HILBERT'S TENTH PROBLEM OVER RINGS OF NUMBER-THEORETIC INTEREST

BJORN POONEN

Contents

1. Introduction

This article is a survey about analogues of Hilbert's Tenth Problem over various rings, especially rings of interest to number theorists and algebraic geometers. For more details about most of the topics considered here, the conference proceedings [DLPVG00] is recommended.

2. The original problem

Hilbert's Tenth Problem (from his list of 23 problems published in 1900) asked for an algorithm to decide whether a diophantine equation has a solution. More precisely, the input and output of such an algorithm were to be as follows:

input: a polynomial $f(x_1, \ldots, x_n)$ having coefficients in $\mathbb{Z}$

Date: February 28, 2003.

These notes form the basis for a series of four lectures at the Arizona Winter School on "Number theory and logic" held March 15–19, 2003 in Tucson, Arizona. The author was supported by a Packard Fellowship.

output: YES or NO, according to whether $\exists \vec{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ with $f(\vec{a}) = 0$.

Matijasevič [Mat70], building on earlier work of Davis, Putnam, and Robinson [DPR61], showed that no such algorithm exists.

3. Turing machines and decision problems

To make sense of this negative result, we need a precise notion of algorithm. In Hilbert's time, a mathematically precise notion had not yet been developed. In the 1930s, several rigorous models of computation were proposed, one of which was the Turing machine. These were soon proved to be equivalent, in terms of what they could compute. This made believable the *Church-Turing thesis*, which is the assertion that every purely mechanical procedure can be carried out by a Turing machine. Because of this, "algorithm" will be taken to mean "Turing machine".

An informal description of a Turing machine may be more enlightening than a mathematically precise definition. (For the latter, see [HU79].) A Turing machine is equivalent to a finite-length program (in C++, say) running on a physical computer, except that the computer is not subject to physical errors (such as data loss from power outages) and its memory is unlimited. In the model, the memory is sometimes taken as an infinite tape, initialized to the binary representation of the nonnegative integer input, such as

$\cdots$	0	0	0	0	0	1	1	0	1

or to all zeros if there is no input. During the operation of the computer, it reads and writes characters to the memory tape, and may or may not print characters on a separate output tape, following the rules of its program. It might run forever, or it might halt when some condition specified by the program is satisfied.

We can consider Turing machines accepting other objects as input if we fix an encoding of these objects as nonnegative integers. For example, a polynomial with integer coefficients could be represented by the concatenation of the ASCII codes of the characters in a TEX file giving the polynomial. The exact encoding procedure does not matter, as long as a Turing machine can convert between the proposed encodings.

Definition 3.1. A *decision problem* is simply a subset S of the possible inputs. We say that a Turing machine *solves the decision problem* S if

(1) for each possible input, it halts after a finite number of steps; and
(2) when it halts, the content of the output tape is "YES" if the input belonged to S, and "NO" otherwise.

Remark 3.2. Each Turing machine can be encoded by a nonnegative integer, namely the ASCII code for the C++ program. Thus there are only countably many Turing machines. On the other hand, there are uncountably many decision problems, so some decision problems cannot be solved by Turing machines.

The modern interpretation of Hilbert's Tenth Problem is that it asks whether there exists a Turing machine that can solve the decision problem where the input is a multivariable polynomial equation, and S is the set of such polynomial equations that have a solution in integers.

4. Recursive and listable sets

Definition 4.1. A subset $S \subseteq \mathbb{Z}$ is called *recursive* if there exists an algorithm (Turing machine) with input and output as follows:

input: an integer n
output: YES or NO, according to whether $n \in S$.

Remark 4.2. Although the algorithm is required to halt on every input, there is no requirement on the running time of the algorithm. If for a given decision problem, there exists an algorithm whose running time is bounded by some polynomial function of the bit length of the input, then the problem is said to belong to the class P. For example, it is obvious that the set of prime numbers is recursive, but it is a nontrivial theorem [AKS02] that this decision problem is in P.

Remark 4.3. Quantum computers cannot solve any more decision problems than Turing machines, because they can be *simulated* by Turing machines. A difference in computational power can exist only when running times are taken into account: the simulation of an n-step quantum computation seems to require an exponential number of steps on a Turing machine, so it is conjectured that the class QP of problems solvable by a quantum computer in polynomial time is strictly larger than P.

Definition 4.4. A subset $S \subseteq \mathbb{Z}$ is called *listable* or *recursively enumerable* if there is a Turing machine such that S is the set of integers that it prints out when left running forever.

Remark 4.5. The definition of listable is unchanged if we insist that the Turing machine print each element of S exactly once: if there is a Turing machine T that prints exactly the elements of S, but possibly prints some elements many times, one can find another Turing machine T' that prints the same elements, but each exactly once. Namely, T' can mimic the operation of T, but store in a table the integers that have been printed so far, and censor the output of T whenever T would have printed an integer that is already in the table.

Proposition 4.6. *Every recursive subset $S \subseteq \mathbb{Z}$ is listable.*

Proof. We are given a Turing machine T that decides membership in S. Construct a new Turing machine T' that applies T to test 0, 1, -1, 2, -2, ... for membership in S, in order, printing those integers n for which T shows that $n \in S$. Since T spends only a finite amount of time testing each integer, running T' forever eventually prints out all elements of S, and nothing else. □

Example 4.7. Let

$$S = \{\, a \in \mathbb{Z} : \exists x, y, z \in \mathbb{Z} \text{ such that } x^3 + y^3 + z^3 = a \,\}.$$

Then S is listable, since one can write a program that loops over $B = 1, 2, \ldots$ and for each B, loops over x, y, z in the range $-B$ to B, and computes and prints $x^3 + y^3 + z^3$. It is unknown whether S is recursive! (It has been conjectured that $S = \{\, a \in \mathbb{Z} : a \not\equiv \pm 4 \pmod 9 \,\}$; if this were true, then of course S would be recursive.)

5. The Halting Problem

The *Halting Problem* asks whether there exists a Turing machine with input and output as follows:

input: a computer program p and integer x. (The program can be encoded as a nonnegative integer for input into the Turing machine.)
output: YES or NO, according to whether the program eventually halts (instead of entering an infinite loop) when run on input x.

