PROBLEMS CONNECTING LOGIC AND NUMBER THEORY

BARRY MAZUR

In the recent conference (May 10, 11) at Harvard University[1] I was asked to take part in a question-and-answer session with Carol Wood and Bjorn Poonen regarding questions that relate Mathematical Logic to Number Theory.

1. Our three "discussion problems."

Bjorn Poonen discussed the "recognition problem" for finitely generated rings (and fields). That is, given two finitely generated *commutative* rings A and B, presented in terms of generators and relations, is there a decision procedure to determine whether or not these rings are isomorphic (this being, one would think, a basic issue for algebraic geometry!). Of course, if one drops the requirement of commutativity, one comes up against the unsolvablity of the corresponding problem for finitely generated groups (by taking A and B simply to be integral group rings).

Carol Wood brought up cases where model theory, applied to number theoretic problems provided bounds that are impressively good! Model Theory—in some instances—yields significantly new proofs of theorems obtained by the number-theorists [2]. In other instances, model theory achieves startling results for problems not yet considered by number theorists [3]. Carol Wood discussed the recent article of Pila and Wilkie ([**PW07**]) that provides asymptotic upper bounds (as a function of the variable T) for the number of $\mathbf{Q}$-rational points of height $\leq T$ that

[1]MAMLS@Harvard, a meeting on the intersections of logic and mathematics. I want to thank Rehana Patel for organizing it and inviting us to participate.

[2]For example, Hrushovski's model-theoretic proof of the Manin-Mumford Conjecture was recently revisited and formulated as a (new) number theoretic proof in [**PR06**].

[3]For example, explicit bounds for the number of transcendental points on the intersection of subvarieties of semi-abelian varieties and a given finitely generated subgroup [**HP00**]. These bounds are double exponentials in the rank of the finitely generated group.

lie in a given semi-analytic set $X \subset \mathbf{R}^n$ but are outside any positive-dimensional semi-algebraic set contained in X.

I talked about examples of unsolvable problems given in Diophantine language (following Matiyasevich). Specifically, the negative solution of Hilbert's Tenth Problem. Here are some notes on this[4].

2. Comments on Hilbert's Tenth Problem

Following recent work on this problem it is useful to phrase the discussion for a general commutative ring A finitely presented over $\mathbf{Z}$ or over $\mathbf{Q}$, and of infinite cardinality[5].

The basic question is:

> Does there exist a finite algorithm to determine whether any finite system of polynomial equations in finitely many variables with coefficients in A has a solution in A or not?

Here, in a nutshell, is the general status of this question we inherited from Hilbert and from "classical work" (Julia Robinson/Davis/Putnam/ Matiyasevich). The culminating theorem is Matiyasevich's:

Theorem 2.1. Every recursively enumerable[6] subset of $\mathbf{Z}$ is diophantine (relative to $\mathbf{Z}$).

This fundamental result, of course, gives a negative answer to the question above, but does far more than just that.

For example:

(1) The result implies that relatively benign subsets of $\mathbf{Z}$ can be diophantinely described, as well. This is not as clear as one

[4]I want to thank Bjorn and Carol for their comments about, and corrections to, an early draft of these notes.

[5]Of course, the historically interesting case for this problem is $A = \mathbf{Z}$ or $A = \mathbf{Q}$. A close translation of Hilbert's formulation of the problem is as follows:

> Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

[6]I'm told, by Bjorn, that logicians these days are suggesting that the terminology "computably enumerable" replace "recursively enumerable".

might think even for the most familiar subsets, and seems interesting to me: for example, there is a polynomial over $\mathbf{Z}$ whose set of positive values is the set of *exactly all* prime numbers for integral substitution of its variables. A specific such polynomial (taking hardly two dozen lines of print) is given in **[JSWW76]**.

(2) One is not yet finished mining this for concrete versions of "unsolvable problems" but it clearly will give us a wealth of such problems. See, for example, recent postings of Harvey Friedman; these have possible relations to Mnëv's (1988) result that any scheme over $\mathbf{Z}$ can be expressed as a moduli space classifying configurations[7] of finite points in $\mathbf{P}^2$. Harvey Friedman poses nine different "Families of Problems" regarding configurations of rational lines in the Euclidean plane, These problems ask for existence or nonexistence of integral intersections (with various properties) of linear configurations. Friedman discusses whether the problems in each of these families can be done in ZFC or whether there are examples of problems in that family that cannot: apparently three of Friedman's problem-families can be solved in ZFC, three cannot, and for the remaining three—if Hilbert's Tenth Problem (over $\mathbf{Q}$) is undecidable—then these cannot be done in ZFC.

More recent work (Denef/Denef-Lipschitz/Pheidas/Shalpentokh/Poonen) developed ideas that culminated in the following result:

Theorem 2.2. If a certain stability result in the arithmetic of elliptic curves holds[8] over K, then for any number field K every recursively enumerable subset of $\mathcal{O}_K$, the ring of integers in K is diophantine (relative to $\mathcal{O}_K$).

