Hilbert’s Tenth Problem for Fixed $d$ and $n$

William Gasarch

Abstract

Hilbert’s 10th problem, stated in modern terms, is

Find an algorithm that will, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$, determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Davis, Putnam, Robinson, and Matiyasevich showed that there is no such algorithm. But what if we bound the degree of the polynomial? The number of variables? This paper surveys what is known for these cases.

1 Hilbert’s Tenth Problem

In 1900 Hilbert proposed 23 problems for mathematicians to work on over the next 100 years (or longer). The 10th problem, stated in modern terms, is

Find an algorithm that will, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$, determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Hilbert probably thought this would inspire much deep number theory, and it did inspire some. But the work on this problem took a very different direction. Davis-Putnam-Robinson [9] showed that determining if an exponential diophantine equation has a solution in $\mathbb{Z}$ is undecidable. Their proof coded Turing machines into such equations. Matiyasevich [20] extended their work by showing how to replace the exponentials with polynomials. Hence the algorithm that Hilbert wanted is not possible. For a self contained proof from soup to nuts see Davis’ exposition [8]. For more about both the proof and the implications of the result see the book of Matiyasevich [21].

This raises the obvious question of what happens for particular numbers of variables $n$ and degree $d$. I thought that surely there must be a grid on the web where the $d$-$n$-th entry is

- $D$ if the problem for degree $\leq d$, and $\leq n$ variables is Decidable.

---

*The University of Maryland at College Park, gasarch@umd.edu
• U if the problem for degree $\leq d$, and $\leq n$ variables is Undecidable.

• ? if the status of the problem for degree $\leq d$, and $\leq n$ variables is unknown.

There is a graph in a German paper, by Bayer et al. [4], that has the information I want, though it’s hard to read. So putting that aside I ask Why has the quest for a grid not gotten more attention? Here are some speculations.

1. Logicians work on showing that determining if there is a solution in $\mathbb{N}$ is undecidable. Number theorists worked on showing that determining if there is a solution in $\mathbb{Z}$ is decidable. Since Logicians worked in $\mathbb{N}$ and Number Theorists in $\mathbb{Z}$, a grid would need to reconcile these two related problems.

2. There is a real dearth of positive results, so a grid would not be that interesting.

3. The undecidable results often involve rather large values of $d$, so the grid would be hard to draw.

4. Timothy Chow offered this speculation in an email to me: One reason there isn’t already a website of the type you envision is that from a number-theoretic (or decidability) point of view, parameterization by degree and number of variables is not as natural as it might seem at first glance. The most fruitful lines of research have been geometric, and so geometric concepts such as smoothness, dimension, and genus are more natural than, say, degree. A nice survey by a number theorist is the book Rational Points on Varieties by Bjorn Poonen [24]. Much of it is highly technical; however, reading the preface is very enlightening. Roughly speaking, the current state of the art is that there is really only one known way to prove that a system of Diophantine equations has no rational solution.

An alternative to a grid is a paper to collect up all that is known and point to open problems. This article is that paper. None of the results are mine.

Another alternative is to have a table where, for each $n$, the largest value of $d$ for which the problem is decidable, and the smallest value of $d$ for which the problem is known to be undecidable. Anyone can take this paper and create such a table.

In Section 2 we will relate the problem of seeking solutions in $\mathbb{Z}$ with the problem of seeking solutions in $\mathbb{N}$. In Section 3 we will present values of $(d,n)$ where the problem is undecidable. In Section 4 we will present values of $(d,n)$ where the problem is decidable. In Sections 5 and 6 we look at restricted sets of polynomials. In Section 7 we will discuss the vast area between the decidable and undecidable cases. In Section 8 we will briefly present Matiyasevich discussion of what Hilbert really wanted in contrast to what happened.
2 Definitions and Reconciling $\mathbb{N}$ with $\mathbb{Z}$

Notation 2.1.

1. $H_{\mathbb{Z}}(d, n)$ is the problem where the degree is $\leq d$, the number of variables is $\leq n$, and we seek a solution in $\mathbb{Z}$.

2. $H_{\mathbb{N}}(d, n)$ is the problem where the degree is $\leq d$, the number of variables is $\leq n$, and we seek a solution in $\mathbb{N}$.

