DESCRIPTIONS OF BJORN POONEN'S LECTURE SERIES AND STUDENT PROJECT

1. Course description: Hilbert's Tenth Problem

In 1900, Hilbert proposed a list of 23 problems for 20th century mathematicians to work on. Problem #10 was

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

The problem can be made precise using modern terminology: Find an algorithm (i.e., Turing machine) to decide, given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether there exists a solution with $x_1, \ldots, x_n \in \mathbb{Z}$. Matijasevič, following work of Davis, Putnam, and Robinson, proved that no such algorithm exists. Hence one says that "Hilbert's Tenth Problem is undecidable." Since then, researchers have asked, what happens when $\mathbb{Z}$ is replaced by some other commutative ring R?

The lectures in this course will focus on the open problems that arise when R is a ring of arithmetic interest. For example, it is not known whether an algorithm exists $R = \mathbb{Q}$, the field $\mathbb{Q}$ of rational numbers. The question over $\mathbb{Q}$ is of fundamental interest to arithmetic geometers, because it is equivalent to the existence of algorithm for deciding whether a variety over $\mathbb{Q}$ has a rational point. Attempts to reduce the question over $\mathbb{Q}$ to the question over $\mathbb{Z}$ come into conflict with conjectures of Mazur on the topology of rational points.

For most number fields K, the question for the ring of integers of K is another open problem. We will discuss how elliptic curves might be used to prove undecidability for such rings. If time permits, we may also mention analogues for function fields.

Prerequisites. Attendees are expected to know, as a minimum:

- basic algebraic number theory, such as unique factorization of fractional ideals for rings of integers of number fields
- what affine and projective varieties are (see the first few pages of [Har77])
- enough about elliptic curves to understand the *statement* of the Mordell-Weil Theorem for elliptic curves over number fields (see [Sil92], or the more elementary [ST92])
- what a first order sentence in the language of rings is (see Chapter II of [EFT94], or any other introduction to logic).

2. Project description: Hilbert's Tenth Problem for rings of integers of number fields

Let $F \subseteq K$ be number fields, and let $\mathcal{O}_F$ and $\mathcal{O}_K$ be their rings of integers. The paper [Poo02] proves that if there is an elliptic curve E over F such that $E(F)$ and $E(K)$ both have rank 1 (as abelian groups), then the undecidability of Hilbert's Tenth Problem for $\mathcal{O}_F$

Date: October 21, 2002.

implies the undecidability of Hilbert's Tenth Problem for $\mathcal{O}_K$. As a corollary, if there exists an elliptic curve E over $\mathbb{Q}$ such that $E(\mathbb{Q})$ and $E(K)$ have rank 1, then Hilbert's Tenth Problem over $\mathcal{O}_K$ is undecidable.

The project will be to prove the following generalization: if there is an elliptic curve E over F such that $E(F)$ and $E(K)$ both have rank 1 *as modules over the endomorphism ring of E over F*, then the undecidability of Hilbert's Tenth Problem for $\mathcal{O}_F$ implies the undecidability of Hilbert's Tenth Problem for $\mathcal{O}_K$. Other possible open problems are given at the end of [Poo02], but I suspect that these are more difficult.

The students in the small group participating in this project will need to prepare as follows, before the Winter School begins:

- Study chapters 1 through 8 of [Sil92], if you do not already know this material (arithmetic of elliptic curves).
- Read [Poo02].

3. Further reading

It is not necessary to read the following in order to follow my lectures or to participate in my project, but I mention them for those who want more. The book [DLPVG00], which is the proceedings of a 1999 conference on Hilbert's Tenth Problem, is the best single reference for this material. The articles by Pheidas and Zahidi, by Shlapentokh, by Pheidas, and by Cornelissen and Zahidi in that book will be particularly relevant to my lectures. For an exposition of Matijasevič's original proof, see the paper [JM91].

And for those who just cannot get enough, Hilbert's Tenth Problem is now available on the web:

`http://logic.pdmi.ras.ru/Hilbert10/`

References

[DLPVG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, American Mathematical Society, Providence, RI, 2000, Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999.

[EFT94] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical logic*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1994, Translated from the German by Margit Meßmer.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[JM91] J. P. Jones and Y. V. Matijasevič, *Proof of recursive unsolvability of Hilbert's tenth problem*, Amer. Math. Monthly **98** (1991), no. 8, 689–709.

[Poo02] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), Springer Lecture Notes in Computer Science **2369**, Berlin, 2002, pp. 33–42, `arXiv:math.NT/0204001`.

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[ST92] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `poonen@math.berkeley.edu`