Hilbert's Tenth Problem

Andrew J. Ho

June 8, 2015

1 Introduction

In 1900, David Hilbert published a list of twenty-three questions, all unsolved.

The tenth of these problems asked to perform the following:

> 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 in a finite number of operations whether the equation is solvable in rational integers.

(Note that in the above, a "rational integer" just means an integer.)

The problem was resolved in the negative by Yuri Matiyasevich in 1970.

In the following paper, I will give a brief introduction to the theory of Diophantine sets as well as the theory of computability. I will then present the Matiyasevich-Robinson-Davis-Putnam (MRDP) theorem, which is immediately comprehensible given just a cursory understanding of the mathematical basics, and give some details of its proof. Finally, I will present some further work in the area of Diophantine computability and various applications or corollaries of the celebrated MRDP theorem.

To restate Hilbert's Tenth Problem in modern terms: "Given a polynomial equation with integer coefficients, is there an algorithm for Turing machines which can decide, in a finite amount of time, whether or not a set of integer solutions to the polynomial equation exists?" Phrased in these terms, two observations become evident. First, we see that Hilbert almost foresaw the concept of algorithmic unsolvability before it was developed by Turing, Church, et al. Second, we see that the question hints at a deep, fundamental connection between number theory, a storied field with much history, and the modern field of computability theory.

2 Diophantine equations and sets

First, we shall begin with a formal definition of a Diophantine equation.

Definition 1. *Let $D(x_1, \ldots, x_m)$ be a polynomial in n variables with integer coefficients which admits only integer values for $x_1, \ldots, x_m$. The equation $D(x_1, \ldots, x_m) = 0$ is called **Diophantine**.*

More generally, we usually speak of a Diophantine equation as accepting two sets of inputs. That is, $D(a_1, \ldots, a_n, x_1, \ldots, x_m)$ takes as input an n-tuple, called its parameters, and an m-tuple, called its unknowns. (Intuitively, we immediately recognize that $n \leq m + 1$.)

Definition 2. *Let S be a subset of all n-tuples of integers and consider an arbitrary Diophantine equation. If for every $a \in S$ there exists an m-tuple $(x_1, \ldots, x_m)$ such that $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$, and the converse is also true, then the set S is **Diophantine**. The **dimension** of the set is m. Similarly, we consider D to be a **Diophantine representation** of S.*

To save ourselves some work, let us consider the problem of limiting ourselves to the natural numbers.

Lemma 1. *Every natural number can be decomposed as the sum of squares of four integers, not necessarily unique. (This is known as* Lagrange's four-square theorem.*)*

Proof. The proof is given in Niven and Zuckerman (1960). It is surprisingly involved. □

Theorem 1. *The problem of determining the existence or nonexistence of solutions to a Diophantine equation which accepts natural numbers is reducible to the problem of determining the existence or nonexistence of solutions to a Diophantine equation which accepts integer values. The opposite is also true.*

Proof. Since $\mathbb{N} \in \mathbb{Z}$, the second part is trivially true.

To prove the first part, consider a Diophantine equation $D(x_1, \ldots, x_m) = 0$, accepting only natural numbers for $x_1, \ldots, x_m$.

Write $x_n = y_{n,1}^2 + y_{n,2}^2 + y_{n,3}^2 + y_{n,4}^2$ for every n where each y is an integer; from Lagrange's four-square theorem, this is guaranteed to be possible. Substituting into D, we obtain a Diophantine equation in $4m$ variables, all of which are integers. □

Diophantine sets and relations behave very well with respect to logical operations, which we can see in the following theorem.

Theorem 2. *The union of two Diophantine sets of the same dimension is Diophantine. The intersection of two Diophantine sets, of same or different dimension, is Diophantine.*

Proof. Let S_1, S_2 be two Diophantine sets and let D_1, D_2 be their Diophantine representations. If they are both of dimension m, then the Diophantine equation $D_1(x_1, \ldots, x_m) \times D_2(x_1, \ldots, x_m) = 0$ has a Diophantine set $S_1 \cup S_2$. Moreover, regardless of dimension, $D_1^2 + D_2^2 = 0$ has a Diophantine set $S_1 \cap S_2$. □

3 Computability theory

For the purposes of the present paper, it is unnecessary to consider the full formalization of a Turing machine. It suffices to be aware that a Turing machine is a generalization of the idea of computers capable of doing basic tasks and accept procedural lists of elementary instructions.