3. $H_{\mathbb{Z}}(d, n) = D$ means that there is an algorithm to decide $H_{\mathbb{Z}}(d, n)$.

4. $H_{\mathbb{Z}}(d, n) = U$ means that there is no algorithm to decide $H_{\mathbb{Z}}(d, n)$.

5. Similarly for $H_{\mathbb{N}}(d, n)$ equal to D or U.

The four parts of the next lemma are usually stated with $x_1, x_2, x_3 \in \mathbb{N}$ or $x_1, x_2, x_3, x_4 \in \mathbb{N}$, and not in the iff form we use. However, we need these statements in the form we present them.

Lemma 2.2.

1. $x \in \mathbb{N}$ and $x$ is not of the form $4^a(8b + 7)$ (where $a, b \in \mathbb{N}$) iff there exists $x_1, x_2, x_3 \in \mathbb{Z}$ such that
   
   $$x = x_1^2 + x_2^2 + x_3^2.$$  

2. $x \in \mathbb{N}$ and $x \equiv 1 \pmod{4}$ iff there exists $x_1, x_2, x_3 \in \mathbb{Z}$ such that (1) $x_1, x_2 \equiv 0 \pmod{2}$, (2) $x_3 \equiv 1 \pmod{2}$, and
   
   $$x = x_1^2 + x_2^2 + x_3^2.$$  

3. $n \in \mathbb{N}$ iff there exists $x_1, x_2, x_3 \in \mathbb{Z}$ such that $n = x_1^2 + x_2^2 + x_3^2 + x_3$.

Proof.

1) This is Legendre’s three-square theorem. It is sometimes called the Gauss-Legendre Theorem.

2) Since $x \equiv 1 \pmod{4}$, $x$ satisfies the hypothesis of Part 1. Hence there exists $x_1, x_2, x_3$ such that
   
   $$x = x_1^2 + x_2^2 + x_3^2.$$  

Take this equation mod 4.

$$1 \equiv x_1^2 + x_2^2 + x_3^2 \pmod{4}.$$  

It is easy to see that the only parities of \(x_1, x_2, x_3\) that work are for two of them to be even and one of them to be odd.

3) Let \(n \in \mathbb{N}\). Note that \(4n + 1\) satisfies the premise of Part 1. By Part 1 there exists \(x_1, x_2, x_3 \in \mathbb{Z}\) such that

\[
4n + 1 = (2x_1)^2 + (2x_2)^2 + (2x_3 + 1)^2
\]

\[
4n + 1 = 4x_1^2 + 4x_2^2 + 4x_3^2 + 4x_3 + 1
\]

\[
n = x_1^2 + x_2^2 + x_3^2 + x_3.
\]

\[\square\]

**Theorem 2.3.**

1. If \(H_N(2d, 3n) = D\), then \(H_N(d, n) = D\).

2. If \(H_N(d, n) = U\), then \(H_Z(2d, 3n) = U\). This is the contrapositive of Part 1.

3. If \(H_Z(f(d, n), 2n + 2) = D\), then \(H_N(d, n) = D\) where

\[f(d, n) = \max\{2d, (2n + 3)2^n\}\]

4. If \(H_N(d, n) = U\), then \(H_Z(f(d, n), 2n + 2) = U\). This is the contrapositive of Part 3.

**Proof.**

1) Let \(p \in \mathbb{Z}[x_1, \ldots, x_n]\). We want to know if there is a solution in \(\mathbb{N}\).

   Let \(q\) be the polynomial of degree \(2d\) with \(3n\) variables that you get if you replace each \(x_i\) with \(x_{i1}^2 + x_{i2}^2 + x_{i3}^2 + x_{i3}\) where \(x_{i1}, x_{i2}, x_{i3}\) are \(3\) new variables. By Lemma 2.2.3 we have:

   - \(p\) has a solution in \(\mathbb{N}\) iff \(q\) has a solution in \(\mathbb{Z}\).

   Use that \(H_Z(2d, 3n) = D\) to determine if \(q\) has a solution. Hence \(H_N(d, n) = D\).

