Hilbert's Tenth Problem and Mazur's Conjectures in Large Subrings of number fields
Presentation by Kirsten Eisentraeger

1 Motivation

The motivating problem:

Hilbert's Tenth Problem: Find an algorithm to decide, given a polynomial equation $f(x_1, \cdots, x_n) = 0$ with $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$, whether or not it has a solution with $x_1, \cdots, x_n \in \mathbb{Z}$.

In 1970, this problem was solved by Matiyasevich (building on work of Davis, Putnam, and Robinson), showed that no such algorithm exists. Thus, we say that Hilbert's Tenth Problem is **undecidable**.

Before this problem was solved, people already generalized this problem to arbitrary commutative rings R:

Hilbert's Tenth over R: Find an algorithm to decide, given a polynomial equation $f(x_1, \cdots, x_n) = 0$ with $f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$, whether or not it has a solution with $x_1, \cdots, x_n \in R$.

Hilbert's Tenth over $\mathbb{Q}$ is still an open problem, as is Hilbert's Tenth over K a number field.

Despite this, we can answer Hilbert's tenth negatively for some rings $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$.

Theorem: Let K be a number field over which there is an elliptic curve defined over K whose K-rank is 1. For every $t > 1$ and every collection $\delta_1, \cdots, \delta_t$ of nonnegative computable real numbers whose sum is 1, the set of nonarchimedean valuations of K may be partitioned into t mutually disjoint subsets $s_1, \cdots, s_t$ of densities $\delta_1, \cdots, \delta_t$ such that Hilbert's Tenth is undeciable over $\mathcal{O}_{K,s_i}$.

Here $\mathcal{O}_{K,s_i} = \{x \in K \mid \text{ord}_{\mathcal{O}} x \geq 0 \forall \mathfrak{p} \notin s_i\}$

Remark: We believe such curves exist for all number fields K.

Example: $K = \mathbb{Q}, t = 2$. The nonarchimedean valuations are in bijective correspondence with the primes $\mathcal{P}$. The theorem implies that $P = S_1 \cup S_2$ with $S_1 \cap S_2 = \varnothing$, S_1 and S_2 recursive and of prescribed density and such that Hilbert's Tenth for $\mathbb{Z}[S_1^{-1}]$ and H10 for $\mathbb{Z}[S_2^{-1}]$ is undecidable. If we take densities 0 and 1, we get a strengthening of Poonen's earlier result, which did not address the undecidability of the density 0 set.

Some known results:

- H10 is decidable over
  - finite fields
  - p-adic fields (Ax-Kochen, Ersov)
  - real-closed fields
- H10 is undecidable over
  - function fields of curves over finite fields (Pheidas, Shlapentokh, Videla, Eisentraeger)
  - some rings of integers of number fields (any ring of integers if Shafarevich-Tate conjecture holds [Mazur-Rubin])

Today's theorem generalizes techniques of Poonen (2002) and Poonen-Shlapentokh (2005) and Eisentraeger-Everest (2009)

Outline of Talk

- Sketch proof for $K = \mathbb{Q}$, $t = 2$
- Say something about densities and Mazur's conjecture at the end

2 Outline of Proof

Definition 1. Let R be a commutative ring. A subset $A \subseteq R^k$ is **diophantine over** R if there exists a polynomial $f(x_1, \cdots, x_k, y_1, \cdots, y_m)$ with coefficients in R such that $A = \{x \in R \,|\, \exists y_1, \cdots, y_m \in R : f(x_1, \cdots, x_k, y_1, \cdots, y_m) = 0\}$

Examples: (1) $\mathbb{N}$ is diophantine over $\mathbb{Z}$: $x \in \mathbb{N}$ if and only if $\exists y_1, \cdots, y_4 \in \mathbb{Z}$ such that $y_1^2 + \cdots + y_4^2 - x = 0$

(2) The set of primes is diophantine

Proving undecidability through reductions: Let K be a number field, $R \subseteq K$ a subring

Proposition 1. *If $\mathbb{Z}$ is diophantine over R then H10 / R is undecidable.*

Assume for contradiction that we have an H10 algorithm for R. Take an equation $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$ and regard it as a polynomial over R. Then as $\mathbb{Z}$ is diophantine consider its defining equation over R. Then to decide whether or not f has solutions in $\mathbb{Z}$ it suffices to determine whether or not $f^2 + g_1^2 + \cdots + g_n^2 = 0$ for g_i saying that x_i is an element of $\mathbb{Z}$. This contradicts the undecidability of H10 for $\mathbb{Z}$.