Theorem 5.1 (Turing)**.** *The Halting Problem is undecidable; that is, no Turing machine can solve it.*

Proof. We will use an encoding of programs as nonnegative integers, and identify programs with numbers. Suppose there were an algorithm for deciding when program p halts on input x. Then we could write a new program H such that

$$H \text{ halts on input } x \quad \Longleftrightarrow \quad \text{program } x \text{ does not halt on input } x.$$

Taking $x = H$, we find a contradiction: H halts on input H if and only if H does not halt on input H. □

Corollary 5.2. *There exists a listable set that is not recursive.*

Proof. Let S be the set of numbers $2^p 3^x$ such that program p halts on input x. By Theorem 5.1, S cannot be recursive. On the other hand, we can write a program that eventually lists all elements of S: loop over $N = 1, 2, \ldots$, and during iteration N, for each $p, x \leq N$, run program p on input x for N steps, and print $2^p 3^x$ if it halts within these N steps. Hence S is listable. □

6. Diophantine sets

Definition 6.1. A subset $S \subseteq \mathbb{Z}^n$ is *diophantine* if there is a polynomial

$$p(\vec{t}, \vec{x}) \in \mathbb{Z}[t_1, \ldots, t_n, x_1, \ldots, x_m]$$

such that

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

Example 6.2. The subset $\mathbb{N} := \{0, 1, 2, \ldots\}$ of $\mathbb{Z}$ is diophantine, since for $a \in \mathbb{Z}$,

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

Example 6.3. The subset $\mathbb{Z} - \{0\}$ of $\mathbb{Z}$ is diophantine, because every nonzero integer is the product of an integer coprime to 2 and an integer coprime to 3: we have

$$\begin{aligned} a \neq 0 \quad &\Longleftrightarrow \quad (\exists b, c \in \mathbb{Z}) \quad a = bc \ \wedge\ (b, 2) = (1) \ \wedge\ (c, 3) = (1) \\ (b, 2) = (1) \quad &\Longleftrightarrow \quad (\exists p, q \in \mathbb{Z}) \quad bp + 2q = 1 \\ (c, 3) = (1) \quad &\Longleftrightarrow \quad (\exists r, s \in \mathbb{Z}) \quad cr + 3s = 1. \end{aligned}$$

so

$$a \neq 0 \quad \Longleftrightarrow \quad (\exists b, c, p, q, r, s \in \mathbb{Z}) \quad (a - bc)^2 + (bp + 2q - 1)^2 + (cr + 3s - 1)^2 = 0.$$

(Alternatively, one could make use of $\mathbb{Z} - \{0\} = \mathbb{Z}_{>0} \cup \mathbb{Z}_{<0}$, and prove that a union of two diophantine subsets of $\mathbb{Z}$ is diophantine, but the first method we used generalizes more easily to rings of integers of arbitrary number fields.)

Earlier we defined "listable" only for subsets of $\mathbb{Z}$, but the same definition makes sense for subsets of $\mathbb{Z}^n$. Diophantine subsets of $\mathbb{Z}^n$ are listable: an example of this was already given in Example 4.7, and the same proof works in general.

Much deeper is the fact that the converse holds; this very important result was conjectured by M. Davis:

Theorem 6.4 (Davis-Putnam-Robinson and Matijasevič)**.** *A subset of $\mathbb{Z}^n$ is diophantine if and only if it is listable.*

We will refer to Theorem 6.4 as the DPRM Theorem; a proof will be sketched in the next section. For now, we give some corollaries.

Corollary 6.5. *Hilbert's Tenth Problem has a negative answer.*

Proof. By Corollary 5.2, there exists a subset $S \subseteq \mathbb{Z}$ that is listable but not recursive. By Theorem 6.4, S is diophantine, so there exists a polynomial $p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \ldots, x_m]$ such that

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

If the answer to Hilbert's Tenth Problem were positive, then in particular, we would have an algorithm that could decide, given $a \in \mathbb{Z}$, whether $p(a, \vec{x}) = 0$ has a solution $\vec{x} \in \mathbb{Z}^n$. In other words, we would be able decide whether a given integer a belongs to S. This contradicts the fact that S is not recursive. □

Before the DPRM Theorem was proved, it was known that it would have also the following amusing corollary. Some people at the time viewed this as evidence *against* the DPRM Theorem.

Corollary 6.6 (Prime-producing polynomials)**.** *There exists a polynomial $F \in \mathbb{Z}[x_1, \ldots, x_n]$ such that*

$$\{\, F(\vec{a}) : \vec{a} \in \mathbb{Z}^n \,\} \cap \mathbb{Z}_{>0}$$

is exactly the set of prime numbers.

Proof. The set P of primes is listable. By Theorem 6.4, it is therefore diophantine, so there exists a polynomial $p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \ldots, x_m]$ such that

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

Then the polynomial

$$F(y_1, y_2, y_3, y_4, \vec{x}) := (1 - p(y_1^2 + y_2^2 + y_3^2 + y_4^2, \vec{x})^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

has the desired property: $F(y_1, y_2, y_3, y_4, \vec{x})$ will be positive exactly when $p(y_1^2 + y_2^2 + y_3^2 + y_4^2, \vec{x}) = 0$, which for given $y_1, \ldots, y_4$ is possible if and only if $y_1^2 + y_2^2 + y_3^2 + y_4^2$ is prime; in this case the value of F is that prime. □

7. Outline of proof of the DPRM Theorem

The proof of the DRPM theorem we outline is not the original one; it has been simplified over the years by many authors. We need a few definitions.

Definition 7.1. A function $\mathbb{Z}^n \to \mathbb{Z}^m$ is *diophantine* if and only if its graph is a diophantine subset of $\mathbb{Z}^{n+m}$. Similarly one can say what it means for a relation to be diophantine.

Definition 7.2. An *exponential polynomial* is an expression built up from positive integers and variables using addition, multiplication, and exponentiation.

Example 7.3. The expression $2x^{3y^x z+x^2}+5$ is an exponential polynomial.

Definition 7.4. A subset $S \subseteq \mathbb{Z}_{>0}^n$ is *exponential diophantine* if there are exponential polynomials E_1, E_2 in variables $t_1, \ldots, t_n, x_1, \ldots, x_m$ such that

$$S = \{\, \vec{a} \in \mathbb{Z}_{>0}^n : (\exists \vec{x} \in \mathbb{Z}_{>0}^m)\ E_1(\vec{a}, \vec{x}) = E_2(\vec{a}, \vec{x}) \,\}.$$

The proof of the DPRM Theorem now proceeds as follows:

(1) Show that exponentiation is diophantine. More precisely, the 3-variable relation $a = b^c$ (restricted to positive integers, say) is diophantine. Historically, this part came last. This part of the proof is purely number-theoretic, and is the trickiest, even though the number theory involved is elementary. It uses nothing deeper than the fact that the Pell equation $x^2 - dy^2 = 1$ for nonsquare $d \in \mathbb{Z}_{>0}$ has infinitely many solutions in positive integers.

(2) Using the fact that exponentiation is diophantine, show that various other number-theoretic relations are diophantine. For example, the 3-variable binomial coefficient relation $c = \binom{a}{b}$ is diophantine. The 2-variable relation $a \preceq b$ saying that the locations of the 1's in the binary representation of a are a subset of the locations for b is diophantine: an 1852 theorem of Kummer states that $a \preceq b$ if and only if $\binom{b}{a}$ is odd. This step involves more elementary number theory.

(3) Using the "subroutines" built in the previous step, show that there are exponential polynomials E_1 and E_2 such that program t eventually prints u if and only if there exists $\vec{x} = (x_1, \ldots, x_m)$ with $E_1(t, u, \vec{x}) = E_2(t, u, \vec{x})$. To do this, x_1 could for example represent the number of steps in a partial computation, and some of the other variables x_i could encode the the complete operation of the Turing machine during the first x_1 steps, and the exponential equation should say imply these x_i are such that they represent a valid computation that results in program t printing u in step x_1. (Actually, it is easier to work with *register machines* instead of Turing machines: this is another model of computation, whose operation is easier to model by exponential equations, but which is equivalent in computational power.)

