THE ALGORITHMICS COLUMN

BY

THOMAS ERLEBACH

Department of Informatics
University of Leicester
University Road, Leicester, LE1 7RH.
t.erlebach@leicester.ac.uk

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, and 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 $\le d$, and $\le n$ variables is Undecidable.
- ? if the status of the problem for degree $\le d$, and $\le n$ 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 [25]. 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 that gives, 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's discussion of what Hilbert really wanted in contrast to what happened.

2 Definitions and Reconciling $\mathbb{N}$ with $\mathbb{Z}$

Notation 2.1.

1. $\mathrm{H}\mathbb{Z}(d, n)$ 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. $\mathrm{H}\mathbb{N}(d, n)$ 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. $\mathrm{H}\mathbb{Z}(d, n) = \mathrm{D}$ means that there is an algorithm to decide $\mathrm{H}\mathbb{Z}(d, n)$.

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

5. Similarly for $\mathrm{H}\mathbb{N}(d, n)$ 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 2. By Part 2 there exists $x_1, x_2, x_3 \in \mathbb{Z}$ such that

$$4n + 1 = (2x_1)^2 + (2x_2)^2 + (2x_3 + 1)^2$$

$$4n + 1 = 4x_1^2 + 4x_2^2 + 4x_3^2 + 4x_3 + 1$$

$$n = x_1^2 + x_2^2 + x_3^2 + x_3.$$

□

Theorem 2.3.

1. *If* $\mathrm{H}\mathbb{Z}(2d, 3n) = \mathrm{D}$*, then* $\mathrm{H}\mathbb{N}(d, n) = \mathrm{D}$.
2. *If* $\mathrm{H}\mathbb{N}(d, n) = \mathrm{U}$*, then* $\mathrm{H}\mathbb{Z}(2d, 3n) = \mathrm{U}$. *This is the contrapositive of Part 1.*
3. *If* $\mathrm{H}\mathbb{Z}(f(d, n), 2n + 2) = \mathrm{D}$*, then* $\mathrm{H}\mathbb{N}(d, n) = \mathrm{D}$ *where*
$$f(d, n) = \max\{2d, (2n + 3)2^n\}.$$
4. *If* $\mathrm{H}\mathbb{N}(d, n) = \mathrm{U}$*, then* $\mathrm{H}\mathbb{Z}(f(d, n), 2n + 2) = \mathrm{U}$. *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 $\mathrm{H}\mathbb{Z}(2d, 3n) = \mathrm{D}$ to determine if q has a solution. Hence $\mathrm{H}\mathbb{N}(d, n) = \mathrm{D}$.

3) This was proven by Sun [30].

□

Theorem 2.4.

1. *If* $\mathrm{H}\mathbb{N}(d, n) = \mathrm{D}$ *then* $\mathrm{H}\mathbb{Z}(d, n) = \mathrm{D}$.
2. *If* $\mathrm{H}\mathbb{Z}(d, n) = \mathrm{U}$ *then* $\mathrm{H}\mathbb{N}(d, n) = \mathrm{U}$. *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

$(\exists \vec{b})[q_{\vec{b}}$ has a solution in $\mathbb{N}$].

The result follows. □

In the next section we summarize what is known about $\mathrm{H}\mathbb{N}(d, n)$.

3 When is $\mathrm{H}\mathbb{N}(d, n) = \mathrm{U}$? $\mathrm{H}\mathbb{Z}(d, n) = \mathrm{U}$?

In 1980 Jones [16] announced 16 pairs (d, n) for which $\mathrm{H}\mathbb{N}(d, n) = \mathrm{U}$. As far as I can tell, this paper does not have proofs, nor was that its intent. In 1982 Jones [17] provided proofs for 13 of these pairs (12 in Theorem 4 and 1 in Section 3). As far as I can tell, there are 3 results that were stated in Jones-1980 but for which there are no proofs in either Jones-1980 or Jones-1982. I hasten to add that I am not an expert in the field and it is possible that (1) the 3 result are there implicitly, or (2) the 3 results can be obtained by similar techniques, or even (3) the results are there but I somehow missed them.

I emailed Jones about this and he responded by saying that the proofs of those 3 results are in both Jones-1980 and Jones-1982 (so option 3 above). Unfortunately my deadline for submitting this article prevented me from pursuing this matter any further.

