Hilbert’s Tenth Problem

Determining the Solvability of Diophantine Equations

Hilbert's Problems

- In 1900, Hilbert published a list of 23 problems which were supposed to be some of the most important problems at the time – i.e. problems that the 19th century had left for the 20th century to solve
- The first problem (concerning geometry) was solved in 1900 itself using Dehn Invariants
- Today, only 3 of them are unsolved* (one of them being the Riemann Hypothesis)

Hilbert’s Tenth Problem

“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.”

Diophantine Equations

- Polynomials in any number of variables with only integral coefficients
- D (x1, x2… xn) = 0
- Considered solvable if it has integral solutions

Turing Machines

- We ask our Turing Machines yes/no questions, or questions of the form 'does this input belong to a set S in Σ^*'
- Given some input, there are 3 possibilities: The program says 'yes', the program says 'no', or the program never terminates
- A set S is called semi-decidable or recursively enumerable if there exists a Turing Machine which terminates and says 'yes' whenever the input belongs to S. It may or may not terminate otherwise
- A set S is called decidable or recursive if both S and the complement of S are decidable
- Church-Turing Thesis: Any 'effectively computable' function (in the intuitive sense) is a computable function (in terms of Turing Machines)

Hilbert's Tenth Problem is Semidecidable

- List of all possible n-tuples can be generated one-by-one
- Check if each one works
- If there is a solution, we will eventually find it and the machine will halt.

Hilbert’s Tenth Problem

- Hilbert’s 10th problem took 70 years to solve and was the work of mainly 4 mathematicians – Yuri Matiyasevich, Julia Robinson, Martin Davis, and Hilary Putnam* (the main result in the proof is often called the MRDP theorem after their initials). They proved that there was no such ‘process’! (i.e. it is an undecidable problem).
- Completely elementary proof!

Martin Davis, Julia Robinson, Yuri Matiyasevich

Diophantine Equations

Observation 1: Determining whether a system of Diophantine equations is solvable is equivalent to determining whether a single Diophantine equation is solvable

D1(x1, ...xm) = 0, & ... Dk(x1,...xm) = 0 has a solution ⇔ D1^2(x1, ... xm) ... + Dk^2(x1,...xm) = 0 has a solution

Diophantine Equations

Observation 2: It is sufficient to find a method to decide whether a Diophantine equation of degree 4 has a solution

- Introduce new variables and get a system of equations of the form where each equation is of the form a = b+c and a = bc
- Convert to a single equation

Diophantine Equations

Observation 3: We may restrict to non-negative solutions only

- Reducing from integral to non-negative: D(x1, x2... xn) = 0 has an integral solution ⇔ D(a1-b1, a2-b2...an-bn) = 0 has a non-negative solution
- Reducing from non-negative to integral: D(x1, x2, ...xn) = 0 has a solution ⇔ D(x1, x2...xn) = 0 & x1= a1^2 + b1^2+c1^2+d1^2 ... & xk=an^2 + bn^2+cn^2+dn^2 has a solution (from Four-Square Theorem)

Four-Square Theorem: Every nonnegative integer can be represented as a sum of four non-negative integer squares

Diophantine Sets

- A **parametric Diophantine Equation** is a Diophantine Equation D(a1, a2...an, x1, x2... xm) where the variables are separated into *parameters* a1, a2... an and *unknowns* x1, x2... xm
- By fixing the parameters, we get Diophantine Equations in m variables which can be either solvable or unsolvable depending on the values of the parameters
- Hence, there is a set M ⊂ N^n associated with every parametric Diophantine equation in m parameters = set of n-tuples (a1, a2... an) ⊂ N^n such that D(a1, a2... an, x1, x2...xm)=0 is solvable
- Such a set is said to be a **Diophantine Set** of **dimension n**, and the corresponding equation is the **Diophantine Representation** of it
- We can also define **Diophantine Properties**, **Diophantine Relations** and **Diophantine Functions**
- Q: Which subsets of N^n are Diophantine?