For more details, see the exposition in [JM91].

8. First order formulas

In this section we reinterpret some of the earlier concepts using terminology of first order logic. For a precise definition of "first order formula" and so on, see Chapter II of [EFT94].

Loosely speaking, a *first order formula in the language of rings* is an expression built up from the symbols $+, \cdot, 0, 1, =, (,)$, the logical relations $\wedge$ ("and"), $\vee$ ("or"), $\neg$ ("not"), the quantifers $\forall$ ("for all") and $\exists$ ("there exists"), and variables $x, y, z, \ldots$. For instance,

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

is a first order formula. In this example, the variables y, z, w are *bound* by quantifiers, and the variable x is free. A first order formula in which all variables are bound by quantifiers is called a *first order sentence*.

If a first order formula is of the form

$$(\exists x_1)(\exists x_2)\dots(\exists x_n)\ S$$

where S is a combination of equations involving $+, \cdot, 0, 1, =, \wedge, \vee$ and variables but no quantifiers and no $\neg$, then it is called a *positive existential formula*. If moreover S consists of a single equation (no logical operators), then this first order formula is called a *diophantine formula*.

Let R be any ring. (All our rings are commutative with 1.) A first order sentence has a truth value obtained by interpreting it in the usual way, letting the bound variables run over the elements of R. On the other hand, if $\phi(x_1, \dots, x_n)$ is only a first order formula (where $x_1, \dots, x_n$ are the free variables), then we get a truth value $\phi(a_1, \dots, a_n)$ only after values $a_i \in R$ are substituted for the x_i. Thus a first order formula ϕ with n free variables defines a subset of R^n, namely $\{\, \vec{a} \in R^n : \phi(a_1, \dots, a_n) \,\}$.

Definition 8.1. A subset of R^n arising in this way from a positive existential (resp. diophatine) formula is called *positive existential over R* (resp. *diophantine over R*).

Example 8.2. The notion of "a subset that is diophantine over $\mathbb{Z}$" agrees with the definition of "diophantine subset of $\mathbb{Z}^n$" given in Section 6.

Remark 8.3. Adding a symbol for $-$ does not change the notion of positive existential set or diophantine set, since $x - y = z$ is equivalent to $x = y + z$.

Remark 8.4. The collection of positive existential subsets of R^n is closed under finite unions and intersections.

Occasionally we may consider the notions above where the language of rings is supplemented by symbols for certain elements of R. For example, if $R = \mathbb{Z}[t]$, then we might allow equations involving the symbol "t".

Proposition 8.5. *Let R be a ring for which there exist polynomials $f(x, y), g(x, y) \in R[x, y]$ such that for $a, b \in R$,*

$$f(a, b) = 0 \quad \Longleftrightarrow \quad a = 0 \text{ and } b = 0,$$
$$g(a, b) = 0 \quad \Longleftrightarrow \quad a = 0 \text{ or } b = 0.$$

If the language is supplemented with enough symbols for elements that the coefficients of f and g can be expressed in terms of these elements, then the collection of positive existential sets equals the collection of diophantine sets.

Proof. The nontrivial part is to show that positive existential sets are diophantine. We transform an arbitrary positive existential formula into a diophantine formula defining the same subset by repeatedly performing the following operations:

- Transform each polynomial equation $p = q$ to $p - q = 0$.
- Transform each conjunction of polynomial equations $(p = 0) \wedge (q = 0)$ to $f(p, q) = 0$.
- Transform each disjunction of polynomial equations $(p = 0) \vee (q = 0)$ to $g(p, q) = 0$.

□

Corollary 8.6. *If R is an integral domain whose fraction field K is not algebraically closed, then the collection of positive existential sets equals the collection of diophantine sets, provided that enough symbols for constants have been added to the language.*

Proof. We apply Proposition 8.5. Take $g(x, y) = xy$. Choose a nontrivial finite extension K' of K, let $\{\alpha, \beta\}$ be part of a K-basis of K', and let $f(x, y) = rN_{K'/K}(\alpha x + \beta y)$ where $N_{K'/K}$ denotes the norm, and $r \in R - \{0\}$ is chosen to clear denominators, so that f has coefficients in R. This works provided that enough symbols have been added to the language so that the coefficients of f are expressible in terms of the elements of R represented by these symbols. □

Definition 8.7. The *first order theory* (resp. *positive existential theory*) of R in the language of rings is the set of first order sentences (resp. positive existential sentences) in the language that are true when the variables are considered to run over elements in R. ("First order theory" is often abbreviated to "theory".) The theory (resp. positive existential theory) is called *decidable* if there is a Turing machine that takes as input a first order sentence (resp. positive existential sentence) and decides whether it belongs to the theory.

Remark 8.8. These definitions make sense also for languages supplemented by a finite collection of symbols. (They might make sense for some languages with countably many symbols as well, but in this case, one must take care to specify how the sentences are encoded as integers for input into the Turing machine.)

By Corollary 8.6, to say that Hilbert's Tenth Problem has a negative answer is equivalent to the statement that the positive existential theory of $\mathbb{Z}$ (in the language of rings) is undecidable.

9. Generalizing Hilbert's Tenth Problem to other rings

Definition 9.1. Let R be a ring.

(1) *Hilbert's Tenth Problem over R* asks whether there exists an algorithm with input and output as follows:
   input: $f \in \mathbb{Z}[x_1, \ldots, x_n]$
   output: YES or NO, according to whether $(\exists \vec{a} \in R^n)\ f(\vec{a}) = 0$. (There is a unique ring homomorphism $\mathbb{Z} \to R$, so it makes sense to evaluate f at elements of R.)

(2) If $S \subseteq R$, then *Hilbert's Tenth Problem over R with coefficients in S* is the same as above, except that f has coefficients in S instead of $\mathbb{Z}$; this terminology assumes that an encoding of elements of S has been specified.

An argument similar to that proving Corollary 8.6 implies that for many rings R, Hilbert's Tenth Problem over R is equivalent to asking whether the positive existential theory of R is decidable.

10. Hilbert's Tenth Problem over particular rings: summary

As usual, $\mathbb{Q}$ is the field of rational numbers, $\mathbb{R}$ is the field of real numbers, $\mathbb{C}$ the field of complex numbers, $\mathbb{Q}_p$ is the field of p-adic numbers (where p is a prime), and $\mathbb{F}_q$ is the finite field of q elements (where q is a prime power). A *number field* is a finite extension K of $\mathbb{Q}$, and its ring of integers $\mathcal{O}_K$ is defined as the integral closure of $\mathbb{Z}$ in K. A *global function field* is a finite extension of the *rational function field* $\mathbb{F}_p(t)$ for some prime p, where t is an indeterminate. A *p-adic field* is a finite extension of $\mathbb{Q}_p$ for some prime p.

