

Trevor Wooley
Trevor.Wooley@bristol.ac.uk

(joint work with Per Salberger)

We report on work that provides estimates for the number of rational points on complete intersections having degree large compared to the dimension. Such estimates may be applied in estimating mean values of Weyl sums, and in allied problems concerning quasi-diagonal behaviour.

Vojta's conjecture on blowups and the *abc*

Yu Yasufuku
yyasufuku@gc.cuny.edu

Vojta's conjecture is a height inequality, and its consequences include many deep results/conjectures in Diophantine geometry such as the Mordell Conjecture (Faltings' theorem) and the Bombieri–Lang conjecture. In this talk, I will describe some cases of the conjecture for blowup varieties using explicit height computations, and then discuss their connection with a special case of the *abc* conjecture.

Simultaneous zeros of a cubic and quadratic form over the p-adic numbers

Jahan Zahid
jahan.zahid@jesus.ox.ac.uk

Emil Artin conjectured that any system of r homogeneous polynomials of degrees $d_1 + ... + d_r$ in at least $d_1^2 + ... + d_r^2 + 1$ variables have a common non-trivial solution over the $\mathfrak{p}$-adic numbers. We shall prove this in the case of a cubic and quadratic form, provided $p \geq a$. A value of a shall be revealed in the talk.