Diophantine Sets

Example 1: The property of being an even number is Diophantine (similarly for odd)

Example 2: The relation <= is Diophantine

Example 3: The relation =/= is Diophantine

Diophantine Sets

Property 1: Diophantine Sets are closed under Union

Property 2: Diophantine Sets are closed under Intersection

Property 3: Diophantine Sets are closed under Projection

We can also use Diophantine functions as terms

Q: Are Diophantine Sets closed under complementation?

Diophantine Sets

Example 4: The function rem(b,c) is Diophantine

Example 5: Divisibility, the congruence relation with respect to a certain modulus, and the function div(b,c) are Diophantine

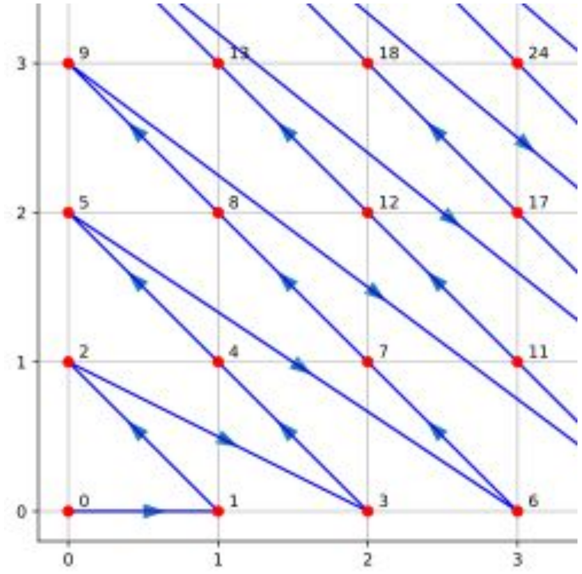
Example 7: gcd and lcm are Diophantine

MRDP/Matiyasevich's Theorem

The class of Diophantine Sets is precisely the class of Turing Semidicable Sets

Cantor Encoding

- Want to encode sequences of numbers
- We can encode pairs as follows: (0,0), (0,1), (1,0), (0,2), (1,1)… = 0, 1, 2, 3, 4 … resp.
- i.e. (a,b) is encoded as **Cantor (a,b)** = $((a+b)^2 + 3a + b)/2$
- Retrieving the elements:
  - $a = \mathrm{Elema}(c) \Leftrightarrow \exists b$ s.t. $((a+b)^2 + 3a + b) = 2c$
  - $b = \mathrm{Elemb}(c) \Leftrightarrow \exists a$ s.t. $((a+b)^2 + 3a + b) = 2c$
- Cantor, Elema, and Elemb are Diophantine functions



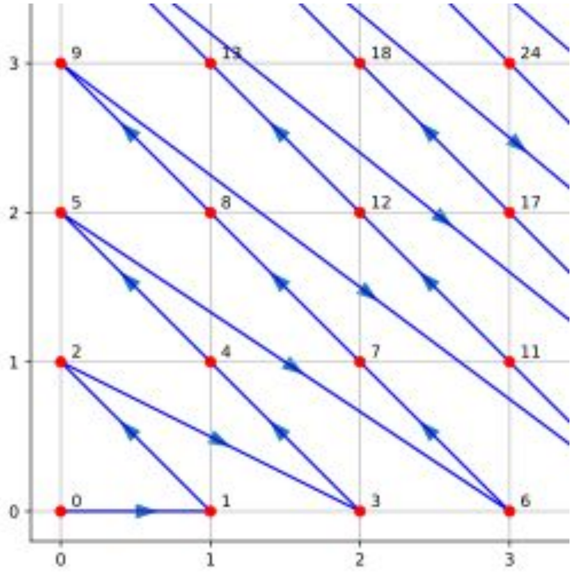
Cantor Encoding

- Can encode (a1, a2, … an) as a single number :

  Cantor_n (a1, a2… an) = Cantor (a1, Cantor (a2, Cantor (a3…. Cantor (an-1, an))))

- an = Elem n,m (c) ⇔ ∃ a1, a2,… an-1, an+1,…am s.t. 2^(2^n) Cantor (a1, a2…an) = 2^(2^n) c

- Each of Elem n,m is a different Diophantine function. We want a single Diophantine function Elem (n,m,c) -> use positional encoding instead!