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 (1) the 3 results of Jones for which I cannot tell if there are proofs, though Jones says there are, and (2) the result of Sun. We state the results of the form $\mathrm{H}\mathbb{N}(d, n) = \mathrm{U}$ and then apply Theorem 2.3 to obtain results of the form $\mathrm{H}\mathbb{Z}(d', n') = \mathrm{U}$ (except for Sun's result which is already about $\mathrm{H}\mathbb{Z}$).

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 4.6×10^{44}. These are probably upper bounds that might be able to be lowered with a careful examination of the proofs.

Theorem 3.1.

1. $\mathrm{H}\mathbb{N}(4, 58) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(8, 174) = \mathrm{U}$.

2. $\mathrm{H}\mathbb{N}(8, 38) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(16, 114) = \mathrm{U}$.

3. $\mathrm{H}\mathbb{N}(12, 32) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(24, 96) = \mathrm{U}$.

4. *(Announced by Jones in 1980. I have been unable to find a proof. See the beginning of this section for the full story.)*

   $\mathrm{H}\mathbb{N}(16, 29) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(32, 87) = \mathrm{U}$.

5. $\mathrm{H}\mathbb{N}(20, 28) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(40, 84) = \mathrm{U}$.

6. $\mathrm{H}\mathbb{N}(24, 26) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(48, 78) = \mathrm{U}$.

7. $\mathrm{H}\mathbb{N}(28, 25) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(56, 75) = \mathrm{U}$.

8. *(Announced by Jones in 1980. I have been unable to find a proof. See the beginning of this section for the full story.)*

   $\mathrm{H}\mathbb{N}(36, 24) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(72, 72) = \mathrm{U}$.

9. $\mathrm{H}\mathbb{N}(96, 21) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(192, 63) = \mathrm{U}$.

10. $\mathrm{H}\mathbb{N}(2668, 19) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(5336, 57) = \mathrm{U}$.

11. $\mathrm{H}\mathbb{N}(200000, 14) = \mathrm{U}$ *hence*

    $\mathrm{H}\mathbb{Z}(400000, 42) = \mathrm{U}$ *and* $\mathrm{H}\mathbb{Z}(31 \times 2^{14}, 30) = \mathrm{U}$.

12. *(Announced by Jones in 1980. I have been unable to find a proof. See the beginning of this section for the full story.)*

    $\mathrm{H}\mathbb{N}(6.6 \times 10^{43}, 13) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(13.2 \times 10^{43}, 28) = \mathrm{U}$.

13. $\mathrm{H}\mathbb{N}(1.3 \times 10^{44}, 12) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(2.6 \times 10^{44}, 36) = \mathrm{U}$.

14. $\mathrm{H}\mathbb{N}(4.6 \times 10^{44}, 11) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(9.2 \times 10^{44}, 24) = \mathrm{U}$.

15. $\mathrm{H}\mathbb{N}(8.6 \times 10^{44}, 10) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(17.2 \times 10^{44}, 22) = \mathrm{U}$.

16. $\mathrm{H}\mathbb{N}(1.6 \times 10^{45}, 9) = \mathrm{U}$ *hence* $\mathrm{H}\mathbb{Z}(3.2 \times 10^{45}, 20) = \mathrm{U}$. *(Jones' 1982 paper presents the proof of this result and credits it to Matiyasevich.)*

17. $\mathrm{H}\mathbb{Z}(d, 11) = \mathrm{U}$ *for some rather large d. The number d is not stated. (This is due to Sun [31].)*

4 When is $\mathrm{H}\mathbb{Z}(d, n) = \mathrm{D}$? $\mathrm{H}\mathbb{N}(d, n) = \mathrm{D}$?

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*

$$\mathrm{FROB}(\vec{a}) = \left\{\sum_{i=1}^{n} a_i x_i \colon x_1, \ldots, x_n \in \mathbb{N}\right\}.$$

It is known that $\mathrm{FROB}(\vec{a})$ 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, $\mathrm{FROB}(\vec{a})$ 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*

$$\mathrm{FROB}(a_1, a_2) = F \cup \{dx \colon x \geq a_1a_2 - a_1 - a_2 + 1\}$$

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

For the general case there is no neat formula; however, finding $\mathrm{FROB}(\vec{a})$ 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*

   $$\mathrm{FROB}(\vec{a}) = F \cup \{dx \colon x \geq M\}$$

   and

   $(M - 1)d \notin \mathrm{FROB}(\vec{a})$.