3) This was proven by Sun [30].

\[\square\]

**Theorem 2.4.**

1. If \(H_N(d, n) = D\) then \(H_Z(d, n) = D\).

2. If \(H_Z(d, n) = U\) then \(H_N(d, n) = U\). This is the contrapositive of part 1.
Proof. Let \( p \in \mathbb{Z}[x_1, \ldots, x_n] \). We want to know if there is a solution in \( \mathbb{Z} \). For each \( \vec{b} = (b_1, \ldots, b_n) \in \{0, 1\}^n \) let \( q_{\vec{b}}(x_1, \ldots, x_n) \) be formed as follows: for every \( i \) where \( b_i = 1 \), replace \( x_i \) with \(-x_i\). It is easy to see that \( p \) has a solution in \( \mathbb{Z} \) iff 
\[
(\exists \vec{b}) [q_{\vec{b}} \text{ has a solution in } \mathbb{N}].
\]
The result follows. \( \square \)

In the next section we summarize what is known about \( H_N(d, n) \).

3 When is \( H_N(d, n) = U? \) \( H_Z(d, n) = U? \)

In 1980 Jones [16] announced 16 pairs \((d, n)\) for which \( H_N(d, n) = U \). In 1982 Jones [17] provided proofs of 13 of these pairs. Hence there are 3 announced results whose proofs seem to have never appeared. (Jones-1982 would have been the obvious place for these proofs.)

In the theorem below we present all 16 statements from the Jones-1980 paper along with a result by Sun [31] from 2020. We note the 3 suspect results of Jones and the (non-suspect) result of Sun. We state the results of the form \( H_N(d, n) = U \) and then apply Theorem 2.3 to obtain results of the form \( H_Z(d', n') = U \) (except for Sun’s result which is already about \( H_Z \)).

The proofs involve very clever use of elementary number theory to get the degrees and number-of-variables reduced.

In some of the results there are absurdly large numbers like \( 4.6 \times 10^{44} \). These are probably upper bounds that might be able to be lowered with a careful examination of the proofs.

Theorem 3.1.

1. \( H_N(4, 58) = U \) hence \( H_Z(8, 174) = U \).

2. \( H_N(8, 38) = U \) hence \( H_Z(16, 114) = U \).

3. \( H_N(12, 32) = U \) hence \( H_Z(24, 96) = U \).

4. (Announced by Jones in 1980; however, we do not know of a proof.)
   \( H_N(16, 29) = U \) hence \( H_Z(32, 87) = U \).

5. \( H_N(20, 28) = U \) hence \( H_Z(40, 84) = U \).

6. \( H_N(24, 26) = U \) hence \( H_Z(48, 78) = U \).

7. \( H_N(28, 25) = U \) hence \( H_Z(56, 75) = U \).
8. (Announced by Jones in 1980; however, we do not know of a proof.)
\[ HN(36, 24) = U \text{ hence } HZ(72, 72) = U. \]

9. \[ HN(96, 21) = U \text{ hence } HZ(192, 63) = U. \]

10. \[ HN(2668, 19) = U \text{ hence } HZ(5336, 57) = U. \]

11. \[ HN(200000, 14) = U \text{ hence } HZ(400000, 42) = U \text{ and } HZ(31 \times 2^{14}, 30) = U. \]

12. (Announced by Jones in 1980; however, we do not know of a proof.)
\[ HN(6.6 \times 10^{43}, 13) = U \text{ hence } HZ(13.2 \times 10^{43}, 28) = U. \]

13. \[ HN(1.3 \times 10^{44}, 12) = U \text{ hence } HZ(2.6 \times 10^{44}, 36) = U. \]

14. \[ HN(4.6 \times 10^{44}, 11) = U \text{ hence } HZ(9.2 \times 10^{44}, 24) = U. \]

15. \[ HN(8.6 \times 10^{44}, 10) = U \text{ hence } HZ(17.2 \times 10^{44}, 22) = U. \]

16. \[ HN(1.6 \times 10^{45}, 9) = U \text{ hence } HZ(3.2 \times 10^{45}, 20) = U. \text{ (Jones’ 1982 paper presents the proof of this result and credits it to Matijasevic.)} \]

17. \[ HZ(d, 11) = U \text{ for some rather large } d. \text{ The number } d \text{ is not stated. (This is due to Sun [37].)} \]

4 When is \( HZ(d, n) = D? \) \( HN(d, n) = D? \)

We will need a brief discussion of the following problem which is attributed to Frobenius.

