

Why number theory is hard

Bjorn Poonen

University of California at Berkeley

March 15, 2007

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

What is number theory?

Why number theory is hard

Bjorn Poonen

- **Number theory** is the branch of mathematics that was developed to study properties of

- **Integers:**

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

- **Rational numbers:** (ratios of integers, like $-3/5$, $2/7$)

$$\mathbb{Q} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}.$$

- It is one of the oldest branches of mathematics, originating in the work of the ancient Babylonians and Greeks, and (independently somewhat later) the Chinese and Indians.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Applications of number theory

Although number theory was originally studied for its own sake (and often still is), it motivated the development of mathematical theories that later turned out to have important applications:

- **Error-correcting codes:** essential for CD players, satellite communications, . . .
- **Cryptography:** security for electronic banking, online use of credit cards, digital signatures, . . .

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Some famous problems about integers

Why number theory is hard

Bjorn Poonen

Much of number theory is ultimately motivated by problems about the solutions to *equations* in which the variables represent unknown integers, sometimes required to satisfy additional restrictions.

- **Fermat's last theorem:** The equation $x^n + y^n = z^n$ has no solution in positive integers x, y, z, n with $n > 2$.
(proved)
- **Goldbach conjecture:** Given an even integer $a \geq 4$, the equation $x + y = a$ has a solution in prime numbers.
- **Twin primes conjecture:** There exist infinitely many pairs of primes (p, q) satisfying $p + 2 = q$.
- **Sums of three cubes conjecture:** If a is an integer not of the form $9n + 4$ or $9n + 5$, then $x^3 + y^3 + z^3 = a$ has a solution in integers x, y, z .

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 29?$$

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 29?$$

Yes: $(x, y, z) = (3, 1, 1)$.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 30?$$

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Why number theory is hard

Bjorn Poonen

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 30?$$

Yes: $(x, y, z) = (-283059965, -2218888517, 2220422932)$.

(discovered in 1999 by E. Pine, K. Yarbrough, W. Tarrant, and M. Beck, following an approach suggested by N. Elkies.)

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 33?$$

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Do there exist integers x, y, z such that

$$x^3 + y^3 + z^3 = 33?$$

Unknown.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Examples of polynomial equations

Why number theory is hard

Bjorn Poonen

Do there exist integers x, y, z such that

$$\begin{aligned} & 536x^{287196896} - 210y^{287196896} + 777x^3y^{16}z^{4732987} \\ & - 1111x^{54987896} - 2823y^{927396} + 27x^{94572}y^{9927}z^{999} \\ & - 936718x^{726896} + 887236y^{726896} - 9x^{24572}y^{7827}z^{13} \\ & + 89790876x^{26896} + 30y^{26896} + 987x^{245}y^6z^{6876} \\ & + 9823709709790790x^{28} - 1987y^{28} + 1467890461986x^2y^6z^4 \\ & + 80398600x^2z^{12} - 27980186xy + 3789720156y^2 + 9328769x \\ & - 1956820y - 27589324985727098790768645846898z = 389? \end{aligned}$$

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Hilbert's tenth problem

D. Hilbert, in the 10th of the list of 23 problems he published after a famous lecture in 1900, asked his audience to find a method that would answer all such questions.

Hilbert's tenth problem (H10)

Find an algorithm that solves the following problem:

input: *a multivariable polynomial $f(x_1, \dots, x_n)$ with integer coefficients*

output: *YES or NO, according to whether there exist integers a_1, a_2, \dots, a_n such that $f(a_1, \dots, a_n) = 0$.*

He wanted the algorithm to be as mechanical as, say, the grade-school algorithm for multiplying integers. It should require no insight on the part of the user.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

What is an algorithm?

- In 1900 there was no formal notion of algorithm.
- In the 1930s, several definitions were proposed (lambda-definable functions, recursive functions, functions computable by a Turing machine), and were shown to be equivalent. A **Turing machine** is essentially what we could call a computer, except idealized in that it never crashes, never runs out of memory, etc.
- The equivalence led people to accept the following belief:

Church-Turing thesis

Any function that can be computed by a purely mechanical procedure can be computed by a Turing machine.

- Now H10 could be formulated precisely, by asking for a *Turing machine* that could decide the solvability of a multivariable polynomial equation in integers.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Hilbert's tenth problem (H10)

Find a Turing machine that solves the following problem:

input: $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$

output: YES or NO, according to whether there exists $\vec{a} \in \mathbb{Z}^n$ with $f(\vec{a}) = 0$.

