Mathematisches Forschungsinstitut Oberwolfach

Report No. 3/2003

Miniworkshop:
Hilbert's Tenth Problem, Mazur's Conjecture and Divisibility Sequences

January 19th – January 25th, 2003

The mini workshop was devoted to various questions arising from the solution of Hilbert's Tenth Problem by Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich and other problems on the boundary of Logic and Algebra. Among other questions, the following problems were discussed during this meeting: counterexamples to Mazur's conjecture for the large subrings of $\mathbf{Q}$ and number fields; diophantine undecidability over large subrings of $\mathbf{Q}$ and number fields; Mazur's conjectures and diophantine models over number fields and function fields of positive characteristic; using divisibility sequences and their generalizations to construct diophantine models of $\mathbf{Z}$; diophantine undecidability and definability over some function fields and rings of characteristic 0; using r.e. sets in proofs of diophantine undecidability; generalizations of Büchi's Question; bounded versions of HTP; uniformity in the Mordell-Lang theorem; distinguished automorphisms of algebraically closed fields.

Abstracts

From Elliptic Curves to Jacobians

Gunther Cornelissen

Let E be an elliptic curve over $\mathbf{Q}$ and P a point of infinite order on E. Let $\{h_n\}$ denote the sequence of square roots of the denominators of the x-coordinates of nP on E in a Weierstrass model. We use the theory of elliptic divisibility sequences to show that there exists an r (depending on the height of P and the bad fibres of E) such that $m|n \iff h_{rm}|h_{rn}$.

We conjecture that there exists such a curve and a point P and a set R of primes inert in at least one of finitely many quadratic number fields such that any sufficiently large h_n has a primitive odd order prime divisor from R. If this is true, the predicate from Jan Van Geel's talk can be used to construct a diophantine model of $(\mathbf{Z}, +, |)$ in $\mathbf{Q}$.

We speculate on how this conjecture generalizes to genus-2 Jacobians with real multiplication. The trouble is that denominator sequences on the corresponding Kummer surface don't form a divisibility sequence anymore. If an analogous conjecture could be formulated for one such Kummer surface, then it would imply that $S := (\mathcal{O}, +, |)$ is definable in $\mathbf{Q}$ for some real quadratic order $\mathcal{O}$. Since Lipshitz has shown that multiplication is definable in S, we would get that the diophantine theory of $\mathbf{Q}$ is undecidable and Mazur's conjecture is wrong.

Transferring HTP from One Ring to Another

Martin Davis

The following theorem is intended to illustrate the possible advantages of applying the detailed study of r.e. sets:

Let $\mathcal{M}$ be a computable ring. Let S be a simple set Diophantine over $\mathcal{M}$ as follows:

$$S = \{y \in Z \mid (\exists x_1, \ldots, x_n \in \mathcal{M}) p(y, x_1, \ldots, x_n) = 0\}$$

where p is a polynomial with coefficients in $\mathcal{M}$. Let σ be a homomorphic map of $\mathcal{M}$ onto the ring $\mathcal{L}$. Let

$$R = \{y \in Z \mid (\exists x_1, \ldots, x_n \in \mathcal{L}) p^\sigma(y, x_1, \ldots, x_n) = 0\}$$

where p^σ is the image of p under σ. Then if $\bar{R}$ is infinite, the set R is simple, and therefore Hilbert's 10th problem over $\mathcal{L}$ is unsolvable.

The Myth of Hypercomputation

Martin Davis

Under the banner of "hypercomputation" various claims are being made for the feasibility of modes of computation that go beyond what is permitted by Turing computability. We show that such claims fly in the face of the inability of all currently accepted physical theories to deal with infinite precision real numbers. When the claims are viewed critically, it is seen that they amount to little more than the obvious comment that if non-computable inputs are permitted, then non-computable outputs are attainable.

Hilbert's Tenth Problem for Function Fields of Surfaces over $\mathbb{C}$

Kirsten Eisenträeger

We prove that Hilbert's Tenth Problem for function fields of surfaces over $\mathbb{C}$ has a negative answer. This generalizes Kim and Roush's result for $\mathbb{C}(t_1, t_2)$. Let K be the function field of a surface over $\mathbb{C}$. In the proof we use rank one elliptic curves over K to show that there exists a diophantine model of $(\mathbb{Z}, +, \cdot)$ over K.

The Arithmetic of Bilinear Recurrence Sequences

Graham Everest

We discuss the arithmetic of bilinear recurrence sequences taking the theory of linear recurrence sequences as a paradigm. The linear theory suggests one should look for periodicity, growth rates, Zsigmondy's theorem on primitive divisors and prime terms. In the binary linear case there is an underlying compact group (the circle) which makes these questions particularly approachable. In the binary bilinear case the underlying group is an elliptic curve. This makes it possible to prove analogous results but there are some surprises. For example, in the bilinear theory it is expected that only finitely many terms are primes and this is provable in certain cases.