Given a set of relatively prime positive integers \( \vec{a} = (a_1, \ldots, a_n) \) find the set

\[ \text{FROB}(\vec{a}) = \left\{ \sum_{i=1}^{n} a_i x_i : x_1, \ldots, x_n \in \mathbb{N} \right\}. \]

It is known that \( \text{FROB}(\vec{a}) \) is always cofinite. We will need to look at the case where the \( a_1, \ldots, a_n \) may have a gcd of \( d \neq 1 \). In this case, \( \text{FROB}(\vec{a}) \) is always a cofinite subset of \( d\mathbb{N} \).

The \( n = 2 \) case was solved by James Joseph Sylvester in 1884:
Lemma 4.1. Let \( a_1, a_2 \in \mathbb{N} \). Let \( d = \gcd(a_1, a_2) \). There exists a finite set \( F \subseteq d\mathbb{N} \) such that

\[
\text{FROB}(a_1, a_2) = F \cup \{dx : x \geq a_1a_2 - a_1 - a_2 + 1\}
\]

and \((a_1a_2 - a_1 - a_2)d \notin \text{FROB}(a_1, a_2)\).

For the general case there is no neat formula; however, finding \( \text{FROB}(\vec{a}) \) is decidable. There has been much work on this problem. Beihoffer et al. [5] gives a fast algorithm and many prior references to other algorithms. We state the relevant lemma.

Lemma 4.2. Let \( a_1, \ldots, a_n \in \mathbb{N} \). Let \( d = \gcd(a_1, \ldots, a_n) \).

1. There exists finite \( F \) and an \( M \in \mathbb{N} \) such that

\[
\text{FROB}(\vec{a}) = F \cup \{dx : x \geq M\}
\]

and \((M - 1)d \notin \text{FROB}(\vec{a})\).

2. There is an algorithm that will, given \( a_1, \ldots, a_n \), find \( F \) and \( M \).

And now for the main theorem of this section!

Theorem 4.3.

1. For all \( d \), \( \text{H}_Z(d, 1) = D \) and \( \text{H}_N(d, 1) = D \). There is an algorithm that finds all of the integers roots (which may be the empty set).

2. For all \( n \), \( \text{H}_Z(1, n) = D \).

3. For all \( n \), \( \text{H}_N(1, n) = D \).

4. \( \text{H}_Z(2, 2) = D \).

5. \( \text{H}_N(2, 2) = D \).

6. For all \( n \), \( \text{H}_Z(2, n) = D \) and \( \text{H}_N(2, n) = D \).

Proof. 
1) These are both easy consequences of the rational root theorem: If \( a_dx^d + \cdots + a_1x + a_0 \in \mathbb{Z}[x] \) has a rational root \( \frac{p}{q} \) then \( p \) divides \( a_0 \) and \( q \) divides \( a_n \).

The above algorithm does not find the roots. One can modify the algorithm so that it does find the roots; however, that would be a slow algorithm. Cucker et al. [7] gave a polynomial time algorithm for finding the set of integer roots.
2) Given $\sum_{i=1}^{n} a_i x_i = b$ where $a_1, \ldots, a_n, b \in \mathbb{Z}$, we need to determine if there is a solution in $\mathbb{Z}$.

First find $d = \gcd(a_1, \ldots, a_n)$. If $d$ does not divide $b$ then there are no solutions in $\mathbb{Z}$. If $d$ does divide $b$ then there is a solution in $\mathbb{Z}$: Let $x'_1, \ldots, x'_n$ be such that $\sum_{i=1}^{n} a_i x'_i = d$ and let $x_i = \frac{b_i}{d}$.

