UNIVERSITY OF OXFORD

MMathPhil Mathematics & Philosophy

Part C: M-level Dissertation (CD)

HILBERT'S TENTH PROBLEM AND THE DECIDABILITY OF VARIOUS RINGS

CANDIDATE NUMBER: 900223

March 15, 2013

Contents

1 Introduction

On 8th of August 1900, David Hilbert presented a list of 23 problems at the International Congress of Mathematicians in Paris. These problems are the famous "Hilbert's problems". In this paper, we will be discussing Hilbert's Tenth Problem and the extension of the original problem. Here is a close translation found in Matiyasevich book [23]:

> *"Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers."*

The problem was shown to be unsolvable by collaborated work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich.

Section 2 gives an exposition of Martin Davis' paper [5] on the unsolvability of the original Hilbert's Tenth Problem. Section 3 gives an exposition of Paul Cohen's paper [3] which shows that the full theory of reals is decidable. We then briefly study, in Section 4, the progress on Hilbert's Tenth Problem over the rationals which is currently an open problem. Finally, we finish with an observation, in Section 5 that I made whilst looking at the survey of results on the Hilbert's Tenth Problem and the decidability of various rings.

1.1 Notations

Throughout the paper, for a given ring R, we will write "H10/R" as a shorthand for the Hilbert's Tenth Problem over R. The precise meaning of this is explained in section 3.1. We will also write "¬H10/R" as a shorthand for the unsolvability of H10/R. Next, we will write $\bar{x}$ as a shorthand for the list $x_1, ..., x_n$ where n is determined in context.

2 Hilbert's Tenth Problem over $\mathbb{Z}$

This section will give an exposition of Martin Davis' paper *Hilbert's Tenth Problem Is Unsolvable* [5]. It will cover the key ideas from Davis' paper in a similar fashion. The Theorems and Definitions in this section are directly quoted from the paper with possibly changes in some notations or wording. Due to the space constraints, we will state and assume without proof some elementary facts from Number theory used in the paper. Also, we won't go into the proof of the theorem which says that the exponential function is Diophantine. Although the theorem provides one of the core tools for the answer to the problem, the proofs are mainly number theoretic and falls outside our interests in this paper.

2.1 Summary of the proof

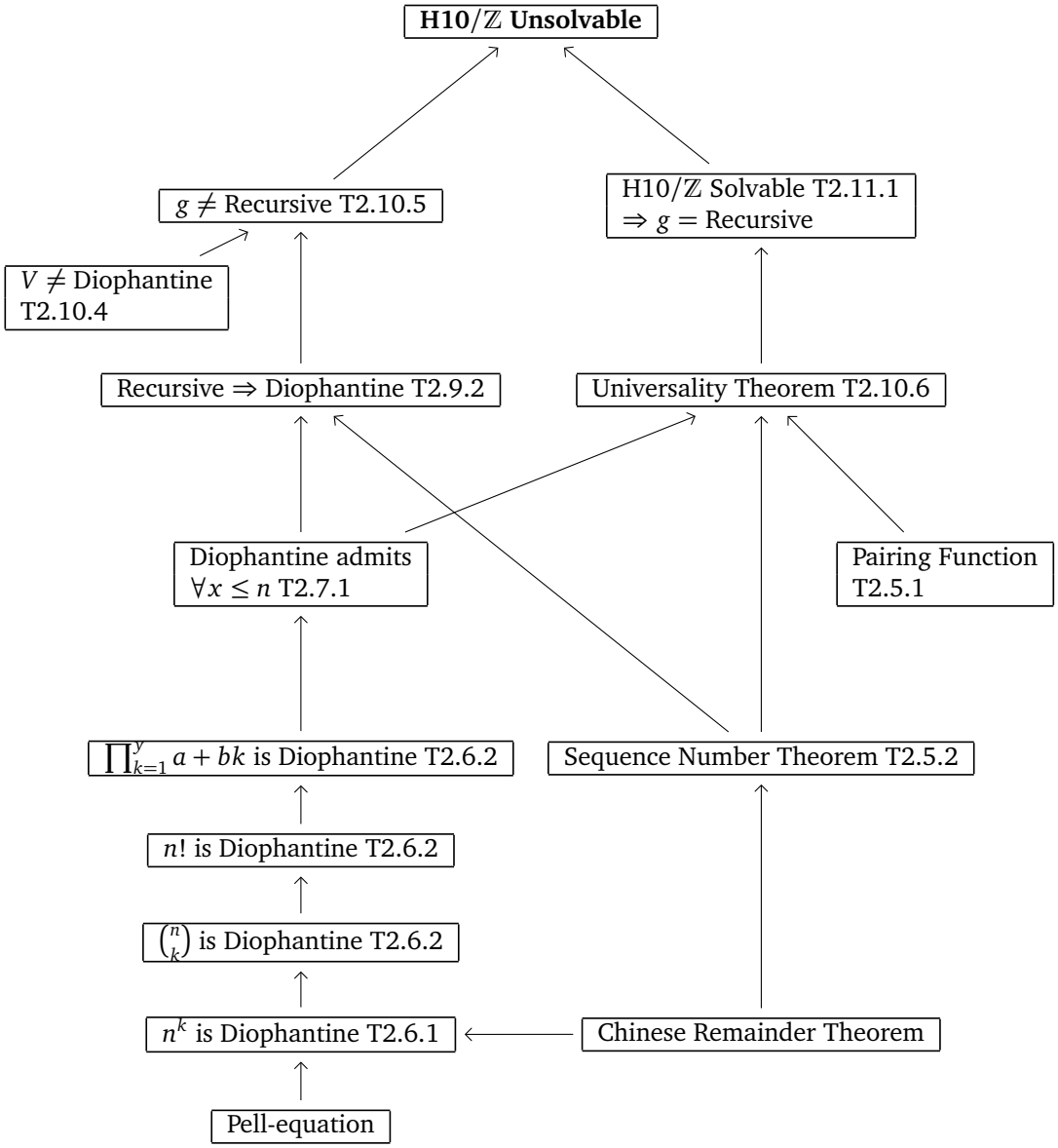


Diagram of the proof of unsolvability of Hilbert's Tenth Problem over $\mathbb{Z}$.

2.2 Positive integers

We wish to show that no algorithm exists to decide whether a polynomial root has an integer solution or not. However, as Davis points out, it suffices to show that there is no algorithm to decide whether a polynomial has a *positive* solution or not. To see why, suppose there is an algorithm to decide whether a given polynomial has an integer solution or not. Let a polynomial $f(x_1, ..., x_n)$ be given. Now consider a polynomial $g(p_1, q_1, r_1, s_1, ..., p_n, q_n, r_n, s_n)$ given by $g = f(1 + p_1^2 + q_1^2 + r_1^2 + s_1^2, ..., 1 + p_n^2 + q_n^2 + r_n^2 + s_n^2)$. So by assumption, the algorithm can decide if g has an integer solution or not. Now by a famous theorem of Lagrange, any non-negative integer can be written as a sum of squares of four integers. In other words,

$$(\exists p_1, q_1, r_1, s_1, ..., p_n, q_n, r_n, s_n)[g(p_1, q_1, r_1, s_1, ..., p_n, q_n, r_n, s_n) = 0]$$
$$\Leftrightarrow$$
$$(\exists p_1, q_1, r_1, s_1, ..., p_n, q_n, r_n, s_n)[f(1+p_1^2+q_1^2+r_1^2+s_1^2, ..., 1+p_n^2+q_n^2+r_n^2+s_n^2)]$$
$$\Leftrightarrow$$
$$(\exists x_1 > 0, ..., x_n > 0)[f(x_1, ..., x_n) = 0]$$

So in this way, the algorithm can be used to decide if f has a *positive* solution or not. So by contrapositive, if no algorithm exists to decide if a polynomial has a positive solution or not, then no algorithm exists which decides if a polynomial has an integer solution or not.

With this fact in mind, we will only be dealing with positive numbers in this proof. When we say 'numbers', we mean *positive* numbers by default unless explicitly stated otherwise.

2.3 Diophantine sets and functions

Roughly speaking, a set or a function is said to be Diophantine if it can be described by a polynomial equation. More precisely:

Definition 2.3.1. A set S of ordered n-tuples of positive integers is called *Diophantine* if there is a polynomial $P(x_1, ..., x_n, y_1, ..., y_m)$, where $m \geq 0$, with integer coefficients such that a given n-tuple $\langle x_1, ..., x_n \rangle$ belongs to S if and only if there exist positive integers $y_1, ..., y_m$ for which

$$P(x_1, ..., x_n, y_1, ..., y_m) = 0$$

We can also express it in logical symbols:

$$\langle x_1, ..., x_n \rangle \in S \Leftrightarrow (\exists y_1, ..., y_m)[P(x_1, ..., x_n, y_1, ..., y_m) = 0]$$

Or equvalently:

$$S = \{\langle x_1, ..., x_n\rangle : (\exists y_1, ..., y_m)[P(x_1, ..., x_n, y_1, ..., y_m) = 0]\}$$

Remark. Strictly speaking, we should let polynomials only have positive coefficients. We can actually achieve an equivalent definition of Diophantine sets using polynomials of positive coefficients by writing

$$\langle x_1, ..., x_n\rangle \in S \Leftrightarrow (\exists y_1, ..., y_m)[P_1(x_1, ..., x_n, y_1, ..., y_m) = P_2(x_1, ..., x_n, y_1, ..., y_m)]$$

for some P_1 and P_2 with positive integer coefficients. However, this difference doesn't affect the rest of the proof and it makes for more convenient notation to allow ourselves negative coefficients.

Here are some of my own examples of Diophantine sets.

Example 2.3.2. *The following are Diophantine sets:*

(i) The positive integers, $\mathbb{Z}^+$

$$x \in S \Leftrightarrow x = x$$

(ii) Odd numbers

$$x \in S \Leftrightarrow \exists y(x = 2y - 1)$$

(iii) Pythagorean triples

$$\langle x, y, z\rangle \in S \Leftrightarrow x^2 + y^2 = z^2$$

(iv) Square numbers

$$x \in S \Leftrightarrow \exists y(y^2 = x)$$

(v) Elephantine triples
Elephantine triples are triples of the form $\langle \frac{1}{a}, \frac{1}{b}, \frac{1}{c}\rangle$ such that there exists n such that $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{n}{n+1}$. For a given Elephantine triple $\langle \frac{1}{a}, \frac{1}{b}, \frac{1}{c}\rangle$, we claim that triples $\langle a, b, c\rangle$ are Diophantine.

$$\langle x, y, z\rangle \in S \Leftrightarrow \exists n((n + 1)(bc + ac + ab) = nabc)$$

(vi) Polite Numbers
Polite Numbers are sum of two or more consecutive numbers. The fact that Polite Numbers are Diophantine is not immediately obvious. However, it is known that Polite Numbers are exactly those numbers which are not

powers of 2. The proof is not included in this paper but can be found in [11]. The Diophantine equation describing numbers which are not powers of 2 is taken from Davis' Example (i) in [5, p. 235].

$$x \in S \Leftrightarrow (\exists y, z)(x = y(2z + 1))$$

Next, we define what it means for a function to be Diophantine. As before, we are only working with positive integers and so by a 'function' we mean a positive integer valued function on one or more positive integer arguments.

Definition 2.3.3. A function f of n arguments is called *Diophantine* if

$$\{\langle x_1, ..., x_n, y\rangle : y = f(x_1, ..., x_n)\}$$

is a Diophantine set, (i.e., f is Diophantine if its "graph" is Diophantine).

We end this section with some more useful Diophantine relations taken from Davis' paper.

Lemma 2.3.4. The following are Diophantine:

1. $x|y$ "x divides y"

$$x|y \Leftrightarrow \exists n(y = nx)$$

2. $x \equiv y \mod z$

$$x \equiv y \mod z \Leftrightarrow \exists n(x + y = nz)$$

3. $x < y$ and $x \leq y$

$$x < y \Leftrightarrow \exists n(y = x + n) \text{ and } x \leq y \Leftrightarrow \exists n(y + 1 = x + n)$$

2.4 Existential formulas

In this section, we will consider the Diophantine sets from the perspective of Model Theory. I will assume that the reader is comfortable with notions like terms, atomic formulas and first order sentences/formulas. These are defined in Part C Model theory course [17]. Also, we will be working with the whole of $\mathbb{Z}$ and not just the positive integers in this section. The results shown in this section also hold for the positive integers but as we will be discussing these results in further sections for general rings, we will show

the results for $\mathbb{Z}$.

In the first order language of $\langle \mathbb{Z}; +, \cdot, 0, 1 \rangle$, the terms are simply multivariable polynomials with integer coefficients. This follows easily from the definition of terms in the language. Hence the atomic formulas in the language are of the form $g(x_1, ..., x_n) = h(x_1, ..., x_n)$ where g and h are polynomials with integer coefficients. These are equivalent to the formula $f(x_1, ..., x_n) = 0$ where $f = g - h$. Hence we can see that the sets definable by atomic formulas in $\langle \mathbb{Z}; +, \cdot, 0, 1 \rangle$, i.e.

$$\{\langle a_1, ..., a_n \rangle \in \mathbb{Z}^n : \langle \mathbb{Z}; +, \cdot, 0, 1 \rangle \vDash \alpha(a_1, ..., a_n), \alpha \text{ atomic}\}$$

are Diophantine sets.

We can expand our collection of first order formulas which define Diophantine sets.

Lemma 2.4.1. *If $f(x_1, ..., x_n)$ and $g(x_1, ..., x_n)$ are formulas which define Diophantine sets, then the following formulas define Diophantine sets:*

1. $f(x_1, ..., x_n) \wedge g(x_1, ..., x_n)$
2. $f(x_1, ..., x_n) \vee g(x_1, ..., x_n)$
3. $\exists x_i f(x_1, ..., x_n)$.

Proof. If $f(x_1, ..., x_n)$ and $g(x_1, ..., x_n)$ define Diophantine sets, then by definition, there will be polynomials $P(x_1, ..., x_n, y_1, ..., y_m)$ and $Q(x_1, ..., x_n, z_1, ..., z_k)$ (where y_i and z_j do not coincide) such that for any $\langle a_1, ..., a_n \rangle \in \mathbb{Z}^n$,

$$f(a_1, ..., a_n) \Leftrightarrow \exists y_1, ..., y_m [P(a_1, ..., a_n, y_1, ..., y_m) = 0]$$

and

$$g(a_1, ..., a_n) \Leftrightarrow \exists z_1, ..., z_k [Q(a_1, ..., a_n, z_1, ..., z_k) = 0].$$

So now for each case,

1. $f(x_1, ..., x_n) \wedge g(x_1, ..., x_n)$:

$$\begin{aligned} f(\bar{a}) \wedge g(\bar{a}) &\Leftrightarrow \exists \bar{y} [P(\bar{a}, \bar{y}) = 0] \wedge \exists \bar{z} [Q(\bar{a}, \bar{z}) = 0] \\ &\Leftrightarrow \exists \bar{y}, \bar{z} [P(\bar{a}, \bar{y}) = 0 \wedge Q(\bar{a}, \bar{z}) = 0] \qquad \text{since } y_i \text{ and } z_j \text{ do not coincide} \\ &\Leftrightarrow \exists \bar{y}, \bar{z} [(P(\bar{a}, \bar{y}))^2 + (Q(\bar{a}, \bar{z}))^2 = 0] \end{aligned}$$

2. $f(x_1,...,x_n) \vee g(x_1,...,x_n)$:

$$\begin{aligned} f(\bar{a}) \vee g(\bar{a}) &\Leftrightarrow \exists \bar{y}[P(\bar{a},\bar{y}) = 0] \vee \exists \bar{z}[Q(\bar{a},\bar{z}) = 0] \\ &\Leftrightarrow \exists \bar{y},\bar{z}[P(\bar{a},\bar{y}) = 0 \vee Q(\bar{a},\bar{z}) = 0] \\ &\Leftrightarrow \exists \bar{y},\bar{z}[P(\bar{a},\bar{y}) \cdot Q(\bar{a},\bar{z}) = 0] \end{aligned}$$

3. $\exists x_i f(x_1,...,x_n)$:

$$\exists x_i f(a_1,...,a_{i-1},\bar{x_i},a_{i+1},...,a_n) \Leftrightarrow \exists x_i \exists \bar{y}[P(a_1,...,a_{i-1},x_i,a_{i+1},...,a_n,\bar{y}) = 0]$$

the right hand sides define Diophantine sets by definition so we are done. □

Are there any other operations we can work with? Two other candidates are $\neg$ negation and $\forall x$ the universal quantifier. If we can add these operations in our collection of formulas defining Diaphontine sets, they will be very powerful tools. Unfortunately, they are in fact *too* powerful. This is because Diophantine sets aren't closed under taking negations or adding universal quantifiers, in general, and we will see some counter examples later on. However, Diophantine sets are closed under taking these two operations in a restricted settings. Firstly, Diophantine sets are closed under taking negation inside a quantifier free formula. This is due to the Lemma below.

Lemma 2.4.2. *If $f(x_1,...,x_n)$ is equivalent to a polynomial equation, then $\neg f(x_1,...,x_n)$ defines a Diophantine set.*

Proof. Suppose $f(x_1,...,x_n)$ is equivalent to a polynomial equation $P(x_1,...,x_n) = 0$ (notice no existential quantifiers which is crucial). Then, for any $\langle a_1,...,a_n\rangle \in \mathbb{Z}^n$, we claim:

$$P(a_1,...,a_n) \neq 0 \Leftrightarrow \exists u,v,w[u \cdot P(a_1,...,a_n) = (2v-1)(3w-1)]$$

The right hand side of the equation is a variation of the claim from the Introduction in Prunescu's paper [32]. The paper stated $x \neq 0 \Leftrightarrow \exists u,v[u \cdot x = (2v-1)(3v-1)$ in two variables without proof. But I will include my own proof of the claim above with three variables. The right hand side is in the form which defines Diophantine sets so showing this claim is enough.

"$\Leftarrow$"
Suppose $P(a_1,...,a_n) = 0$. Then for any u, $u \cdot P(a_1,...,a_n)$ will equal zero.

Also, since 2 and 3 have no multiplicative inverse in $\mathbb{Z}$ and since $\mathbb{Z}$ is an integral domain, the right hand side cannot equal zero for any v or w. So there cannot exist u, v and w satisfying the equation. So we showed "$\Leftarrow$".

"$\Rightarrow$"
Suppose $P(a_1, ..., a_n) \neq 0$. We wish to show that there are integers u, v and w such that $u \cdot P(x_1, ..., x_n) = (2v-1)(3w-1)$. Now if the value of $P(a_1, ..., a_n)$ is odd, say $2k-1$, then simply let $u = 3k-1$, and $v = w = k$. Then clearly, $u \cdot P(a_1, ..., a_n) = (2v-1)(3w-1)$ holds. If on the other hand $P(a_1, ..., a_n)$ is even, then $P(a_1, ..., a_n)$ can be written in the form $2^k \cdot (2m-1)$ for some integer m. Next, it's easy to check that $2^k \equiv 1$ or $2 \mod 3$. So we consider the two cases.

- Case: $2^k \equiv 1 \mod 3$
  Then $2 \cdot 2^k \equiv 2 \mod 3$. So $2 \cdot 2^k = 3t - 1$ for some integer t. Now simply let $u = 2, v = m$ and $w = t$. Then

$$\begin{aligned} u \cdot P(a_1, ..., a_n) &= 2 \cdot 2^k \cdot (2m-1) \\ &= (3t-1)(2m-1) \\ &= (3w-1)(2v-1). \end{aligned}$$

  So $u \cdot P(a_1, ..., a_n) = (2v-1)(3w-1)$ holds.

- Case: $2^k \equiv 2 \mod 3$
  Then, $2^k = 3t - 1$ for some integer t. So let $u = 1, v = m$ and $w = t$. Then

$$\begin{aligned} u \cdot P(a_1, ..., a_n) &= 1 \cdot 2^k \cdot (2m-1) \\ &= (3t-1)(2m-1) \\ &= (3w-1)(2v-1). \end{aligned}$$

  So $u \cdot P(a_1, ..., a_n) = (2v-1)(3w-1)$ holds.

This completes the proof. □

This now allows us to prove:

Theorem 2.4.3. *Sets defined by existential formulas of the form $\exists x_1, ..., x_n \theta(x_1, ..., x_n)$, where θ is a quantifier free formula, are Diophantine sets.*

Proof. By the Disjunctive Normal Form theorem, we can write θ in a disjunctive normal form:

$$\bigvee_i \bigwedge_{j_i} \psi_{j_i}$$

where ψ_{j_i} are atomic formulas or negations of atomic formulas. In turn, using the commutativity of $\wedge$, we can rewrite θ as:

$$\bigvee_i \left(\bigwedge_{j_i} \alpha_{j_i} \wedge \bigwedge_{k_i} \neg \alpha_{k_i} \right),$$

where α are atomic formulas. Now we already saw that atomic formulas in $\langle \mathbb{Z}; +, \cdot, 0, 1 \rangle$ are polynomial equations of the form $P(x_1, ..., x_n) = 0$. So by iterative execution of Lemma 2.4.1(1), we see that $\bigwedge_{j_i} \alpha_{j_i}$ define Diophantine sets. As for the negated atomic formulas, Lemma 2.4.2 tells us that they define Diophantine sets. So again, by Lemma 2.4.1(1), $\bigwedge_{k_i} \neg \alpha_{k_i}$ define Diophantine sets. In turn, $\bigwedge_{j_i} \alpha_{j_i} \wedge \bigwedge_{k_i} \neg \alpha_{k_i}$ are Diophantine. Next, θ defines Diophantine set by Lemma 2.4.1(2). Finally, Lemma 2.4.1(3) tells us $\exists x_1, ..., x_n \theta(x_1, ..., x_n)$ defines a Diophantine set. □

The notion of existential formulas will be discussed further in Section 3.2.

As for the universal quantifier, we will show later in Section 2.7 that *bounded* universal quantifiers can be included in the language of Diophantine sets.

2.5 Two important tools

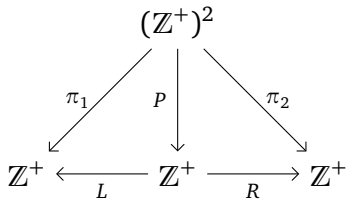
Two very important Diophantine functions will be needed in various parts of the proofs for H10/$\mathbb{Z}$. These are: Pairing function, and Sequence number function.

Pairing Function

Later on, we will wish to 'encode' ordered pairs of numbers $\langle a, b \rangle$ by a single number n in a Diophantine way. We wish to do this in a way such that we can 'retrieve' the ordered pair back. In other words, we want Diophantine functions $P : (\mathbb{Z}^+)^2 \to \mathbb{Z}^+$, $L : \mathbb{Z}^+ \to \mathbb{Z}^+$ and $R : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that:

$$P : \langle a, b \rangle \mapsto P(\langle a, b \rangle)$$
$$L : P(\langle a, b \rangle) \mapsto a$$
$$R : P(\langle a, b \rangle) \mapsto b$$

In other words, we want the following diagram to commute:



(π_i is the projection map to the ith coordinate)

This is possible as we have a (Diophantine) bijection $(\mathbb{Z}^+)^2 \sim \mathbb{Z}^+$. As with Davis' paper, the bijection we will use will be based on the Triangular numbers $T(n)$:

$$T(n) = 1 + 2 + ... + n = \frac{n(n+1)}{2}.$$

Now for a given $z \in \mathbb{Z}^+$, as T is an increasing function, there will be a unique $n \geq 0$ such that:

$$T(n) < z \leq T(n+1).$$

And since by definition $T(n+1) = T(n) + n + 1$, z can be written as:

$$z = T(n) + y; \text{ for some unique } y \leq n+1.$$

Now writing $n = x + y - 2$ for some unique $x \in \mathbb{Z}^+$, (since x and y are positive, the -2 is needed to keep $n \geq 0$) we have:

$$z = T(x + y - 2) + y.$$

Expanding out T, we get:

$$z = \frac{(x+y-2)(x+y-1)}{2} + y.$$

Now we're done because we can take $P(\langle x, y\rangle) = z$, $L(z) = x$ and $R(z) = y$. Also note that by construction, P is a bijective map as required.

We are now ready to prove:

Theorem 2.5.1. *(Pairing Function Theorem). There are Diophantine functions $P(x,y), L(z), R(z)$ such that*
(1) for all x, y, $L(P(x,y)) = x$, $R(P(x,y)) = y$,
(2) for all z, $P(L(z), R(Z)) = z$, and
(3) for all z, $L(z) \leq z$ and $R(z) \leq z$.

Proof. (1) and (2) are clear by construction above, so we just need to show that the functions are Diophantine and (3).

We can see that P, L and R are Diophantine as:

$$\begin{aligned} z{=}P(x,y) &\iff 2z = (x+y-2)(x+y-1)+2y \\ x{=}\ L(z) &\iff (\exists y)[2z = (x+y-2)(x+y-1)+2y\,] \\ y{=}\ R(z) &\iff (\exists x)[2z = (x+y-2)(x+y-1)+2y\,] \end{aligned}$$

As for (3), notice that:

$$x-1, y-1 \leq x+y-2 = n \leq T(n) < T(n)+y = z,$$

so $x, y \leq z$.

□

Sequence Number Theorem

The Sequence Number Theorem is, in a sense, an extension of the Pairing Function Theorem. This is because the theorem allows us to 'encode' a finite sequence of numbers $a_1, ..., a_N$ by some number u and then retrieve the sequence back by some given function. More precisely:

Theorem 2.5.2. *(Sequence Number Theorem). There is a Diophantine function $S : (\mathbb{Z}^+)^2 \to \mathbb{Z}^+$ such that*
(1) $S(\langle i,u\rangle) \leq u$, and
(2) for each sequence $a_1, ..., a_N$, there is a number u such that

$$S(\langle i,u\rangle) = a_i \text{ for } 1 \leq i \leq N.$$

Proof. Let $\langle i,u\rangle$ be given. Then we can find the values of $L(u)$ and $R(u)$ by the Pairing functions. By dividing $L(u)$ by $1+iR(u)$, one can write for some $n \in \mathbb{Z}^+$:

$$L(u) = (n-1)(1+iR(u)) + r;\ 0 < r \leq 1+iR(u)$$

Now we define a function $S : (\mathbb{Z}^+)^2 \to \mathbb{Z}^+$ given by:

$$S(\langle i,u\rangle) = r$$

S is a well defined function as the remainder r is unique. We claim that S satisfies the properties laid out in the theorem.

S is Diophantine

By definition, $r = S(\langle i,u\rangle)$ if and only if there exists some $n \in \mathbb{Z}^+$ such that $L(u) = n(1+iR(u)) + r$ and $0 < r \leq 1 + iR(u)$. In turn, $r = S(\langle i,u\rangle)$ if and only if the following system of equations has a solution:

$$\begin{aligned} x &= L(u) \\ y &= R(u) \\ x &= (n-1)(1+iy) + r \\ r + m - 1 &= 1 + iy \end{aligned}$$

Clearly, each equation is Diophantine (the first two due to the Pair Function Theorem) and we already showed that a system of equations can be reduced to a single equation in a Diophantine way, so S is indeed a Diophantine function.

S satisfies (1)

Since $L(u) = (n-1)(1+iR(u)) + r$, we have $S(\langle i,u\rangle) \leq L(u)$. Also, we know from the Pair Function Theorem, that $L(u) \leq u$. So $S(\langle i,u\rangle) \leq u$.

S satisfies (2)

Let $a_1, ..., a_N$ be given. Choose $n \in \mathbb{Z}^+$ big enough such that $n \cdot N!$ is bigger than each of $a_1, ..., a_N$. Denote $n \cdot N!$ as y. Then by elementary number theory, the numbers $1+y, 1+2y, ...1+Ny$ are pairwise coprime. So by the Chinese Remainder Theorem, there is a number x such that:

$$\begin{aligned} x &\equiv a_1 \mod 1+y \\ x &\equiv a_2 \mod 1+2y \\ &\cdots \\ x &\equiv a_N \mod 1+Ny \end{aligned}$$

Of course x needs to be a *positive* number but this can always be done by adding big enough multiple of $\prod_{k=1}^{N} 1+ky$ to x. Next, with x and y we found, let $u = P(\langle x,y\rangle)$. Then $x = L(u)$ and $y = R(u)$ so we have

$$a_i \equiv L(u) \mod 1 + iR(u);\ \text{for i=1,2,...,N.}$$

Finally, since by construction, $a_i < y = R(u)$, we have $a_i < 1 + iR(u)$. In other words, $a_i = S(\langle i,u\rangle)$.

We have shown that S satisfies the conditions, so we are done. □

2.6 Exponential function is Diophantine

One of the main mechanisms for the proof of $\neg$H10/$\mathbb{Z}$ is the exponential function.

Theorem 2.6.1. *The exponential function*

$$\exp(n,k) = n^k$$

is Diophantine.

Davis gives a proof of the theorem using the Pell equation:

$$x^2 - dy^2 = 1,$$

where $x, y \geq 0$, $d = a^2 - 1$ for some $a > 1$. The actual proof of this theorem runs over many pages of elementary number theory. As mentioned in the beginning of the paper, the proof of this theorem lies outside our interests and will not be included here.

Using this theorem, Davis also proves that the following important functions are Diophantine:

Theorem 2.6.2. *The following functions are Diophantine:*

1. $f(n,k) = \binom{n}{k}$
2. $g(n) = n!$
3. $h(a,b,y) = \prod_{k=1}^{y} a + bk$

The proof of this theorem will not be included for the same reasons.

The fact that the exponential function is Diophantine gives us an interesting example. The Diophantine equation is my own formulation.

Example 2.6.3. *The negation of Fermat's Last Theorem is equivalent to finding a solution to a Diophantine equation.*

Proof. The negation of the Fermat's Last Theorem(FLT) is that there is x, y, z and $n > 2$ such that $x^n + y^n = z^n$:

$$\neg FLT \Leftrightarrow (\exists x, y, z, n, a, b, c, d)[n = d+2 \wedge a = x^n \wedge b = y^n \wedge c = z^n \wedge a+b = c].$$

□

This relation tells us that the Fermat's Last Theorem is false if and only if there is a solution to the right hand side of the relation. As we know from Andrew Wiles [39], there can be no solution to the equation.

2.7 Bounded universal quantifiers

Although we can't have the universal quantifiers, we can however have the next best thing. We will show in this section that Diophantine sets are closed under taking *bounded* universal quantifiers of the form:

$$\forall x \leq n \ldots \text{ which we take it to mean } \forall x(x > n \vee \ldots).$$

Theorem 2.7.1. *If P is a polynomial and*

$$S = \{\langle y, x_1, ..., x_n\rangle : (\forall z \leq y)(\exists y_1, ..., y_m)[P(y, z, x_1, ..., x_n, y_1, ..., y_m) = 0]\},$$

then S is Diophantine.

We prove this by first proving three lemmas.

Lemma 2.7.2.

$$\forall z \leq y(\exists y_1, ..., y_m)[P(y, z, x_1, ..., x_n, y_1, ..., y_m) = 0$$
$$\Longleftrightarrow$$
$$\exists u(\forall z \leq y)(\exists y_1 \leq u, ..., y_m \leq u)[P(y, z, x_1, ..., x_n, y_1, ..., y_m) = 0]$$

Proof.
"$\Leftarrow$" Trivial.
"$\Rightarrow$" The left hand side implies for each $z = 1, ..., y$, there exists corresponding numbers $y_{z_1}, ...y_{z_m}$ such that

$$P(y, z, x_1, ..., x_n, y_{z_1}, ...y_{z_m}) = 0.$$

Then taking $u = \max\{y_{z_i} : z = 1, ...y,\ i = 1, ...m\}$, we are done. □

Lemma 2.7.3. *Let $P(y, z, x_1, ..., x_n, y_1, ..., y_m)$ be given. Then there is a polynomial $Q(y, u, x_1, ..., x_n)$ with the properties:*

(1) $Q(y, u, x_1, ..., x_n) > y$ and $Q(y, u, x_1, ..., x_n) > u$,

(2) If $z \leq y$ and $y_1, ..., y_m \leq u$ then $|P(y, z, x_1, ..., x_n, y_1, ..., y_m)| \leq Q(y, u, x_1, ..., x_n)$.

Proof. We can express $P(y, z, x_1, ..., x_n, y_1, ..., y_m)$ in a general form:

$$\sum_{i=1}^{N} c_r y^{a_i} z^{b_i} x_1^{q_{i_1}} x_2^{q_{i_2}} \cdots x_n^{q_{i_n}} y_1^{s_{i_1}} y_2^{s_{i_2}} \cdots y_m^{s_{i_m}}$$

where c_r are positive or negative. Now we simply let $Q(y,u,x_1,...,x_n)$ equal to:

$$y+u+\sum_{i=1}^{N}|c_r|y^{a_i+b_i}x_1^{q_{i_1}}x_2^{q_{i_2}}\cdots x_n^{q_{i_n}}u^{s_{i_1}+s_{i_2}+\cdots+s_{i_m}}$$

Then clearly, $Q = y+u+\sum_{i=1}^{N}\cdots > y$ and u so (1) holds.
For (2), observe that:

$$z \le y \text{ implies } y^{a_i}z^{b_i} \le y^{a_i+b_i}$$
$$y_1,...,y_m \le u \text{ implies } y_1^{s_{i_1}}y_2^{s_{i_2}}\cdots y_m^{s_{i_m}} \le u^{s_{i_1}+s_{i_2}+\cdots+s_{i_m}}$$

So $|P(y,z,x_1,...,x_n,y_1,...,y_m)| \le Q(y,u,x_1,...,x_n)$ □

Lemma 2.7.4. *Let $P(y,z,x_1,...,x_n,y_1,...,y_m)$ be given and let $Q(y,u,x_1,...,x_n)$ satisfy (1) and (2) as above. Then,*

$$(\forall z \le y)(\exists y_1 \le u,...,y_m \le u)[P(y,z,x_1,...,x_n,y_1,...,y_m)=0]$$

if and only if there are $c,t,a_1,...,a_m$ such that the following hold:

(a) $1+ct = \prod_{z=1}^{y}(1+zt)$

(b) $t = Q(y,u,x_1,...,x_n)!$

(c) $1+ct \mid \prod_{z=1}^{u}(a_i-j)$ *for each* $i=1,...m$

(d) $P(y,c,x_1,...,x_n,a_1,...,a_m) \equiv 0 \mod 1+ct$

Proof.
"⇐" We need to show that for each $z=1,...,y$, there are positive numbers $y_{z_1},...,y_{z_m}$ such that:

(i) $1 \le y_{z_i} \le u$

(ii) $P(y,z,x_1,...,x_n,y_{z_1},...,y_{z_m})=0.$

Finding the candidates
For each z, let p_z be a prime factor of $1+zt$.
For each z, let y_{z_i} be the remainder when a_i is divided by p_z for each $i=1,...,m$. We also note that this means $a_i \equiv y_{z_i} \mod p_z$ and $y_{z_i} < p_z$.
We now have candidates for $y_{z_1},...,y_{z_m}$ so we just need to show that the numbers y_{z_i} satisfies (i) and (ii).

Showing (i)
For each i,

$$\begin{aligned} p_z|1+zt & \qquad \text{(By definition of } p_z\text{)} \\ 1+zt|1+ct & \qquad \text{(Since } 1+ct=\prod_{z=1}^{y}(1+zt) \text{ by (a))} \\ 1+ct|\prod_{z=1}^{u}(a_i-j) & \qquad \text{(By (c))} \end{aligned}$$

Therefore, $p_z|\prod_{z=1}^{u}(a_i-j)$ and as p_z is prime, p_z must divide a_i-j for some $j=1,...u$. This together with the note above implies:

$$j \equiv a_i \equiv y_{z_i} \mod p_z$$

Now any divisor of $1+zt$ cannot divide t (elementary number theory). Also, since $t = Q(y,u,x_1,...,x_n)!$ (by (b)), any divisor of $1+zt$ must be bigger than $Q(y,u,x_1,...,x_n)$ (otherwise, it would divide t). In particular, $p_z > Q(y,u,x_1,...,x_n)$. We also know by (1) that $Q(y,u,x_1,...,x_n) > u$, so $p_z > u$ which in turn gives $1 \leq j \leq u < p_z$. In summary, we have j and y_{z_i} such that $j \equiv y_{z_i} \mod p_z$ which are both less than p_z. This gives us:

$$1 \leq y_{z_i} = j \leq u$$

so we showed (i).

Showing (ii)

$$\begin{aligned} 1+ct \equiv 1+zt \equiv 0 \mod p_z & \qquad \text{(Since } p_z \text{ divides both)} \\ z+zct \equiv c+zct \mod p_z & \qquad \text{(Multiplying both sides by } z \text{ and } c \text{ respectively)} \\ z \equiv c \mod p_z & \qquad \text{(Taking away } zct \text{ on both sides)} \end{aligned}$$

So we have $z \equiv c \mod p_z$ and $y_{z_i} \equiv a_i \mod p_z$ (from (i)). Therefore:

$$P(y,z,x_1,...,x_n,y_{z_1},...,y_{z_m}) \equiv P(y,c,x_1,...,x_n,a_1,...,a_m) \mod p_z$$

because replacing values by another which is equivalent modulo p_z in a polynomial doesn't change the value of the polynomial modulo p_z (elementary number theory). Now (d) gives us:

$$P(y,z,x_1,...,x_n,y_{z_1},...,y_{z_m}) \equiv 0 \mod p_z.$$

Also (3), together with $> Q(y, u, x_1, ..., x_n)$ from (i) gives us:

$$|P(y, z, x_1, ..., x_n, y_1, ..., y_m)| < p_z$$

which gives us:

$$P(y, z, x_1, ..., x_n, y_{z_1}, ..., y_{z_m}) = 0.$$

So we showed (ii) and hence we showed "⇐".

"⇒" Now suppose for each $z = 1, ..., y$, there are positive numbers $y_{z_1}, ..., y_{z_m}$ all less than or equal to u such that

$$P(y, z, x_1, ..., x_n, y_{z_1}, ..., y_{z_m}) = 0.$$

We need to show that there are numbers $c, t, a_1, ..., a_m$ such that (a),(b),(c) and (d) are satisfied.
To find t, simply let $t = Q(y, u, x_1, ..., x_n)!$. This satisfies (b).

To find c, let c be the number such that $1 + ct = \prod_{z=1}^{y}(1 + zt)$. This is possible as $\prod_{z=1}^{y}(1+zt) \equiv 1 \mod t$ (If we expand out the product, all terms except 1 will have a factor of t in it). This satisfies (a).

To find $a_1, ..., a_m$, we will make use of the Chinese Remainder Theorem. First we show that the numbers $1+1t, 1+2t, ..., 1+yt$ are pairwise coprime. Suppose $1 \leq k < l \leq y$ and suppose for a contradiction that there is some prime p, p divides $1+kt$ and $1+lt$. Then, p divides $(1+lt)-(1+kt) = (l-k)t$. Again, we know from elementary number theory that $p \nmid t$ which means $p|l-k$ as p is prime. Now $l-k < y$ so $p < y$. Since $y < Q(y, u, x_1, ..., x_n)$ by (1), we have $p < Q(y, u, x_1, ..., x_n)$ which means $p|Q(y, u, x_1, ..., x_n)! = t$ which we know can't happen. Therefore $1+1t, 1+2t, ..., 1+yt$ are pairwise coprime. So the Chinese Remainder Theorem applies, and for each $1 \leq i \leq m$, there exists a number a_i such that

$$a_i \equiv y_{z_i} \mod 1 + zt, \text{ for } z = 1, ..., y.$$

To show that (d) is satisfied, we first note that $c \equiv z \mod 1 + kt$ which is true by the same argument of showing $c \equiv z \mod p_z$ from above but replacing p_z by $1 + zt$. This means that:

$$P(y, c, x_1, ..., x_n, a_1, ..., a_m) \equiv P(y, z, x_1, ..., x_n, y_{z_1}, ..., y_{z_m}) \mod 1 + zt$$

and the right hand side of the equation equals to 0 by assumption. So we deduce $1 + zt$ divides $P(y, c, x_1, ..., x_n, a_1, ..., a_m)$ for each z. But since $1 +$

$1t, 1+2t, ..., 1+yt$ are pairwise coprime, the product, i.e. $1+ct$ divides $P(y, c, x_1, ..., x_n, a_1, ..., a_m)$ (elementary number theory). So:

$$P(y, c, x_1, ..., x_n, a_1, ..., a_m) \equiv 0 \mod 1+ct$$

which shows (d) is satisfied.

To show (c), we first recall $a_i \equiv y_{z_i} \mod 1+zt$ for each i, and this implies $1+zt | a_i - y_{z_i}$. But by assumption, $1 \leq y_{z_i} \leq j$ which means $1+zt | \prod_{z=1}^{u}(a_i - j)$ as the product will contain a factor of $a_i - y_{z_i}$ when $j = y_{z_i}$. Again, $1+1t, 1+2t, ..., 1+yt$ are pairwise coprime so the product $1+ct$ also divides $\prod_{z=1}^{u}(a_i - j)$. This shows (c) is satisfied.
So "⇒" is shown to hold.

So we're done. □

Finally, we can now easily prove Theorem 2.7.1 using the three Lemmas we just shown.

Proof. Let $P(y, z, x_1, ..., x_n, y_1, ..., y_m)$ be given. Then:

$$\begin{aligned}
\langle y, \bar{x} \rangle \in S &\Leftrightarrow (\forall z \leq y)(\exists \bar{y})[P(y, z, \bar{x}, \bar{y}) = 0]\} \\
&\Leftrightarrow \exists u (\forall z \leq y)(\exists \bar{y} \leq u)[P(y, z, \bar{x}, \bar{y}) = 0] \qquad \text{(Lemma 2.7.2)} \\
&\Leftrightarrow \text{there are } c, t, a_1, ..., a_m \text{ such that} \\
&\quad \text{the following holds:} \\
&\quad (a) 1+ct = \prod_{z=1}^{y}(1+zt) \\
&\quad (b) t = Q(y, u, x_1, ..., x_n)! \\
&\quad (c) 1+ct | \prod_{z=1}^{u}(a_i - j) \text{ for each } i = 1, ...m \\
&\quad (d) P(y, c, x_1, ..., x_n, a_1, ..., a_m) \equiv 0 \mod 1+ct
\end{aligned}$$

by Lemma 2.7.3 and Lemma 2.7.4. As the last four conditions are Diophantine equations, we are done. □

2.8 Further examples of Diophantine sets

With the introduction of bounded universal quantifiers into the language of Diophantine sets, we can show that basically all the usual sets are Dio-

phantine. In fact, it will be very difficult to come up with examples of non-Diophantine sets. We begin with further examples of Diophantine sets we can now describe using bounded quantifiers. These examples are my own. Techniques from other sources are highlighted.

Examples 2.8.1. *The following are Diophantine:*

(i) Fibonacci numbers

(ii) Goldbach's conjecture

Proof.

(i) Fibonacci numbers
(This proof follows Davis' technique in proving "Primitive Recursion is Diophantine" in his Theorem 6.1 [5, p. 259]). The sequence of Fibonacci numbers are defined by the first two terms $a_1 = 1$ and $a_2 = 1$. Then, a_{n+2} is obtained by the formula $a_{n+2} = a_n + a_{n+1}$. This sequence can be captured by the combination of the Sequence Number Theorem and the bounded quantifiers. In essence, we define a sequence with the two initial terms and add the property that for any two consecutive terms less than $n+2$, the next term is the sum of the two terms:

$$x \in S \Leftrightarrow x = 1 \vee (\exists n)[\text{“}x = a_{n+2}\text{”}]$$

where “$x = a_{n+2}$” is to mean:

$$\begin{aligned}(\exists u)[(&S(1,u) = 1 \wedge S(2,u) = 1 \wedge S(n+2,u) = x \\ &\wedge (\forall m \leq n+2)(m = n+2 \vee m = n+1 \vee \\ &(\exists a,b)(a = S(m,u) \wedge b = S(m+1,u) \wedge S(m+2,u) = a+b))]\end{aligned}$$

(ii) Goldbach's conjecture
Again, as with Example 2.6.3, we shall express the negation of Goldbach, i.e. there exists an even number greater than two such that it is not a sum of any two primes:

$$\begin{aligned}\neg\text{Goldbach} \Leftrightarrow (\exists n,m)[n = 2(m+1) \wedge (\forall p \leq n, q \leq n)(\exists a,b)(p = (a+1)(b+1) \\ \vee\ q = (a+1)(b+1) \vee p+q < n \vee p+q > n)]\end{aligned}$$

The Diophantine expression of “not prime” is taken from Davis' paper Example (ii) in [5, p. 235]

□

2.9 Recursive functions

With the addition of bounded universal quantifiers in our language of Diophantine sets, we have all the tools we'll need for completion of the proof. Our language of Diophantine sets are powerful enough to show that all recursive functions are Diophantine. Recursive functions are computable functions. More relevant to the context, they are the functions which have algorithms to compute the values.

Definition 2.9.1. The *recursive functions* are all those functions obtainable from the initial functions:
Constant unit function: $c(x) = 1$
Successor function: $s(x) = x + 1$
Projection function: $U_i^n(x_1, ..., x_n) = x_i$, $1 \leq i \leq n$
Sequence number function: $S(i, u)$ (as in Theorem 2.5.2)
iteratively applying the three operations:

COMPOSITION yields the function

$$h(x_1, ..., x_n) = f(g_i(x_1, ..., x_n), ..., g_m(x_1, ..., x_n))$$

from the given functions $g_1, ..., g_m$ and $f(y_1, ..., y_m)$.

PRIMITIVE RECURSION yields the function $h(x_1, ..., x_n, m)$ which satisfies the equations:

$$h(x_1, ..., x_n, 1) = f(x_1, ..., x_n)$$
$$h(x_1, ..., x_n, l + 1) = g(t, h(x_1, ..., x_n, l), x_1, ..., x_n),$$

from the given functions f, g.
When $n = 0$, f becomes a constant so that h is obtained directly from g.

MINIMALIZATION yields the function:

$$h(x_1, ..., x_n) = \min\{y : f(x_1, ..., x_n, y) = g(x_1, ..., x_n, y)\}$$

from the given functions f, g assuming that f, g are such that for each $x_1, ..., x_n$ there is at least one y satisfying the equation $f(x_1, ..., x_n, y) = g(x_1, ..., x_n, y)$; (i.e., h must be everywhere defined).

We now prove one of the key theorem for the $\neg$H10/$\mathbb{Z}$:

Theorem 2.9.2. *Recursive functions are Diophantine.*

Proof. All initial functions are clearly Diaphontine and $S(i,u)$ was shown to be Diaphontine in Theorem 2.5.2. So it is enough to show that the Diaphontine functions are closed under the three operations of recursion.

Composition This is straightforward enough:

$$\begin{aligned} y = h(x_1,...,x_n) &\Leftrightarrow \text{“}y = f(g_1(x_1,...,x_n),...,g_m(x_1,...,x_n)\text{”} \\ &\Leftrightarrow (\exists t_1,...,t_m)[t_1 = g_1(x_1,...,x_n) \wedge \ldots \\ &\wedge\ t_m = g_m(x_1,...,x_n) \wedge y = f(t_1,...,t_m)] \end{aligned}$$

The last expression is Diophantine as f and g were assumed to be Diophantine.

Primitive Recursion This is a generalisation of the technique used in proving that the Fibonacci numbers were Diophantine. We prove this using the Sequence Number Theorem and bounded universal quantifiers:

$$\begin{aligned} & y = h(x_1,...,x_n,m) \\ & \Leftrightarrow (\exists u)(\forall l \leq m)\text{“}h(\bar{x},l) = S(l,u) \wedge S(m,u) = y\text{”} \\ & \Leftrightarrow (\exists u)\text{“}S(1,u) = f(\bar{x}),(\forall l < m)(S(l+1,u) = g(l,S(l,u),\bar{x})),S(m,u) = y\text{”} \\ & \Leftrightarrow (\exists u,v)[(v = S(1,u) \wedge v = f(x_1,...,x_n)) \\ & \wedge\ (\forall l \leq m)((l = m) \vee (\exists w)(w = S(l+1,u) \\ & \wedge\ w = g(l,S(l,u),x_1,...,x_n))) \wedge y = S(m,u)] \end{aligned}$$

The last expression is Diophantine as f and g were assumed to be Diophantine, $S(i,u)$ is Diophantine and $\forall l \leq m$ is Diophantine.

Minimalization

$$\begin{aligned} & y = h(x_1,...,x_n,m) \\ & \Leftrightarrow \text{“}f(\bar{x},y) = g(\bar{x},y) \text{ and } y \text{ is the smallest such number”} \\ & \Leftrightarrow \text{“}f(\bar{x},y) = g(\bar{x},y) \wedge (\forall y < n)f(\bar{x},y) \neq g(\bar{x},y)\text{”} \\ & \Leftrightarrow \text{“}f(\bar{x},y) = g(\bar{x},y) \wedge (\forall y < n)(f(\bar{x},y) < g(\bar{x},y) \vee f(\bar{x},y) > g(\bar{x},y)\text{”} \\ & \Leftrightarrow (\exists v)[v = f(\bar{x},y) \wedge v = g(\bar{x},y)] \\ & \wedge\ (\forall l \leq y)[l = y \vee (\exists s,t)(s = f(\bar{x},l) \wedge g(\bar{x},l) \wedge (s < t \vee t < s)] \end{aligned}$$

The last expression is Diophantine as f and g were assumed to be Diophantine, $\forall l \leq y$ is Diophantine and $s < t$ is Diophantine.

□

In fact, the converse can also be shown to be true quite straightforwardly. This is proven in Theorem 6.1 Davis' paper. However, we won't go through the proof because this direction is not needed for the proof of $\neg$H10/$\mathbb{Z}$.

2.10 A universal Diophantine set

We will set up an explicit enumeration of all the Diophantine sets of positive integers.

We first give an enumeration of all the polynomials of *positive* coefficients. Clearly, any polynomial of positive coefficients is a result of the number 1, finite list of variables and finite number of successive addition and multiplications. So we will set up an enumeration which contains 1, all the variables and successive additions and multiplications. This is how Davis does it using the Pairing function. Let

$$P_1 = 1.$$

Then, let us split the positive numbers into three groups: 0,1,2 mod 3. One group will list all the variables $x_0, x_1, x_2, ...$, one group will list additions of the previous terms in the sequence of P_i and the last group will list multiplications of the previous terms, like so:

$$\begin{aligned} P_1 &= 1 \\ P_{3i-1} &= x_{i-1} \\ P_{3i} &= P_{L(i)} + P_{R(i)} \\ P_{3i+1} &= P_{L(i)} \cdot P_{R(i)} \end{aligned}$$

One can roughly see how this gives us the enumeration of the polynomials. Davis' paper doesn't include a proof of this but I will include my own proof of it in this paper. The term 'length of a polynomial' is a notation I came up with for this specific proof. I acknowledge my friend Gergely Szucs who spotted the error for my original notion whilst proof reading and suggested an alternative one below.

Lemma 2.10.1. *The sequence $P_0, P_1, P_2, ...$ gives us an enumeration of all polynomials of positive coefficients.*

We will prove this by induction on the lengths of polynomials where the lengths of polynomials are to be defined as below.

Definition 2.10.2. Given a polynomial $P(x_1, ..., x_n)$ which will be in the form $\sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_j^{i_j}$, the *length* of P, denoted by $l(P)$, is defined by:

$$\sum_{i=1}^{m} \left(|a_i| \sum_{j=1}^{n} (i_j + 1) \right)$$

By the way polynomials are constructed, this is clearly well defined.

Proof. We will show that for all P, there exists some n such that $P = P_n$. We proceed by induction on $l(P)$.

- *Base case:*
  Suppose $l(P) = 1$. Then by definition, P equals to 1 or x_k for some positive number k. If the former, $P = P_1$ and if the latter, $P = P_{3k-1}$.

- *Inductive step*
  Suppose true for all polynomials with length strictly less than t. Let

  $$P = \sum_{i=1}^{m} a_i \prod_{j=1}^{n} x_j^{i_j}$$

  and let $l(P) = t$. If t is greater than 1, then by definition of the length, there are two cases:

  1. There are two non zero polynomials Q and R such that $P = Q + R$
     In this case, since Q and R are non zero, they must have length at least 1 and hence their lengths are strictly less than t.
  2. P is a monic monomial
     In this case, P will be of the form $\prod_{j=1}^{n} x_j^{i_j}$. Since we assumed $l(P) > 1$, then P must be of the form $Q \cdot R$ for some monic monomials Q and R with length at least 1. So again, there are Q and R such that their length are strictly less than t.

  In short, there exist polynomials Q and R such that either $P = Q + R$ or $P = Q \cdot R$ with $l(Q) < t$ and $l(R) < t$. So inductive hypothesis applies for Q and R. So there exist numbers q and r such that $Q = P_q$ and $R = P_r$. Then, we have $P = P_{3P(\langle q,r \rangle)}$ if former and $P = P_{3P(\langle q,r \rangle)+1}$ if the latter, where $P(\langle q, r \rangle)$ is the pairing function. This is because

  $$P_{3P(\langle q,r \rangle)} = P_{L(P(\langle q,r \rangle))} + P_{R(P(\langle q,r \rangle))} = P_q + P_r$$

and

$$P_{3P(\langle q,r\rangle)+1} = P_{L(P(\langle q,r\rangle))} \cdot P_{R(P(\langle q,r\rangle))} = P_q \cdot P_r.$$

by the properties of the pairing function and by definition of P_i.

So by induction, we have that all polynomials of positive coefficients are included in $P_1, P_2, ...$ □

Now it's easy to give an enumeration of all Diophantine sets of positive integers.

Theorem 2.10.3. *$D_1, D_2, ...$ defined by:*

$$D_n = \{x_0 : (\exists x_1, ..., x_n)[P_{L(n)}(x_0, x_1, ...x_n) = P_{R(n)}(x_0, x_1, ...x_n)\},$$

where "$P_i(x_0, ..., x_n)$" means at most $x_0, ..., x_n$ variables appear in P_i, gives us an enumeration of all Diophantine sets of positive integers.

Proof. There are two things to check. Firstly, do $P_{L(n)}(x_0, x_1, ...x_n)$ and $P_{R(n)}(x_0, x_1, ...x_n)$ make sense? In other words, is it the case that at most $x_0, ..., x_n$ variables appear in $P_{L(n)}$ and $P_{R(n)}$? Yes, it is the case because recall that $L(n), R(n) \leq n$, and so roughly at most $x_0, ..., x_{\lceil \frac{n}{3} \rceil}$ ($\lceil \frac{n}{3} \rceil$ is to mean the smallest integer bigger than $\frac{n}{3}$) can appear in either $P_{L(n)}$ or $P_{R(n)}$ which is certainly small enough.

Secondly, do $D_1, ...$ really cover all Diophantine sets of positive integers? Again, the answer is yes because by definition, any Diophantine set of positive integers can be written as:

$$\{x_0 : (\exists x_1, ..., x_n)[Q(x_0, x_1, ...x_n) = 0\}$$

for some polynomial Q of positive or negative integers. However, by taking away all the terms in the polynomial with negative coefficients on both sides, we will get two polynomials Q_1 and Q_2 with only positive coefficients such that:

$$Q(x_0, x_1, ...x_n) = 0 \Leftrightarrow Q_1(x_0, x_1, ...x_n) = Q_2(x_0, x_1, ...x_n).$$

In turn, these Q_1 and Q_2 can be written as $P_{L(i)}$ and $P_{R(i)}$ for some number i as shown above. So we are done. □

Now that we have a complete enumeration of all the Diophantine sets of positive integers, we are ready to give our first non-Diophantine set.

Theorem 2.10.4. *$V = \{n : n \notin D_n\}$ is not Diophantine.*

Proof. This largely follows Cantor's diagonal argument. If by contradiction V was Diophantine, then for some fixed i, $V = D_i$ as $D_1, ...$ gives complete enumeration of all Diophantine sets of positive integers. Now we ask: does $i \in V$?

$$i \in V \Leftrightarrow i \in D_i$$

since $V = D_i$. But also,

$$i \in V \Leftrightarrow i \notin D_i$$

by definition of V. This is a contradiction.
So V is not Diophantine. □

Now using Theorem 2.9.2 and Theorem 2.10.4, we can show that the test function g which decides whether x belongs to D_n or not is not Diophantine.

Theorem 2.10.5. *The function g defined by:*

$$g(x,n) = \begin{cases} 1 & \text{if } x \in D_n, \\ 2 & \text{if } x \notin D_n \end{cases}$$

is not recursive.

Proof. If g was recursive, then by Theorem 2.9.2, it would be Diophantine. So there will be a polynomial P such that

$$y = g(n,x) \Leftrightarrow (\exists y_1, ..., y_m)[P(x,n,y,y_1,...,y_m)].$$

But if there was such P, then we should be able to write V as

$$V = \{x : (\exists y_1, ..., y_m)[P(x,2,y,y_1,...,y_m)]\}$$

, and hence showing that V is Diophantine. This contradicts Theorem 2.10.4.
So g cannot be recursive. □

To finish this section, we prove one more theorem. It turns out, surprisingly, that the relation "$x \in D_n$" is Diophantine.

Theorem 2.10.6. *(Universality Theorem) $\{\langle x,n\rangle : x \in D_n\}$ is Diophantine.*

Proof. What makes this proof possible is the fact that the D_n are constructed recursively. We already saw that we can translate recursion in our language of Diophantine sets using the Sequence Number Theorem and bounded universal quantifiers. This is exactly how it will be proved. We claim that:

$$\begin{aligned} x \in D_n \Leftrightarrow & (\exists u)[S(1,u) = 1 \wedge S(2,u) = x \\ & \wedge (\forall i \leq n)(S(3i,u) = S(L(i),u) + S(R(i),u)) \\ & \wedge (\forall i \leq n)(S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)) \\ & \wedge S(L(n),u) = S(R(n),u)]. \end{aligned}$$

Clearly, the right hand side of the relation is Diophantine and so it's enough to prove the equivalence.

"$\Rightarrow$"
By definition,

$$D_n = \{x : (\exists x_1, ..., x_n)[P_{L(n)}(x, x_1, ..., x_n) = P_{R(n)}(x, x_1, ..., x_n)]\}.$$

So if $x \in D_n$, then by definition, there are numbers $m_1, ..., m_n$ such that $P_{L(n)}(x, m_1, ..., m_n) = P_{R(n)}(x, m_1, ..., m_n)$. So to find u, let u be the number such that

$$S(j,u) = P_j(x, m_1, ..., m_n)$$

for $j = 1, 2, ..., 3n+2$. Then clearly, for all $i \leq n$,

$$\begin{aligned} S(1,u) &= P_1(x, m_1, ..., m_n) = 1 \\ S(2,u) &= P_2(x, m_1, ..., m_n) = x \\ S(3i-1,u) &= P_{3i-1}(x, m_1, ..., m_n) = m_{i-1} \\ S(3i,u) &= P_{3i}(x, \bar{m}) = P_{L(i)}(x, \bar{m}) + P_{R(i)}(x, \bar{m}) = S(L(i),u) + S(R(i),u) \\ S(3i+1,u) &= P_{3i+1}(x, \bar{m}) = P_{L(i)}(x, \bar{m}) \cdot P_{R(i)}(x, \bar{m}) = S(L(i),u) + S(R(i),u) \\ S(L(n),u) &= P_{L(n)}(x, \bar{m}) = P_{R(n)}(x, \bar{m}) = S(R(n),u). \end{aligned}$$

So the right hand side holds.

"$\Leftarrow$"
Suppose the right hand side is true for given x and n. Are there numbers $m_1, ..., m_n$ such that $P_{L(n)}(x, m_1, ..., m_n) = P_{R(n)}(x, m_1, ..., m_n)$? Choose

$$m_1 = S(5,u), m_2 = S(8,u), ..., m_n = S(3n+2,u).$$

Then we claim that

$$S(j,u) = P_j(x, m_1, ..., m_n)$$

for $j = 1, 2, ..., 3n+2$. This is because, similar to above, for all $i \leq n$,

$$\begin{aligned}
P_1(x, \bar{m}) &= 1 = S(1, u) \text{ (Assumption on RHS)} \\
P_2(x, \bar{m}) &= x = S(2, u) \text{ (Assumption on RHS)} \\
P_{3i-1}(x, \bar{m}) &= m_{i-1} = S(3i-1, u) \text{ (By the way } m_i \text{ are defined)} \\
P_{3i}(x, \bar{m}) &= P_{L(i)}(x, \bar{m}) + P_{R(i)}(x, \bar{m}) = S(L(i), u) + S(R(i), u) = S(3i, u) \\
P_{3i+1}(x, \bar{m}) &= P_{L(i)}(x, \bar{m}) \cdot P_{R(i)}(x, \bar{m}) = S(L(i), u) + S(R(i), u) = S(3i+1, u) \\
P_{L(n)}(x, \bar{m}) &= S(L(n), u) = S(R(n), u) = P_{R(n)}(x, \bar{m}).
\end{aligned}$$

So we're done. □

In section 2.7, we mentioned that Diophantine sets aren't closed under including "not" and unbounded "for all" operations. Now we can see why. The universality theorem tells us that there is a polynomial P such that

$$x \in D_n \Leftrightarrow (\exists y_1, ..., y_m)[P(x, n, y_1, ..., y_m) = 0].$$

So,

$$\begin{aligned}
x \in V &\Leftrightarrow \text{“}x \notin D_x\text{”} \\
&\Leftrightarrow \neg(\exists y_1, ..., y_m)[P(x, x, y_1, ..., y_m) = 0] \\
&\Leftrightarrow (\forall y_1, ..., y_m)[P(x, x, y_1, ..., y_m) < 0 \vee P(x, x, y_1, ..., y_m) > 0].
\end{aligned}$$

In other words, if "not" and "for all" were admissible, V would be Diophantine which contradicts Theorem 2.10.4.

2.11 Hilbert's Tenth Problem over $\mathbb{Z}$ is unsolvable

Now we are finally ready to prove $\neg$H10/$\mathbb{Z}$.

Theorem 2.11.1. *Hilbert's Tenth Problem over the ring of integers is not solvable.*

Proof. By the universality theorem 2.10.6, there is a polynomial P such that

$$x \in D_n \Leftrightarrow (\exists y_1, ..., y_m)[P(x, n, y_1, ..., y_m) = 0].$$

Now if there was an algorithm which decides whether Diophantine polynomials has positive integer solutions or not, then the algorithm can be used to test whether or not the equation

$$P(x, n, y_1, ..., y_m) = 0$$

has a solution. In other words, whether or not $x \in D_n$. So this algorithm can compute the function $g(x, n)$ as defined in Theorem 2.10.5. But if a function has a computing algorithm, then it will be a recursive function, i.e. g will be recursive. This is a contradiction to Theorem 2.10.5. So there cannot be such an algorithm. So we're done. □

The step from the function having a computing algorithm to deducing that it must be a recursive function is due to Church's thesis which says that effectively computable functions are recursive. Admittedly, this is a thesis and not a proved theorem. This is because the notions like 'computable' and 'algorithm' are informal and non mathematical notions and hence cannot be proven formally. However, most mathematicians accept this thesis, i.e. recursive functions are what we mean by functions having a computing algorithm. For further reading, see for example, [4].

3 Field of Reals

3.1 Extending Hilbert's Tenth Problem

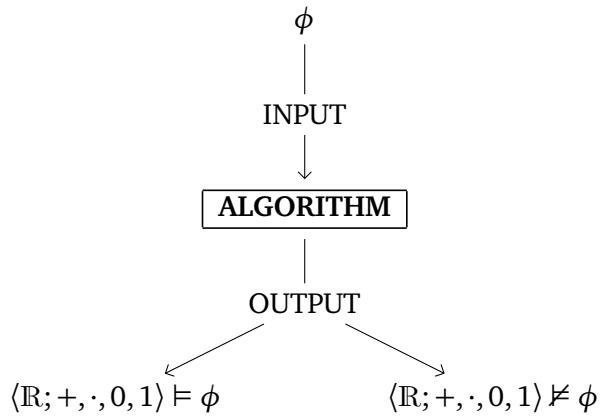
As we saw in the previous section, Hilbert's Tenth Problem over the ring of integers is unsolvable. We can extend Hilbert's original problem to different rings: given a ring R(with identity), is there an algorithm which decides whether or not a polynomial ring with integer coefficients has a solution in R? i.e.

Input : $f \in \mathbb{Z}[x_1, ..., x_n]$
Output : YES or NO, according to whether there are $a_1, ..., a_n \in R$ such that $f(a_1, ..., a_n) = 0$.

This definition is taken from Poonen's paper [29] and as he also notes, this definition makes sense because there is a unique ring homomorphism from $\mathbb{Z}$ to R.

3.2 Outline

In this section, we will show that H10/$\mathbb{R}$ is solvable by proving something stronger: the whole first order theory of $\mathbb{R}$ is decidable. In other words, we will prove that there is a decision procedure (an algorithm) which decides for *any sentence* ϕ in the first order language $\mathscr{L}\langle +, \cdot, 0, 1\rangle$, whether or not $\langle \mathbb{R}; +, \cdot, 0, 1\rangle \vDash \phi$.



In Theorem 2.4.3, we showed that existential formulas in the first order language of $\langle \mathbb{Z}; +, \cdot, 0, 1\rangle$ define Diophantine sets. This relationship extends

to the general ring $\langle R; +, \cdot, 0, 1\rangle$. We do have to be careful though because the polynomials we used to "translate" operations such as negation may not work in other rings. For example, in the reals,

$$P(a_1, ..., a_n) \neq 0 \Leftrightarrow \exists u, v, w[u \cdot P(a_1, ..., a_n) = (2v - 1)(3w - 1)]$$

does not hold because 2 and 3 have divisors $\frac{1}{2}$ and $\frac{1}{3}$ respectively. However, we can come up with alternative equations such as:

$$P(a_1, ..., a_n) \neq 0 \Leftrightarrow \exists u[u \cdot P(a_1, ..., a_n) = 1].$$

We can therefore see why then the decidability of the full first order theory of a ring implies solvability of H10/R. This is because if the full theory is decidable, then there will be an algorithm which decides for any sentence in the language of the ring, whether it is true or false. So the algorithm will also decide whether or not existential sentences, which are equivalent to Diophantine equations, are true or not i.e. whether or not there exist solutions for the polynomials.

We prove that $\langle \mathbb{R}; +, \cdot, 0, 1\rangle$ is decidable by proving something even stronger: that $\langle \mathbb{R}; +, -, \cdot, 0, 1, <\rangle$ is decidable. Notice that if there is a decision procedure for the extended language, this procedure will decide for our original language as well. Addition of the minus sign makes writing the proof more convenient. As for the inequality sign, this is necessary in order to prove Tarski's theorem which says that $\langle \mathbb{R}; +, -, \cdot, 0, 1, <\rangle$ admits quantifier elimination, in a decidable way. Roughly, this proof shows that there is an algorithm which takes any formula ϕ in $\mathscr{L}\langle +, -, \cdot, 0, 1, <\rangle$, which gives out another formula ψ in $\mathscr{L}\langle +, -, \cdot, 0, 1, <\rangle$ without any quantifiers such that

$$\langle \mathbb{R}; +, -, \cdot, 0, 1, <\rangle \vDash \phi \leftrightarrow \psi.$$

If we have such an algorithm, then truth of any sentence can be determined by simply checking the truth of a sentence without any quantifiers. Checking the truth of a sentence without any quantifiers is a simple arithmetic check of given numbers such as $25^2 - 72 \cdot 18 > 0$ which is easily checked by computation.

The fact that the inequality is necessary can be seen easily by considering a formula $\exists y(y^2 = x)$. In context of real numbers, this basically says "$x \geq 0$" as all non negative real numbers have square roots. But it's quite clear that one can't express this without any quantifiers with only one variable x. This example is from Poonen's paper [29, p. 10].

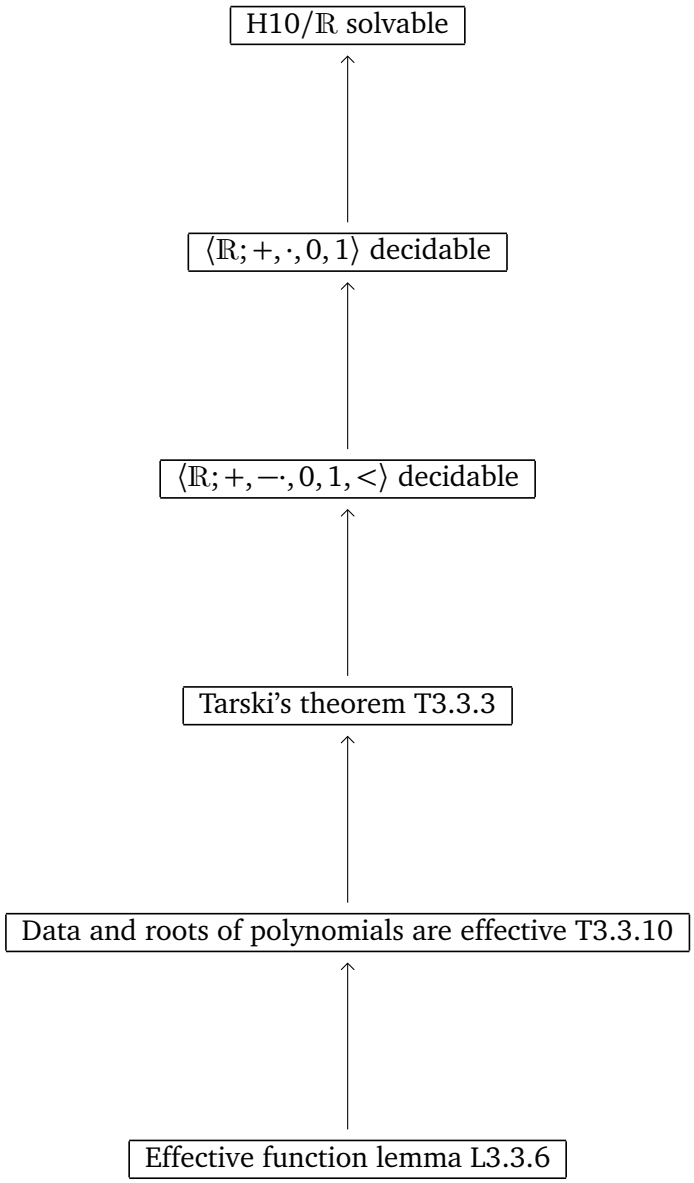


Diagram of the proof of solvability of Hilbert's Tenth Problem over $\mathbb{R}$.

3.3 Proof of decidability of $\mathbb{R}$

This section will give an exposition of Paul J. Cohen's paper [3] which shows that the first order sentences in the language of real numbers are decidable. We will include my own proofs of some of the claims in the paper without proof and also will expand some of the sketch of proofs. We will assume that the reader knows what we mean by 'Field of Reals' and 'first order sentences'.

Definition 3.3.1. A *polynomial relation* is a relation $A(x_1, ..., x_n)$ which is a Boolean function of polynomial inequality relations(PIR) of the form $p(x_1, ..., x_n) > 0$, where p is a polynomial with integral coefficients in $\mathbb{R}$.

The term "Boolean function" means a formula in the first order language of logic with the operations $\neg$ and $\wedge$. We will also use and $\vee$, $\rightarrow$ and $\leftrightarrow$ in the usual sense as a short hand notation for an equivalent expression only using $\neg$ and $\wedge$.

Theorem 3.3.2. *All first order sentences of our theory $\mathbb{R}$ is logically equivalent to the form $Q_1 x_1 \cdots Q_n x_n A(x_1, ..., x_n)$, where the Q_i are quantifiers $\exists$ or $\forall$, and A is a polynomial relation.*

Cohen states this without proof and we won't include the proof either. This is essentially Prenex Normal Form theorem (15.1) in Logic B1a [18] which is proved using induction on complexity of formulas.

Theorem 3.3.3. *If $A(x_1, ..., x_n)$ is a polynomial relation, $n > 1$, then we can find by a primitive recursive procedure a polynomial relation $B(x_2, ..., x_n)$ such that $\exists x_1 A(x_1, ...x_n) \Leftrightarrow B(x_2, ..., x_n)$. If $n = 1$, there is a primitive recursive procedure which decides $\exists x_1 A(x_1)$.*

In section 2, we gave an enumeration of all polynomials of positive integer coefficients. From this, it is not much harder to give an enumeration of all polynomial relations, though we won't give an explicit enumeration here. With this in mind, it makes sense to talk about "primitive recursive procedure" to find polynomial relations. It means that there is a recursive function $F : \mathbb{N} \rightarrow \mathbb{N}$ which "maps" a polynomial relation to another polynomial relation via their enumeration. However, as with Cohen, we won't prove the decision procedure formally using an explicit recursive function as that would become too technical. Instead, we will describe an informal procedure to get from one polynomial relation to another.

Definition 3.3.4. We define a function sgn:$\mathbb{R} \to \mathbb{R}$ by:

$$\text{sgn}(x) = \begin{cases} -1 & \text{if } x < 0 \\ 0 & \text{if } x = 0 \\ 1 & \text{if } x > 0 \end{cases}$$

Definition 3.3.5. A real-valued function $f(x_1, ..., x_n)$ *effective* if there is a primitive recursive procedure which to every polynomial relation $A(y, y_1, ..., y_m)$ assigns a polynomial relation $B(x_1, ..., x_n, y_1, ..., y_m)$ such that

$$A(f(\bar{x}), y_1, ..., y_m) \Leftrightarrow B(x_1, ..., x_n, y_1, ..., y_m).$$

Here are some examples of basic simple functions. The proofs are my own.

Lemma 3.3.6. *These functions are effective:*

- $x + y$
- $x \cdot y$
- $\text{sgn}(x)$

Proof.

- $x + y$
  Clearly, for any polynomial relation $A(z, t_1, ..., t_m)$, $A(x + y, t_1, ..., t_m)$ is also a polynomial relation except it is of variables $x, y, t_1, ..., t_m$. So let $B = A(x + y, \bar{t})$ and we're done.

- $x \cdot y$
  Similarly, $A(x \cdot y, t_1, ..., t_m)$ is also a polynomial relation.

- $\text{sgn}(x)$
  For any polynomial relation $A(z, t_1, ..., t_m)$ be given. We define B to be:

  $$B = [x < 0 \to A(-1, \bar{t})] \wedge [x = 0 \to A(0, \bar{t})] \wedge [x > 0 \to A(1, \bar{t})]$$

  (Strictly speaking, "$x < 0$" and "$x = 0$" are not allowed but this is fine because we can take them to mean $-x > 0$ and $\neg(-x > 0) \wedge \neg(x > 0)$ respectively. B is clearly equivalent to $A(\text{sgn}(x), \bar{t})$. Now to show that B is a polynomial relation, we need to show that it is a boolean function of PIRs(polynomial inequality relations). This is straightforward as B is a Boolean function of A, $x < 0$, $x = 0$ and $x > 0$ which are all Boolean functions of PIRs. Also, Boolean functions of Boolean functions of PIRs are simply Boolean functions of PIRs.

- $|x|$
  For any polynomial relation $A(z, t_1, ..., t_m)$ be given. We define B to be:

$$B = [x > 0 \to A(x, \bar{t})] \wedge [\neg x > 0 \to A(-x, \bar{t})]$$

□

Lemma 3.3.7. *Suppose $f : \mathbb{R}^n \to \mathbb{R}^m$ and $g : \mathbb{R}^m \to \mathbb{R}^k$ are effective functions. Then $g \circ f$ is also effective. In other words, effective functions are closed under composition.*

Here is my proof of it.

Proof. Let $f : \mathbb{R}^n \to \mathbb{R}^m$ and $g : \mathbb{R}^m \to \mathbb{R}^k$, effective functions, be given. Now let a polynomial relation $A(z_1, ..., z_k, y_1, ..., y_l)$ be given. We wish to show that we can find by primitive recursive procedure a polynomial relation $B(x_1, ..., x_n, y_1, ..., y_l)$ such that:

$$A(g(f(x_1, ..., x_n)), y_1, ..., y_l) \Leftrightarrow B(x_1, ..., x_n, y_1, ..., y_l).$$

Since g is effective, one can find a polynomial relation B_g such that for all $\bar{x} \in \mathbb{R}^m$:

$$A(g(x_1, ..., x_m), y_1, ..., y_l) \Leftrightarrow B_g(x_1, ..., x_m, y_1, ..., y_l).$$

This means that:

$$A(g(f(x_1, ..., x_n)), y_1, ..., y_l) \Leftrightarrow B_g(f(x_1, ..., x_n), y_1, ..., y_l).$$

In turn, f is effective, one can find a polynomial relation B_f such that:

$$B_g(f(x_1, ..., x_n), y_1, ..., y_l) \Leftrightarrow B_f(x_1, ..., x_n, y_1, ..., y_l).$$

So, letting $B = B_f$, we have:

$$\begin{aligned} A(g(f(x_1, ..., x_n)), y_1, ..., y_l) &\Leftrightarrow B_g(f(x_1, ..., x_n), y_1, ..., y_l) \\ &\Leftrightarrow B_f(x_1, ..., x_n, y_1, ..., y_l) = B(x_1, ..., x_n, y_1, ..., y_l) \end{aligned}$$

So we're done. □

Lemma 3.3.8. *$f(x_1, ..., x_n)$ is effective if there is a primitive recursive function which, for all $k \in \mathbb{N}$, assigns a polynomial relation $C(c_0, ..., c_k, x_1, ..., x_n, z)$ such that*

$$C(\bar{c}, \bar{x}, z) \Leftrightarrow z = \text{sgn}(c_0 + \cdots + c_k f(\bar{x})^k).$$

Essentially, what this Lemma tells us is that we need only care about the sgn of functions and not the exact values. This is because by definition, all polynomial relations are built from inequalities of the form $p > 0$. Cohen didn't include a proof of this but I will give my own proof of it here.

Proof. Let $f(x_1, ..., x_n)$ be given. Suppose there is a primitive recursive function as described in the Lemma. We wish to show that there is a primitive recursive procedure which to every polynomial relation $A(y, y_1, ..., y_m)$ assigns a polynomial relation $B(x_1, ..., x_n, y_1, ..., y_m)$ such that

$$A(f(\bar{x}), y_1, ..., y_m) \Leftrightarrow B(x_1, ..., x_n, y_1, ..., y_m).$$

We will prove by induction on the number of PIR $p_i > 0$ in the polynomial relation $A(y, y_1, ..., y_m)$.

- Base case: There is only one PIR in A.
  Then A will either be just a single PIR $p(y, y_1, ..., y_m) > 0$ or the negation of it. Note, we can write $p(y, y_1, ..., y_m)$ as a polynomial $q = c_0 + ... + c_k y^k$ of a single variable y where the coefficients c_i are in $\mathbb{R}[y_1, ..., y_m]$. Then by assumption, we can find a polynomial relation $C(\bar{c}, \bar{x}, z)$ such that

  $$C(\bar{c}, \bar{x}, z) \Leftrightarrow z = \text{sgn}(c_0 + \cdots + c_k f(\bar{x})^k).$$

  Then we claim that $B(\bar{x}, \bar{y}) = C(\bar{c}, \bar{x}, 1)$ for the former and $B(\bar{x}, \bar{y}) = \neg C(\bar{c}, \bar{x}, 1)$ for the latter gives us the polynomial relation we want. The definition makes sense because as we recall, $c_i \in \mathbb{R}[y_1, ..., y_m]$. If the former,

  $$\begin{aligned}
  A(f(\bar{x}), \bar{y}) &\Leftrightarrow q(f(\bar{x})) > 0 && \text{(By assumption)} \\
  &\Leftrightarrow c_0 + \cdots + c_k f(\bar{x})^k > 0 && \text{(By definition of } q\text{)} \\
  &\Leftrightarrow 1 = \text{sgn}(c_0 + \cdots + c_k f(\bar{x})^k) && \text{(By definition of sgn)} \\
  &\Leftrightarrow C(\bar{c}, \bar{x}, 1) && \text{(By definition of C)} \\
  &\Leftrightarrow B(\bar{x}, \bar{y}) && \text{(By definition of B)}
  \end{aligned}$$

  If the latter,

  $$\begin{aligned}
  A(f(\bar{x}), \bar{y}) &\Leftrightarrow \neg q(f(\bar{x})) > 0 && \text{(By assumption)} \\
  &\Leftrightarrow \neg c_0 + \cdots + c_k f(\bar{x})^k > 0 && \text{(By definition of } q\text{)} \\
  &\Leftrightarrow \neg 1 = \text{sgn}(c_0 + \cdots + c_k f(\bar{x})^k) && \text{(By definition of sgn)} \\
  &\Leftrightarrow \neg C(\bar{c}, \bar{x}, 1) && \text{(By definition of C)} \\
  &\Leftrightarrow B(\bar{x}, \bar{y}) && \text{(By definition of B)}
  \end{aligned}$$

- Inductive step: Suppose true for number of PIRs less than N for some $N > 1$. Suppose now number of PIRs in A equals N.

  Then, $A = D \wedge E$ or $A = \neg(D \wedge E)$ for some polynomial relations D and E whose number of PIRs are less than N. So the inductive hypothesis applies to D and E. So one should be able to find some polynomial relation B_D and B_E such that:

  $$D(f(\bar{x}), \bar{y}) \iff B_D(\bar{x}, \bar{y}) \text{ and } E(f(\bar{x}), \bar{y}) \iff B_E(\bar{x}, \bar{y})$$

  Now let $B(\bar{x}, \bar{y}) = B_D(\bar{x}, \bar{y}) \wedge B_E(\bar{x}, \bar{y})$, if former, and $B(\bar{x}, \bar{y}) = \neg(B_E(\bar{x}, \bar{y}) \wedge B(\bar{x}, \bar{y}))$, if latter. These are clearly polynomial relations. Then, if former:

  $$\begin{aligned} A(f(\bar{x}), \bar{y}) &\iff D(f(\bar{x}), \bar{y}) \wedge E(f(\bar{x}), \bar{y}) && \text{(By assumption)} \\ &\iff B_D(\bar{x}, \bar{y}) \wedge B_E(\bar{x}, \bar{y}) && \text{(By inductive hypothesis)} \\ &\iff B(\bar{x}, \bar{y}) && \text{(By definition of B)} \end{aligned}$$

  If latter:

  $$\begin{aligned} A(f(\bar{x}), \bar{y}) &\iff \neg(D(f(\bar{x}), \bar{y}) \wedge E(f(\bar{x}), \bar{y})) && \text{(By assumption)} \\ &\iff \neg D(f(\bar{x}), \bar{y}) \vee \neg E(f(\bar{x}), \bar{y}) && \text{(By tautology)} \\ &\iff \neg B_D(\bar{x}, \bar{y}) \vee \neg B_E(\bar{x}, \bar{y}) && \text{(By inductive hypothesis)} \\ &\iff \neg(B_D(\bar{x}, \bar{y}) \wedge B_E(\bar{x}, \bar{y})) && \text{(By tautology)} \\ &\iff B(\bar{x}, \bar{y}) && \text{(By definition of B)} \end{aligned}$$

So by induction, we are done. □

Definition 3.3.9. Let $p(x)$ be a polynomial in one variable. By a *graph* of $p(x)$ we mean a k-tuple $t_1 < t_2 < \cdots < t_k$ such that, in each interval of the form $(-\infty, t_1), (t_i, t_i + 1), (t_k, \infty)$, p is monotonic. By the *data* of the graph we mean the k-tuple $\langle t_1, ..., t_k \rangle$, $\text{sgn}(p(t_i))$ for $1 \leq i \leq k$, $\text{sgn}(p(t_1 - 1) - p(t_1))$, and $\text{sgn}(p(t_k + 1) - p(t_k))$.

In other words, the graph of p is a tuple of its extreme/stationary points, i.e. where its gradient/derivative is zero. Of course as p is a polynomial there can only be finitely many stationary points so the definition makes sense.

Theorem 3.3.10. *Let a polynomial $p(x) \equiv a_n x^n + \cdots + a_0$ be given. Then for each $n \in \mathbb{N}$, the following statements A_n and B_n hold:*

- *A_n The maps T_i and S_i given by:*

$$\begin{aligned} T_i &: (a_0, ..., a_n) \mapsto t_i \\ S_0 &: (a_0, ..., a_n) \mapsto \text{sgn}(p(t_1 - 1) - p(t_1)) \\ S_i &: (a_0, ..., a_n) \mapsto \text{sgn}(p(t_i)) \\ S_{k+1} &: (a_0, ..., a_n) \mapsto \text{sgn}(p(t_k + 1) - p(t_k)), \end{aligned}$$

  where $\langle t_1, ..., t_k \rangle$ is the graph of $p(x)$, are effective.

- *B_n The maps M and R_i given by:*

$$\begin{aligned} M &: (a_0, ..., a_n) \mapsto m \text{ where } m \text{ is the number of roots of } p \\ R_i &: (a_0, ..., a_n) \mapsto \xi_i \text{ where } \xi_i \text{ is ith root of } p, \end{aligned}$$

  for $1 \leq i \leq m$, are effective.

Proof. We prove A_n and B_n by a simultaneous induction on n.

- Base case: $n = 0$
  If $n = 0$, then p is a constant. So A_n and B_n holds both trivially.

- Inductive step
  Suppose both statements hold for all cases less than n for some $n > 0$.

  A_n:
  Now suppose $\deg(p) = n$. We consider its derivative $p'(x)$. The degree of $p'(x)$ is at most $n - 1$ and so the inductive hypothesis applies. Also, the coefficients of $p'(x)$ are $na_n, (n-1)a_{n-1}, ..., 2a_2, a_1$. As we can see, they are simply the coefficients of $p(x)$ multiplied by a constant number. They are effective functions of the coefficients of $p(x)$. More precisely, the function $a_k \mapsto ka_k$ is effective. This is because by Lemma 3.3.6 $x \cdot y$ is effective. By B_n then, the map from the coefficients of $p'(x)$ to the roots of $p'(x)$ are effective. Since composition of effective functions are effective by Lemma 3.3.7, the map from the coefficients of $p(x)$ to the roots of $p'(x)$ must be effective functions. But the roots of $p'(x)$ are the extreme points of $p(x)$, i.e. gives us the graph of $p(x)$. So each T_i are effective maps. Also, S_i must be effective as well because sgn, $x + y$, $x \cdot y$ are effective (Lemma 3.3.6) and effective functions are closed under compositions.

B_n:

- M is effective
  By A_n, we can find sgn $(p(t_1-1)-p(t_1))$, sgn$(p(t_2))$,...,sgn$(p(t_k))$, sgn$(p(t_k+1)-p(t_k))$ by effective functions S_i. This gives us enough information to show that the map M is effective.

sgn$(p(t_i))$	**sgn**$(p(t_{i+1}))$	**Roots**
1	1	No root in $[t_i, t_{i+1}]$
1	0	Exactly one root $\xi = t_{i+1}$
1	-1	Exactly one root $\xi \in (t_i, t_{i+1})$
0	1	Exactly one root $\xi = t_i$
0	0	This cannot happen for a polynomial
0	-1	Exactly one root $\xi = t_i$
-1	1	Exactly one root $\xi \in (t_i, t_{i+1})$
-1	0	Exactly one root $\xi = t_{i+1}$
-1	-1	No root in $[t_i, t_{i+1}]$

sgn $(p(t_1-1)-p(t_1))$	**sgn**$(p(t_1))$	**Roots**
1	1	No root $\xi \leq t_1$
1	0	Exactly one root $\xi = t_1$
1	-1	Exactly one root $\xi < t_1$
0	0	This cannot happen for a polynomial
-1	1	Exactly one root $\xi < t_1$
-1	0	Exactly one root $\xi = t_1$
-1	-1	No root $\xi < t_1$

sgn$(p(t_k))$	**sgn** $(p(t_k+1)-p(t_k))$	**Roots**
1	1	No root $\xi > t_k$
1	0	Exactly one root $\xi = t_k$
1	-1	Exactly one root $\xi > t_k$
0	0	This cannot happen for a polynomial
-1	1	Exactly one root $\xi > t_k$
-1	0	No root $\xi > t_k$
-1	-1	No root $\xi > t_k$

If sgn$(p(t_i))$ and sgn$(p(t_{i+1}))$ differ, then this means $t_i \leq 0 \leq t_{i+1}$ or $t_{i+1} \leq 0 \leq t_i$. Since p is continuous and monotone between t_i and t_{i+1}, then by the Intermediate Value Theorem, p will cross the x axis exactly once between t_i and t_{i+1} inclusive. On the other hand, if sgn$p(t_i)$ and sgn$p(t_{i+1})$ don't differ, as p is con-

tinuous, this means that p stays on one side of the x-axis, i.e. p doesn't cross the x-axis. The other case to consider is when $\text{sgn}(p(t_i)) = 0$. In this case, this is a "double root". Also, by nature of polynomials, two consecutive stationary points cannot have equal y value. Therefore, there is exactly one root between t_{i-1} and t_{i+1} in this case. Finally, we check the ends. Suppose for definiteness, $\text{sgn}(p(t_k)) > 0$. Now either $\text{sgn}(p(t_k+1) - p(t_k)) > 0$ or $\text{sgn}(p(t_k+1) - p(t_k)) < 0$. If the former, then the polynomial is increasing from a positive stationary point so p will not cross x-axis again. If the latter, then the polynomial is decreasing and will cross the x-axis one last time. In short, the map M which gives the total number of roots will be given by:

$$M(\bar{a}) = m = \frac{1}{2}\sum_{i=0}^{k+1} |S_{i+1}(\bar{a}) - S_i(\bar{a})|$$

which is clearly effective.

– R_i are effective
Since t_i are stationary points, at most one root belongs to each of these intervals $(-\infty, t_1), ..., (t_k, \infty)$. It's also a possibility that the roots equal to some t_i. But these cases are easy to handle as T_i had been shown to be effective in A_n. So suppose a root $\xi_j \in (t_\alpha, t_{\alpha+1})$ for some $1 \leq \alpha \leq k$. We'll show that the map $R_j : \bar{a} \mapsto \xi_j$ is effective via Lemma 3.3.8. So let $q(x) = c_0 + \cdots + c_m x^m$. We wish to show that sgn $q(R)$ is an effective function of $(c_0, ..., c_m)$. Now let s be the remainder when q is divided by p:

$$q = ap + s$$

where $\deg(s) < n$. Notice $q(\xi_j) = a(\xi_j)p(\xi_j) + s(\xi_j) = a(\xi_j) \cdot 0 + s(\xi_j) = s(\xi_j)$ which means sgn $(q(\xi_j))$ = sgn $(s(\xi_j))$. Also, it is clear that the coefficients of s are effectively mapped from $c_0, ..., c_m$, by Euclid's algorithm for division. Consequently, if we can show that the map from the coefficients of s to $\text{sgn}(s(\xi_j))$ is effective, then this is equivalent to showing that the map from $c_0, ..., c_m$ to $\text{sgn}(q(\xi_j))$ is effective. Then by Lemma 3.3.8, we show that R_j is effective.

Since $\deg(s) < n$, inductive hypotheses A_n and B_n applies and we can find the stationary points $u_1 < \cdots < u_l$ and the roots $v_1 <$

$\cdots < v_r$. Let us combine the two lists in one: $w_1 < \cdots < w_{l+r}$. Next, add the "end points", $w_0 = -\infty, w_1, ..., w_{l+r}, w_{l+r+1} = +\infty$. Now $\operatorname{sgn}(s)$ is constant in (w_i, w_{i+1}) for $0 \leq i \leq l+r+1$ and so if we can know for which β, $\xi_j \in (w_\beta, w_{\beta+1})$ or $\xi_j = w_\beta$, then we can easily determine $\operatorname{sgn}(s(\xi_j))$. There are two cases to consider. First case is when no w_i is in $(t_\alpha, t_{\alpha+1})$. In this case, there will be some β such that $w_\beta \leq t_\alpha < \xi_j < t_{\alpha+1} \leq w_{\beta+1}$. So we found the required β. The second case is when some w_i are in $(t_\alpha, t_{\alpha+1})$. Suppose then $w_{\beta_1} < \cdots w_{\beta_K}$ all lie inside $(t_\alpha, t_{\alpha+1})$. If for some i, $w_i = \xi_j$, or equivalently if $\operatorname{sgn}(p(w_i)) = 0$ (since ξ_j is the only root in $(t_\alpha, t_{\alpha+1})$) then we're done as $\operatorname{sgn}(\xi_j)$ is mapped effectively from the coefficients of s. Otherwise, consider the values $\operatorname{sgn}(p(w_{\beta_1}))$,...,$\operatorname{sgn}(p(w_{\beta_K}))$ which are all result of effective maps. Then there will be some β such that $\operatorname{sgn}(p(w_\beta)) = -1$ and $\operatorname{sgn}(p(w_{\beta+1})) = 1$. In this case, $t_\alpha < w_\beta < \xi_j < w_{\beta+1} < t_{\alpha+1}$. So we found the required β.

The end points are handled similarly.

□

We are now ready to prove Tarski's quantifier elimination theorem:

Proof. Let a polynomial relation $A(x_1, ..., x_n)$ be given. Then A can be seen as be a boolean function of polynomial inequalities of the form $p_j(x_1, ..., x_n) > 0$. Each p_j can be seen as a single variable polynomial inequality $q_j(x_1) > 0$ with coefficients in $\mathbb{R}[x_2, ..., x_n]$ for some q_j. So in other words,

$$A(x_1, ..., x_n) = F(q_1(x_1) > 0, q_2(x_1) > 0, ..., q_m(x_1) > 0),$$

where F is the Boolean function of the relations $q_i(x_1) > 0$. Now since all q_j have finite degree, Theorem 3.3.10 tells us that there are effective maps $\operatorname{sgn}(T_i^j)$ and R_i^j which gives us the sign of stationary points and the roots q_j. Now since there are at most finitely many maps $\operatorname{sgn}(T_i^j)$ and R_i^j, one can write down all the different possible cases of the different values each $\operatorname{sgn}(T_i^j)$ can take and the different possible relative positions of T_i^j and R_i^j for all i and j. Each of these cases can be described by polynomial relations $A_1, ..., A_N$. For each case, by looking at the values of $\operatorname{sgn}(T_i^j)$ and the relative positions of T_i^j and R_i^j, we can decide whether or not $\exists x_1 A(x_1, ..., x_n)$ would be satisfied. Then we can picke out all the cases in which $\exists x_1 A(x_1, ..., x_n)$ is satisfied. So let $A_{l_1}, ..., A_{l_M}$ be the corresponding polynomials describing

the above cases. Then $\exists x_1 A(x_1, ..., x_n) \iff A_{l_1} \vee \cdots \vee A_{l_M}$. Now since the right hand side is a polynomial relation of effective functions $\text{sgn}(T_i^j)$, T_i^j and R_i^j, there will be polynomials $B_1(x_2, ..., x_n), ..., B_M(x_2, ..., x_n)$ such that $A_{l_k} \iff B_k(x_2, ..., x_n)$ for each $1 \leq k \leq M$. Then, letting $B = B_1 \vee \cdots \vee B_M$, we have

$$\exists x_1 A(x_1, ..., x_n) \iff B(x_2, ..., x_n).$$

This completes the proof. □

4 Developments on H10/$\mathbb{Q}$

Hilbert's Tenth Problem over the field of rationals is currently one of the main open problem in this field of Mathematics. We will briefly study some of the main results that has been shown so far.

4.1 Hasse's Principle

Hasse's principle, also known as the local-global principle, roughly asks how much the local fields tell us about the global field. In context of the rationals, the global field is $\mathbb{Q}$ and the local fields are all the completions of $\mathbb{Q}$(i.e. extension of $\mathbb{Q}$ in which all Cauchy sequences converge). By Ostrowski's theorem (see for example [15]) all completions of $\mathbb{Q}$ are $\mathbb{Q}_p$, the field of p-adics, for each prime p and $\mathbb{R}$. Hasse's principle is then:

> Given a polynomial q over $\mathbb{Q}$, q has a root in $\mathbb{Q}$ if and only if it has a root in $\mathbb{R}$ and all p-adic fields $\mathbb{Q}_p$.

If this principle holds for all polynomials, then this would provide a very strong tool for answering Hilbert's Tenth Problem over $\mathbb{Q}$. This is because as we've shown in Section 3, there is a decision procedure to know whether or not a given polynomial has a root in $\mathbb{R}$. Also, although we haven't covered it in this paper, Cohen's second half of the paper gives a proof of decidability of $\mathbb{Q}_p$ for any prime p. Of course this isn't enough as these don't give a decision procedure to decide whether or not a given polynomial has a root in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p. However, it is still much easier to work in these local fields with techniques such as the Hensel's lemma.

It turns out the principle isn't true for all polynomials. For example, Ernest Selmer showed that the equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution in all the p-adic fields and $\mathbb{R}$ but not in $\mathbb{Q}$. However, Hermann Minkowski showed that for polynomials of Quadratic forms, the principle holds. This is the Hasse-Minkowski's Theorem. Hasse-Minkowski's Theorem allowed Julia Robinson to prove that the field of rationals is undecidable which is discussed in the next section. For further reading on this topic, see [12].

4.2 Undecidability of the first order theory of $\mathbb{Q}$

This section will give an exposition of Julia Robinson's Phd thesis [34] which shows that the field of rationals is undecidable. As with Robinson, we will write upper case letters for rational numbers and lower case letters for integers.

Theorem 4.2.1. *A rational number N is an integer if and only if it satisfies the formula*

$$\forall A, B[(\phi(A,B,0) \wedge \forall M(\phi(A,B,M) \rightarrow \phi(A,B,M+1))) \rightarrow \phi(A,B,N)]$$

where $\phi(A,B,K)$ stands for $\exists X, Y, Z(2 + ABK^2 + BZ^2 = X^2 + AY^2)$.

The forward direction is straightforward enough.

Proof. "⇒"
Suppose N is an integer and suppose A and B satisfy

$$\phi(A,B,0) \text{ and } \forall M(\phi(A,B,M) \rightarrow \phi(A,B,M+1)).$$

Then by induction, $\phi(A,B,n)$ will hold for any non negative integer n. So if N is non negative, $\phi(A,B,N)$ will hold. Now notice the definition of $\phi(A,B,K)$:

$$\exists X, Y, Z(2 + ABK^2 + BZ^2 = X^2 + AY^2),$$

and we notice that K appears only once as a square. In other words,

$$\phi(A,B,K) \Leftrightarrow \phi(A,B,-K)$$

for any rational number K. Therefore, $\phi(A,B,N)$ will hold for any integer N. □

The converse takes a bit more work. We will first need the five Lemmas below. The first two, as Robinson notes are consequences of Hasse-Minkowski's theorem which we discussed in Section 4.1.

Lemma 4.2.2. *If p is a prime and $p \equiv 3 \mod 4$ then $X^2+Y^2-pZ^2$ represents a non-zero rational number M, if and only if M is not of the form*

$$p \cdot k \cdot S^2 \text{ with } \left(\frac{k}{p}\right) = 1$$
$$\text{or} \quad k \cdot S^2 \quad \text{with } k \equiv p \mod 8$$

Lemma 4.2.3. *If p and q are odd primes with $p \equiv 1 \mod 4$ and $\left(\frac{q}{p}\right) = -1$ then $X^2 + qY^2 - pZ^2$ represents a non-zero rational number M if and only if M is not of the form*

$$p \cdot k \cdot S^2 \text{ with } \left(\frac{k}{p}\right) = -1$$
$$\text{or} \quad q \cdot k \cdot S^2 \text{ with } \left(\frac{k}{q}\right) = -1$$

Lemma 4.2.4. *If p is a prime and $p \equiv 3 \mod 4$ then*

$$2 + pM^2 + pZ^2 = X^2 + Y^2$$

has a solution for X, Y, and Z if and only if the denominator of M in lowest terms is odd and is coprime with p.

Proof. Let $M = \frac{n}{d}$ in lowest terms, i.e. n and d are coprime. To begin, we have

$$\begin{aligned} 2 + pM^2 + pZ^2 = X^2 + Y^2 &\Leftrightarrow 2 + pM^2 = X^2 + Y^2 - pZ^2 \\ &\Leftrightarrow 2 + p\frac{n^2}{d^2} = X^2 + Y^2 - pZ^2 \\ &\Leftrightarrow 2d^2 + pn^2 = (dX)^2 + (dY)^2 - p(dZ)^2 \\ &\Leftrightarrow 2d^2 + pn^2 = X'^2 + Y'^2 - pZ'^2 \\ &\qquad \text{for some rational numbers } X', Y' \text{ and } Z' \end{aligned}$$

So we can see $M = \frac{n}{d}$ satisfies the equation if and only if $2d^2 + pn^2$ can be written as $X^2 + Y^2 - pZ^2$ for some rational numbers X, Y and Z. So we will be working with $2d^2 + pn^2$ which we denote m.

"$\Leftarrow$"
Suppose d is odd and coprime with p. We will show that m satisfies the right hand side conditions for Lemma 4.2.2 which then tells us m can be written in the form $X^2 + Y^2 - pZ^2$.

- $m \neq p \cdot k \cdot S^2$ with $\left(\frac{k}{p}\right) = 1$
  Since p is prime, p being coprime with d just means $p \nmid d$. Then elementary number theory tells us $p \nmid 2d^2 + pn^2 = m$. Now suppose for a contradiction $m = p \cdot k \cdot S^2$ with $\left(\frac{k}{p}\right) = 1$. Let $S = \frac{u}{v}$ where u and v are coprime. Then $mv^2 = p \cdot k \cdot u^2$. This means $p|mv^2$. Since we showed $p \nmid m$, we must have $p|v^2$ and hence $p|v$. So this means $p^2|mv^2 = p \cdot k \cdot u^2$. But $\left(\frac{k}{p}\right) = 1$ implies $p \nmid k$ and we assumed u and v are coprime which means $p \nmid u$. But this means $p^2 \nmid p \cdot k \cdot u^2$, a contradiction. So we're done.

- $m \neq k \cdot S^2$ with $k \equiv p \mod 8$
  We have $m = 2d^2 + pn^2$, d odd and $p \equiv 3 \mod 4$. Also, elementary number theory tells us

$$l^2 \equiv \begin{cases} 1 \mod 4 & \text{if } l \text{ is odd} \\ 0 \mod 4 & \text{if } l \text{ is even} \end{cases} \tag{1}$$

  for any integer l. Hence,

$$\begin{aligned} m &= 2d^2 + pn^2 \\ &\equiv 2 \cdot 1^2 + pn^2 \mod 4 && \text{since } d \text{ is odd} \\ &\equiv 2 - n^2 \mod 4 && \text{since } p \equiv 3 \equiv -1 \mod 4 \\ &\equiv 2 \mod 4 && \text{if } n \text{ is even} \\ &\quad 1 \mod 4 && \text{if } n \text{ is odd.} \end{aligned}$$

  In other words, $m \equiv 2$ or $1 \mod 4$. Now suppose for a contradiction $m = k \cdot S^2$ with $k \equiv p \mod 8$ and $S = \frac{u}{v}$ where u and v are coprime. Then $mv^2 = k \cdot u^2$. Since we showed $m \equiv 2$ or $1 \mod 4$, then $mv^2 \equiv 2, 1$ or $0 \mod 4$ depending on v. On the other hand, $k \equiv p \mod 8$ implies $k \equiv p \mod 4$ which in turn implies $k \equiv 3 \mod 4$ as $p \equiv 3 \mod 4$. So this means $k \cdot u^2 \equiv 3$ or $0 \mod 4$ depending on v. Therefore, the only way for the two to coincide is if both sides equal to zero mod 4 and this only happens when u and v are both even. But this contradicts the fact that u and v are coprime. So we're done.

So by Lemma 4.2.2, we're done.

"$\Rightarrow$"
We will show that if the right hand side conditions are not met, then m cannot be written in the form $X^2 + Y^2 - pZ^2$. Again we show this using Lemma 4.2.2

- d is not odd
  Then $2|d$ so we can write $d = 2r$ for some integer r. This means $m = 8r^2 + pn^2$. Since d is even, n must be odd as the two are coprime. So elementary number theory tells us $n^2 \equiv 1 \mod 8$. This means then that $m \equiv p \mod 8$. So letting $S = 1$, Lemma 4.2.2 tells us m cannot be written in the form $X^2 + Y^2 - pZ^2$. So we're done.

- d is not coprime with p
  Since p is prime, this means $p|d$ and we can write $d = ps$ for some integer r. Then

  $$m = 2d^2 + pn^2 = 2p^2s^2 + pn^2 = p(2ps^2 + n^2).$$

  Let us write $k = 2ps^2 + n^2$. Since $p|d$ and d and n are coprime, $p \nmid n$ and hence $p \nmid k$. Therefore,

  $$\left(\frac{k}{p}\right) = \left(\frac{2ps^2 + n^2}{p}\right) = \left(\frac{n^2}{p}\right) = 1,$$

  since $p \nmid n$. So letting $S = 1$, we have $m = p \cdot k \cdot S^2$ with $\left(\frac{k}{p}\right) = 1$, so Lemma 4.2.2 tells us m cannot be written in the form $X^2 + Y^2 - pZ^2$. So we're done.

This completes the proof. □

Lemma 4.2.5. *If p and q are odd primes with $p \equiv 1 \mod 4$ and $\left(\frac{q}{p}\right) = -1$, then*

$$2 + pqM^2 + pZ^2 = X^2 + qY^2$$

has a solution for X, Y, and Z if and only if the denominator of M in lowest terms is odd and is coprime with p and q.

Proof. Let $M = \frac{n}{d}$ in lowest terms and let $m = 2d^2 + pqn^2$. Similar to the proof of Lemma 4.2.4, it suffices to show that m can be written in the form $X^2 + qY^2 - pZ^2$ if and only if d is coprime with p and q.

"$\Leftarrow$"
Suppose d is coprime with p and q. Then m is also coprime with p and q. Then by the similar argument in Lemma 4.2.4, the right hand side conditions of Lemma 4.2.3 are satisfied. Therefore, m can be written in the form $X^2 + qY^2 - pZ^2$.

"$\Rightarrow$"
We will show that if the right hand side conditions are not met, then m cannot be written in the form $X^2 + qY^2 - pZ^2$. Again we show this using Lemma 4.2.3.

- d not coprime with p
  Since p is prime, this means $p|d$ so we can write $d = pr$ for some integer r. Then

  $$m = 2d^2 + pqn^2 = 2p^2r^2 + pqn^2 = p(2pr^2 + qn^2).$$

  Let us write $k = 2pr^2 + qn^2$. Since $p|d$ and d and n are coprime, $p \nmid n$. Also, $\left(\frac{q}{p}\right) = -1$ so $p \nmid q$. Hence $p \nmid k$. Therefore,

  $$\begin{aligned}
  \left(\frac{k}{p}\right) &= \left(\frac{2pr^2 + qn^2}{p}\right) \\
  &= \left(\frac{qn^2}{p}\right) \\
  &= \left(\frac{q}{p}\right) \cdot \left(\frac{n^2}{p}\right) && \text{Top multiplicative property} \\
  &= \left(\frac{q}{p}\right) \cdot 1 && \text{Since } p \nmid n \\
  &= -1 && \text{By assumption.}
  \end{aligned}$$

  So writing $S = 1$, we see that $m = p \cdot k \cdot S^2$ with $\left(\frac{k}{p}\right) = -1$. Therefore by Lemma 4.2.3, m cannot be written in the form $X^2 + qY^2 - pZ^2$.

- d not coprime with q

The argument is exact parallel of the previous case except we have:

$$\begin{aligned}
\left(\frac{k}{q}\right) &= \left(\frac{2qr^2+pn^2}{q}\right) \\
&= \left(\frac{pn^2}{q}\right) \\
&= \left(\frac{p}{q}\right)\cdot\left(\frac{n^2}{q}\right) && \text{Top multiplicative property} \\
&= \left(\frac{p}{q}\right)\cdot 1 && \text{Since } q \nmid n \\
&= \left(\frac{q}{p}\right)\cdot(-1)^{\frac{p-1}{2}\frac{q-1}{2}} && \text{By the reciprocity law} \\
&= -1\cdot(-1)^{\frac{p-1}{2}\frac{q-1}{2}} && \text{By assumption.} \\
&= -1 && \text{Since by assumption, } p \equiv 1 \mod 4.
\end{aligned}$$

So m cannot be written in the form $X^2+qY^2-pZ^2$.

This completes the proof. □

Lemma 4.2.6. *If p is a prime and $p \equiv 1 \mod 4$ then there is an odd prime q such that $\left(\frac{q}{p}\right) = -1$.*

Proof. Let s be any non-residue of p. Then $s+p$ will be a non-residue of p as well. This is because if $x^2 \equiv s+p \mod p$, then $x^2 \equiv s \mod p$ which contradicts the fact that s is non-residue of p. Also note that since $p \equiv 1 \mod 4$ and hence odd, either s or $s+p$ is going to be odd. Therefore s or $s+p$ is going to be odd non-residue of p. Without loss of generality, let s be odd. Then each $p_1, ..., p_n$, the prime factors of s, will be odd. If, by contradiction, p_i are all residue of p, then for each i, we have $x_i^2 \equiv p_i \mod p$ for some x_i. Now letting $x = \prod_{i=1}^{n} x_i$,

$$x^2 = \left(\prod_{i=1}^{n} x_i\right)^2 = \prod_{i=1}^{n} x_i^2 \equiv \prod_{i=1}^{n} p_i = s \mod p$$

which contradicts our assumption s being non-residue of p. So there will be an odd prime factor of s which is non-residue of p. Let this number be q and we're done. □

We are now ready to prove the other direction of our main theorem.