Quadratic forms and divisibility

Jan Van Geel

We show that there is a diophantine definition in the rational number of the relation between rational numbers x and y "an odd order pole in R of x is a pole of y", where R is any set of primes inert in one of finitely many quadratic number fields. This generalizes an observation of Pheidas from the case where there is only one quadratic field, namely $\mathbf{Q}(i)$. In particular, the Dirichlet density of R can be chosen arbitrarily large $\neq 1$, not just equal to $1/2$.

Distinguished Automorphisms of Algebraically Closed Fields

Moshe Jarden

Extend the first order language of fields to a language $\mathcal{L}$ by adding e unary function symbols $\Sigma_1, \ldots, \Sigma_e$. The structures of $\mathcal{L}$ we consider are $\langle \tilde{\mathbb{Q}}, \sigma_1, \ldots, \sigma_e \rangle$ where $\sigma_1, \ldots, \sigma_e$ are elements of the absolute Galois group $\mathrm{Gal}(\mathbb{Q})$ of $\mathbb{Q}$. Denote the set of all sentences of the extended language which hold in $\langle \tilde{\mathbb{Q}}, \sigma_1, \ldots, \sigma_e \rangle$ for all but a Haar measure 0 of e-tuples $(\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\mathbb{Q})^e$ by $\mathrm{Almost}(\tilde{\mathbb{Q}}, \Sigma_1, \ldots, \Sigma_e)$. We prove:

Theorem: (a) The theory of finite graphs is interpretable in $\mathrm{Almost}(\tilde{\mathbb{Q}}, \Sigma_1, \ldots, \Sigma_e)$.

(b) Arithmetic is interpretable in $\mathrm{Almost}(\tilde{\mathbb{Q}}, \Sigma_1, \ldots, \Sigma_e)$.

(c) While θ ranges over all sentences of $\mathcal{L}$, the probability $\mathrm{Prob}(\theta)$ that θ holds in $\langle \tilde{\mathbb{Q}}, \sigma_1, \ldots, \sigma_e \rangle$ ranges over all definable real numbers between 0 and 1.

Here we call a nonnegative number r **definable** if there exists a formula $\phi(x, y)$ of Arithmetic such that for all $a, b \in \mathbb{N}$, $\phi(a, b)$ holds in $\mathbb{N}$ if and only if $\frac{a}{b} > r$. In particular if a recursive sequence of real numbers approaches r from above, then r is decidable.

(d) The formula $\frac{\pi}{4} = \sum_{i=0}^{\infty} (-1)^{i+1} \frac{1}{2i+1}$ implies that $\frac{\pi}{4}$ is definable. In particular, by (c), there exists sentences θ with $\mathrm{Prob}(\theta)$ transcendental.

An analogue of HTP for rings of analytic functions

Thanases Pheidas

Let $\mathcal{H}_z(D)$ be the ring of complex-valued functions, analytic on an open superset of a connected set $D \subset \mathbf{C}^r$, with nonempty interior.

Question: Is the existential theory of $\mathcal{H}_z(D)$ decidable, in the language which contains symbols for addition, multiplication, a predicate for the constant functions and constant symbols for 0, 1 and z?

At this point the question is open. We have "undecidability" results for the analogous problem for $z = (z_1, z_2)$ (two variables). Analogous negative results are known for the $p-$adic analogue $\mathbf{C}_p$ of $\mathbf{C}$.

Bounded Versions of Hilbert's Tenth Problem and $NP = co\text{-}NP$

Chris Polett

We discuss the provability of Matjasevich-Robinson-Davis-Putnam (MRDP) result in weak systems of arithmetic. It is a well-known result of Gaifman and Dimitricopoulos that $I\Delta_0{+}exp$ proves MRDP. What was shown in their result was that every bounded formula in their language could be rewritten as a formula consisting of an existential block of quantifiers followed by an equation of the form $p = q$ where p and q are polynomials. By Parikh's Theorem, $I\Delta_0{+}exp$ cannot prove the existence of superexponentially fast growing functions. Therefore, one could ask whether if one expanded the language by such a function but restricted syntactically $I\Delta_0{+}exp$'s access to it, then one could obtain a system unable to prove MRDP in this new language. This is possible because now the bounds on the quantifiers that need to be eliminated are larger than before. In fact, we construct a system that cannot prove MRDP and show as well that it cannot prove $NP = co\text{-}NP$ in a certain very uniform way.

Hilbert's Tenth Problem over large subrings of $\mathbb{Q}$

Bjorn Poonen

We give the first examples of infinite sets of primes S such that Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$ has a negative answer. In fact, we can take S to be a density 1 set of primes. We show also that for some such S there is a punctured elliptic curve E' over $\mathbb{Z}[S^{-1}]$ such that the topological closure of $E'(\mathbb{Z}[S^{-1}])$ in $E'(\mathbb{R})$ has infinitely many connected components.