3) We can phrase any problem we need to solve as follows: Let $a_1, \ldots, a_n \in \mathbb{N}$ and $b_1, \ldots, b_m, b \in \mathbb{N}$. Is there a solution in $\mathbb{N}$ of

$$\sum_{i=1}^{n} a_i x_i = b + \sum_{i=1}^{m} b_i y_i.$$ 

Let $d_a = \gcd(a_1, \ldots, a_n)$ and $d_b = \gcd(b_1, \ldots, b_m)$. By Lemma 4.2:

- There is an algorithm that will find finite set $F_a$ and an $M_a \in \mathbb{N}$ such that

$$\left\{ \sum_{i=1}^{n} a_i x_i : x_1, \ldots, x_n \in \mathbb{N} \right\} = F_a \cup \{ xd : x \geq M_a \}$$

- There is an algorithm that will find finite set $F_b$ and an $M_b \in \mathbb{N}$ such that

$$\left\{ b + \sum_{i=1}^{n} b_i x_i : x_1, \ldots, x_n \in \mathbb{N} \right\} = F_b \cup \{ b + xd : x \geq M_b \}$$

Once we have $F_a, M_a, F_b, M_b$ it is easy to determine if $\{ F_a \cup \{ xd : x \geq M_a \} \}$ and $\{ F_b \cup \{ b + xd : x \geq M_b \} \}$ intersect. If so, then there is a solution to the original equation, and of not, then there is not.

4) Gauss [12] (27, Art, 216-221) proved this. For a more modern approach, Lagarias [18] (Theorem 1.2.iii) showed that if $p(x, y) \in \mathbb{Z}[x, y]$ of degree 2 has a solution then there is a short proof for this fact (short means of length bounded by a polynomial in the size of the coefficients). Formally he showed that the following set is in NP.

$$\{(a, b, c, d, e, f) \in \mathbb{Z}^6 : (\exists x, y \in \mathbb{Z})[ax^2 + bxy + cx^2 + dx + ey + f = 0]\}. $$

(There is a solver on the web here: [https://www.alpertron.com.ar/QUAD.HTM](https://www.alpertron.com.ar/QUAD.HTM))

5) Gauss’s method to determine if $f(x, y) \in \mathbb{Z}[x, y]$, of degree 2, has a solution in $\mathbb{Z}$ finds all of the solutions in a nice form. From this form one can determine if there are any solutions in $\mathbb{N}$. 
6) For all \( n \), \( HZ(2, n) = D \) and \( HN(2, n) = D \). This is a sophisticated theorem due to Siegel [28]. See also Grunewald and Segal [13]. This result uses the Hasse-Minkowski Theorem (see Page 32 of Grunewald-Segal).

□

5 Some Decidable Subcases

5.1 The Curious Case of \( HZ(3, 2) \)

The case of \( HZ(3, 2) \) is almost solved.

Def 5.1. An elements of \( \mathbb{Q}[x_1, \ldots, x_n] \) is absolutely irreducible if it is irreducible over \( \mathbb{C} \). For example,
\[
x^2 + y^2 - 1 \quad \text{is absolutely irreducible, but} \quad x^2 + y^2 = (x + iy)(x - iy) \quad \text{is not.}
\]

A combination of results by Baker and Cohen [3], Poulakis [25], and Poulakis [26] imply the following theorem:

Theorem 5.2. There is an algorithm which, given any absolutely irreducible polynomial \( P(x, y) \in \mathbb{Z}[x, y] \) of degree 3, determines all integer solutions of the equation \( P(x, y) = 0 \). (See Poulakis [26] for a more precise definition of determines all integer solutions in the case that there are an infinite number of them.)

The original algorithm (from Baker and Coates) is not practical; however, Peth et al [27] and Stroker-Tzankis [29] have practical algorithms. There is also an algorithm for solving a large class of cubic equations implemented in SageMath.

So why isn’t \( HZ(3, 2) = D \)? Because the case where \( P(x, y) \) has degree 3 but is not absolutely irreducible is still open.

5.2 If the Variables Are Separated...

Ibarra and Dang proved the following.