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, $\mathrm{H}\mathbb{Z}(d, 1) = \mathrm{D}$ and $\mathrm{H}\mathbb{N}(d, 1) = \mathrm{D}$. There is an algorithm that finds all of the integer roots (which may be the empty set).*

2. *For all n, $\mathrm{H}\mathbb{Z}(1, n) = \mathrm{D}$.*

3. *For all n, $\mathrm{H}\mathbb{N}(1, n) = \mathrm{D}$.*

4. $\mathrm{H}\mathbb{Z}(2, 2) = \mathrm{D}$.

5. $\mathrm{H}\mathbb{N}(2,2) = \mathrm{D}$.

6. *For all n,* $\mathrm{H}\mathbb{Z}(2,n) = \mathrm{D}$ *and* $\mathrm{H}\mathbb{N}(2,n) = \mathrm{D}$.

Proof.
1) These are both easy consequences of the rational root theorem: If $a_d x^d + \cdots a_1 x + a_0 \in \mathbb{Z}[x]$ 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 $x_i = \frac{bx_i'}{d}$.

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

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

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

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

Once we have F_a, M_a, F_b, M_b it is easy to determine if $\{F_a \cup \{xd \colon x \geq M_a\}$ and $\{F_b \cup \{b + xd \colon x \geq M_b\}$ intersect. If so, then there is a solution to the original equation, and if 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`)

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, $\mathrm{H}\mathbb{Z}(2, n) = \mathrm{D}$ and $\mathrm{H}\mathbb{N}(2, n) = \mathrm{D}$. 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 $\mathrm{H}\mathbb{Z}(3, 2)$

The case of $\mathrm{H}\mathbb{Z}(3, 2)$ is almost solved.

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

A combination of results by Baker and Cohen [3], Poulakis [26], and Poulakis [27] 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 [27] 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, Pethő et al. [24] 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 $\mathrm{H}\mathbb{Z}(3, 2) = \mathrm{D}$? 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
$(z_1 + z_2 < z_3 + 12) \wedge (z_1 + z_4 = 17)$ is a Presburger formula, but
$z_1 z_2 = 13$ is not.

Theorem 5.4. *The following is decidable:*
Instance
(1) For $1 \le i \le k$ 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*

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

holds.

6 The Curious Case of $x^3 + y^3 + z^3 = k$

Rather than looking at $\mathrm{H}\mathbb{Z}(d, n)$ let's focus on 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 $k \not\equiv 4, 5 \pmod 9$, $x^3 + y^3 + z^k = k$ has a solution in $\mathbb{Z}$.

2. Elkies [10] 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 [11] modified and implemented Elkies algorithm and determined the following: The only $k \le 1000$, $k \not\equiv 4, 5 \mod 9$, where they did not find a solution were

   33, 42, 74, 114, 165, 390, 579, 627, 633, 732, 795, 906, 921, and 975.

   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 $k \leq 1000$, $k \not\equiv 4, 5 \mod 9$, where no solution is known are:

   114, 165, 390, 579, 627, 633, 732, 795, 906, 921, and 975.

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 the 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 $H\mathbb{N}$ or $H\mathbb{Z}$ 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 $H\mathbb{Z}(d, 1) = D$, $(\forall n)[H\mathbb{Z}(2, n) = D]$, and $H\mathbb{Z}(8, 174) = U$. The following are unknown:

1. $H\mathbb{Z}(3, 2), H\mathbb{Z}(3, 3), H\mathbb{Z}(3, 4), \ldots$.

2. $H\mathbb{Z}(4, 2), H\mathbb{Z}(4, 3), H\mathbb{Z}(4, 4), \ldots$.

3. $H\mathbb{Z}(5, 2), H\mathbb{Z}(5, 3), H\mathbb{Z}(5, 4), \ldots$.

4. $H\mathbb{Z}(6, 2), H\mathbb{Z}(6, 3), H\mathbb{Z}(6, 4), \ldots$.