Definition 3. *A subset S of $\mathbb{N}$ is called* ***recursive*** *if there exists an algorithm which accepts a natural number n and is guaranteed to terminate after a finite amount of time, after which it correctly outputs the truth value of the statement $n \in S$.*

Definition 4. *A subset S of $\mathbb{N}$ is called* ***recursively enumerable*** *if there exists an algorithm which accepts a natural number n and, if $n \in S$, is guaranteed to terminate in a finite amount of time and confirm that $n \in S$. The algorithm need not be guaranteed to terminate for inputs $n \notin S$, but must not give any incorrect answers.*

It is easy to see from the above that all recursive sets are recursively enumerable. However, the fact that there exist recursively enumerable sets that are not recursive is nontrivial. The difference between the conditions is clear; recursively enumerable sets are not required to terminate if the input is not in the solution set S. However, it is not immediately clear that the set of recursively enumerable sets that are not also recursive is nonempty. Thankfully, we have the following theorem:

Theorem 3. *A* ***simple set*** *is a set that is co-infinite and recursively enumerable but also such that every infinite subset of its complement is not recursively enumerable. Simple sets are not recursive.*

Proof. Given in Soare (1987). □

We may reformulate a different definition of *recursively enumerable* in order to make the resolution of Hilbert's Tenth Problem a little easier.

Definition 5. *A set S is* ***recursively enumerable*** *if there exists an algorithm that enumerates S.*

It is not immediately clear that this definition is equivalent to the previously stated one. However, it is straightforward to prove.

Theorem 4. *The two given definitions of recursive enumerability are equivalent.*

Proof. Take a set $S \subset \mathbb{N}$. First suppose that there exists an algorithm that is guaranteed to terminate on inputs contained in S and run infinitely for inputs not contained in S. Let this algorithm be denoted $A(n)$ where n is its input.

To show that there exists an algorithm for enumerating the members of S, consider the following construction: Run $A(0)$ for one time step, then run $A(0), A(1)$ for one time step, then run $A(0), A(1), A(2)$ for one time step, and so on and so forth. This described algorithm will "eventually" reach arbitrarily large timesteps for $A(n)$ given any choice of n, and so for all $n \in S$ it is guaranteed to confirm that $n \in S$ in a finite span of time. Modify $A(n)$ to print n if it halts, and we have the desired enumeration.

Conversely we shall suppose that there exists an algorithm that enumerates S; call it A. To construct an algorithm $B(n)$ that halts only if $n \in S$, simply run A and halt if n is printed. □

4 The MRDP theorem

The most succint statement of the MRDP theorem is as follows:

Theorem 5. *A set is Diophantine if and only if it is recursively enumerable.*

The existence of recursively enumerable sets that are not recursive immediately resolves Hilbert's Tenth Problem, because it implies the existence of a Diophantine set that is not recursive.

To see this, consider the following reasoning: Let S be a Diophantine set and let $D(a, x_1, \dots, x_m)$ be its Diophantine representation. By definition, $a \in S$ if and only if there exists $a \in \mathbb{N}$ such that $D(a_1, \dots, a_n, x) = 0$ has a solution m-tuple $(x_1, \dots, x_m)$. Suppose also that there *does* exist an algorithm capable of deciding the solvability of arbitrary Diophantine equations. This algorithm would be capable of deciding, in a finite amount of time, whether or not $a \in S$. As such, this would mean that every Diophantine set is recursive. However, the MRDP theorem asserts that every set is Diophantine if and only if it is recursively enumerable, so this implies that all recursively enumerable sets are also recursive, which is untrue. The contradiction yields a negative answer to Hilbert's Tenth Problem.

4.1 Overview of the proof

The proof can be very generally separated into two major parts. First, Davis, Putnam, and Robinson showed in 1961 that every recursively enumerable set is *exponential Diophantine*, which is defined as the following:

Definition 6. *A set is **exponential Diophantine** if its Diophantine representation is a polynomial which allows exponentiation.*

(The definition is rough at the moment, but hopefully the meaning will become clarified in a more detailed treatment later on.)