Definition 2. A diophantine model of $\mathbb{Z}$ over R is a set $A \subseteq R^n$ that is diophantine over R together with a bijection $\mathbb{Z} \to A$ under which the graphs of addition and multiplication in $\mathbb{Z}$ correspond to subsets of A^3 that are diophantine over R.

Proposition 2. *If R admits a diophantine model of $\mathbb{Z}$ then H10/R is undecidable*

Proof. As above. $\square$

We will use the existence of the elliptic curve in the hypothesis to produce such a diophantine model of $\mathbb{Z}$. This is tricky though- when taking multiples of points in an elliptic curve E on integral points we *divide*, which may take us to a rational non-integral point.

Proof of theorem: Construction of the diophantine model. Take any elliptic curve $E/\mathbb{Q}$ of rank 1, so that $E(\mathbb{Q}) \cong \mathbb{Z} \oplus E(\mathbb{Q})_{tors}$.

Let Q be a generator for $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

Let $P = zQ$ (suitable multiple of the generator) so that P has integral coordinates.

Fix a Weierstrass equation for $E : y^2 = x^3 + ax + b$.

Outline of construction:

Step 1: Construct two sequences of primes which are disjoint (they have nothing to do with what S_1 and S_2 look like) $\ell_1 < \ell_2 < \cdots$ and $\ell'_1 < \ell'_2 < \cdots$. The choice of these sequences is crucial to let us control the orders of certain valuations of points to make addition and multiplication work out.

Step 2: Construct four sets T_1, R_1, T_2, R_2 s.t. $T_1 \cap R_1 = \varnothing$, $T_2 \cap R_2 = \varnothing$, $T_1 \cap T_2 = \varnothing$, and $R_1 \cap R_2 = \varnothing$. We will get undecidability for S_1, S_2 which are such that $T_1 \subseteq S_1 \subseteq \mathcal{P} - R_1$ and $T_2 \subseteq S_2 \subseteq \mathcal{P} - R_2$. In general we can't get R_1 or R_2 infinite.

Choose T_1, T_2, R_1, R_2 such that

$$E(\mathbb{Z}[S_1^{-1}]) \cap z \cdot E(\mathbb{Q}) = \bigcup \{\pm \ell_i(P)\} + \text{finite set}$$

and

$$E(\mathbb{Z}[S_2^{-1}]) \cap z \cdot E(\mathbb{Q}) = \bigcup \{\pm \ell_i'(P)\} + \text{finite set}$$

and so T_1 should contain all primes appearing in the denominators of the $\ell_i P$; similarly for the T_2.

R_1 should contain primes that appear in the denominator of points ℓP for $\ell \neq \ell_i$; similarly for R_2.

Step 3: Construct S_1, S_2 with $S_1 \cup S_2 = \mathcal{P}$ and $S_1 \cap S_2 = \varnothing$.

Step 4: Let $x_n = x(nP)$ (the x-coordinate of nP). Let $A_1 := \{x_{\ell_1}, x_{\ell_2}, \cdots\}$ and $A_2 := \{x_{\ell_1'}, x_{\ell_2'}, \cdots\}$. Now the A_k are in bijection with $\mathbb{Z}$ just by the correspondence $x_{\ell_i} \leftrightarrow i$. The A_i are respectively diophantine over $\mathbb{Z}[S_i^{-1}]$, which depends heavily in the choice of prime sequences in step 1.

For steps 2 and 3, we need elliptic divisibility sequences: we have that $x_n = x(nP) = \dfrac{A_n}{B_n^2}$ with P on E of infinite order, such that $\gcd(A_n, B_n) = 1$, $B_n > 0$. We say that $B_1, B_2, \cdots$ is an elliptic divisibility sequence, so $B_n | B_m$ whenever $n | m$.

To define $R_1, R_2 (\cdots, R_t)$, need to show that denominators of points ℓP have many prime divisors (in order to choose enough primes to put into the R_i).

Definition 3. Let $(B_n)_{n \geq 1}$ be an elliptic divisibililty sequence for P. An integer $d > 1$ is a prime divisor of B_n if

- $d | B_n$
- $\gcd(d, B_m) = 1$ for all B_m with $0 < m < n$.

Theorem 1. *Let p be a prime, $q = p^{t-1}$ for $t > 1$. Let $Q \in E(\mathbb{Q})$ be a point of infinite order, $p = q \cdot Q$. Let B_n be an elliptic divisibility sequence for P. Then for every large enough n coprime to p the term B_n has at least t primitive divisors.*

For number fields, you have to talk about primitive prime *ideal* divisors, most everything else works the same (though there's some tricky combinatorics involved)