5. $H\mathbb{Z}(7, 2), H\mathbb{Z}(7, 3), H\mathbb{Z}(8, 4), \ldots$.

6. $\text{H}\mathbb{Z}(8,2), \text{H}\mathbb{Z}(8,3), \text{H}\mathbb{Z}(8,4), \ldots, \text{H}\mathbb{Z}(8,173)$.

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, $\text{H}\mathbb{Z}(d,n) = \text{U}$? We present an informed opinion by paraphrasing and combining two passages from Sun [30, pages 209 and 211]:

1. Matiyasevich and Robinson [22] showed there is a d such that $\text{H}\mathbb{N}(d,13) = \text{U}$.

2. Matiyasevich showed there is a d such that $\text{H}\mathbb{N}(d,9) = \text{U}$. By Theorem 2.3 we have that there is a d' with $\text{H}\mathbb{Z}(d',20) = \text{U}$.

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

$$(\forall d)[\text{H}\mathbb{Z}(d,2) = \text{D}]$$

   but it points in that direction.

4. (Direct quote from page 209.) *In fact, A. Baker, Matijasevič and Robinson even conjectured that* $\exists^3$ *is undecidable over* $\mathbb{N}$. In our notation, there exists d such that $\text{H}\mathbb{N}(d,3) = \text{U}$.

Suggestions:

1. Since a grid for $\text{H}\mathbb{N}(d,n)$ or $\text{H}\mathbb{Z}(d,n)$ 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 $\text{H}\mathbb{N}(d,n) = \text{U}$ or $\text{H}\mathbb{Z}(d,n) = \text{U}$ 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 [23], Yedidia 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. $\mathrm{H}\mathbb{Q}(d, n)$ is the problem where the degree is $\le d$, the number of variables is $\le n$, and we seek a solution in $\mathbb{Q}$.

Matiyasevich [19] (Page 18) gives good reasons why Hilbert might have actually wanted to solve $\mathrm{H}\mathbb{Q}$. Hilbert stated the tenth problem as $\mathrm{H}\mathbb{Z}$; however, if $\mathrm{H}\mathbb{Z}$ is solvable then $\mathrm{H}\mathbb{Q}$ is solvable. He might have thought that the best way to solve $\mathrm{H}\mathbb{Q}$ is to solve $\mathrm{H}\mathbb{Z}$.

What is the status of $\mathrm{H}\mathbb{Q}$ 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, James Jones, Chris Lastowski, David Marcus, Yuri Matiyasevich, Andras Salamon, 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

[1] Scott Aaronson. The busy beaver frontier (an open problems column). *SIGACT News*, 53(3):31–55, 2020. https://www.cs.umd.edu/users/gasarch/open/busybeaver.pdf.

[2] Alan Baker. On the representation of integers by binary forms. *Philosophical Transactions of the Royal Society of London*, 263:173–191, 1968.

[3] Alan Baker and John Coates. Integer points on curves of genus 1. *Mathematical Proceedings of the Cambridge Philosophical Society*, 67:595–602, 1970.

[4] Jonas Bayer, Marco David, Simon Dubischar, Malte Haßler, Abhik Pal, Michael Schmalian, and Benedikt Stock. Zusammengestellt von Stephanie Schiemann. Beeindruckende Mathematik-Erfolge im 53. Bundeswettbewerb ‚Jugend forscht'. Mitteilungen der Deutschen Mathematiker-Vereinigung, 26(2–3), 2018.
https://www.degruyter.com/view/journals/dmvm/26/2-3/article-p55.xml?language=de.

[5] Dale Beihoffer, Jemimah Hendry, Albert Nijenhuis, and Stan Wagon. Faster algorithms for Frobenius Numbers. *Electronic Journal of Combinatorics*, 12(R27), 2005.
https://www.combinatorics.org/ojs/index.php/eljc/article/view/v12i1r27.

[6] Andrew Booker. Cracking the problem with 33, 2019.
https://arxiv.org/abs/1903.04284.

[7] Felipe Cucker, Pascal Koiran, and Steve Smale. A polynomial time algorithm for diophantine equations in one variable. *Journal of Symbolic Computation*, 27:21–29, 1999.

