

Write down a random polynomial equation in two or more variables with coefficients in the ring of integers, and—chances are—it will be very tricky to find all its solutions; often you will be quite challenged by the question of whether or not it *has* solutions.

Hilbert spurred mathematicians to systematically investigate the general question: *How solvable are such diophantine equations?* I will talk about this, and its relevance to specific number theoretic projects, and then aim towards some recent work, joint with Karl Rubin.

Hilbert formulated the question (his “10th Problem”) more specifically for systems of polynomial equations over the ring \mathbf{Z} of rational integers, but we can ask it for any ring. Explicitly, is there is an algorithm that has

- as input: any finite system of polynomial equations in many variables with coefficients in a ring R , and gives
- as output: the words *Yes* or *No* indicating whether or not the system has a solution in R ?

We don't know the answer to this for the extremely important special case of $R =$ the field of rational numbers. But, thanks to the classic theorem of Matiyasevic we know that for the ring of rational integers the question has a *negative* answer: There is no such algorithm that tells you whether a system of polynomial equations with rational integral coefficients has a solution in rational integers.

As for $R =$ the ring of integers in a specific number field K , here we are in a strange state of knowledge today: as a consequence of recent work, joint with Karl Rubin, we know that one of two things must go awry: Either

- Our long-conjectured algorithm for the determination of rational points on elliptic curves over K is incorrect (and incorrect in a big way!) or
- There is no algorithm that tells you whether a system of polynomial equations with the ring of integers of K has a solution in that ring.

I will describe the background for these results, and some of the new open problems that seem interesting to investigate.