Second, Matiyasevich was able to show in 1970 that sets which are exponential Diophantine sets are also Diophantine, that is, that exponentiation is a Diophantine relation.

The immediate corollary, of course, is the MRDP theorem.

4.2 Every recursively enumerable set is exponential Diophantine

Davis et al. (1960) give the full proof, which is quite technical and will not be reproduced. However, they do give some interesting corollaries to their main theorem, stated below:

Theorem 6. *Every recursively enumerable set is exponential Diophantine.*

Applying the same argument as before, we may see that:

Corollary 1. *There exists no algorithm for the determination of solvability of arbitrary exponential Diophantine equations.*

Proof. By contradiction. Identical to proof for Diophantine equations from the full MRDP theorem. □

Perhaps a little more interestingly, they note the following corollary:

Corollary 2. *There exists an algorithm which will accept a particular axiomatization of number theory and output an exponential Diophantine equation which has no solution, but cannot be proved to be unsolvable from the given axiomatization.*

Compare to the following statement of Godel's first incompleteness theorem:

Theorem 7. *In any sufficiently strong system of arithmetic, there exists a statement that is true, but cannot be proven to be true in that system.*

From this "incomplete" version of the MRDP theorem alone, we already see a remarkable connection between Godelian incompleteness and number theory.

4.3 Exponential Diophantine sets are Diophantine

Let $\beta_b(0) = 1$ and $\beta_b(n+1) = b\beta_b(n)$. Let $\alpha_b(0) = 0$, $\alpha_b(1) = 1$, and $\alpha_b(n+1) = b\alpha_b(n+1) - \alpha_b(n)$ for $b \geq 2$.

Before we may prove that exponentiation is Diophantine, we must prove that some sets defined by recurrent relations are Diophantine, which is surprisingly much easier. After the development of two lemmas, we then can arrive at the primary result.

Lemma 2. *The set of pairs* $\{(a,b)|b \geq 2 \wedge \exists n\ [a = \alpha_b(n)]\}$ *is Diophantine.*

Proof. Rewrite the second-order recurrent relation α asked

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix},$$

where we take $\alpha_b(-1) = -1$. This can be simplified by writing $A_b(0) = E$ and $A_b(n+1) = A_b(n)\Xi_b$, where

$$E = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \Xi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}.$$

It follows that $A_b(n) = \Xi_b^n$. Since $\det(Xi_b) = 1$, it follows that $\det(A_b(n)) = \underbrace{\det(\Xi_b) \cdot \det(\Xi_b)}_{n \text{ times}} = 1$. Expanding this out fully, we get

$$\alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1) = \alpha_b^2(n-1) - b\alpha_b(n-1)\alpha_b(n) + \alpha_b^2(n =)1.$$

As such, if we have natural numbers x, y, b satisfying $x^2 - bxy + y^2 = 1$, then one of x, y is $\alpha_b(m+1)$ and the other is $\alpha_b(m)$ for some natural number m, if such an m exists.

It has been shown by Matiyasevich (a full proof is given in Matiyasevich (1993)) that this is true. The argument is essentially inductive. □

Next, we have the following lemma, which is rather difficult to prove.

Lemma 3. *The set of triples* $\{(a,b,c)|b \geq 4 \wedge a = \alpha_b(c)\}$ *is Diophantine.*

Proof. The proof is rather technical, but a full exposition can be found in Matiyasevich (1993). It adds no insight and so is omitted. □

Finally, we find ourselves capable of demonstrating that exponentiation is Diophantine.

Theorem 8. *The set of triples* $\{(a,b,c)|a = b^c\}$ *is Diophantine.*

Proof. The idea is that we ought to be able to prove that $\alpha_b(n)$ grows approximately exponentially, so exponentiation is Diophantine. More precisely, we are able to prove that

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n$$

via induction. This is basically clear from inspection of the definition of $\alpha_b(n+2)$. This then implies that

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \geq \frac{(bx+3)^c}{x^c} \geq b^c$$

for large enough x. How large does x need to be?