Table 1 contains, for various rings R, the answers to the questions

Ring R	Hilbert's 10^{th} Problem	First order theory
$\mathbb{C}$	YES	YES (elimination theory)
$\mathbb{R}$	YES	YES [Tar51]
$\mathbb{F}_q$	YES	YES (trivial)
p-adic fields	YES [Ner63]	YES [AK66], [Erš65a]
$\mathbb{F}_q((t))$	?	?
number field	?	NO [Rob59]
$\mathbb{Q}$	?	NO [Rob49]
global function field	NO [Shl92], [Eis03]	NO
$\mathbb{F}_q(t)$	NO [Phe91], [Vid94]	NO [Erš65b], [Pen73]
$\mathbb{C}(t)$	?	?
$\mathbb{C}(t,u)$	NO [KR92b]	NO
$\mathbb{R}(t)$	NO [Den78]	NO
$\mathcal{O}_K$	? (NO for some $\mathcal{O}_K$)	NO (corollary of NO for K)
$\mathbb{Z}$	NO [Mat70]	NO [Göd31]

TABLE 1. Answer to Hilbert's Tenth Problem, and decidability of the first order theory, for various rings

(1) Does Hilbert's Tenth Problem over R have a positive answer? That is, is there an algorithm to decide whether a multivariable polynomial with integer coefficients has a zero over R? (In certain cases, we allow other coefficients: see below.)
(2) Is the first order theory of R decidable?

A question mark ? signifies that the answer is not known, except that the answer to Hilbert's Tenth Problem over the rings of integers $\mathcal{O}_K$ of number fields is known for some number fields K (the answer is NO when it is known): see Section 14. In particular, the answer to Hilbert's Tenth Problem over a number field K is not known for any K.

In the case where R is $\mathbb{F}_q(t)$ or a finite extension (another global function field) or $\mathbb{F}_q((t))$, we consider Hilbert's Tenth Problem over R with coefficients in $\mathbb{F}_q(t)$, and for the first order theory, we augment the language by including a symbol for t and a symbol for a field generator of $\mathbb{F}_q$. In the cases of $\mathbb{C}(t)$, $\mathbb{R}(t)$, and $\mathbb{C}(t,u)$, we consider polynomials with coefficients in $\mathbb{Z}[t]$ or $\mathbb{Z}[t,u]$, and introduce symbols for t and u, as appropriate. In all other cases, the input polynomials in Hilbert's Tenth Problem have coefficients in (the image of) $\mathbb{Z}$, and the language used is simply the language of rings, with no added symbols for constants other than 0 and 1.

The rings in Table 1 are grouped as follows: archimedean fields, finite fields, nonarchimedean local fields, global fields, function fields over archimedean fields, and rings of integers. They are listed roughly in order of increasing "arithmetic complexity". There is no formal definition of arithmetic complexity, but for example, for fields k we can measure the size of the absolute Galois group $\mathrm{Gal}(k^s/k)$, where k^s is a separable closure of k. Although this may go against conventional wisdom, global function fields may be considered more complex than number fields, because their arithmetic contains "extra structure" coming from the Frobenius endomorphism; in any case this is what has been used in proving a

negative answer to Hilbert's Tenth Problem over such fields. Domains may be considered more complex than their fraction fields, since they have "extra structure" coming from the divisibility relation.

Remark 10.1. For any ring, the decidability of the first order theory implies a positive answer to Hilbert's Tenth Problem. This explains why we have not given references in every box in Table 1. When the answer in one of the two boxes in a row was known before the other, references are given in both boxes.

11. Decidable fields

In the cases where the first order theory is decidable, the decidability is a consequence of an effective elimination of quantifiers for a theory in some (possibly enlarged) language. *Elimination of quantifiers* means that given a first order formula ϕ involving bound variables x_i and free variables y_j, there is a quantifier-free formula ψ involving only the y_j such that the set of $\vec{y}$ for which ϕ is true equals the corresponding set for ψ. The elimination of quantifiers is *effective* if there is a Turing machine that takes ϕ as input and outputs a possible ψ. If a theory admits an effective elimination of quantifiers, and the truth of quantifier-free sentences is decidable, then the theory is decidable.

The fact that $\mathbb{C}$ in the language of rings has an effective elimination of quantifiers was essentially known in the 19^{th} century, except that they did not think to state things in this way. In fact, there is an elimination of quantifiers for any algebraically closed field k: it is equivalent to Chevalley's Theorem in algebraic geometry which states that the image of a constructible set under a projection is constructible. (A subset of k^n, where k is an algebraically closed field, is called *constructible* if it is a Boolean combination of sets of the form $\{\, \vec{x} \in k^n : f(\vec{x}) = 0 \,\}$ for $f \in k[x_1, \ldots, x_n]$. By *projection*, we mean a surjective k-linear map $k^n \to k^m$.)

The theory of $\mathbb{R}$ in the language of rings does *not* admit elimination of quantifiers, since the formula $(\exists x)\ y = x^2$ is not equivalent to an quantifier-free formula involving only y: a Boolean combination of subsets of $\mathbb{R}$ defined by polynomial equations either is finite or has finite complement in $\mathbb{R}$, and hence cannot equal $\mathbb{R}_{\geq 0}$. On the other hand, Tarski [Tar51] showed that the theory of $\mathbb{R}$ in the language of rings augmented by a symbol $\leq$ (interpreted in the usual way) does admit an effective elimination of quantifiers. For instance, $(\exists x)\ y = x^2$ is equivalent to the quantifier-free formula $0 \leq y$.

Similarly, the theory of a p-adic field k in the language of rings does not admit elimination of quantifiers, but Macintyre [Mac76] showed that it does after one introduces symbols V and P_d for each $d \geq 2$, corresponding to the 1-variable predicates

$$\begin{aligned} V(x) \quad &\iff \quad x \text{ is in the valuation ring of } k, \\ P_d(x) \quad &\iff \quad x \text{ is a } d^{\text{th}} \text{ power in } k. \end{aligned}$$

Remark 11.1. The first proofs of decidability for p-adic fields were not based on this elimination of quantifiers.

12. Hilbert's Tenth Problem over $\mathbb{Q}$

12.1. **Existence of rational points on varieties.** Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. We refer to Chapter 1 of [Sil92] for the definitions regarding algebraic sets and varieties. In

particular, varieties are assumed to be quasi-projective and $\overline{\mathbb{Q}}$-irreducible. If X is a variety over $\mathbb{Q}$, then $X(\mathbb{Q})$ denotes the set of rational points; if X is affine, then $X(\mathbb{Q})$ is simply the set of solutions in rational numbers to the system of polynomial equations defining X.

Proposition 12.1. *Hilbert's Tenth Problem over $\mathbb{Q}$ is equivalent to the question of whether there exists a Turing machine with input and output as follows:*

input: *a variety X over $\mathbb{Q}$*
output: *YES or NO, according to whether $X(\mathbb{Q}) \neq \emptyset$.*

We also get an equivalent problem if "variety" is replaced by "algebraic set" or by "nonsingular affine variety".

Proof. Assume that there is an algorithm for deciding the most special of these problems, namely the existence of rational points on nonsingular affine varieties. We must construct an algorithm for arbitrary algebraic sets X. The new algorithm will work by induction on $\dim X$.