[8] Martin Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, pages 233–2695, 1973.
https://www.math.umd.edu/~laskow/Pubs/713/Diophantine.pdf.

[9] Martin Davis, Hillary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Annals of Mathematics*, 74:425–436, 1961.

[10] Noam Elkies. Rational points near curves and small nonzero $|x^3 - y^3|$ via lattice reductions. In *Algorithmic Number Theory*, volume 1838 of *Lecture notes in computer science*, pages 33–63, 2000.
https://arxiv.org/abs/math/0005139.

[11] Andreas-Stephan Elsehans and Jorg Jahnel. New sums of three cubes. *Mathematics of Computation*, 78(266), 2009.
https://www.ams.org/journals/mcom/2009-78-266/S0025-5718-08-02168-6/S0025-5718-08-02168-6.pdf.

[12] Carl F. Gauss. *Disquisitiones Arithmetica (English Translation)*. Springer-Verlag, New York, Heidelberg, Berlin, 1986.

[13] Fritz J. Grunewald and Dan Segal. On the integer solutions of quadratic equations. *J. Reine Angew. Math.*, 569:13–45, 2004.

[14] Roger Heath-Brown. The density of zeros of forms for which weak approximation fails. *Mathematics of Computation*, 59(200):612–623, 1992.

[15] Sander Huisman. Newer sums of three cubes, 2016.
`https://arxiv.org/abs/1604.07746`.

[16] James Jones. Undecidable diophantine equations. *Bulletin of the American Mathematical Society*, 3(2):859–862, 1980.
`https://www.ams.org/journals/bull/1980-03-02/S0273-0979-1980-14832-6/S0273-0979-1980-14832-6.pdf`.

[17] James Jones. Universal diophantine equations. *Journal of Symbolic Logic*, 47(3):549–571, 1982.
`http://www.jstor.org/stable/2273588?seq=1#metadata_info_tab_contents`.

[18] Jeffrey Lagarias. Succinct certificates for the solvability of binary quadratic diophantine equations. In *20th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 47–54. IEEE, 1979.
`https://arxiv.org/pdf/math/0611209.pdf`.

[19] Yuri Matiyasevich. Hilbert's tenth problem: What can we do with diophantine equations?
`https://logic.pdmi.ras.ru/~yumat/personaljournal/H10history/H10histe.pdf`.

[20] Yuri Matiyasevich. Enumerable sets are diophantine (Russian). *Doklady Academy Nauk, SSSR*, 191:279–282, 1970. Translation in Soviet Math Doklady, Vol 11, 1970.

[21] Yuri Matiyasevich. *Hilbert's Tenth Problem*. MIT press, Cambridge, 1993.

[22] Yuri Matiyasevich and Julia Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, pages 521–553, 1975.

[23] Pascal Michel. Problems in number theory from busy beaver competitions, 2013. `https://arxiv.org/pdf/1311.1029v1.pdf`.

[24] Attila Pethő, Horst G Zimmer, Josef Gebel, and Emanuel Herrmann. Computing all S-integral points on elliptic curves. *Mathematical Proceedings of the Cambridge Philosophical Society*, 127:383–402, 1970.

[25] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate studies in mathematics*. American Mathematics Society, 2017.

[26] Dimitrios Poulakis. Points entiers sur les courbes de genre 0. *Colloquium Mathematicae*, 66:1–7, 1993.

[27] Dimitrios Poulakis. Solving genus zero diophantine equations with at most two infinite valuations. *Journal of Symbolic Computation*, 33:479–491, 2002.

[28] Carl Ludwig Siegel. Zur Theorie der quadratischen Formen. *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse*, 3:21–46, 1972.

[29] Roel Stoeker and Nikoluas Tzanakis. Computing all integer solutions of a genus 1 equation. *Mathematics of Computation*, 72(1917–1933), 2003.

[30] Zhi-Wei Sun. A new relation-combining theorem and its application. *ZL*, 38:209–212, 1992.
`http://maths.nju.edu.cn/~zwsun/14z.pdf`.

[31] Zhi-Wei Sun. Further results on Hilbert's tenth problem. *Science China Mathematics*, 2021.

[32] Adam Yedidia and Scott Aaronson. A relatively small Turing machine whose behaviour is independent of set theory, 2016. `https://arxiv.org/abs/1605.04343`.