Suppose $b = c = 0$. Then

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = 1.$$

Also for $b = 0$, $c > 0$, $x > 4$, we have the edge case

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < \frac{4^c}{(x-1)^c} \leq 1.$$

Finally, for $b > 0$ and $x > 16c$, we have

$$\begin{aligned}\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} &\leq \frac{(bx+4)^c}{(x-1)^c} \\ &\leq \frac{(1+4/x)^c}{(1-1/x)^c} b^c \\ &\leq \frac{b^c}{(1-1/x)^c(1-4/x)^c} \\ &\leq \frac{b^c}{(1-4/x)^{2c}} \\ &\leq \frac{b^c}{1-8c/x} \\ &\leq b^c\left(1+\frac{16c}{x}\right).\end{aligned}$$

It follows that we have the desired inequality when

$$x > 16(c+1)(b+1)^c.$$

An immediate corollary is that, when x is sufficiently large,

$$b^c = \alpha bx + 4(c+1) \text{ div } \alpha_x(c+1).$$

The Diophantine nature of div and of α_x then demonstrates that exponentiation is Diophantine. □

5 Looking beyond the MRDP theorem

5.1 Prime-producing polynomials

Poonen (2006) describes a fashion in which the MRDP theorem immediately demonstrates the existence of a prime-producing polynomial, in the sense that there exists some polynomial $P(x_1, \ldots, x_n)$ over the integers such that for every n-tuple $(x_1, \ldots, x_n)$, $P(x_1, \ldots, x_n) \in \mathbb{P}$ (it is prime) or $P \leq 0$, and every prime number may be produced in this fashion.

Theorem 9. *There exists a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $\{P(x_1, \ldots, x_n) | \forall n,\ x_n \in \mathbb{Z}\} = \mathbb{P}$.*

Proof. The set of all primes, $\mathbb{P}$, is recursive, and so it is recursively enumerable, and so it is Diophantine by the MRDP Theorem. As such, it has a Diophantine representation $D(p, x_1, \ldots, x_m)$. Then consider the polynomial $F(y, x_1, \ldots . x_m) = (1 - D(y, x_1, \ldots, x_m)^2) \times y$; we have $F \leq 0$ whenever $D(y, x_1, \ldots, x_m)^2 > 0$, meaning that $F \leq 0$ whenever y is not prime, and when y is indeed prime, then $F = y \in \mathbb{P}$. Finally, use Lagrange's four-square theorem to expand the natural number y as the sum of four integers, which completes the proof. □

5.2 Hilbert's Tenth Problem for other rings

Hilbert's Tenth Problem admits an easy generalization for other rings. Following Poonen [6], we may write:

Definition 7. *Let R be a ring.* ***Hilbert's Tenth Problem over*** *R asks if there exists an algorithm that takes as input a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and outputs YES or NO, according to whether there exists $(a_1, \ldots, a_n) \in R^n$ such that $f(a_1, \ldots, a_n) = 0$.*

Interestingly, Hilbert's Tenth Problem has not been resolved for the ring of rationals, $\mathbb{Q}$, yet.

5.3 Relation to other problems

Many problems in mathematics can be phrased in terms of Diophantine sets. For example, the famous **Fermat's Last Theorem** states that no three positive integers a, b, c can satisfy $a^n + b^n = c^n$ for $n > 2$. This is a regular Diophantine equation for any fixed n, but for variable n it becomes an exponential Diophantine equation; however, thanks to the MRDP theorem, we know that exponential Diophantine equations are also just Diophantine equations. That is, we can transform $a^n + b^n = c^n$ into a regular Diophantine equation somehow. As such, the problem of proving Fermat's Last Theorem is reduced to "simply" ascertaining if the corresponding Diophantine equation has any solutions.

Consider also **Goldbach's conjecture**, which states that every even integer greater than 2 is the sum of two prime numbers. Let G be the set of even numbers greater than 2 but not the sum of two primes. Suppose we take some particular number $a > 2$; we can easily check if it is a counterexample to Goldbach's conjecture or not via simple brute force computation. As such, the set G is recursively enumerable and so G is a Diophantine set. As such, there exists some Diophantine equation which has a solution if and only if Goldbach's conjecture does not hold, so if Hilbert's Tenth Problem had a positive resolution, we would easily be able to check if Goldbach's conjecture is true or not.