Every algebraic set can be written as a finite union of irreducible components, so we may assume that X is irreducible (over $\mathbb{Q}$). If X is not $\overline{\mathbb{Q}}$-irreducible, and $Y_1, \dots, Y_r$ are the $\overline{\mathbb{Q}}$-irreducible components, then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the Y_i, but any rational point of X is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and hence must lie in $\bigcap_{i=1}^{r} Y_i$, which is an algebraic subset over $\mathbb{Q}$ of lower dimension. Thus, by induction, we may assume that X is a variety. The singular locus of X is a closed subset of smaller dimension, so by induction, we reduce to considering its complement, which is a nonsingular variety. Any nonsingular variety is a finite union of affine subvarieties, and these will also be nonsingular.

Finally, we remark that all these reductions can be done effectively by a Turing machine. □

Remark 12.2. One gets an equivalent problem even if one allows "abstract varieties" in the sense of Weil (see [Har77, II.§4]), because these too can written as a finite union of affine subvarieties.

Question 12.3. Does one get an equivalent problem if one replaces "variety" by "nonsingular projective variety"? The answer is not clear.

Definition 12.4. Let X be an algebraic set over $\mathbb{Q}$, and $S \subseteq X(\mathbb{Q})$. Then S is called *diophantine over* $\mathbb{Q}$ if there exists a morphism of algebraic sets $f : Y \to X$ such that $S = f(Y(\mathbb{Q}))$.

Remark 12.5. It is easy to see that a subset S of $\mathbb{A}^n(\mathbb{Q}) = \mathbb{Q}^n$ is diophantine in this new sense if and only if S is positive existential over $\mathbb{Q}$ in the sense of Definition 8.1, and Corollary 8.6 says the latter is equivalent to S being diophantine over $\mathbb{Q}$ in the sense of Definition 8.1.

12.2. **Inheriting a negative answer from $\mathbb{Z}$?** Suppose that $\mathbb{Z}$ were diophantine over $\mathbb{Q}$. Then given a polynomial equation $f(x_1, \dots, x_n) = 0$ over $\mathbb{Z}$ we could construct a system of polynomial equations over $\mathbb{Q}$ by taking the original equation over $\mathbb{Z}$ together with, for each $i = 1, 2, \dots, n$, an extra equation $g_i(x_i, \dots) = 0$ involving x_i and a new set of variables, such that in any rational solution of the system, the equation $g_i = 0$ forces $x_i \in \mathbb{Z}$. In other words, the original polynomial equation has a solution over $\mathbb{Z}$ if and only if the associated system has a solution over $\mathbb{Q}$. Also, by Corollary 8.6, the system over $\mathbb{Q}$ is equivalent to a single polynoimal equation over $\mathbb{Q}$. Thus we could encode Hilbert's Tenth Problem over $\mathbb{Z}$

as a subproblem of Hilbert's Tenth Problem over $\mathbb{Q}$, and this could be done effectively. Since Hilbert's Tenth Problem over $\mathbb{Z}$ has a negative answer, it would follow that Hilbert's Tenth Problem over $\mathbb{Q}$ has a negative answer.

A similar argument proves more generally that if there is a diophantine model of the ring $\mathbb{Z}$ over $\mathbb{Q}$, then the negative answer to Hilbert's Tenth Problem over $\mathbb{Z}$ implies a negative answer over $\mathbb{Q}$. By a diophantine model, we mean the following:

Definition 12.6. A *diophantine model* of the ring $\mathbb{Z}$ over $\mathbb{Q}$ is a diophantine set $S \subseteq X(\mathbb{Q})$ for some algebraic set X over $\mathbb{Q}$, equipped with a bijection $\phi : \mathbb{Z} \to S$ such that the graphs of addition and multiplication (subsets of $\mathbb{Z}^3$) correspond to diophantine subsets of $S^3 \subseteq X^3(\mathbb{Q})$.

Remark 12.7. If (S, ϕ) is a diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$, then ϕ is automatically a recursive function (i.e., a Turing machine can compute its value on any input). The Turing machine can search the subset G_+ of S^3 corresponding to the graph of $+$ for a triple of the form (a_0, a_0, a_0) to find the point a_0 that is $\phi(0)$. then $\phi(0)$ must be a_0. Then it can search the subset $G_\cdot$ of S^3 corresponding to the graph of $\cdot$ for a triple of the form (a_1, a_1, a_1) with $a_1 \neq a_0$; this gives the point a_1 with $\phi(1) = a_1$. Search G_+ for (a_1, a_1, a_2); then $\phi(2) = a_2$. Search G_+ for (a_{-1}, a_1, a_0); then $\phi(-1) = a_{-1}$, and so on.

Remark 12.8. If E is an elliptic curve over $\mathbb{Q}$, then E can be made into a group variety, and this makes the set $E(\mathbb{Q})$ into a group. The Mordell-Weil Theorem [Sil92, VIII.4.1] states that $E(\mathbb{Q})$ is a finitely generated abelian group. (Actually this was proved by Mordell alone; Weil generalized the result to abelian varieties over arbitrary number fields.) Moreover, one can find an elliptic curve E over $\mathbb{Q}$ such that $E(\mathbb{Q}) \simeq \mathbb{Z}$. It has been suggested that in this case $E(\mathbb{Q})$ might be a good candidate for a diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$, since under the bijection $\mathbb{Z} \to E(\mathbb{Q})$, the graph of $+$ on $\mathbb{Z}$ already corresponds to a diophantine subset of $E^3(\mathbb{Q})$. Unfortunately it is not clear whether the graph of $\cdot$ on $\mathbb{Z}$ corresponds to a diophantine subset of $E^3(\mathbb{Q})$.

12.3. **Mazur's Conjecture.** If X is an algebraic set over $\mathbb{Q}$, then the set $X(\mathbb{R})$ inherits a topology from the topology of $\mathbb{R}$. In particular, if X is affine, contained in $\mathbb{A}^n$, then $X(\mathbb{R}) \subseteq \mathbb{R}^n$ is given the subspace topology. Several variants of the following conjecture are discussed in [Maz92] and [Maz95].

Conjecture 12.9 (Mazur)**.** If X is a variety over $\mathbb{Q}$, then the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has at most finitely many connected components.

Mazur's Conjecture is known to hold when X is a curve: this follows from the Mordell-Weil Theorem and Faltings' Theorem [Fal83] that $X(\mathbb{Q})$ is finite for curves X of genus > 1. It is also known for abelian varieties, where again it follows from the Mordell-Weil Theorem.

Remark 12.10. Mazur originally asked also whether for a smooth variety X over $\mathbb{Q}$ such that $X(\mathbb{Q})$ was Zariski dense in X, the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ is the union of connected components of $X(\mathbb{R})$. This stronger version of the question turned out to have a negative answer [CTSSD97].