Exponentiation is Diophantine...

- The function b^c is also Diophantine (not at all trivial! This was the last piece of the proof)
- Assuming this fact, we can freely* use exponentiation in our equations

Julia Robinson, unaware of Davis's work, investigates the connection of the exponential function to the problem, and attempts to prove that EXP, the set of triplets (a, b, c) for which $a = b^c$, is Diophantine. Not succeeding, she makes the following *hypothesis* (later called J.R.):

> *There is a Diophantine set D of pairs (a, b) such that $(a, b) \in D \Rightarrow b < a^a$ and for every positive k*, there exists $(a, b) \in D$ *such that* $b > a^k$.

Using properties of the Pell equation, she proves that J.R. implies that EXP is Diophantine, as well as the binomial coefficients, the factorial, and the primes.

Positional Coding

- Let the code of $a_1, a_2 \ldots a_n$ be the value of $a_n a_{n-1} \ldots a_1$ in some base b
- We will also include b, n in our code
- i.e. the positional code of $(a_1, a_2 \ldots a_n)$ is $\mathrm{Cantor}_3(a_1b^0+a_2b^1+\ldots+a_nb^{n-1}, b, n)$
- Given some code (a,b,c) we can retrieve the dth element of the tuple via $e = \mathrm{Elem}(a,b,d) \Leftrightarrow \exists xyz$ s.t. $[d=z+1 \;\&\; a=x^d+eb^z+y \;\&\; e<b \;\&\; y<b^z]$
- We now know that these are Diophantine Functions

Positional Coding

We can now easily show the following functions are Diophantine!

- **nCm**
- **m!**
- **Prime**(a)

Positional Coding

We can now easily show the following functions are Diophantine!

- **nCm:** From binomial theorem, $((b+1)^n, b, n+1)$ is the positional code of $(nC0, nC1, \ldots nCn)$ for sufficiently large b
- **m!** $= \lim_{n \to \infty} n^m/(nCm)$. Use div on sufficiently large n
- **Prime**(a) $\Leftrightarrow a>1$ & $\gcd(a,(a-1)!)=1$

Diophantine Representation of Primes

- D (a, x1, ...xm) = 0 has a solution ⇔ (x0 + 1)(1-D^2(x0, ..., xm))-1 = a has a solution

THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

$$
\begin{aligned}
(1)\qquad & (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2 \\
& -[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2 \\
& -[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\
& -[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}
$$

as the variables range over the nonnegative integers.

***Degree 25 Polynomial in 26 variables (- every letter of the alphabet)**

Positional Coding

Using the prime function, it is now possible to construct the following Diophantine functions:

- Checking if a given code(a,b,c) is valid: $a<b^c$ and $b>=2$
- Concatenation of codes
- Checking if two codes encode the same tuple
- Repeat (a, b, n) = $a(b^c-1)/(b-1)$
- Applying function on every element of a tuple: given Diophantine function F in m arguments, we can construct F[beta] s.t. F[beta](p_1, p_2... p_n, c) = ($F(p_{11}, p_{21}, \dots p_{n1}), \dots, F(p_{1m}, p_{2m}, \dots p_{nm})$)

Connection to Other Problems

We can now see that a positive solution to Hilbert's Tenth Problem would allow us to resolve all of these*:

- Fermat's Last Theorem: $(p+1)^{(s+3)} + (q+1)^{(s+3)} = (r+1)^{(s+3)}$ has no solutions
- Catalan's Conjecture: The only consecutive powers of natural numbers are 8 and 9
- Using Bounded Universal Quantifiers, one can also show that the Goldbach Conjecture and Riemann Hypothesis are special cases of Hilbert's Tenth Problem

Connection to Other Problems– Goldbach Conjecture

- $2a+4$ cannot be expressed as the sum of two primes $\Leftrightarrow \forall z<a+1\ \exists xy\ (z+2=(x+2)(y+2) \lor 2a+2-z = (x+2)(y+2))$
- Then, $\exists a \forall z<a+1\ \exists xy\ (z+2=(x+2)(y+2) \lor 2a+2-z = (x+2)(y+2))$ is a single Diophantine Equation which is solvable iff the Goldbach Conjecture is false

