Mini-Workshop on "Explicit Problems in Diophantine Analysis and Geometry"

in frame of the ESI-Program "Heights in Diophantine geometry, group theory and additive combinatorics"
November 29-30, 2013

Organizer: Clemens Fuchs
Supported by: Austrian Science Fund (FWF): P24574-N26

It is a classical and very old problem to find the rational, resp. integral, solutions of a given system of polynomial equations with rational coefficients. In geometric terms this amounts to find the rational points on algebraic varieties. Main tools for the mathematical study (called Diophantine Analysis) of Diophantine problems of this type include the Thue-Siegel-Roth-Schmidt method and Baker's method on linear forms in logarithms of algebraic numbers for number fields and the generalization of the ABC-theorem due to Brownawell and Masser for function fields. Since working with equations is somewhat limited, it is a modern approach to study Diophantine problems that have additionally a geometrical meaning (this approach is studied in Diophantine Geometry). Here the solution set to a Diophantine problem is viewed e.g. as a scheme of finite type over the spectrum of the ring of integers and then also tools from algebraic geometry are used to study it. In these investigations of Diophantine problems, heights play an important role in order to control the size of the algebraic numbers resp. functions that are involved. In this mini-workshop we collect experts to present and discuss new progress on explicit Diophantine problems. The talks will include questions on Diophantine tuples, rational and integral points on curves and (fibered) surfaces also in connection with problems related to linear recurrences and parameterized families of Diophantine equations over function fields as well as lacunary rational functions that are composite (in particular from a computational point of view).

Speakers:
Andrej Dujella (Zagreb)
Lajos Hajdu (Debrecen)
Rafael von Känel (Bonn)
Roland Paulin (Salzburg)
Attila Pethő (Debrecen)
Ákos Pintér (Debrecen)
Mingxi Wang (Salzburg)
Volker Ziegler (Linz)

Program

All lectures take place in the ESI Boltzmann Lecture Hall.

Friday, November 29, 2013:

14:30 - 14:45: Opening
Welcome words and short presentation of the FWF-project P24574

14:45 - 15:30: **Rafael von Känel** (MPIM Bonn)
Modularity and integral points on moduli schemes

15:40 - 16:25: **Lajos Hajdu** (University of Debrecen)
Explicit solution of exponential diophantine equations using a Hasse-type principle

16:35 - 17:20: **Roland Paulin** (University of Salzburg)
The minimal degree of morphisms between curves

17:30 - 18:15: **Ákos Pintér** (University of Debrecen)
Variations on a theme: the power values of power sums

Saturday, November 30, 2013:

09:30 - 10:15: **Attila Pethő** (University of Debrecen)
On a key exchange protocol based on Diophantine equations

10:25 - 11:10: **Volker Ziegler** (RICAM Linz)
On the number of prime factors of $\prod_{a,b\in A}(ab+1)$ *for small sets* A

11:20 - 12:05: **Mingxi Wang** (University of Salzburg)
Curves and special points for families of abelian varieties

12:15 - 13:00: **Andrej Dujella** (University of Zagreb)
On the existence of rational Diophantine quintuples with the property $D(q)$

Abstracts

Andrej Dujella (University of Zagreb)
Title: *On the existence of rational Diophantine quintuples with the property $D(q)$*
Abstract: We investigate for which rational numbers q there are infinitely many sets consisting of five nonzero rationals such that the product of any two of them plus q is a square of a rational number. We will present recent joint work with Clemens Fuchs, where we show that there are infinitely many square-free such q, and on assuming the Parity Conjecture for the twists of an explicitly given elliptic curve we derive that the density of such q is at least one half. We will mention some other known results and open problems concerning integer and rational Diophantine m-tuples.