Def 5.3. \( P(z_1, \ldots, z_n) \) is a Presburger Relation if it can be expressed with \( \mathbb{Z}, =, +, <, \) and the usual logical symbols. For example
\[
(z_1 + z_2 < z_3 + 12) \land (z_1 + z_4 = 17) \quad \text{is a Presburger formula, but} \quad z_1z_2 = 13 \quad \text{is not.}
\]

Theorem 5.4. The following is decidable:

Instance
(1) For \( 1 \leq i \leq k \) polynomial \( p_i(y) \in \mathbb{Z}[y] \), and linear functions \( F_i(\vec{x}), G_i(\vec{x}) \in \mathbb{Z}[x_1, \ldots, x_n] \), and (2) a Presburger relation \( R(z_1, \ldots, z_k) \).
Question Does there exist \( y, \vec{x} \) such that

\[
R(p_1(y)F_1(\vec{x})) + G_1(\vec{x}), \ldots, p_k(y)F_k(\vec{x}) + G_1(\vec{x})
\]

holds.

6 The Curious Case of \( x^3 + y^3 + z^3 = k \)

Rather than looking at \( \mathbb{H}\mathbb{Z}(d, n) \) lets focus in one one equation that has gotten a lot of attention:

\[
x^3 + y^3 + z^3 = k.
\]

It is easy to show that, For \( k \equiv 4, 5 \pmod{9} \), there is no solution in \( \mathbb{Z} \). What about for \( k \not\equiv 4, 5 \pmod{9} \)?

1. Heath-Brown [14] conjectured that there are an infinite number of \( k \not\equiv 4, 5 \pmod{9} \) for which there is a solution in \( \mathbb{Z} \). Others think that, for all \( k \not\equiv 4, 5 \pmod{9} \), \( x^3 + y^3 + z^3 = k \) has a solution in \( \mathbb{Z} \).

2. Elkies [11] devised an efficient algorithm to find solutions to \( x^3 + y^3 + z^3 = k \) if there is a bound on \( x, y, z \).

3. Elsehans and Jahnel [10] modified and implemented Elkies algorithm and determined the following: The only \( k \leq 1000, k \not\equiv 4, 5 \pmod{9} \), where they did not find a solution were


Their work, and the work of all the items below, required hard mathematics, clever computer science, and massive computer time.

4. Huisman [15] found a solution for \( k = 74 \). For many other values of \( k \) where there were solutions, Huisman found additional solutions.

5. Booker [6] found a solution for \( k = 33 \).

6. Booker found a solution for \( k = 42 \). This has not been formally published yet; however, the \( x, y, z \) can be found on the Wikipedia site: https://en.wikipedia.org/wiki/Sums_of_three_cubes

7. The only \( k \leq 1000, k \not\equiv 4, 5 \pmod{9} \), where no solution is known are:

Consider the function that, on input \( k \), determines if \( x^3 + y^3 + z^3 = k \) has a solution in \( \mathbb{Z} \). Is this function computable?

1. I suspect the function is computable. Why? What would a proof that this function is not computable look like? It would have to code a Turing machine computation into a very a restricted equation. This seems unlikely to me. Note also that it may be the case the equation has a solution for every \( k \not\equiv 4, 5 \pmod{9} \), in which case decision problem is not just decidable—it’s regular!

2. Daniel Varga has suggested there may be a proof that does not go through Turing machines. Perhaps some other undecidable problem? Also, there may be new techniques we just have not thought of yet.

7 Discussion

If I was to draw the grid for \( H_N \) or \( H_Z \) mentioned in the introduction there would be a large space of problems that are open. We give an example of a part of that space.

Recall that \( H_Z(d, 1) = D, (\forall n)[H_Z(2, n) = D] \), and \( H_Z(8, 174) = U \). The following are unknown:

1. \( H_Z(3, 2), H_Z(3, 3), H_Z(3, 4), \ldots \)
2. \( H_Z(4, 2), H_Z(4, 3), H_Z(4, 4), \ldots \)
3. \( H_Z(5, 2), H_Z(5, 3), H_Z(5, 4), \ldots \)
4. \( H_Z(6, 2), H_Z(6, 3), H_Z(6, 4), \ldots \)
5. \( H_Z(7, 2), H_Z(7, 3), H_Z(8, 4), \ldots \)
6. \( H_Z(8, 2), H_Z(8, 3), H_Z(8, 4), \ldots, H_Z(8, 173) \).