Turing Machines

- Consists of a finite alphabet Σ = s0, s1,s2...sn, an infinite tape divided into cells (each cell can store one letter), a set of ‘states’ Q = q1, q2...qn, and a ‘transition function’ = set of instructions (= (A,Q,D): Q x Σ -> Σ xQx{L,S,R})
- We have an initial position on the tape
- We have an initial state and two halt states– one corresponding to ‘yes’ and one corresponding to ‘no’
- s0 is special ‘empty’ symbol and * is left end-marker
- The input to the Turing Machine is some finite string written on some portion of the tape
- At each step, our Turing machine looks at the alphabet in the cell it is in, and the state it is in, and uses the transition function to determine which state to go to, what to rewrite on the cell, and whether to move the tape head to the left, to stay in the same position, or move to the right
- Input corresponding to (a1,...an) = <*, 0, 1, 1., 1, 0, 1,1 ...1, 0, ... 0, 1,1 ...1>

Semidecidable Sets are Diophantine

- Let the Turing Machine T have number of states = v and alphabet size = w
- At any point in the computation, the current configuration of the Turing Machine can be represented using two tuples:
    - (s1, s2,...sm,...sl-1, sl), the Tape tuple; contains the current tape contents
    - (0, 0,...i,...0, 0) is the Position tuple; stores current position (location of i) and i (current state)
- Use positional coding in some base beta, with beta > v, w
- Goal: To construct a Diophantine equation D(p, t, x1,...xm) = 0 such that for valid p, t, the equation is solvable iff T halts with initial configuration given by p, t

Semidecidable Sets are Diophantine

- Want to construct NextT(p,t) which gives Tape tuple one step later:
  - Let A(i,j) = alphabet given by transition function if 0<i<=v, 0<=j<=w are valid (piecewise-Diophantine equations are diophantine), else j (if i = 0)
  - t' = NextT(p,t) ⇔ ∃w[t'=A[beta](p,t,w)]
- Want to construct NextP(p,t) which gives Position tuple one step later:
  - Let pR = pbeta, pL = p div beta, tR = tbeta, tL = t div beta (i.e. tuples shifted* one to the left or right)
  - Construct function DQ similar to A above but which takes in as input current position in p, t, and elements to the left and right in p, t
  - p' = NextP(p,t) ⇔ ∃w[p' = DQ(beta)(p_beta, p, p div beta, t beta, t, t div beta, w)]

Semidecidable Sets are Diophantine

- Want to define iterated Next i.e. AfterP(k, p, t) and AfterT(k, p, t)
  - If we choose l such that p, t < beta^l-k-2, then we know that currently <= l-k-2 cells are filled and in k steps, < l cells will be filled, so we can choose l as size of all our codes
  - Construct ‘super-configuration’ pL, pR, pM, tL, tR, tM
  - Consider this ‘super-machine’ with multiple tape heads. Can use same NextP, NextT functions to find next configuration on the super-machine
  - Codes of size kl or (k-1)l

Semidecidable Sets are Diophantine

- p’ = AfterP(k,p,t) and t’ = AfterT(k,p,t) ⇔ ∃ l, pL, pR, pM, tL, tR, tM s.t.
  - p, t < beta^l-k-2
  - pR = NextP (pL, tL)
  - tR = NextT (pL, tL)
  - <pL, beta, kl> = <p, beta, l> + <pM, beta, (k-1)l>
  - <pR, beta, kl> = <pM, beta, (k-1)l> + <p’, beta, l>
  - (analagous statements for t)
  - p’, t’ < beta^l

Semidecidable Sets are Diophantine

- D we wanted to construct; set of (p,t) on which T halts: ∃ k, r s.t. [Elem(AfterT(k,p,t), beta, r) = final_state]
- Initial configuration:
  - p = <1, 0, 0, ...> = 1
  - t = <*, 0, 1, ... 1, 0, 1..., 1... 0, 1,... ,1>
  - <t, beta, a> = <*, beta, 1> + <0, beta, 1> + <Repeat(1, beta, a_1), beta, a_1> + <0, beta, 1> +... + <0, beta, 1> + <Repeat(1, beta, a_n), beta, a_n>
- Final function: combine the above three equations

Halting Problem

- Q: Is the problem of determining when a machine halts decidable?