Uniformity in the Mordell-Lang theorem

Thomas Scanlon

Several theorems (and conjectures) in diophantine geometry assert that certain arithmetically defined sets of points on varieties (ie finitely generated subgroups of complex tori, the special points on Shimura varieties) must meet subvarieties of the ambient variety in a finite union of sets of a very special form. For example, if A is an abelian variety over $\mathbb{C}$ and $\Gamma \leq A(\mathbb{C})$ is a finitely generated subgroup, then for any closed subvariety $X \subseteq A$, the set $\Gamma \cap X(K)$ is a finite union of cosets of subgroups of Γ.

We show how uniform versions of these finiteness results follow immediately from their non-uniform versions via an application of the definability of types in algebraically closed fields.

[It should be noted that the speaker was not the only person to make this observation. It had been noted by Hrushovski, Pillay, and possibly others.]

Ring Version of Mazur's Conjecture.

Alexandra Shlapentokh

Barry Mazur has conjectured that the topological closure of any variety $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components. We consider this conjecture in a ring setting. Given an integrally closed subring R of a number field we investigate the number of connected components of the topological closure of $V(R)$ in $\mathbb{R}$ or $\mathbb{C}$.

On a Question of Büchi

Xavier Vidaux

We generalize a question of Büchi : Let R be an integral domain and $k \geq 2$ an integer. Is there an algorithm to solve in R any given system of polynomial equations, each of which is linear in the $k-$th powers of the unknowns?

We examine variances of this problem for $k = 2, 3$ and for R a field of rational functions of characteristic zero. We obtain negative answers, provided that the analogous problem over $\mathbf{Z}$ has a negative answer. In particular we prove that the generalization of Büchi's question for fields of rational functions over a real-closed field F, for $k = 2$, has a negative answer if the analogous question over $\mathbf{Z}$ has a negative answer.

Mazur's Conjectures, Diophantine Models and HTP

Karim Zahidi
(joint work with Gunther Cornelissen)

We discuss the relation between Hilbert's tenth problem for the field of rational numbers and a conjecture by Mazur concerning the topology of rational points on algebraic varieties. More precisely, Mazur conjecture states that for any algebraic variety V defined over $\mathbf{Q}$, the topological closure of the set of rational points $V(\mathbf{Q})$ inside $V(\mathbf{R})$ consists of finitely many components. Mazur remarked that if this conjecture is true, $\mathbf{Z}$ can not be a diophantine subset of $\mathbf{Q}$. We show that from the validity of the conjecture we obtain that there is no diophantine model of integer arithmetic in $\mathbf{Q}$. So a proof of the negative answer to HTP($\mathbf{Q}$) along traditional lines will fail if Mazur's conjecture is correct. We also discuss a non-archimedean version of the conjecture and show that the non-archimedean conjecture is false for function fields over finite fields.

Edited by Alexandra Shlapentokh

Participants

Dr. Gunther Cornelissen
cornelis@math.uu.nl
Mathematisch Instituut
Universiteit Utrecht
P.O.Box 80.010
NL-3508 TA Utrecht

Prof. Dr. Martin Davis
martin@eipye.com
3360 Dwight Way
Berkeley CA 94704-2523 - USA

Kirsten Eisentraeger
eisentra@Math.Berkeley.EDU
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720-3840 - USA

Prof. Dr. Graham R. Everest
g.everest@uea.ac.uk
School of Mathematics
University of East Anglia
GB-Norwich NR4 7TJ

Prof. Dr. Jan van Geel
jvg@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Moshe Jarden
jarden@post.tau.ac.il
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978 - ISRAEL

Prof. Dr. Yuri Matiyasevich
yumat@pdmi.ras.ru
Steklov Mathematical Institute
POMI
Fontanka 27
St. Petersburg 191011 - RUSSIA

Prof. Dr. Thanases Pheidas
pheidas@math.uch.gr
Department of Mathematics
University of Crete
Knossos Ave,
71409 Heraklion, Crete - Greece

Dr. Chris Pollett
cpollett@yahoo.com
Pollett@mathcs.sjsu.edu
Dept. of Mathematics and Computer
Science
San Jose State University
214 MacQuarrie Hall
San Jose CA 95192-0103 - USA

Prof. Dr. Bjorn Poonen
poonen@math.berkeley.edu
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720-3840 - USA

Prof. Dr. Thomas Scanlon
scanlon@math.berkeley.edu
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720-3840 - USA

Prof. Dr. Alexandra Shlapentokh
shlapentokha@mail.ecu.edu
Dept. of Mathematics
East Carolina University
Greenville NC 27858-4353 - USA

Xavier Vidaux
vidaux@maths.ox.ac.uk
Mathematical Institute
Oxford University
24 - 29, St. Giles
GB-Oxford OX1 3LB

Dr. Karim Zahidi
zahidi@logique.jussieu.fr
Equipe Logique Mathématique
Universite Paris VII
2, Place Jussieux
F-75251 Paris Cedex 05