Hilber’s Tenth Problem: Recent Development

J'ignore • 9 Jul 2025

The famous Hilbert’s tenth problem concerns the decidablity for the problem of determining existence of solutions to systems of polynomial equations over various rings and fields. One of the case of most interest to number theorists is that over the integers, which has been shown in 1970s by Matiyasevich et al. that the answer is negative, i.e. there doesn’t exists an algorithm that can determine the solvability of an arbitrary diophantine equation (and one can even construct such a polynomial explicitly from the proof, see this mathoverflow answer). Roughly speaking the idea is that diophantine equations are rich and complex enough to simulate a computer. More precisely, call $A \subseteq \mathbb{Z}$ a *diophantine set* if there exists a (multivariate) polynomial $P(n, x_1, ...x_m)$ with integer coefficients such that

$$A = \{n \in \mathbb{Z} : P(n, \vec{x}) \text{ has a solution over } \mathbb{Z}^m\}.$$

It is easy to see every diophatine set is recursively enumerable (r.e.), i.e. there exists an computation procedure that prints every elements of A and nothing else. The upshot is that the converse is true, and the undecidability follows from that of the Halting’s Problem, a r.e. problem that is not decidable.

Other than $\mathbb{Z}$ another case of central interest is that over $\mathbb{Q}$. This amounts to a decision procedure for existence of rational points on an arbitrary variety, which is very hard and seems unlikely to exist in general. One path towards a negative solution is to show that $\mathbb{Z}$ is a diophantine subset of $\mathbb{Q}$, but assuming a very strong conjecture in arithmetic geometry, that is, the Bombieri-Lang conjecture, this is impossible, as shown in this paper by Koenigsmann (The primary goal of Koenigsmann is to show that $\mathbb{Q} \setminus \mathbb{Z}$ is diophatine!). For some reason the argument doesn’t appear in the publicated version. For the record let me sketch it below.

First we need the version of Bombieri-Lang from Hindry & Silverman’s Diophantine geometry, section F.5.2:

> Let X be a projective variety. The *special subset* Sp_X of X is the Zariski closure of the union of all images of nontrivial rational maps $A \dashrightarrow X$, where A is an abelian variety. If X is defined over a number field k, and let $U := X \setminus Sp_X$, the conjecture states that $U(k')$ is finite for every finite extension k'/k.

The intuition for this conjecture is that varieties of general type have few rational points (see this mathoverflow question for how to think of general type variety). In dimension one this is precisely Mordell's conjecture proved by Faltings. The version of Bombieri-Lang stated above is even stronger (By this answer, a variety of general type cannot be dominated by abelian varieties.), and essentially it states that almost all rational points are accounted by abelian varieties. (Note that projective spaces have a dense set of rational points, but of course they are dominated by product of $\mathbb{P}^1$, which is, in turn, dominated by elliptic curve.)

Assuming this conjecture, and using another result of Faltings on finiteness of integral points on $A \setminus D$ where A is an abelian variety and D is an ample divisor (see Corollary 6.2 of this paper), we easily conclude that if $V(\mathbb{Q})$ is Zariski dense in V for a hypersurface $V \subseteq \mathbb{A}^{n+1}$, then so is the subset of $V(\mathbb{Q})$ consisting of points with first coordinate in $\mathbb{Q} \setminus Z$, which implies that no infinine subset of $\mathbb{Z}$ can be a diophantine subset of $\mathbb{Q}$.

There is another conjecture by Mazur of topological flavour that also rules out $\mathbb{Z}$ being Diophantine over $\mathbb{Q}$. It states that the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has finitely many connected component.

Apart from $\mathbb{Q}$, people would also like to generalize the undecidability of polynomial equations to other rings of integers O_K of a number field K, such as the ring of Gaussian integers $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$. The crucial barrier is to prove the exponential relation $\{(a, b, c) \in \mathbb{N} : a = b^c\}$ is diophantine (which serves as a fundamental building block for showing other r.e. relations are diophantine). This step is done by Yuri Matiyasevich, and it uses the fact that the solution to Pell's equation $x^2 - dy^2 = 1$ form an abelian group of rank 1 (norm one elements of the algebraic torus $Res_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}\mathbb{G}_m$), which only works for certain fields (like totally real fields). The use of Pell's equation seems to related to Pell's number, which are numerators and denomiantors of solution to Pells equations, have exponential growth.

Therefore, instead of using Pell's equation (whose group of solutions may not have rank 1 over higher number fields), the idea of Poonen & Shlapentokh is to replace it with other finitely generated abelian groups, such as the group of rational points of elliptic curves. This line of attack probably goes back to Jan Denef, in particular this paper answering Hilbert's tenth problem over the function field $\mathbb{R}(t)$ in the negative. We will mention more about Hilbert's tenth problem over function fields in the future (hopefully).

The upshot is that they successfully reduce the Hilbert's tenth problems over an arbitrary ring of integers to a statement about existence of certain elliptic curves:

> (Shlapentokh, Theorem 1.9) If L/K is an extension of number fields and if there exists an elliptic curve E/K such that $rkE(K) = rkE(L) > 0$, then $\mathcal{O}_K$ is Diophantine over $\mathcal{O}_L$. In particular, if Hilbert's tenth problem over $\mathcal{O}_K$ has a negative answer, so is that over $\mathcal{O}_L$.

The intuition why this theorem is true is that the existence of such an elliptic curve allows us to 'assess' K since after killing all the torsion points defined over L we have $rE(K) = rE(L)$ for $r \gg 0$. See this for a simple proof in the special case where $rkE(K) = rkE(L) = 1$.

Finally for the climax, two separate groups of mathematicians have shown that the hypothesis to the above theorem indeed holds. One of the team (Peter Koymans and Carlo Pagano) uses 2-Selmer groups of elliptic curve (and a blackbox Green-Tao type result for number fields) and another one (Levent Alpöge, Manjul Bhargava, Wei Ho, and Ari Shnidman) uses l-Selmer groups of Jacobians of hyperelliptic curves (and also a result from additive combinatorics albeit more classical). More on this in the next post.

Edit: We give an outline as to how Matiyasevich showed the graph of $x = y^n$ is Diophatine (for anecdote see here). Using Pell's equation we can show that $\{\phi^n : n \in \mathbb{N}\} \subseteq \mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$ is diophantine. More generally, if $\mathcal{O} := \mathbb{Z}[t]/(t^2 - bt + 1)$, then we can take $\phi = \phi_b :=$ image of t. The key step is to show the graph $\{(n, \phi^n) : n \in \mathbb{N}\}$ is diophatine. The rough idea is that using the Bernoulli's identity $\phi^{kn} = 1 + k(\phi^n - 1) \mod (\phi^n - 1)^2$, we can get $k = \frac{\phi^{kn}-1}{\phi^n-1} \mod \phi^n - 1$. Along similar lines we can show a stronger lemma that $\{(b, n, \phi_b^n)\}$ is diophatine. Then

$$x = y^n \Leftrightarrow x \text{ is the nearest integer to } \frac{\phi_{yb}^n}{\phi_b^n}$$

for $b \gg y, n$. This is because $\phi_b = b - O(1/b)$. Using the exponential relation we can show lots of other relations are diophantine as well, e.g.

- coefficient of b^d in the base b expansion of $x = \lfloor \frac{x}{b^d} \rfloor \mod b$;
- $\binom{n}{k}$ is the coefficient of b^k in the base b expansion of $(b+1)^n$;
- $k! = \lfloor \frac{n^k}{\binom{n}{k}} \rfloor$ for $n > (k+1)^{k+2}$

Using these relations we can encode computation (e.g. we can now talk about sequences).