More generally, one could ask for an algorithm for solving a **system** of polynomial equations, but this would be equivalent, since

$$f_1 = \dots = f_m = 0 \iff f_1^2 + \dots + f_m^2 = 0.$$

Theorem (Davis-Putnam-Robinson 1961 + Matijasevič 1970)

No such algorithm exists.

This is what I mean by “number theory is hard”.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

The halting problem

Why number theory is hard

Bjorn Poonen

Computer programs sometimes enter infinite loops.

Halting problem

Construct a *debugger*, a procedure $D(p, x)$ that can detect whether a program will enter an infinite loop when fed a given input:

input: a computer program p , and input x to the program

output: *HALTS* if p with input x eventually stops, *LOOPS* if it enters an infinite loop.

An early result of computer science (Turing, 1936) states that no such debugger exists:

The halting problem is unsolvable.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Proof that the halting problem is unsolvable

Why number theory is hard

Bjorn Poonen

- We will use an encoding of programs as nonnegative integers, and hence identify programs with numbers.
- Suppose that there *were* a debugger $D(p, x)$.
- Then we could write a new program T such that for any input x ,

T halts on input $x \iff$ program x does not halt on input x .

- Taking $x = T$, we find a contradiction:

T halts on input $T \iff T$ does not halt on input T .

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Recursive sets

Let A be a set of integers (a subset of \mathbb{Z}).

Definition

A is called **recursive** if there is an algorithm for deciding membership in A :

input: $a \in \mathbb{Z}$

output: *YES* if $a \in A$, *NO* otherwise

Example

The set of prime numbers is recursive.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

DPRM

Prime-producing polynomials

Riemann hypothesis

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Listable sets vs. recursive sets

Why number theory is hard

Bjorn Poonen

Definition

A is **listable** (**recursively enumerable**) if there is a Turing machine such that A is the set of integers that it prints out when left running forever.

Example

The set of integers expressible as a sum of three cubes is listable.

(Print out $x^3 + y^3 + z^3$ for all $|x|, |y|, |z| \leq 10$, then print out $x^3 + y^3 + z^3$ for $|x|, |y|, |z| \leq 100$, and so on.)

It is not known whether this set is recursive.

But it *is* known that there is a listable set is not recursive: one such set is the set of ASCII codes of programs that halt.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Diophantine sets

Why number theory is hard

Bjorn Poonen

Definition

A is **diophantine** if there exists

$$p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \dots, x_m]$$

such that

$$A = \{a \in \mathbb{Z} : (\exists \vec{x} \in \mathbb{Z}^m) p(a, \vec{x}) = 0\}.$$

Example

The subset $\mathbb{N} := \{0, 1, 2, \dots\}$ of \mathbb{Z} is diophantine, since for $a \in \mathbb{Z}$,

$$a \in \mathbb{N} \iff (\exists x_1, x_2, x_3, x_4 \in \mathbb{Z}) x_1^2 + x_2^2 + x_3^2 + x_4^2 - a = 0.$$

If H10 had a positive answer, then *every diophantine set would be recursive*.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Negative answer to H10

Why number theory is hard

Bjorn Poonen

Recall from the past two slides:

- There exists a listable set that is not recursive.
- If H10 had a positive answer, every diophantine set would be recursive.

What Davis-Putnam-Robinson-Matijasevič really proved is:

DPRM theorem: Diophantine \iff listable

(They showed that the theory of diophantine equations is rich enough to simulate any computer!)

Therefore

- There exists a *diophantine* set that is not recursive.
- H10 has a negative answer.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Summary

Why number theory is hard

Bjorn Poonen

To paraphrase this lecture so far:

- Understanding the behavior of computer programs is hard. (The halting problem is unsolvable.)
- Any computer program can be “simulated” by a diophantine equation; thus the halting problem is embedded as a subproblem of H10.
- Since the halting problem is unsolvable, H10 must be unsolvable too.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

More fun consequences of the DPRM theorem

Why number theory is hard

Bjorn Poonen

“Diophantine \iff listable” has applications beyond the negative answer to H10:

- Prime-producing polynomials
- Diophantine statement of the Riemann hypothesis

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Prime-producing polynomials

Why number theory is hard

Bjorn Poonen

Theorem

There is a multivariable polynomial F such that the positive integers in its range (as a function $\mathbb{N}^n \rightarrow \mathbb{Z}$) are exactly the prime numbers.

Proof:

- By DPRM, the set of prime numbers is diophantine.
- Thus there is a polynomial $f(t, x_1, \dots, x_n)$ such that for each $a \in \mathbb{Z}$, the equation $f(a, x_1, \dots, x_n) = 0$ is solvable if and only if a is a prime number.