The situation is worse than it looks. From the discussion in Section 6 we know that the status of the following function is unknown: Given \( k \), determine if \( x^3 + y^3 + z^3 = k \) has a solution in \( \mathbb{Z} \).

What is the smallest \( n \) such that, for some \( d \), \( H_Z(d, n) = U \)? We present an informed opinion by paraphrasing and combining two passages from Sun [30, pages 209 and 211]:

1. Matijasevic and Robinson [23] showed there is a \( d \) such that \( H_N(d, 13) = U \).
2. Matijasevic showed there is a $d$ such that $H_N(d, 9) = U$. By Theorem 2.3 we have that there is a $d'$ with $H_Z(d', 20) = U$.

3. Baker [2] showed the following is decidable: Given $p \in \mathbb{Z}[x, y]$, $p$ homogeneous, does it have a solution in $\mathbb{Z}$? This does not show that

$$(\forall d)[H_Z(d, 2) = D]$$

but it points in that direction.

4. (Direct quote from page 209.) In fact, A. Baker, Matijasevic and Robinson even conjectured that $3^3$ is undecidable over $\mathbb{N}$. In our notation, there exists $d$ such that $H_N(d, 3) = U$. Note that this implies $H_Z(d, 3) = U$.

Suggestions:

1. Since a grid for $H_N(d, n)$ or $H_Z(d, n)$ is somewhat cumbersome there should be a website of results.

2. That website should also include classes of equations such as $x^3 + y^3 + z^3 = k$ and what is known about them.

3. Work on showing $H_N(d, n) = U$ or $H_Z(d, n) = U$ seems to have stalled. Perhaps the problems left are too hard. Perhaps the problems left could be resolved but it would be very messy. Perhaps computer-work could help (see next point). Perhaps deeper number theory is needed (current results seem to use clever but somewhat elementary number theory). Perhaps the problems left are decidable. In any case, there should be an effort in this direction.

4. There has been some work on getting Universal Turing machines down to a very small number of states and alphabet size. See, for example, the work of Aaronson [1], Michel [22], Yedida and Aaronson [32]. See also the following blog post on this site: https://vzn1.wordpress.com that you get by clicking on MENU and looking for Undecidability: The Ultimate Challenge.

There has even been some computer work done in writing compilers for these machines. It is plausible that by starting from these rather small machines, smaller polynomials may suffice to simulate them.
8 What Would Hilbert Do?

**Def 8.1.** \(HQ(d, n)\) is the problem where the degree is \(\leq d\), the number of variables is \(\leq n\), and we seek a solution in \(Q\).

Matiyasevich [19] (Page 18) gives good reasons why Hilbert might have actually wanted to solve \(HQ\). Hilbert stated the tenth problem as \(HZ\); however, if \(HZ\) is solvable then \(HQ\) is solvable. He might have thought that the best way to solve \(HQ\) is to solve \(HZ\).

What is the status of \(HQ\) now? It is an open question to determine if it is decidable. Hence the problem Hilbert plausibly intended to ask is still open.

9 Acknowledgement

We thank Blogger vzn, Timothy Chow, Thomas Erlebach, Lance Fortnow, Brogdan Grechuk, Nathan Hayes, Chris Lastowski, David Marcus, Yuri Matiyasevich, Yuang Shen, Joshua Twitty, Larry Washington, Daniel Varga, Zan Xu, for helpful discussions.

We are particularly grateful to the following people.

1. Timothy Chow for his comments in Section 1 and help with the discussion in Section 6 of \(x^3 + y^3 + z^3 = k\).
2. Brogdan Grechuk for telling us about the material that is now in Section 5.1.
3. Yuri Matiyasevich for pointing us to many results of which we were unaware.

References


https://www.combinatorics.org/ojs/index.php/eljc/article/view/v12i1r27

https://arxiv.org/abs/1903.04284


https://www.math.umd.edu/~laskow/Pubs/713/Diophantine.pdf


https://arxiv.org/abs/math/0005139


https://arxiv.org/abs/1604.07746


http://www.jstor.org/stable/2273588?seq=1#metadata_info_tab_contents


https://logic.pdmi.ras.ru/~yumat/personaljournal/H10history/H10histe.pdf


http://maths.nju.edu.cn/~zwsun/14z.pdf