PROGRAM OF WORKSHOP "NEW METHODS IN HILBERT'S TENTH PROBLEM"

February 9–13, 2009

Organisers: Yu. V. Matiyasevich, B. Z. Moroz, and B. Poonen

Monday, February 9

10:45 **Yuri Matitasevich: New technique for existential arithmetization of Diophantine equation**

A new method of coding Diophantine equations is proposed. This method allows

(i) checking that a coded sequance of natural numbers is a solution of a coded equation without decoding;

(ii) defining, by a purely existential formula, the code of an equation equivalent to a system of indefinitely many copies of an equation represented by its code.

The new method leads to a much simpler construction of a universal Diophantine equation and to the existential arithmetization of Turing machines, register machines, and partial recursive functions.

14:00 **Thanases Pheidas: A survey on decidability in algebra (after the 19th century)**

We survey the following: Elimination theory (a) addition and order over the integers (Presburger), (b) addition, multiplication and order over the reals (Tarski, Seidenberg, Cohen), (c) addition and multiplication over the p-adic numbers and fields of power series in one variable and of positive characteristic (Ax-Kochen, Ershov, Cohen, Kochen, Macintyre), (d) addition and divisibility over the integers (Lipshitz), (e) addition and exponentiation (Semenov), (f) similar results (to the integer case) for rings of polynomials (Pheidas, Sirokofskich), (g) the algebraic theory of the integers modulo almost all primes (Ax). We also discuss: (h) some extensions (names of authors to be given in the talk), (i) open problems (we focus on the algebraic theory of fields of power series in positive characteristics and a problem of Grothendieck).

Tuesday, February 10

9:00 **Jean-Louis Colliot-Thélène: Obstruction de Brauer–Manin entière pour les formes quadratiques entières et les espaces homogènes (Integral Brauer–Manin obstruction for integral quadratic forms and homogeneous spaces)**

An integer may be represented by a quadratic form over each ring of p-adic integers and over the reals without being represented by this quadratic form over the integers. More generally, such failure of a local-global principle may occur for the representation of one integral quadratic form by another integral quadratic form. Many such examples may be accounted for by a Brauer–Manin obstruction for the existence of integral points on schemes defined over the integers. For several types of homogeneous spaces of linear algebraic groups, this obstruction is shown to be the only obstruction to the existence of integral points. This talk describes work of Fei Xu and the speaker (homogeneous spaces of semisimple groups) and work of Harari (homogeneous spaces of a torus).

10:45 **Karl Rubin: Growth (or not) of ranks of elliptic curves in cyclic extensions of number fields**

Suppose E is an elliptic curve over a number field K. In recent joint work with Barry Mazur, we studied the growth of the Selmer rank of E in cyclic extensions F/K of prime power degree. By refining our methods, it is possible to give criteria under which $E(K)$ and $E(F)$ both have Mordell–Weil rank one.

14.00 **Martin Davis: Representation theorems for r.e. sets vs. plain unsolvability with a conjecture about Poonen's large subring of $\mathbb{Q}$.**

Unsolvability theorems often come associated with a representation theorem for r.e. sets. H10 unsolvability for the integers is a corollary of Matiyasevich's Theorem/MRDP/DPRM. The unsolvability of the word problem of groups is a corollary of Higman's theorem, which is also such a representation theorem. Work on extensions of H10 has focused on plain unsolvability, although representation theorems are often easily obtainable and are worthwhile. I will apply these ideas to a recent large subring of $\mathbb{Q}$ by Poonen, and I will propose a conjecture involving simple r.e. sets whose truth would imply that H10 is unsolvable over $\mathbb{Q}$.

Wednesday, February 11

9.00 **Xavier Vidaux: Büchi's problem (a survey)**
Büchi's Problem asks for a positive integer constant M such that the following is true: *A sequence of M or more integer squares, with second difference constant and equal to 2, is of the form $(x+n)^2$, $n = 0, \dots, M-1$, for some integer x.* Proposed in 1970, Büchi's Problem is still open. We will explain the relation among the following problems: a) Büchi's Problem, b) Hilbert's Tenth Problem, c) the problem of simultaneous representation of integers by diagonal quadratic forms, and d) a conjecture of Lang about the locus of rational points on a variety. Then we will explain how to generalize this problem to other domains and for higher powers, and give a survey of the results obtained so far. Finally, we will address some open questions and we will give an outline of the ideas used in the proofs.

