On the Hilbert’s tenth problem in finitely generated rings

Bogdan Grechuk • 19 Feb 2026

The newest issue of *Inventiones Mathematicae* features a remarkable paper by Alpöge, Bhargava, Ho, and Shnidman (Alpöge et al. 2026) that settles a vast generalization of Hilbert’s tenth problem: they prove that there is no algorithm to decide solvability of polynomial equations in *any* infinite commutative ring that is finitely generated over $\mathbb{Z}$.

In his celebrated 1900 list of problems, Hilbert asked for an algorithm that determines, for any multivariable polynomial

$$P(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n],$$

whether the Diophantine equation

$$P(x_1, \dots, x_n) = 0$$

has a solution in integers.

This is a well-posed computational problem: one is given a finite object (a polynomial), and one seeks a finite procedure to decide whether solutions exist. However, in 1970, Matiyasevich—building on foundational work of Davis, Putnam, and Robinson—proved that no such algorithm can exist. This result, now known as the Davis–Putnam–Robinson–Matiyasevich (DPRM) theorem, shows that Hilbert’s tenth problem over $\mathbb{Z}$ has a negative answer.

The same question can be asked over other number systems. For instance:

- Over $\mathbb{R}$, there *does* exist an algorithm: Tarski’s quantifier-elimination theorem implies that one can decide whether a system of polynomial equations and inequalities has a real solution.
- Over $\mathbb{Q}$, the problem remains one of the central open questions in number theory.

This naturally leads to a broader perspective: instead of restricting attention to $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, one may ask the same question over arbitrary rings.

Recall that a *ring* R is a set equipped with two operations, addition and multiplication, satisfying:

1. $(R, +)$ is an abelian group,
2. multiplication is associative and admits a multiplicative identity $1 \in R$,
3. distributivity holds:

$$a(b+c) = ab + ac, \qquad (b+c)a = ba + ca.$$

A ring is called *commutative* if $ab = ba$ for all $a, b \in R$.

A ring R is said to be *finitely generated over* $\mathbb{Z}$ if there exist elements

$$r_1, \dots, r_n \in R$$

such that every element $r \in R$ can be written in the form

$$r = P(r_1, \dots, r_n)$$

for some polynomial $P \in \mathbb{Z}[x_1, \dots, x_n]$.

In other words, R is obtained from $\mathbb{Z}$ by adjoining finitely many elements and taking all polynomial combinations of them.

Many familiar rings arise in this way:

- $\mathbb{Z}$ itself (generated by the empty set).
- Polynomial rings such as

  $$\mathbb{Z}[x], \qquad \mathbb{Z}[x, y],$$

  generated over $\mathbb{Z}$ by the indeterminates x (or x, y).
- Rings of the form

  $$\mathbb{Z}\left[\frac{1}{2}\right]$$

  generated by adjoining the element $1/2$.
- Quadratic integer rings such as
- $$\mathbb{Z}[\sqrt{2}], \qquad \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right].$$

  More generally, the ring of integers $\mathcal{O}_K$ of any number field K is finitely generated over $\mathbb{Z}$.

These examples show that finitely generated rings encompass a vast and natural class of arithmetic objects, including coordinate rings from algebraic geometry and rings arising in number theory.

Given any infinite commutative ring R, one may ask whether there exists an algorithm that determines, in a finite number of steps, whether a given polynomial equation with coefficients in R has a solution in R.

Matiyasevich's theorem answers this negatively for the special case $R = \mathbb{Z}$. The breakthrough of Alpöge, Bhargava, Ho, and Shnidman (Alpöge et al. 2026), and independently Koymans and Pagano (Koymans and Pagano 2024), is that the same phenomenon holds in dramatically greater generality.

Theorem 1 *Let R be any infinite commutative ring that is finitely generated over $\mathbb{Z}$. Then there is no algorithm that, given a multivariate polynomial P with coefficients in R, determines whether the equation $P = 0$ has a solution with all variables in R.*

In other words, undecidability is not a peculiarity of the integers: it is a universal feature of all infinite finitely generated rings.

Both sets of authors in fact established a special case: Hilbert's tenth problem has a negative answer in the ring of integers of *any* number field. The full strength of Theorem 1 follows from this result together with earlier work of Eisenträger (Eisenträger 2003), which shows how undecidability transfers from rings of integers of number fields to arbitrary infinite finitely generated rings.

References

Alpöge, Levent, Manjul Bhargava, Wei Ho, and Ari Shnidman. 2026. "Rank Stability in Quadratic Extensions and Hilbert's Tenth Problem for the Ring of Integers of a Number Field." *Invent. Math.* 243 (3): 1129–39. https://doi.org/10.1007/s00222-025-01392-3.

Eisenträger, Kirsten. 2003. "Hilbert's Tenth Problem and Arithmetic Geometry." PhD thesis, University of California, Berkeley.

Koymans, Peter, and Carlo Pagano. 2024. "Hilbert's Tenth Problem via Additive Combinatorics." *arXiv Preprint arXiv:2412.01768*.