Proposition 12.11. *Assume Mazur's Conjecture. If X is any algebraic set, and S is a diophantine subset of $X(\mathbb{Q})$ then the closure of S in $X(\mathbb{R})$ has at most finitely many connected components.*

Proof. The reduction process in Section 12.1 shows that Mazur's Conjecture for varieties implies the analogous statement for algebraic sets. Now suppose $S \subseteq X(\mathbb{Q})$ is diophantine. Then there is a morphism of algebraic sets $f : Y \to X$ such that $S = f(Y(\mathbb{Q}))$. We know that the topological closure $\overline{Y(\mathbb{Q})}$ of $Y(\mathbb{Q})$ in $Y(R)$ has finitely many components, say n of them. Since $f : Y(\mathbb{R}) \to X(\mathbb{R})$ is continuous, it maps connected subsets of $Y(\mathbb{R})$ to connected subsets of $X(\mathbb{R})$, so $f(\overline{Y(\mathbb{Q})})$ has at most n connected components. The closure of a connected set is connected, and the closure of a finite union is the union of the closures, so $\overline{f(\overline{Y(\mathbb{Q})})}$ has at most n connected components. But elementary topology shows $\overline{f(\overline{Y(\mathbb{Q})})} = \overline{f(Y(\mathbb{Q}))}$, and the latter is $\overline{S}$. □

Corollary 12.12. *If $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, then Mazur's Conjecture is false.*

Less obvious is the following result from [CZ00]. We give a slightly simplified version of their original proof.

Proposition 12.13. *If there exists a diophantine model of the ring $\mathbb{Z}$ over $\mathbb{Q}$, then Mazur's Conjecture is false.*

Proof. If there is a diophantine model of $\mathbb{Z}$, then by Example 6.2, there is also a diophantine model S of $\mathbb{N} = \{0, 1, 2, \dots\}$ with $+$ and $\cdot$ over $\mathbb{Q}$. Any algebraic set can be partitioned into finitely many affine algebraic sets, which can then be embedded in a single affine algebraic set, so without loss of generality we may assume that S is a diophantine subset of $X(\mathbb{Q})$ for some affine algebraic set X. We are also given a bijection $\phi : \mathbb{N} \to S$, which by the argument of Remark 12.7 is recursive.

Case 1. S is discrete as a subset of $X(\mathbb{R})$.

Then each point of S is a connected component of $\overline{S}$, so $\overline{S}$ has infinitely many connected components. Thus Proposition 12.11 implies that Mazur's Conjecture is false.

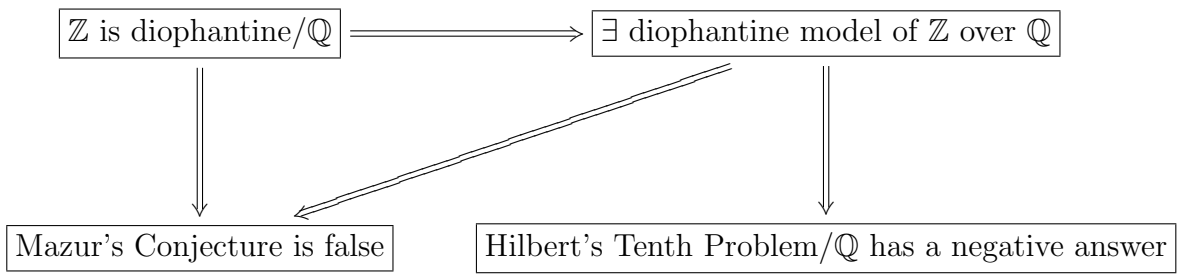
Case 2. There is a non-isolated point $s \in S$.

Fix an embedding $X \hookrightarrow \mathbb{A}^n$, and let $|\ |$ be the Euclidean norm on $\mathbb{A}^n(\mathbb{R}) = \mathbb{R}^n$. Let $m_0 = 0$, and for $i \geq 1$, let m_i be the smallest integer greater than m_{i-1} such that

$$0 < |\phi(m_i) - s| \leq 1/i,$$

Since s is non-isolated, m_i exists. Then $M := \{\, m_i : i = 0, 1, 2, \dots\}$ is a listable subset of $\mathbb{Z}$, so it is diophantine, and it follows that $\phi(M)$ is diophantine. But $\phi(M)$ is a sequence of distinct points in $\mathbb{R}^n$ tending to a limit, so $\overline{\phi(M)}$ has infinitely many connected components. Proposition 12.11 applied to $\phi(M)$ implies that Mazur's Conjecture is false. □

Summarizing, we have the following implications:



Remark 12.14. There is an object more general than "diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$" whose existence would still imply a negative answer to Hilbert's Tenth Problem over $\mathbb{Q}$. Namely, define a *diophantine interpretation* (this terminology is not standard outside this paper) of the ring $\mathbb{Z}$ in $\mathbb{Q}$ to be a diophantine set S equipped with a diophantine equivalence relation $\sim$ and a surjection $\phi : S \to \mathbb{Z}$ inducing an bijection $\frac{S}{\sim} \xrightarrow{\sim} \mathbb{Z}$ such that the inverse images of the graphs of addition and multiplication on $\mathbb{Z}$ are diophantine subsets of S^3. It is not known whether the existence of a diophantine interpretation of $\mathbb{Z}$ in $\mathbb{Q}$ would violate Mazur's Conjecture.

13. Global function fields

Here we outline Pheidas's proof [Phe91] that Hilbert's Tenth Problem over $k := \mathbb{F}_q(t)$ (with coefficients in k) has a negative answer for any odd prime power q.

(1) Show that the set
$$\{\, t^{p^s} : s \in \mathbb{N} \,\}$$
is diophantine over k. (This fact should not surprise those who are familiar with the analogue of Faltings' Theorem for isotrivial curves over function fields of positive characteristic.)

(2) Using the previous step, show that
$$P := \{\, (x, y) \in k^2 : y = x^{p^s} \text{ for some } s \in \mathbb{N} \,\}$$
is diophantine over k.

(3) Define the discrete valuation $v_t : k \to \mathbb{Z} \cup \{+\infty\}$ by $v(t^n p(t)/q(t)) = n$ whenever $p, q \in \mathbb{F}_q[t]$ have nonzero constant terms, and by $v(0) = +\infty$. Show that the corresponding valuation ring $V := \mathbb{F}_q[t]_{(t)}$ is diophantine over k.

(4) Define an equivalence relation $\sim$ on $k^\times$ by
$$x \sim y \quad \iff \quad v_t(x) = v_t(y).$$
This relation is diophantine over k, since $k^\times$ is diophantine, and since for $x, y \in k^\times$,
$$v_t(x) = v_t(y) \quad \iff \quad (\exists c)(\exists d)\ (x = cy)\ \wedge\ (y = dx).$$
Let $|_p$ denote the binary relation on $\mathbb{Z}$ defined by
$$x \mid_p y \iff (\exists s \in \mathbb{Z})\ y = p^s x.$$
Then $(\mathbb{Z}, 0, 1, +, |_p)$ admits a diophantine interpretation in k: the valuation v_t induces an isomorphism $\frac{k^\times}{\sim} \to \mathbb{Z}$ under which 1 maps to 0, t maps to 1, multiplication in $k^\times$ corresponds to $+$ in $\mathbb{Z}$, and the relation P corresponds to $|_p$.