- Define a new polynomial

$$F(t, x_1, \dots, x_n) = t(1 - 2f(t, x_1, \dots, x_n)^2).$$

- If particular nonnegative integers t, x_1, \dots, x_n are plugged into F , the value will be ≤ 0 except possibly if $f(t, x_1, \dots, x_n) = 0$, in which case the value is t .
- The integers t for which $f(t, x_1, \dots, x_n) = 0$ is a possibility are exactly the primes.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

The set of primes equals the set of positive values assumed by the 26-variable polynomial

$$\begin{aligned}
 & (k+2)\{1 - ([wz + h + j - q]^2 \\
 & + [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
 & + [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\
 & + [2n + p + q + z - e]^2 + [e^3(e+2)(a+1)^2 + 1 - o^2]^2 \\
 & + [(a^2 - 1)y^2 + 1 - x^2]^2 + [16r^2y^4(a^2 - 1) + 1 - u^2]^2 \\
 & + [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\
 & + [(a^2 - 1)\ell^2 + 1 - m^2]^2 \\
 & + [ai + k + 1 - \ell - i]^2 + [n + \ell + v - y]^2 \\
 & + [p + \ell(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
 & + [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
 & + [z + p\ell(a - p) + t(2ap - p^2 - 1) - pm]^2\}
 \end{aligned}$$

as the variables range over nonnegative integers
(J. Jones, D. Sato, H. Wada, D. Wiens).

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

Riemann hypothesis

The DPRM theorem gives an explicit polynomial equation that has a solution in integers if and only if the Riemann hypothesis is false.

Proof:

- One can write a computer program that, when left running forever, will detect a counterexample to the Riemann hypothesis if one exists: The *argument principle* implies that for any rectangle γ inside the strip $1/2 < \operatorname{Re} s < 1$, the expression

$$\frac{1}{2\pi i} \int_{\gamma} \frac{\zeta'(s)}{\zeta(s)}$$

counts zeros of $\zeta(s)$ inside γ ; approximate this numerically for every such rectangle γ with rational vertices, and halt if one of these values is provably greater than $1/2$ in absolute value.

- Simulate this program with a diophantine equation.

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

H10 over other rings

Why number theory is hard

Bjorn Poonen

Many problems surrounding Hilbert's tenth problem remain to be solved.

- For instance, it is not known whether there exists an algorithm that decides whether a multivariable polynomial equation has a solution in *rational numbers*.
- One can also consider the solvability problem for other fields or rings.

Some later talks in this conference will consider these problems.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

First-order theory

Why number theory is hard

Bjorn Poonen

- From the point of view of mathematical logic, H10 asks for an algorithm to decide the truth of *positive existential sentences*

$$(\exists x_1 \exists x_2 \cdots \exists x_n) p(x_1, \dots, x_n) = 0.$$

in the language of rings.

- More generally, one can ask for an algorithm to decide the truth of arbitrary *first-order sentences*, in which any number of bound quantifiers \exists and \forall are permitted: a typical such sentence is

$$(\exists x)(\forall y)(\exists z)(\exists w) \quad (x \cdot z + 3 = y^2) \vee \neg(z = x + w)$$

- Even though it is not yet known whether H10 over \mathbb{Q} is unsolvable, J. Robinson proved that the harder problem, for first-order sentences, is unsolvable.

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge

| Ring | H10 | 1st order theory |
|---|-----|------------------|
| \mathbb{C} | YES | YES |
| \mathbb{R} | YES | YES |
| \mathbb{F}_q | YES | YES |
| p -adic fields | YES | YES |
| $\mathbb{F}_q((t))$ | ? | ? |
| number field | ? | NO* |
| \mathbb{Q} | ? | NO* |
| global function field | NO | NO |
| $\mathbb{F}_q(t)$ | NO | NO |
| $\mathbb{C}(t)$ | ? | ? |
| $\mathbb{C}(t_1, \dots, t_n), n \geq 2$ | NO | NO |
| $\mathbb{R}(t)$ | NO | NO |
| \mathcal{O}_k | ? | NO* |
| \mathbb{Z} | NO* | NO |

increasing arithmetic complexity \downarrow

Why number theory is hard

Bjorn Poonen

Number theory

What is it?

Applications

Famous problems

Polynomial equations

H10

Algorithms

Number theory is hard

Computer science

Halting problem

Recursive sets

Listable sets

Negative answer to H10

H10

Diophantine sets

DPRM theorem

Summary

Consequences of DPRM

Prime-producing polynomials

Riemann hypothesis

Related problems

H10 over other rings

First-order sentences

Status of knowledge