Halting Problem is semi-decidable: We can construct a ‘Universal Turing Machine’ which takes as input a Turing Machine T and a word w, simulates the running of T on w, halts if T halts on w and returns the output of T on w.

Halting Problem

Halting Problem is not decidable:

- Suppose the Halting Problem is decidable i.e. there is a Turing Machine which takes as input T, w and returns 'yes' if T halts on T and 'no' otherwise
- Then, there is a Turing Machine H which takes as input T and returns 'yes' if T halts on w = T and 'no' otherwise
- Then there is a Turing Machine J which takes as input T and does not halt if T halts on w = T and halts if T halts on w = T
- Does J halt on itself?

Undecidability of Solvability of Diophantine Equations

- Consider a semidecidable set S whose complement is not semidecidable
- S is Diophantine, hence there exist a class of Diophantine equations parametrized by a which are solvable iff a in S
- Since the complement of S is not semidecidable, there does not exist an algorithm to determine whether even Diophantine Equations from this class are solvable

...Exponentiation is Diophantine

- Finding one example of Julia Robinson Predicates would be enough to complete the proof
- She considered using Pell's Equations:
  - $x^2-(a^2-1)y^2=1$
  - Solutions (pi, qi) satisfy the recurrence relation
    - $p_{i+1} = 2a_p - p_{n-1}$
    - $q_{i+1} = 2a_q - q_{n-1}$
  - The sequences p_i, q_i are periodic modulo any m, and hence so are their linear combinations
  - q_0, q_1... mod (a-1) is periodic with 0, 1, 2... a-2
  - $q_0 - (a-2)p_0, q_1 - (a-2)p_1$... (mod 4a-5) is periodic with start $2^0, 2^1, 2^2$...
  - She showed that if one could find an infinite Diophantine set of a such that the length of the first period is a multiple of the second, then one would have an example of Julia predicates

...Exponentiation is Diophantine

- This approach has not yielded any solutions, but Matiyasevich was inspired by this idea of synchronization of periods to consider the related sequence of Fibonacci Numbers at even positions
- Fibonacci Numbers satisfy $a_0 = 0$, $a_2 = 1$, $a_{2i+2} = 3a_{2i} - a_{2i-2}$
- Sequence grows like $((3+\sqrt{5})/2)^n$, can show that $2^{u-1} < u_{2i} < 3^u$
- Hence, they satisfy J.R.
- Remains to show that the equation is Diophantine

...Exponentiation is Diophantine

- The only solutions to x^2 - y^2 - xy = +-1 are consecutive Fibonacci Numbers (can be proved via induction). x^2-y^2-xy = 1 gives x = a_2i+1, y=a_2i, and x^2-y^2-xy = -1 gives x = a_2i, y=a_2i-1
- Can generalise Fibonacci numbers a_n to phi_m,n given by :
    - phi_m,0 = 0, phi_m,1 = 1, phi_m+1, k = mphi_m,k - phi_m,k-1
    - Which have a similar property for the equation x^2-mxy+y^2=1
- This equals even position Fibonacci numbers for m = 3

...Exponentiation is Diophantine

- Fibonacci Numbers satisfy a_n^2|a_m => a_n|m, which provides some sort of relation between a Fibonacci Number and its index
- He also established some lemmas in modular arithmetic:

Lemma 13. *For any numbers j and k, if $j \leq 2k+1$, then*

$$\varphi_{2(2k+1-j)} \equiv -\varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}.$$