Finally, we may consider the famous **Riemann hypothesis**, which is a statement about the zeroes of Riemann's zeta function. The proof will not be given here, but this, too, can be reduced to checking whether or not a particular Diophantine equation has a solution [4].

We therefore see that three long-standing problems in mathematics (one resolved, two not) can be rephrased in the language of Diophantine equations and sets. Were it true that there existed a universal algorithm to check for the existence of solutions for arbitrary Diophantine equations, we could then apply that algorithm to resolve these mathematical equations in what is guaranteed to be a finite amount of time. This then provides an *intuitive reason* for the negative resolution of Hilbert's Tenth Problem: it would be rather odd if there existed some straightforward algorithmic method to solve these difficult and complex problems. "Thankfully", there is not, and the Goldbach conjecture and Riemann hypothesis remain very nontrivial.

5.4 Solution of Diophantine equations in Gaussian integers

There is a simpler version of Hilbert's Tenth Problem which asks if there is a process for solving Diophantine equations in **Gaussian integers**, *i.e.*complex numbers of the form $a+bi$. Although this may at first seem to be a more complex problem, it may in fact be reduced to the original statement of Hilbert's Tenth Problem.

Consider such an equation:

$$D(\chi_1, \ldots, \chi_n) = 0.$$

It has a solution in Gaussian integers if and only if the following equation has a solution in integers:

$$D(x_1 + y_1 i, \ldots, x_n + y_n i) = 0$$

This follows from the definition of a Gaussian integer.

Now, we can separate the real and imaginary parts by writing

$$D(x_1+y_1 i, \ldots, x_n+y_n i) = D_{\mathrm{R}}(x_1, \ldots, x_n, y_1, \ldots, y_n)+D_{\mathrm{I}}(x_1, \ldots, x_n, y_1, \ldots, y_n).$$

Hence the question of the solvability of D in Gaussian integers is then reduced to the problem of finding a solution to

$$D_{\mathrm{R}}^2(x_1, \ldots, x_n, y_1, \ldots, y_n) + D_{\mathrm{I}}^2(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

in regular integers. As such, the problem of finding solutions in Gaussian integers has been *reduced* to the problem of finding solutions in regular integers.

In the opposite direction, J. Denef [2] was able to reduce the problem of finding a solution to a Diophantine equation $D(x_1, \ldots, x_n) = 0$ in integers to the problem of finding a solution to a Diophantine equation $G(\chi_1, \ldots, \chi_m) = 0$ in Gaussian integers.

As such, the undecidability of Hilbert's Tenth Problem via the MRDP theorem immediately implies the undecidability of Hilbert's Tenth Problem for Gaussian integers.

References

[1] Davis, M., Hilary Putnam, and Julia Robinson. *The Decision Problem for Exponential Diophantine Equations*, Annals of Mathematics. Vol. 74, No. 3, November, 1961.

[2] j. Denef. *Hilbert's Tenth Problem for quadratic rings.* Proceedings of the American Mathematical Monthly, 48(1), 214–220, 1975.

[3] Matiyasevich, Yuri V. *Hilbert's Tenth Problem.* Cambridge: MIT Press, 1993.

[4] Matyiasevich, Yuri V. *Hilbert's Tenth Problem: What Was Done and What Is to Be Done*, Workshop on Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, American Mathematical Society, 1999.

[5] Niven, I., and Herbert S. Zuckerman. *An Introduction to the Theory of Numbers.* Hobokey: Wiley, 1960.

[6] Poonen, Bjorn. *Hilbert's Tenth Problem over Rings of Number-Theoretic Interest.* 2003. http://www-math.mit.edu/ poonen/papers/aws2003.pdf

[7] Smith, P. *The MRDP Theorem.* 2011. http://www.logicmatters.net/resources/pdfs/MRDP.pdf

[8] Soare, Robert I. *Recursively enumerable sets and degrees: A study of computable functions and computably generated sets.* Perspectives in Mathematical Logic. Berlin: Springer-Verlag, 1987.