10:45 **Alexandra Shlapentokh: Using indices of points on an elliptic curve to construct a Diophantine model of $\mathbb{Z}$ and define $\mathbb{Z}$ using one universal quantifier in very large subrings of number fields including $\mathbb{Q}$.**
Let K be a number field and let E be an elliptic curve defined and of rank one over K. For a set $\mathcal{W}_K$ of primes of K, let $O_{K,\mathcal{W}_K} = \{x \in K : \mathrm{ord}_{\mathfrak{p}}\, x \geqslant 0, \forall \mathfrak{p} \notin \mathcal{W}_K\}$. Let $P \in E(K)$ be a generator of $E(K)$ modulo the torsion subgroup. Let $(x_n(P), y_n(P))$ be the affine coordinates of $[n]P$ with $n \neq 0$ with respect to a fixed Weierstrass equation of E. We show that there exists a set $\mathcal{W}_K$ of primes of K of natural density one such that in $O_{K,\mathcal{W}_K}$ multiplication of indices (with respect to some fixed multiple of P) is existentially definable and therefore these indices can be used to construct a Diophantine model of $\mathbb{Z}$. We also show that $\mathbb{Z}$ is definable over $O_{K,\mathcal{W}_K}$ using just one universal quantifier. Both, the construction of a Diophantine model using the indices and the first-order definition of $\mathbb{Z}$ can be lifted to the integral closure of $O_{K,\mathcal{W}_K}$ in any infinite extension K_∞ of K as long as $E(K_\infty)$ is finitely generated and of rank one.

14:00 **Boris Moroz: On a polynomial encoding provability in Gödel–Bernays axiomatic set theory (GB)** (joint work with M. Carl)
We construct a polynomial $P(t, \bar{x})$ in $Z[t, \bar{x}]$ such that the polynomial $P(n, \bar{x})$ has roots in $\mathbb{Z}$ if and only if the n-th formula of GB is

a theorem. As a by-product of that construction, one obtains a hypersurface defined over $\mathbb{Z}$, which presumably has no integer points, although this assertion can not be proved in GB and for its proof requires an additional large cardinal axiom.

Thursday, February 12

9.00 **Jan Denef: A geometric proof of a theorem of Ax–Kochen**
We will sketch a new proof of the celebrated Theorem of Ax and Kochen that any projective hypersurface over the p-adic numbers has a p-adic rational point, if it is given by a homogeneous polynomial with more variables than the square of its degree d, assuming that p is large enough with respect to the degree d. Our proof is purely geometric and (unlike all previous ones) does not use methods from mathematical logic. It is based on Cutkosky's Theorem on Local Monomialization of Morphisms, which is a deep result in algebraic geometry. The method also yields a proof of a conjecture of Colliot-Thélène and generalizations.

10:45 **Laurent Moret-Bailly: Hilbert's tenth problem for holomorphy rings in characteristic zero**

14:00 **Jeroen Demeyer: Hilbert's Tenth Problem for function fields over valued fields in characteristic zero**
Let K be a field with a valuation satisfying the following conditions: both K and the residue field k have characteristic zero; the value group is not 2-divisible; there exists a maximal subfield F in the valuation ring such that $\mathrm{Gal}(\overline{F}/F)$ and $\mathrm{Gal}(\bar{k}/k)$ have the same 2-cohomological dimension and this dimension is finite. Then Diophantine equations are undecidable over any function field of a variety over K. In particular, this result proves undecidability for varieties over $\mathbb{C}((T))$.

Friday, February 13

9.00 **Bjorn Poonen: Smooth H10 and automorphisms of complex varieties**
We prove that there is no algorithms that, given a smooth projective variety $X/\mathbb{C}$, a closed point $x \in X$, and a smooth projective subvariety $Z \subseteq X$, decides whether there exists an automorphism of X mapping x into Z. Along the way, we show that Hilbert's tenth problem for polynomials defining smooth $\mathbb{Q}$-varieties is equivalent to Hilbert's tenth problem for arbitrary polynomials.

10.45 **Florian Pop: Defining valuation rings**

14:00 **Jose Felipe Voloch: Hilbert's 10th problem and cryptography**

Recent developments indicate that there might be an algorithm to decide whether curves have rational points. The next step would be to ask for efficient algorithms. This would have impact in cryptography where recently some cryptosystems have been proposed which were based on the difficulty of finding points on curves. Unfortunately some of these cryptosystems were broken for other reasons and it is still open whether one can design a secure cryptosystem based on this problem. Higher dimensional varieties can also be considered. This talk will discuss these problems and their current status.

15.30 **Martin Davis: Recollections on the early history of Hilbert's tenth problem**