Lemma 21. *For any numbers $a \geq 2$, $m \geq 2$ and j,*

$$\psi_{m,j} \equiv \psi_{a,j} \pmod{m-a}.$$

Lemma 22. *For any numbers l, j and $m \geq 2$, if $l|m-2$, then $\psi_{m,j} \equiv j \pmod{l}$; for any numbers d, j and $m \geq 2$, if $d|m-3$, then $\psi_{m,j} \equiv \phi_{2j} \pmod{d}$.*

- Using these properties, he was able to come up with a short list of necessary and sufficient conditions for v = a_2u

...Exponentiation is Diophantine

Theorem 1. *For any natural numbers u and v, in order that the equation $v = \phi_{2u}$ hold, it is necessary and sufficient that there exist natural numbers l, g, h, m, x, y and z such that*

$$u < l, \tag{35}$$
$$v < l, \tag{36}$$
$$l^2 - lz - z^2 = 1, \tag{37}$$
$$g^2 - gh - h^2 = 1, \tag{38}$$
$$l^2 \mid g, \tag{39}$$
$$l \mid m - 2, \tag{40}$$
$$2h + g \mid m - 3, \tag{41}$$
$$x^2 - mxy + y^2 = 1, \tag{42}$$
$$l \mid x - u, \tag{43}$$
$$2h + g \mid x - v. \tag{44}$$

...Exponentiation is Diophantine

I was spending almost all my free time trying to find a Diophantine relation of exponential growth. There was nothing wrong when a sophomore tried to tackle a famous problem, but it looked ridiculous when I continued my attempts for years in vain. One professor began to laugh at me. Each time we met he would ask: "Have you proved the unsolvability of Hilbert's tenth problem? Not yet? But then you will not be able to graduate from the university!"

Universal Diophantine Equations

Another result proved by Julia Robinson and Yuri Matiyasevich was that of the existence of Universal Diophantine Equations with number of unknowns bounded for Diophantine Sets of any Dimension.

- A Universal Equation has the form U(a1,… an, k1,… kl, y1,… yw) = 0 where a1,… an are called *element parameters* and k1,… kn are called *code parameters*
- It satisfies the property that for any parametric equation D(a1,…an, x1,…xm), there exists a 'code' (k1,…kl) corresponding to D such that U(a1,…an, k1,…kl, y1,…yw) when fixing (k1,…kl) and regarded as a parametric Diametric equation with parameters a1,…an and unknowns y1,…yw, yields exactly the Diophantine Set as D!

Universal Diophantine Equations

- Analogue to ‘Universal Turing Machine’
- It’s easy to see that we can have l=1 by using Cantor Encoding
- But it is also possible to bound w!
- Matiyasevich initially made a rough estimate of 200 unknowns, but they later brought this down to 13 and eventually 9.

Open Problems

- Is Hilbert's Tenth Problem reducible to its restriction to equations of degree 3? Is solvability of Diophantine Equations of degree 3 decidable? (We know that it is decidable for degree 2 and we have shown that it is undecidable for degree 4)
- Do there exist constants d and m such that for every n one can construct a universal equation with n element parameters, a single code parameter, m unknowns, and total degree w.r.t all the variables equal to d i.e. Universal Diophantine Equations bounded in degree?

Extension of Hilbert’s Tenth Problem

“There has been much work on Hilbert's tenth problem for the rings of integers of algebraic number fields. Basing themselves on earlier work by Jan Denef and Leonard Lipschitz and using class field theory, Harold N. Shapiro and Alexandra Shlapentokh were able to prove:

‘Hilbert's tenth problem is unsolvable for the ring of integers of any algebraic number field whose Galois group over the rationals is abelian.’”

References

- ‘Hilbert’s Tenth Problem’ by Yuri V. Matiyasevich
- Yuri Matijasevic, "Diophantine Representation of Enumerable Predicates," Izvestija Akademii Nauk SSSTF.Serija Mathematiceskaja, 35 (1971), pp. 3-30. English translation: Mathematics of the USSR - Izvestija 5 (1971), pp. 1-28.
- ‘My Collaboration with Julia Robinson’ by Yuri Matiyasevich: *Celebratio Mathematica*
- ‘Diophantine Representation of Fibonacci Numbers’ — James P. Jones, University of Calgary