(5) Finally, show that the graph of multiplication is positive existential in the structure $(\mathbb{Z}, 0, 1, +, |_p)$. Then the ring $\mathbb{Z}$ admits a diophantine interpretation in k. Hence Hilbert's Tenth Problem over $\mathbb{Z}$ can be encoded as a subproblem of Hilbert's Tenth Problem over k (with coefficients in k). The negative answer to the former now implies a negative answer to the latter.

Remark 13.1. By encoding elements of $\mathbb{F}_q(t)$ as nonnegative integers in some reasonable way, one can say what it means for a subset of $\mathbb{F}_q(t)$ to be listable. It is not known whether all listable subsets of $\mathbb{F}_q(t)$ are diophantine over $\mathbb{F}_q(t)$. It is not even known whether subsets such as $\mathbb{F}_q[t]$ or $\{\, t^n : n \in \mathbb{N} \,\}$ are diophantine over k.

Remark 13.2. The extensions of Pheidas's result to arbitrary global function fields in [Shl92], [Vid94], and [Eis03] are nontrivial, but the main ideas are the same. These ideas have been successfully applied also to some function fields over *infinite* fields of positive characteristic: see [Shl00] and [Eis03].

14. Rings of integers of number fields

This will be discussed by the group of students working on the project at the 2003 Arizona Winter School, so here we will only state what is known.

Theorem 14.1. *Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. Hilbert's Tenth Problem over $\mathcal{O}_K$ has a negative answer if any of the following hold:*

1. *K is totally real* [Den80].
2. *K is a quadratic extension of a totally real number field or of an imaginary quadratic extension* [DL78].
3. *K has exactly one conjugate pair of nonreal embeddings* [Phe88], [Shl89].
4. *There exists an elliptic curve E over $\mathbb{Q}$ such that the abelian groups $E(\mathbb{Q})$ and $E(K)$ both have rank 1* [Poo02b].

Methods involving p-adic L-series can be used to show that the last condition is satisfied by infinitely many fields K not covered by the other conditions.

Update (January 18, 2010): In 2003, Poonen and Shlapentokh showed that if for every Galois prime-degree extension L/K, there exists an elliptic curve E over K such that $E(K)$ and $E(L)$ have the same positive rank, then Hilbert's Tenth Problem has a negative answer over the ring of integers of each number field. In 2009, the hypothesis was verified by Mazur and Rubin, conditionally on (a weak form of) the conjecture that Shafarevich-Tate groups of elliptic curves are finite.

15. Subrings of $\mathbb{Q}$

Let $\mathcal{P} = \{2, 3, 5, \dots\}$ be the set of prime numbers. Then there is a bijection

$$\begin{aligned} \{\text{subsets of } \mathcal{P}\} &\leftrightarrow \{\text{subrings of } \mathbb{Q}\} \\ S &\mapsto \mathbb{Z}[S^{-1}] \\ \mathcal{P} \cap R^\times &\mapsfrom R \end{aligned}$$

where $R^\times$ denotes the group of invertible elements of the ring R.

For $S \subseteq \mathcal{P}$, what can be said about Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$? If $S = \emptyset$, then $\mathbb{Z}[S^{-1}] = \mathbb{Z}$ and the answer is negative. If $S = \mathcal{P}$, then $\mathbb{Z}[S^{-1}] = \mathbb{Q}$, and the answer is unknown. If for some S the answer is yes, then the answer to Hilbert's Tenth Problem over $\mathbb{Q}$ also is yes, since $\mathbb{Q}$ admits a diophantine interpretation in $\mathbb{Z}[S^{-1}]$ (first generalize Example 6.3 to show that the subset of nonzero elements of $\mathbb{Z}[S^{-1}]$ is diophantine over $\mathbb{Z}[S^{-1}]$ [Shl94, Theorem 4.2], and then represent elements of $\mathbb{Q}$ as fractions of elements of $\mathbb{Z}[S^{-1}]$).

The following proposition is implicit in the work of J. Robinson, and proved explicitly as Proposition 3.1 of [KR92a].

Proposition 15.1. *The subring $\mathbb{Z}_{(p)}$ of rational numbers whose denominator is not divisible by p is diophantine over $\mathbb{Q}$.*

We will not give the proof, but instead simply say that it relies on the *Hasse principle for quadratic forms*, which is the statement that a homogeneous polynomial of degree 2 with coefficients in $\mathbb{Q}$ has a nontrivial zero over $\mathbb{Q}$ if and only if it has a nontrivial zero over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p.

Corollary 15.2. *If $S = \mathcal{P} - F$ for some finite subset $F \subset \mathcal{P}$, then the answer to Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$ is the same as the answer to Hilbert's Tenth Problem over $\mathbb{Q}$.*

Proof. By Proposition 15.1, and the fact that an intersection of diophantine subsets over $\mathbb{Q}$ is diophantine, we see that $\mathbb{Z}[S^{-1}]$ is diophantine over $\mathbb{Q}$. On the other hand, as remarked above, $\mathbb{Q}$ can be interpreted in $\mathbb{Z}[S^{-1}]$. Thus a positive answer to Hilbert's Tenth Problem for either ring implies a positive answer to the other. □

Corollary 15.3. *If S is finite, then Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$ has a negative answer.*

Proof. Using the interpretation of $\mathbb{Q}$ in $\mathbb{Z}[S^{-1}]$, the fact that $\mathbb{Z}_{(p)}$ is diophantine over $\mathbb{Q}$ for any p, and the fact that $\mathbb{Z} = \mathbb{Z}[S^{-1}] \cap \bigcap_{p \in S} \mathbb{Z}_{(p)}$ one can show that $\mathbb{Z}$ is diophantine in $\mathbb{Z}[S^{-1}]$. Hence the known negative answer for Hilbert's Tenth Problem over $\mathbb{Z}$ implies a negative answer for Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$. □

The first answers for infinite S were proved in November 2002 [Poo02a]:

Theorem 15.4. *There exist disjoint recursive sets of primes $T_1, T_2 \subseteq \mathcal{P}$ of natural density zero such that if $T_1 \subseteq S \subseteq \mathcal{P} - T_2$, then*

(a) *There is an affine curve E' over $\mathbb{Z}[S^{-1}]$ such that the topological closure of $E'(\mathbb{Z}[S^{-1}])$ in $E'(\mathbb{R})$ has infinitely many connected components.*
(b) *There exists a diophantine model of the ring $\mathbb{Z}$ over $\mathbb{Z}[S^{-1}]$.*
(c) *Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$ has a negative answer.*

Remark 15.5.

(i) The natural density of a subset $T \subseteq \mathcal{P}$ is defined as
$$\lim_{X \to \infty} \frac{\#\{p \in T : p \leq X\}}{\#\{p \in \mathcal{P} : p \leq X\}},$$
if the limit exists.
(ii) This result was inspired by an earlier result of Shlapentokh [Shl03] which proves statements similar to part (a) of Theorem 15.4 for certain infinite localizations of rings of integers of certain number fields other than $\mathbb{Q}$.

