

- Diophantine sets (eg  $\mathbb{N}$ , cf. Lagrange's Theorem)
- Listable sets (eg the set of integers expressible as a sum of three cubes) – the source of undecidability

Diophantine sets are also listable – same approach with boxes! Even more, the converse is true: Davis-Putnam-Robinson-Matiyasevich proved that diophantine  $\Leftrightarrow$  listable. Thus, the theory of diophantine equations is rich enough to simulate any computer.

The unsolvability of the Halting Problem provides a listable set for which no algorithm can decide membership.

Thus, there exists a diophantine set for which no algorithm can decide membership – Hilbert 10th problem has a negative answer.

- Beyond H10, there are applications of diophantine  $\Leftrightarrow$  listable to the search of prime-producing polynomials and investigation of diophantine statement of the Riemann Hypothesis.
- There is a trick allowing to reduce any diophantine equation to one of degree 4 at most.
- Jones - Sato - Wada - Wiens: the set of primes equals the set of positive values assumed by the 26-variable polynomial.
- The DPRM theorem gives an explicit polynomial equation that has a solution if and only if the Riemann Hypothesis is false.

A computer program can be written such that, if left running forever, it will output a counterexample to the Riemann hypothesis if one exists – this program can be simulated by a diophantine equation!

**Question.** What is the complexity of conversion between a computer program and a diophantine equation?

- Ring of integers of a number field  $k$ :  $\mathcal{O}_k = \{\alpha \in k \mid f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}$
- Conjecture: H10/ $\mathcal{O}_k$  has a negative answer for every number field  $k$ .
- What about H10 over  $\mathbb{Q}$ ? The answer is not known! If  $\mathbb{Z}$  is diophantine over  $\mathbb{Q}$ , then the negative answer for  $\mathbb{Z}$  implies a negative answer for  $\mathbb{Q}$ . However, there is a conjecture (cf. Mazur 1992) that implies that  $\mathbb{Z}$  is not diophantine over  $\mathbb{Q}$ . There was no progress on the conjecture for the varieties beyond the dimension 1.
- H10 is also about the truth of **positive existential sentences**:

$$(\exists x_1 \exists x_2 \cdots \exists x_n) p(x_1, x_2, \dots, x_n)$$

- Robinson, Poonen, Koenigsmann  $\Rightarrow$  Robinson: There is no algorithm to decide the truth of a first-order sentence over  $\mathbb{Q}$ .
- Koenigsmann 2016:  $\mathbb{Q} \setminus \mathbb{Z}$  is diophantine over  $\mathbb{Q}$ .