Karl Rubin and I have recently shown that this stability result holds *if you assume the* 2*-primary part of the classical Shafarevich-Tate Conjecture* **[MR09]**. As a consequence we have shown that, conditional on

[7]By a *configuration type* let us mean a number N and a collection of subsets $S_1, S_2, \ldots S_n$ of the set $[1, 2, \ldots, N]$. The configuration space associated to such a type is the space of all ordered sets of N points in $\mathbf{P}^2$ subject to the requirement that the points corresponding to S_1 are collinear, and ditto for $S_2, \ldots, S_n$.

[8]Specifically the *stability result* asserts that for every prime degree Galois extension of number fields L/K there exists an elliptic curve E over K with

$$\text{rank}E(K) = \text{rank}E(L) > 0.$$

the 2-primary part of the Shafarevich-Tate Conjecture, Hilbert's Tenth problem has a negative answer for the ring of integers in *any* number field.

Since Kirsten Eisenträger has, in her thesis, related Hilbert's Tenth Problem over rings of integers in number fields to a much more general class of rings, one gets—thanks to her work:

Theorem 2.3. Conditional on the 2-primary part of the Shafarevich-Tate Conjecture, Hilbert's Tenth problem has a negative answer for any commutative ring A that is of infinite cardinality, and is finitely generated over $\mathbf{Z}$.

3. The focus on cubics!

One variable is OK; linear and quadratic are OK. There are unsolvable fourth degree polynomials over $\mathbf{Z}$ (in a large number of variables). This focuses on the third degree, and there—to my knowledge—our knowledge essentially stops[9].

4. Rational points on cubic plane curves

A famous half-century-old example here is *Selmer's equation:*

$$3X^3 + 4Y^3 + 5Z^3 \;=\; 0$$

which has NO (nontrivial) solutions over $\mathbf{Q}$ even though all "local indicators" don't rule out the possibility that a rational (nontrivial) solution exists[10] So that particular problem is "solved." But, more generally, we want to know:

> Is there an algorithm to answer—for any third degree polynomial $F(X, Y)$ over $\mathbf{Q}$—the question: is there a pair of rational numbers a, b such that $F(a, b) = 0$?

[9]It is interesting how our lack of understanding of cubics seems to color lots of mathematics, from the ancient concerns in the "one-variable case" having to do with "two mean proportionals," and Archimedes' Prop.4 of Book II of *The Sphere and Cylinder* and Eutocius' commentaries on this, and–of course—the Italian 16c early algebraists.

[10]This projective curve has points rational over every completion of $\mathbf{Q}$.

A proof of the Shafarevich-Tate Conjecture[11] would provide a proof that a certain algorithm works for the general third degree polynomial $F(X, Y)$ and—more generally—to find rational points on curves of genus one. The algorithm itself is currently known, and used quite extensively. If it (always) works, then it gives an answer to the question posed above, and indeed allows us to find the rational points. But we don't know whether it will always terminate (in finite time) to provide us with an answer. The Shafarevich-Tate Conjecture would guarantee termination in finite time. This is a huge subject (the arithmetic theory of elliptic curves) and it would be good to understand it as well as we can possibly understand it. Note the curious irony in the formulation of Theorem 2.3:

> If we have a proof of the (2-primary part of the) Shafarevich-Tate conjecture
>
> *—i.e., colloquially speaking: if the algorithm that enables us to deal with arithmetic of cubic plane curves can be* **proved** *to work—*
>
> then we have a proof of the **non**-existence of a general algorithm for the ring of integers over any number field.

5. Integral points on plane curves of genus one

Here one has a striking explicit result, thanks to Baker's method. Let $f(X_1, X_2) \in \mathbf{Z}[X_1, X_2]$ be an absolutely irreducible polynomial such that the associated projective curve $f = 0$ has genus one. Let $n :=$ the (total) degree of $f(X_1, X_2)$ and let $H :=$ the maximum of the (ordinary) absolute values of the coefficients of $f(X_1, X_2)$. Then there are finitely many integral solutions (a_1, a_2) of the equation $f(X_1, X_2) = 0$ and they are bounded explicitly by the inequality

$$\max\{|a_1|, |a_2|\} \ < \ \exp\exp\exp\{2H^{10n^{10}}\}.$$

For discussion about this, see section 4.4 of [**B75**].

6. Polynomials of degree three in many variables, over $\mathbf{Z}$

We are now left to ponder one of the big open problems in this area:

> Is there an algorithm to answer—with input third degree polynomials $F(X_1, X_2, \ldots, X_n)$ over $\mathbf{Z}$ for arbitrary

[11] In fact, just, the p-primary part of the Shafarevich-Tate Conjecture, for any single prime number p will do it.

$n \geq 3$ —the question of whether there is an n-tuple of integers $(a_1, a_2, \ldots, a_n)$ such that $F(a_1, a_2, \ldots, a_n) = 0$?

In the discussion Curt McMullen asked us to speculate—given current knowledge— what the eventual answer will be. I know what I "want the answer to be" (i.e., solvable, why not?) but I can't give any compelling reason for my optimism. Curt McMullen pointed out that in the topology the recognition problem for manifolds of dimension four or higher is unsolvable (it being related directly to the recognition problem for finitely presented groups, and it is patently solvable for dimension ≤ 2. For manifolds of dimension three the recognition problem is, in fact, solvable, but this is a deep result.