Let us sketch the proof of Theorem 15.4:

(1) Start with an elliptic curve E over $\mathbb{Q}$ such that the finitely generated abelian group $E(\mathbb{Q})$ has rank 1. To simplify the argument, it helps if $E(\mathbb{Q}) \simeq \mathbb{Z}$, $E(\mathbb{R})$ is connected, and E has no complex multiplication over $\mathbb{C}$. The nonsingular projective model of $y^2 = x^3 + x + 1$ is such a curve. Then the affine curve E' will be E with the origin (i.e., point at infinity) removed. Let P be a generator of $E(\mathbb{Q})$.
(2) Use Vinogradov's Theorem [Vin54, p. 180] about equidistribution of the prime multiples of an irrational number modulo 1 to show that the prime multiples of P in $E(\mathbb{Q})$ are dense in $E(\mathbb{R})$, and that in fact every nonempty open subset of $E(\mathbb{R})$ contains ℓP for a positive density of primes ℓ.

(3) Using the previous result, pick a suitable sequence of primes $\ell_1 < \ell_2 < \dots$ such that if y_j is the y-coordinate of $\ell_j P$, then

$$|y_j - j| \leq \frac{1}{10j}$$

for all $j \geq 1$.

(4) Choose T_1 so that $\pm\ell_j P \in E'(\mathbb{Z}[S^{-1}])$ for all j, and choose T_2 so that almost no other multiples of P are in $E'(\mathbb{Z}[S^{-1}])$, whenever $T_1 \subseteq S \subseteq \mathcal{P} - T_2$. Check that if the ℓ_j are chosen carefully, then it is possible to choose T_1 and T_2 as above so that they are recursive and of natural density zero. This already proves part (a) of Theorem 15.4.

(5) Show that $Y = \{y_1, y_2, \dots\}$ is a diophantine model of $\mathbb{Z}_{>0}$ over $\mathbb{Z}[S^{-1}]$, when we use the bijection $\mathbb{Z}_{>0} \to Y$ mapping j to y_j. For this, we use

$$\begin{aligned} m + n = q \quad &\iff \quad |y_m + y_n - y_q| \leq 3/10 \\ m^2 = q \quad &\iff \quad |y_m^2 - y_q| \leq 4/10 \end{aligned}$$

to show that addition and squaring on $\mathbb{Z}_{>0}$ correspond to diophantine relations on Y. Then multiplication can be defined in terms of addition and squaring, since

$$mn = q \quad \iff \quad (m+n)^2 = m^2 + n^2 + q + q,$$

and a diophantine model of $\mathbb{Z}$ over $\mathbb{Z}[S^{-1}]$ can easily be built out of a diophantine model of $\mathbb{Z}_{>0}$ over $\mathbb{Z}[S^{-1}]$.

(6) Finally, the negative answer to Hilbert's Tenth Problem over $\mathbb{Z}$ together with the diophantine model constructed in the previous step gives a negative answer to Hilbert's Tenth Problem over $\mathbb{Z}[S^{-1}]$.

References

[AK66] James Ax and Simon Kochen, *Diophantine problems over local fields. III. Decidable fields*, Ann. of Math. (2) **83** (1966), 437–456.

[AKS02] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, *PRIMES is in P*, August 6, 2002, preprint.

[CTSSD97] J.-L. Colliot-Thélène, A. N. Skorobogatov, and Peter Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), no. 2, 113–135.

[CZ00] Gunther Cornelissen and Karim Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 253–260.

[Den78] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

[Den80] J. Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236.

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391.

[DLPVG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, American Mathematical Society, Providence, RI, 2000, Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436.

[EFT94] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical logic*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1994, Translated from the German by Margit Meßmer.

[Eis03] Kirsten Eisenträger, *Hilbert's Tenth Problem for algebraic function fields of characteristic* 2, Pacific J. Math. (2003?), to appear.

[Erš65a] Ju. L. Eršov, *On the elementary theory of maximal normed fields*, Dokl. Akad. Nauk SSSR **165** (1965), 21–23, Translated in Soviet Math. Dokl. **6** (1965), 1390–1393.

[Erš65b] Ju. L. Eršov, *The undecidability of certain fields*, Dokl. Akad. Nauk SSSR **161** (1965), 27–29.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, Erratum in: Invent. Math. **75** (1984), 381. Translated in: pp. 9–27 of *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986.

[Göd31] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter System I*, Monatshefte für Math. und Physik **38** (1931), 173–198, English translation by Elliot Mendelson: "On formally undecidable propositions of Principia Mathematica and related systems I" in M. Davis, *The undecidable*, Raven press, 1965.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[HU79] John E. Hopcroft and Jeffrey D. Ullman, *Introduction to automata theory, languages, and computation*, Addison-Wesley Publishing Co., Reading, Mass., 1979, Addison-Wesley Series in Computer Science.

[JM91] J. P. Jones and Y. V. Matijasevič, *Proof of recursive unsolvability of Hilbert's tenth problem*, Amer. Math. Monthly **98** (1991), no. 8, 689–709.

[KR92a] K. H. Kim and F. W. Roush, *An approach to rational Diophantine undecidability*, Proceedings of Asian Mathematical Conference, 1990 (Hong Kong, 1990) (River Edge, NJ), World Sci. Publishing, 1992, pp. 242–248.

[KR92b] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbf{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44.

[Mac76] Angus Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), no. 3, 605–610.

[Mat70] Ju. V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282.

[Maz92] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45.

[Maz95] B. Mazur, *Speculations about the topology of rational points: an update*, Astérisque (1995), no. 228, 4, 165–182, Columbia University Number Theory Seminar (New York, 1992).

[Ner63] A. Nerode, *A decision method for p-adic integral zeros of diophantine equations*, Bull. Amer. Math. Soc. **69** (1963), 513–517.

[Pen73] Ju. G. Penzin, *Undecidability of fields of rational functions over fields of characteristic* 2, Algebra i Logika **12** (1973), 205–210, 244.

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620.

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8.

[Poo02a] Bjorn Poonen, *Hilbert's Tenth Problem and Mazur's Conjecture for large subrings of* $\mathbb{Q}$, 2002, `http://math.berkeley.edu/ poonen/papers/subrings.pdf`.

[Poo02b] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of hilbert's tenth problem over rings of algebraic integers*, Algorithmic Number Theory, C. Fieker and D. Kohel (eds.), 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings, Lecture Notes in Computer Science **2369** (Berlin), Springer-Verlag, 2002, pp. 33–42.

[Rob49] Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

[Rob59] Julia Robinson, *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc. **10** (1959), 950–957.

[Shl89] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962.

[Shl92] Alexandra Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Trans. Amer. Math. Soc. **333** (1992), no. 1, 275–298.

[Shl94] Alexandra Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), no. 1, 139–175.

[Shl00] Alexandra Shlapentokh, *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic*, Pacific J. Math. **193** (2000), no. 2, 463–500.

[Shl03] Alexandra Shlapentokh, *A ring version of Mazur's conjecture on topology of rational points*, Internat. Math. Res. Notices (2003), no. 7, 411–422.

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Tar51] Alfred Tarski, *A decision method for elementary algebra and geometry*, University of California Press, Berkeley and Los Angeles, Calif., 1951, 2nd ed.

[Vid94] Carlos R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253.

[Vin54] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Interscience Publishers, London and New York., 1954, Translated, revised and annotated by K. F. Roth and Anne Davenport.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu