Hilbert's 10th Problem Extended to $\mathbb{Q}$

Peter Gylys-Colwell

April 2016

Contents

1 Introduction

During the summer of 1900 at the International Congress of Mathematicians Conference, the famous mathematician David Hilbert gave one of the most memorable speeches in the history of mathematics. Within the speech, Hilbert outlined several unsolved problems he thought should be studied in the coming century. Later that year he published these problems along with thirteen more he found of particular importance.
This set of problems became known as Hilbert's Problems. The interest of this paper is one of these problems in particular: Hilbert's Tenth problem. This was posed originally from Hilbert as follows:

> 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 [3].

The problem was unsolved until 1970, at which time a proof which took 20 years to produce was completed. The proof had many collaborators. Most notable were the Mathematicians Julia Robinson, Martin Davis, Hilary Putman, and Yuri Matiyasevich. The proof showed that Hilbert's Tenth Problem is not possible; there is no algorithm to show whether a diophantine equation is solvable in integers. This result is known as the MDRP Theorem (an acronym of the mathematicians last names that contributed to the paper). The MDRP Theorem not only proved Hilbert's Tenth Problem is impossible, but showed all recursively enumerable sets are diophantine. In this paper we will explore some of the implications and extensions from the groundbreaking proof for Hilbert's Tenth Problem to other domains, in particular, to $\mathbb{Q}$ [4].

2 Background Theory

For the rest of this paper it will be necessary to define some technical terms and introduce some topics of Computation Theory (synonymous with Recursion Theory):
To begin, it should be established Computation Theory is interested mainly in $\mathbb{Z}$ and so unless otherwise stated, assume we are working with $\mathbb{Z}$.

Definition 2.1. An *Algorithm* (synonymous with *Computable Function* and *Recursive Function*) is a self contained set of directions to be performed on a given input to produce an output.

Definition 2.2. A *Recursive Set*, *Decidable Set* or *Computable Set* is a Set such that there is an algorithm which terminates after a finite number of iterations to correctly decide whether or not a given input belongs to the set.

Definition 2.3. A *Recursively Enumerable Set* or *Computably Enumerable Set* is a set where there is an algorithm that can list the set. The algorithm may run forever.

Recursive Sets have some easily verified desirable properties:
The complement of a recursive set is recursive. The union and intersection of recursive sets are also recursive. The preimage for a recursive function which maps to a recursive set is a recursive set. If a set and its complement are recursively enumerable then the set is recursive.

While Recursive Sets and Recursively Enumerable Sets seem very similarly defined, they are not the same. For a set to be Recursive implies that it is Recursively Enumerable, however the converse is not true. There are Recursively Enumerable Sets that are not Recursive.
An example of a set that is Recursively Enumerable but not Recursive can be constructed using Godel numbering which is explained more in section 1.9 of [2].

3 Diophantine Equations

When approaching a solution for Hilbert's tenth problem, Martin Davis reversed the problem [1]. Instead of being given a polynomial and investigating a solution, we will begin with a set of solutions and search for the diophantine equation.

Definition 3.1. We define *Diophantine Sets* as follows:
A subset $A \subset \mathbb{Z}^m$ is called Diophantine if there exists a polynomial $p(T_1, \ldots T_m, \chi_1, \ldots \chi_k)$ with coefficients in $\mathbb{Z}$ such that for any element $(t_1, \ldots, t_m) \in \mathbb{Z}^m$ we have that

$$\exists x_1, \ldots, x_k \in \mathbb{Z} : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots T_m, \chi_1, \ldots \chi_k)$ a *Diophantine definition* of A over $\mathbb{Z}$ [4]

We say $t_1 \ldots t_m$ are the constants and coefficients of the of the diophantine equation, and if $t_1 \ldots t_m$ exist in the diophantine set, then the polynomial $p(t_1, \ldots, t_m, \chi_1, \ldots, \chi_k) = 0$ has a solution in $\mathbb{Z}$.
If the set is computable, then that means there is some algorithm that in a finite amount of steps can determine whether the given diophantine equation has a solution in $\mathbb{Z}$.
Some examples of diophantine equations are as follows:

1. the set of numbers not divisible by two:

$$x \in D \iff \exists y : 2y + 1 = x$$

2. $\mathbb{Z}^+ = \{0, 1, 2 \ldots\}$ is diophantine since

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

   Which is a result established by Lagrange's four square theorem: that any positive integer can be the sum of four squares.

Diophantine Sets have some desirable properties as well:

Lemma 3.1. *Intersections and Unions of diophantine sets are diophantine.*

To show this, we observe that for two diophantine sets C, D with definitions P_1 and P_2 respectively, we observe that

$$(P_1)(P_2)$$

is the definition for $C \cup D$ since the above polynomial is zero at x if and only if $P_1(x) = 0$ or $P_2(x) = 0$. For the intersection we observe

$$(P_1)^2 + (P_2)^2$$

is the definition for $C \cap D$ since the above polynomial is zero at x iff $P_1(x) = 0$ and $P_2(x) = 0$

Theorem 3.2. *Diophantine sets are recursively enumerable.*

To show this, we observe for a diophantine set D with definition $p(t_1, \dots t_m, x_1, \dots x_k)$ we iterate through each element of $\mathbb{Z}^{k+m}$ to see when the diophantine definition of the element is zero.

Theorem 3.3. *All recursively enumerable sets in $\mathbb{Z}$ are diophantine.*

This result is not trivial and was a consequence of the MDRP Theorem [4]. Since there are recursivly enumerable sets that are not computable, it follows that there are diophantine sets that are not recursive.
Summarized in more concrete terms:

Lemma 3.4. *There exists a polynomial $P(x_0, \dots x_n, a_0, \dots a_k)$ over $\mathbb{Z}$ such that it is impossible for an algorithm to exist to determine in a finite number of steps whether*

$$\exists x_0 \dots x_k \in \mathbb{Z}$$

$$P(a_1, \dots a_n, x_0, \dots x_k) = 0$$

for a given $(a_1, \dots a_n) \in \mathbb{Z}^n$

And therefore Hilbert's Tenth Problem is proved impossible. But the topic still has much more work to be done ...

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

While Hilbert Originally posed the problem over $\mathbb{Z}$, this problem can be extended to many different algebraic structures. Specifically an arbitrary ring:

Definition 4.1. A *Ring R* is a set of objects with two binary operations $(+, *)$ with the following properties:
For any $a, b, c \in R$:

$$a + b = b + a$$

$$(a * b), (a + b) \in R$$

$$(a * b) * c = a * (b * c)$$

$$a * (b + c) = a * b + a * c$$

Some examples are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{Z}$ are infinite Rings. Where $*$ is the multiplication operation and $+$ is the addition operation. $\mathbb{Z}$ mod n where $n > 0$ is an example of a finite ring
It follows that the definition of the diophantine set can be extended to any ring. Diophantine equations are just equations of a collection of elements and ring operations, and are therefore well defined on any ring.
One of the largest open problems relating to HTP is its extension to the rationals, $\mathbb{Q}$. At first glance, the reader may think there is some simple way to connect the MDRP theorem which applied to HTP over $\mathbb{Z}$ to the extension over

$\mathbb{Q}$. Unfortunately it has not been that simple.

An interesting result is that if HTP was solvable on $\mathbb{Z}$, then it is solvable on $\mathbb{Q}$. In other words if we knew whether a solution existed in $\mathbb{Z}$, then we know whether a solution exists in $\mathbb{Q}$. This can be shown with the following logic:

If P is a polynomial with integer coefficients then

$$\exists z_1, \ldots, z_k \in \mathbb{Q} : P(z_1, \ldots, z_k) = 0$$

$$\Updownarrow$$

$$\exists x_1, \ldots, x_k, y_1, \ldots, y_k \in \mathbb{Z}, y_1 \ldots y_k \neq 0 : P(\frac{x_1}{y_1}, \ldots, \frac{x_k}{y_k}) = 0$$

We can rewrite

$$P(\frac{x_1}{y_1}, \ldots, \frac{x_k}{y_k}) = 0$$

As a new diophantine equation

$$Q(x_1, \ldots x_k, y_1, \ldots y_k)$$

By multiplying each term of P by the product of the denominators of each term. Then intersecting the diophantine set with definition Q with the diophantine set $\{z \in \mathbb{Z} : z \neq 0\}$. (As shown earlier, intersections of diophantine sets are diophantine).

For example if

$$P = \left(\frac{x_1}{y_1}\right)^5 + \frac{x_2}{y_2} + 4 = 0$$

Q would be

$$Q = x_1^5 y_2 + x_2 y_1^5 + 4 y_1^5 y_2 = 0$$

Therefore if we can determine weather the diophantine equation Q has solutions over $\mathbb{Z}$, we can determine if the original equation has solutions over $\mathbb{Q}$. Unfortunatley this does not establish an if and only if relation since there are diophantine sets over $\mathbb{Z}$ that do not follow the above logic backwards to sets in $\mathbb{Q}$. A specific example would be diophantine sets with definitions where there is a constant term, such as $P(x, y) = x^2 + y^2 + 5$

One approach in relating the result of MDRP to $\mathbb{Q}$ is if $\mathbb{Z}$ is diophantine when viewed as a subset of $\mathbb{Q}$. If $\mathbb{Z}$ has a diophantine definition $p(T, X)$ over $\mathbb{Q}$, then the MDRP result would also apply to $\mathbb{Q}$ and HTP would not be decidable on $\mathbb{Q}$.

This is because of the following logic. We can take the intersection of the diophantine sets

$$D = \mathbb{Z} \cap Q$$

such that Q is an undecidable diophantine set over $\mathbb{Z}$. We know that the intersection of diophantine sets is diophantine, however the set D is not decidable since Q is not decidable over $\mathbb{Z}$

In fact using similar logic we have the following:

Theorem 4.1. *If a Ring R contains $\mathbb{Z}$ and $\mathbb{Z}$ has a diophantine definition on R, then the MDRP theorem applies to R and HTP is unsolvable on R*

Unfortunately there is a Conjecture by Barry Mazur in 1992 which has a direct consequence that there is no diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$. Neither can there be a diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$. [4].

Definition 4.2. A diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ is a mapping $\phi : \mathbb{Z} \to \mathbb{Q}$ that is recursive, injective, and maps diophantine sets in $\mathbb{Z}$ to diophantine sets in $\mathbb{Q}$.

5 Big and Small Ring Approach

In a different approach, we define a new ring to use:

Definition 5.1. Let S be a set of primes in $\mathbb{Q}$. We define a certain ring $O_{\mathbb{Q},S}$ as the subring of $\mathbb{Q}$:

$$\left\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is only divisible by primes in } S\right\}$$

Some examples are as follows:

1. If $S = \{2\}$ then $O_{\mathbb{Q},S} = \{\frac{j}{2^k} : j \in \mathbb{Z}, k \in \mathbb{N}\}$
2. If S is $\emptyset$, then we define $O_{\mathbb{Q},S} = \mathbb{Z}$
3. If S is the set of all primes in $\mathbb{Q}$ then $O_{\mathbb{Q},S} = \mathbb{Q}$

If S is finite and non-empty, we will call $O_{\mathbb{Q},S}$ a *Small Ring*, and if S is infinite then we call $O_{\mathbb{Q},S}$ a *Big Ring.*
These rings have some nice properties relating to diophantine definitions: The set of nonzero elements of a big or small ring is diophantine over that ring. And from Julia Robinsons work [4] we know the following theorem:

Theorem 5.1. *$\mathbb{Z}$ has a diophantine definition over any small subring of $\mathbb{Q}$*

In other words for a given S and its resulting $O_{\mathbb{Q},S}$, there is a polynomial $p(x_0 \dots x_n, a_0 \dots a_k)$ such that

$$\exists a_0 \dots a_k \in O_{\mathbb{Q},S} : p(x_0 \dots x_n, a_0 \dots a_k) = 0$$

$$\Updownarrow$$

$$x_0 \dots x_n, \in \mathbb{Z}$$

It follows that HTP is undecidable for any small subring of $\mathbb{Q}$ as stated in theorem 4.2 of the above section.
Unfortunately, no diophantine definition has been established for big rings of $\mathbb{Q}$ [4].
Without any result relating HTP to $\mathbb{Q}$, we come back empty handed.

6 Conclusion

While no one to this day has established an answer for Hilbert's Tenth Problem extended to $\mathbb{Q}$, this paper explored different avenues for approaching an answer for the problem. The topic is very sophisticated, related with many ideas from different disciplines of mathematics.

It is fascinating how one of the most fundamental structures in algebra, the polynomial, can have such clunky properties. The ideas relating to HTP show just how important it is to study polynomials since recursive enumerable sets constitute many interesting questions in mathematics.

One example in particular is the Riemann hypothesis. We know the zeros of the Riemann-zeta function are recursively enumerable. Therefore they can be expressed as the solutions of a diophantine equation. Finding a diophantine definition for the set of zeros would be an interesting approach to proving the Riemann Hypothesis.

Another area of interest is the work relating to the *universal* diophantine equation explained more detail in section 7 of [1]. Essentially the idea behind the universal diophantine equation is that the set of all diophantine sets is itself recursively enumerable. Therefore there is some diophantine definition for all diophantine sets. To come up with a concrete diophantine defiinition for this universal diophanitne set would be a large milestone in the study of diophatine equations

References

[1] Davis, Martin. "Hilberts Tenth Problem Is Unsolvable. The American Mathematical Monthly, Vol. 80, No. 3 (Mar., 1973), pp. 233-269. Web. http://www.math.umd.edu/ laskow/Pubs/713/Diophantine.pdf

[2] Rogers, Hartley. Theory of Recursive Functions and Effective Computability. New York: McGraw-Hill, 1967. Web. http://www-2.dc.uba.ar/materias/azar/bibliografia/Rogers1987TheoryofRecursiveFunctions.pdf This was in [4] as citation 26

[3] Hilbert, David. "Mathematical Problems." International Congress of Mathematicians. Paris. 1900. Web. http://aleph0.clarku.edu/ djoyce/hilbert/problems.html

[4] Shilapentokh, Alexandra. Defining Integers. Bulletin of Symbolic Logic Volume 17 Number 2, June 2011: 230-51. Print.

[5] Poonen, Bjorn. "Using Elliptic Curves of Rank One towards the Undecidability of Hilbert's Tenth Problem over Rings of Algebraic Integers." Web. http://www-math.mit.edu/ poonen/papers/ants5.pdf