Proof. "$\Leftarrow$"
Let N be given and let $N = \frac{a}{b}$ in lowest terms. Suppose N satisfies

$$\forall A, B[(\phi(A,B,0) \wedge \forall M(\phi(A,B,M) \rightarrow \phi(A,B,M+1))) \rightarrow \phi(A,B,N)]$$

where $\phi(A,B,K)$ stands for $\exists X, Y, Z(2 + ABK^2 + BZ^2 = X^2 + AY^2)$. We wish to show that this means N is in fact an integer. This can be shown if we show $b = \pm 1$. This in turn reduces to showing that $p \nmid b$ for all prime p. Finally, we will show this by showing that all primes equal to 1,2 and 3 modular 4 doesn't divide b which clearly covers all cases.

- $p \nmid b$ for all $p \equiv 2, 3 \mod 4$
  Since by assumption

  $$(\phi(A,B,0) \wedge \forall M(\phi(A,B,M) \rightarrow \phi(A,B,M+1))) \rightarrow \phi(A,B,N)$$

  holds for all A and B, we consider the case when $A = 1$ and $B = p$ where $p \equiv 3 \mod 4$. Lemma 4.2.4 tells us that $\exists X, Y, Z(2 + pM^2 + pZ^2 = X^2 + Y^2)$, i.e. $\phi(1, p, M)$ holds, if and only if the denominator of M in lowest terms is not divisible by 2 or any prime $p \equiv 3 \mod 4$. We claim that $A = 1$ and $B = p$ satisfy the hypothesis

  $$\phi(A,B,0) \wedge \forall M(\phi(A,B,M) \rightarrow \phi(A,B,M+1)).$$

  - $\phi(1, p, 0)$
    If $M = \frac{c}{d}$ in lowest terms and $M = 0$, then this means $c = 0$ and $d = \pm 1$. In this case, the denominator is not divisible by 2 or any prime $p \equiv 3 \mod 4$ so by Lemma 4.2.4, $\phi(1, p, 0)$ holds.
  - $\phi(1, p, M) \rightarrow \phi(1, p, M+1)$
    Suppose $M = \frac{c}{d}$ in lowest terms and $\phi(1, p, M)$ holds. Then by Lemma 4.2.4, d doesn't divide 2 or p. Notice $M + 1 = \frac{c}{d} + 1 = \frac{c+d}{d}$ and since by assumption c and d are coprime, $c + d$ and d are coprime as well. Hence $\phi(1, p, M+1)$ holds by Lemma 4.2.4.

  So the hypothesis is satisfied. This means then $\phi(1, p, N)$ holds. Then by the other implication of Lemma 4.2.4, we have that neither 2 or p divides b.

- $p \nmid b$ for all $p \equiv 1 \mod 4$
  Let q be odd number such that $\left(\frac{q}{p}\right) = -1$ which exists by Lemma 4.2.6.

Then we let $A = q$ and $B = p$. Lemma 4.2.5 tells us $\phi(q, p, M)$ holds if and only if d is not divisible by any prime $p \equiv 1 \mod 4$. Then by the same reasoning as above,

$$\phi(q, p, 0) \wedge \forall M(\phi(q, p, M) \rightarrow \phi(q, p, M + 1))$$

holds. So $\phi(q, p, N)$ holds. Which means $p \nmid b$ for any prime $p \equiv 1 \mod 4$.

This completes the proof. □

We showed in Section 2, $\langle \mathbb{Z}; +, \cdot, 0, 1 \rangle$ is undecidable. Theorem 4.2.1 tells us that $\mathbb{Z}$ is a definable subset of $\mathbb{Q}$ in the first order language $\langle \mathbb{Q}; +, \cdot, 0, 1 \rangle$. Therefore, the proof of undecidablity of $\mathbb{Z}$ translates to the undecidability of $\mathbb{Q}$. So we're done.

4.3 Universal definition of $\mathbb{Z}$ in $\mathbb{Q}$

In the previous section, we studied Robinson's proof of undecidability of $\mathbb{Q}$ by showing that $\mathbb{Z}$ is a definable set in the first order language of $\mathbb{Q}$. This method works in general. If one can show that a ring R can define "$\mathbb{Z}$" using first order formulas, then we can show R is undecidable. Furthermore, if we can show that $\mathbb{Z}$ is *existentially* definable in R, i.e. if there is an existential formula $\phi(v)$ such that $R \vDash \phi(a)$ if and only if $a \in \mathbb{Z}$, then we can show that H10/R is unsolvable. This is because as we saw in Section 2.4, existential formulas define Diophantine sets. So to show that H10/$\mathbb{Q}$ unsolvable, it's enough to show that $\mathbb{Z}$ can be defined existentially in $\mathbb{Q}$. Robinson's definition doesn't work as a proof of unsolvability of H10/$\mathbb{Q}$ because her formula defining $\mathbb{Z}$ is not an existential formula.

Recently, Jochen Koenigsmann, in [16], showed that $\mathbb{Z}$ can be defined *universally* in $\mathbb{Q}$. In other words, there is a formula of the form

$$\forall v_1, ..., v_n \theta(v_1, ..., v_n)$$

which define $\mathbb{Z}$ in $\mathbb{Q}$ where θ is a quantifier free formula. This gives a corollary

$$\mathbb{Q} \setminus \mathbb{Z} \text{ is existentially definable in } \mathbb{Z}.$$

5 An observation

In this final section, we will study an observation I made as I was looking through the known results on the Hilbert's Tenth Problem and the decidability of various rings.

The table below shows some of the main results known on the solvability of Hilbert's Tenth Problem and the decidability of the full theory of various rings.

Ring R	**H10/R solvable?**	**First order theory decidable?**
$\mathbb{C}$	Yes $\Leftarrow$	Yes([25])
$\mathbb{R}$	Yes $\Leftarrow$	Yes [37] ([3], Section 3)
$\mathbb{F}_q$	Yes $\Leftarrow$	Yes (Trivial)
$\mathbb{Q}_p$	Yes [24] $\Leftarrow$	Yes [2], [9] ([3])
$\mathbb{F}_q((t))$	?	?
Number field	?	No [33]
$\mathbb{Q}$	?	No [34](Section 4.2)
Global function field	No [36], [8]	$\Rightarrow$ No
$\mathbb{F}_q(t)$	No [27], [38]	$\Rightarrow$ No [9], [26]
$\mathbb{C}(t)$	?	?
$\mathbb{C}(t,u)$	No [14],	$\Rightarrow$ No
$\mathbb{R}(t)$	No [6]	$\Rightarrow$ No
$\mathcal{O}_K$	?(No for some $\mathcal{O}_K$)	No (corollary of No for K)
$\mathbb{Z}$	No [22]([5], Section 2)	$\Rightarrow$ No [10]
$A[t]$	No [7], [6], [13]	$\Rightarrow$ No
$\mathbb{A}$	Yes [20], [30], [31], [35] $\Leftarrow$	Yes

Notations

$\mathbb{C}$	Algebraically Closed Field
$\mathbb{R}$	Field of Reals
$\mathbb{F}_q$	Finite field of q elements
$\mathbb{Q}_p$	p-adic fields
$\mathbb{F}_q((t))$	Power series field over finite field
$\mathbb{Q}$	Field of Rationals
$\mathbb{F}_q(t)$	Rational function field
$\mathbb{C}(t)$	Function field over complex numbers
$\mathbb{C}(t,u)$	Function field over complex numbers in two variables
$\mathbb{R}(t)$	Function field over the reals
$\mathcal{O}_K$	Integral closure of $\mathbb{Z}$ in K
$\mathbb{Z}$	Ring of integers
$A[t]$	Polynomial ring over an integral domain
$\mathbb{A}$	Ring of algebraic integers

The bottom two results are from Pheidas's summary of results in [28] and the rest are from Poonen's summary of results in [29].

At first, we might consider four possibilities for the result of a given ring R as summarised below.

H10/R	**First order theory**
Solvable	Decidable
Solvable	Undecidable
Unsolvable	Decidable
Unsolvable	Undecidable

However, we already discussed in Section 3.2 that decidability of the first theory of a ring implies solvability of Hilbert's Tenth Problem over the ring. So the possibilities remaining are as below.

H10/R	**First order theory**
Solvable	Decidable
Solvable	Undecidable
Unsolvable	Undecidable

We already have examples of the first case and the bottom case: $\mathbb{R}$ and $\mathbb{Z}$ respectively. However, as I was looking through the survey of results I couldn't find any example of a ring of the middle case, where the Hilbert's

Tenth Problem was solvable but the first order theory undecidable. Even more surprisingly, I couldn't find any comments on this fact. I didn't find any theorems or conjectures on this issue. I also discussed this with my supervisor and it seems like there isn't any known example out there yet. So it may even be the case that all rings with undecidable first order theory have unsolvable Hilbert's Tenth Problem. If this is the case, then it would solve many open problems such as the rationals which is known to have undecidable first order theory (See section 4.2.1). Whilst searching for such an example, the closest example I could find was from Lipshitz's paper in [19].

Theorem 5.0.1. *Existential theory of* $\langle \mathbb{N}, +, |, 0, 1 \rangle$ *is decidable but the full theory is undecidable where* $a|b$ *is the relation "a divides b".*

Existential theory of a language is the set of all true sentences in the language of the form $\exists x_1, ..., x_n \theta$ where θ is a quantifier free formula. Previously, we noted that the Diophantine equations are equivalent to the existential formulas of a given ring. Also, the language is similar to a ring so this example is really close to what we want. The reason it is not exactly what we want is because this is not a ring.

Lipshitz's paper shows that the existential theory of $\langle \mathbb{N}, +, |, 0, 1 \rangle$ is decidable. But the proof of the full theory of $\langle \mathbb{N}, +, |, 0, 1 \rangle$ being undecidable is a consequence of a result shown by Julia Robinson in [34]. Robinson proved that multiplication is definable in $\langle \mathbb{N}, +, |, 0, 1 \rangle$. In other words, she showed that there is a first order formula $\phi(u, v, w)$ involving only the logical symbols, $+$ and $|$ such that for all $n_1, n_2, n_3 \in \mathbb{N}$, $\langle \mathbb{N}, +, |, 0, 1 \rangle \vDash \phi(n_1, n_2, n_3)$ if and only if $n_1 + n_2 = n_3$. This implies that the ring $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ is definable in $\langle \mathbb{N}, +, |, 0, 1 \rangle$. Then the proof of the undecidability of $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ which we proved in Section 2 translates to a proof of undecidability of $\langle \mathbb{N}, +, |, 0, 1 \rangle$.

I think that the question of whether there is a ring R such that H10/R is solvable but the full theory is undecidable is a very interesting question. This is because it is a study of the borderline of Hilbert's Tenth Problem and the Decidability of rings. With more time, I would be very interested to extend this project by trying to construct such a ring or to find an argument as to why there can't be such a ring.

References

[1] http://www.encyclopediaofmath.org/index.php/Algebraically_closed_field.

[2] James Ax and Simon Kochen. Diophantine problems over local fields: Iii. decidable fields. *The Annals of Mathematics*, 83(3):437–456, 1966.

[3] Paul J Cohen. Decision procedures for real and p-adic fields. *Communications on pure and applied mathematics*, 22(2):131–151, 2006.

[4] B. Jack Copeland. The church-turing thesis. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Fall 2008 edition, 2008.

[5] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):pp. 233–269, 1973.

[6] Jan Denef. The diophantine problem for polynomial rings and fields of rational functions. *Trans. Amer. Math. Soc*, 242:391–399, 1978.

[7] Jan Denef. The diophantine problem for polynomial rings of positive characteristic. *Studies in Logic and the Foundations of Mathematics*, 97:131–145, 1979.

[8] Kirsten Eisenträger. Hilbert's tenth problem for algebraic function fields of characteristic 2. *arXiv preprint math/0207029*, 2002.

[9] Yu L Ershov. On the elementary theory of maximal normed fields. In *Dokl. Akad. Nauk SSSR*, volume 165, pages 21–23, 1965.

[10] Kurt Gödel. Über formal unentscheidbare sätze der principia mathematica und verwandter systeme i. *Monatshefte für Mathematik*, 38(1):173–198, 1931.

[11] Terry S. Griggs. 75.44 impolite numbers. *The Mathematical Gazette*, 75(474):pp. 442–443, 1991.

[12] Jeffrey Hatley. Hasse-minkowski and the local-to-global principle. *Senior capstone, UM Amherst: http://www. math. umass. edu/˜ hatley/Capstone. pdf*, 2009.

[13] KH Kim and FW Roush. Undecidability of parametric solutions of polynomial equations. *Proceedings of the American Mathematical Society*, 118(2):345–348, 1993.

[14] Ki Hang Kim and FW Roush. Diophantine undecidability of c(t,u). *Journal of Algebra*, 150(1):35–44, 1992.

[15] Neal Koblitz, Neal Koblitz, Neal Koblitz, and Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 19. Springer-Verlag New York, 1977.

[16] Jochen Koenigsmann. Defining z in q. *arXiv preprint arXiv:1011.3424*, 2010.

[17] Jochen Koenigsmann. C1.1a model theory. http://www.maths.ox.ac.uk/, 2011.

[18] Jochen Koenigsmann. B1a logic. http://www.maths.ox.ac.uk/courses/course/19549/material, 2012.

[19] Leonard Lipshitz. The diophantine problem for addition and divisibility. *Transactions of the American Mathematical Society*, pages 271–283, 1978.

[20] A Macintyre and L. Van Den Dries. The logic of rumnely's local-glocal principle. *Journal für die Riene und Angewandte Mathematik*, 1990.

[21] David Marker. Model theory for algebra and algebraic geometry. http://homepages.math.uic.edu/ marker/orsay/orsay2.pdf.

[22] Ju V Matijasevic. The diophantineness of enumerable sets.(russian). In *Dokl. Akad. Nauk SSSR*, volume 191, pages 279–282, 1970.

[23] Yuri Matiyasevich. *Hilbert's 10th Problem*. MIT press, 1993.

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

[25] Grant Olney Passmore. Understanding algebro-geometric quantifier elimination: Part i, algebraically closed fields of characteristic zero via muchnik.

[26] Yu G Penzin. The undecidability of fields of rational functions over fields of characteristic 2. *Algebra and Logic*, 12(2):116–119, 1973.

[27] Thanases Pheidas. Hilbert's tenth problem for fields of rational functions over finite fields. *Inventiones Mathematicae*, 103(1):1–8, 1991.

[28] Thanases Pheidas. Extensions of hilbert's tenth problem. *Journal of Symbolic Logic*, pages 372–397, 1994.

[29] Bjorn Poonen. HilbertâĂŹs tenth problem over rings of number-theoretic interest. *Note from the lecture at the Arizona Winter School on âĂIJNumber Theory and Logic*, 2003.

[30] A Prestel and J Schmid. Existentially closed domains with radical relations. *J. reine und angew. Math*, 407:178–201, 1990.

[31] Alexander Prestel and Jürgen Schmid. Decidability of the rings of real algebraic and p-adic algebraic integers. *J. reine und angew. Math*, 414:141–148, 1991.

[32] Mihai Prunescu. Diophantine properties of finite commutative rings. *Archive for Mathematical Logic*, 42(3):293–302, 2003.

[33] Julia Robinson. The undecidability of algebraic rings and fields. *Proceedings of the American Mathematical Society*, pages 950–957, 1959.

[34] Julia Bowman Robinson. *Definability and decision problems in arithmetic*. PhD thesis, Univ. of California, Berkeley, 1948.

[35] Robert S Rumely. Arithmetic over the ring of all algebraic integers. *J. reine angew. Math*, 368:127–133, 1986.

[36] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[37] Alfred Tarski. A decision method for elementary algebra and geometry. 1951.

[38] Carlos R Videla. Hilbert's tenth problem for rational function fields in characteristic 2. *Proceedings of the American Mathematical Society*, 120(1):249–254, 1994.

[39] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141(3):pp. 443–551, 1995.