Lajos Hajdu (University of Debrecen)
Title: *Explicit solution of exponential diophantine equations using a Hasse-type principle*
Abstract: Let $a_1, \dots, a_k$, $b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be non-zero integers, c be an integer, and consider the exponential diophantine equation

$$a_1 b_{11}^{\alpha_{11}} \dots b_{1\ell}^{\alpha_{1\ell}} + \dots + a_k b_{k1}^{\alpha_{k1}} \dots b_{k\ell}^{\alpha_{k\ell}} = c$$

in non-negative integers $\alpha_{11}, \dots, \alpha_{1\ell}, \dots, \alpha_{k1}, \dots, \alpha_{k\ell}$. The effective and ineffective theory such problems has a long history. In case of $k = 2$ the exponents can be effectively bounded, while for larger values of k only the number of solutions can be bounded, subject to certain conditions. We start with stating the following Conjecture: Suppose that the above equation has no solutions. Then there is an integer $m \geq 2$ such that the equation does not hold modulo m. The conjecture is a variant of a classical conjecture of Skolem. We show that the conjecture is true for "almost all" cases. Further, we also check its validity for a relatively large set of the parameters involved. The main tool behind our results is a variant of a result of Erdős, Pomerance and Schmutz concerning Carmichael's λ-function. As an application, we present a method for the solution of equations of the above type, under certain assumptions. We give concrete examples, as well. The new results presented are joint with Cs. Bertók.

Rafael von Känel (MPIM Bonn)
Title: *Modularity and integral points on moduli schemes*
Abstract: In this talk we present new Diophantine applications of modularity results. In the first part, we use the Shimura-Taniyama conjecture to prove effective finiteness results for integral points on moduli schemes of elliptic curves. On working out the method for moduli schemes corresponding to Mordell equations, we improve the actual best explicit height

bounds for Mordell equations. In the second part, we combine Faltings' method with Serre's modularity conjecture to establish the effective Shafarevich conjecture for abelian varieties of (product) GL_2-type and then we discuss applications to the effective study of integral points on certain higher dimensional moduli schemes (e.g. Hilbert modular varieties).

Roland Paulin (University of Salzburg)
Title: *The minimal degree of morphisms between curves*
Abstract: The aim of the talk is to study the following problem. Given two smooth projective curves defined over a number field K, can one bound from above the minimum of the degrees of non-constant morphisms defined over K between the two curves? The main result is that for given positive integers d, g, h, there is an effective constant C, depending only on d, g, h, with the following property. Suppose that X, Y are smooth projective curves defined over a number field K which has degree at most d, the genus of both curves is at most g, the Jacobian of X has Faltings height at most h, X has a K-rational point, and there is a non-constant morphism from X to Y defined over K. Then there is a non-constant morphism from X to Y, defined over K, of degree at most C.

Attila Pethő (University of Debrecen)
Title: *On a key exchange protocol based on Diophantine equations*
Abstract: This talk is based on a joint work with Noriko Hirata-Kohno, Nihon University, Japan. We analyze a recent key exchange protocol proposed by H. Yosh, which is based on the hardness to solve Diophantine equations. We show that the public key is very large. We suggest large families of parameters both in the finite field and in the rational integer cases for which the protocol can be secure.

Ákos Pintér (University of Debrecen)
Title: *Variations on a theme: the power values of power sums*
Abstract: In this talk we present some recent results and new directions concerning the Schäffer conjecture which states that the equation $1^k + 2^k + \ldots + x^k = y^n$ in positive integers $k \geq 1, x \geq 2, y \geq 2, n \geq 2$ with $(k, n) \notin \{(1, 2), (3, 2), (3, 4), (5, 2)\}$ possesses only one anomalous solution $(k, x, y, n) = (2, 24, 70, 2)$.

Mingxi Wang (University of Salzburg)
Title: *Curves and special points for families of abelian varieties*
Abstract: We shall prove conditionally that if a curve of a family of abelian varieties intersects infinitely times with the isogeny orbits of a finitely generated group, then it must be of special type. Part of this result has been predicted by the Zilber-Pink conjecture. This is joint work with Qian Lin.

Volker Ziegler (RICAM Linz)
Title: *On the number of prime factors of* $\prod_{a,b\in A}(ab+1)$ *for small sets* A
Abstract: Let $s(k)$ be the smallest integer m such that there is no set S of k primes, such that for some set A of m positive integers $\prod_{a,b\in A}(ab+1)$ has only prime divisors coming from S. For example, one can prove $s(1)=3$ by showing that the Diophantine equation $(ab+1)(ac+1)(bc+1)=p^n$ has no solution (a,b,c,n,p) with $0<a<b<c$ and p prime. The main purpose of this talk is to discuss the computation of $s(k)$ for small k. Of special interest will be the case $k=2$.