7. An Open Question

In the question period, Gerald Sacks suggested that solvability or unsolvability may be only one of a number of different ways of framing questions regarding diophantine algorithms. I agree, and have always liked Serge Lang's attitude towards these matters, who—in effect—focussed much attention to the question of determining whether there are finitely many, as opposed to infinitely many, solutions [12] and asked algebro-geometric questions about structure of the infinitely many solutions when they exist.

In this spirit allow me to formulate a question—without prejudice—that seems worth contemplating even if it is a bit premature to try to make much headway with it.

If V is an algebraic variety over $\mathbf{Q}$ let $X(V; \mathbf{Q}) \subset V$ be the Zariski closure in V of the set $V(\mathbf{Q})$ of $\mathbf{Q}$-rational points of V.

Define $D(V) = D(V; \mathbf{Q}) :=$ the number of irreducible components of $X(V; \mathbf{Q})$.

Suppose that we set out to find upper bounds for this function from algebraic varieties to natural numbers:

$$V \quad \mapsto \quad D(V).$$

Consider, for example, the case where V is an irreducible curve.

- If V is of genus 0, then $D(V)$ is either 0 or 1 depending upon whether V has a rational point or not.

[12] rather than existence or nonexistence of solutions

- If V is of genus one, then
  - $D(V)$ is 0 if V has no rational points,
  - $D(V)$ is 1 if V has infinitely many rational points, and
  - $D(V)$ is the order of the Mordell-Weil group of V over $\mathbf{Q}$, if that group is finite.

  In all cases for V of genus one, then, (using [**M77**]) we get that $D(V) \leq 16$.

- If V is of genus > 1, by Faltings' Theorem $D(V)$ is the (finite) number of rational points of V. Conditional on a conjecture of Lang, Caparoso, Harris and I have shown that $D(V)$ is bounded by a function that depends only on the genus of V.

In sum, we have that (conditional on a conjecture of Lang) for all algebraic varieties V of dimension one,

> $D(V)$ is bounded from above by a function $F(|V_{\mathbf{C}}|)$ that depends only on the homotopy type $|V_{\mathbf{C}}|$ of the complex analytic space associated to V.

Is the above statement true or false for algebraic surfaces? Or, more generally, for algebraic varieties of arbitrary dimension?

Bibliography

[**B75**] A. Baker, *Transcendental Number Theory*, Cambridge Mathematical Library, Cambridge University Press (1975).
[**E03**] A.K. Eisenträger, Hilbert's Tenth Problem and Arithmetic Geometry, PhD Thesis, University of California, Berkeley, 2003.
[**Den80**] J. Denef, Diophantine sets over algebraic integer rings. II, Trans. Amer. Math. Soc. 257 (1980), no. 1, 227-236.
[**DL78**] J. Denef and L. Lipshitz, Diophantine sets over some rings of algebraic integers, J. London Math. Soc. (2) 18 (1978), no. 3, 385-391.
[**H96**] E. Hrushovski, The Mordell-Lang conjecture for function elds. Journal of the American Mathematical Society **9** (1996), no. 3, 667-690.
[**H98**] E. Hrushovski, Proof of Manin's theorem by reduction to positive characteristic, *Model theory and algebraic geometry,* Lecture Notes in Math.,**1696**, Springer, Berlin, (1998) 197-205.
[**H00**] E. Hrushovski, Anand Pillay, Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties. American Journal of Mathematics **122** (2000), no. 3, 439-450.

[**JSWW76**] J. P. Jones, D. Sato, H. Wada and Do. Wiens, Diophantine Representation of the Set of Prime Numbers, The American Mathematical Monthly, **83**, No. 6 (Jun. - Jul., 1976), pp. 449-464.
[**M77**] B. Mazur, Modular Curves and the Eisenstein ideal, Publ. IHES **47** (1977) 33-186.
[**MR09**] B. Mazur and K. Rubin, Ranks of twists of elliptic curves and Hilbert's Tenth Problem, (http://abel.math.harvard.edu/ mazur/) and also on Archiv (arXiv:0904.3709v2 [math.NT] 25 Apr 2009)
[**Phe88**] Thanases Pheidas, Hilbert's tenth problem for a class of rings of algebraic integers, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611-620.
[**PR06**] R. Pink, D. Roessler, On Hrushovski's proof of the Manin-Mumford conjecture (preprint).
[**Po**] Bjorn Poonen, Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers (. . .)
[**PW07**] J. Pila, A.J. Wilkie, The rational points of a definable set, MIMS Eprint .2007.198.
[**Shl89**] Alexandra Shlapentokh, Extension of Hilbert's tenth problem to some algebraic number fields, Comm. Pure Appl. Math. **42** (1989), no. 7, 939- 962.
[**Shl00b**] Alexandra Shlapentokh, Hilbert's tenth problem over number fields, a survey, *Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 107- 137.