Hilbert's 10th Problem Talk

Luke Askew

March 2022

Contents

1 Introduction

In 1900 in Hilbert's famous address to the ICM the problem of finding a concrete process for determining the integral solutions to Diophantine equations was posed to the mathematical community, but this was before we had a good definition for what an algorithm is.

Problem 1.1 (Hilbert's 10th Problem)**.** Is there a turing machine with inputs $f(\underline{x}) \in \mathbb{Z}[\underline{x}]$ which outputs *Yes* if f has an integral solution, a vector $a \in \mathbb{Z}^n$ such that $f(a) = 0$ and *No* otherwise?

However, we have that $\mathbb{Z}$ is initial in the category of rings, so provided any diophantine equation $f \in \mathbb{Z}[\underline{x}]$, we can consider the problem of finding all solutions in $\mathbb{R}$ to $\varphi(f)$ where φ is the natural map $\mathbb{Z}[\underline{x}] \to R[\underline{x}]$. In fact, this problem is unsolved for when $R = \mathbb{Q}$.

Nievely, we might assume that we could get somewhere with the fact that $\mathbb{Z}\varphi(f)$ has an integral solution if and only if $\varphi(f)$ has a solution over $\mathbb{Q}$, but nobody has yet found a bound on the size of the denominator cleared by $\mathbb{Z}$.

2 Impossibility over $\mathbb{Z}$

By the 1970s, the tools existed to prove no such algorithm can exist.

Theorem 2.1 ((1970))**.** *The problem of deciding if a Diophantine equation has integral solutions is equivelant to the halting problem.*

We will sketch one direction after some definitions.

A Turing machine T can be thought of as a computer program in language X which terminates. I will choose to think of these as programs in C which has main return 0. Since we can generate all C programs by iterating over all $ASCII$ values, a countable set, the set of Turing machines is countable. We can get a bijection with the rational numbers by taking each such program when total ordering the naturals by length and then lexographic order.

2.1 Decision Problems

Definition 2.1. A decision problem is a subset of the inputs to a Turing machine.
A Turing machine T solves the decision problem if
(i)for all possible inputs i, T halts
(ii)when T halts, T returns *Yes* if $t \in S$, *No* otherwise

Definition 2.2. The Halting Problem asks if there is a Turing machine T which inputs a program p and $x \in \mathbb{Z}$ and returns *Yes* if $p(x)$ halts, *No* otherwise.

Theorem 2.2 (Turing, (1936))**.** *No Turing machine solves the halting problem.*

Proof. Suppose we can solve the halting problem, so we can define H which halts on a program x if and only if x halts on x. Taking $x = H$ gives a contradiciton. □

2.2 Recursive and Enumerable Sets

Definition 2.3. $S \subseteq \mathbb{Z}$ is recursive provided there is a Turing machine T with input n and output *Yes* if $n \in S$, *No* otherwise.

Example 2.1. Finite sets

Example 2.2. Even numbers, % is implemented in C

Example 2.3. prime numbers, implement a sieve algorithm

Definition 2.4. $S \subseteq \mathbb{Z}$ is listable if there is a Turing machine such that S is the list of integers printed when T runs forever.

Lemma 2.1. *All recursive sets are listable*

Proof. Run the Turing machine for the recursive set over all integers inputs. □

Lemma 2.2. *There exists a listable set which is not recursive: recursive* $\subsetneq$ *listable.*

Proof.

$$S = \{5^p 3^x | p \text{ halts on } x\}$$

Enumerating p countably, we see this is listable. It is not recursive since the Halting problem can't be solved. □

2.3 Diophantine Equations

Definition 2.5. $S \subseteq \mathbb{Z}^n$ is Diophantine if it solves a integral polynomial, that is there i a polynomial $p(\underline{t}, \underline{x}) \in \mathbb{Z}[\underline{t}, \underline{x}]$ such that

$$S = \{a| \text{ there exists } x \text{ giving } p(a, x) = 0\}.$$

Example 2.4. Squares! $p(x, a) = x^2 - a$ has a a solution if and only if x has square a.

Example 2.5. $\mathbb{N}$ is Diophantine. $a \in \mathbb{N}$ iff $x_1^2 + x_2^2 + x_3^2 + x_4^2 = a$, so we could take $p(a, \underline{x}) = x_1^2 + x_2^2 + x_3^2 + x_4^2 - a$.

Example 2.6. $n\mathbb{Z}$ is diophantine. Take c_1, c_2 with $(c_1, c_2) = n$ and use the extended euclidean algorithm to find $p(a, x_1, x_2) = c_1 x_1 + c_2 x_2 - a$.

Theorem 2.3 (Yuri Matiyasevich,Martin Davis, Julia Robinson, Hilary Putnam (1970))**.** *A subset of* $\mathbb{Z}^n$ *is listable if and only if it is Diophantine*

The shortest proof of this theorem I could find was produced by Matiyasevich and a collaborator in 1990 and is still very involved. The idea of the proof is to tie the halting problem to determining recursively enumerable sets are recursive, i.e. that A and A^C are both recursively enumberable. Then DRP sowed that every listable relation can be given by a polynomial in 1967. In 1970, M showed

that exponentiation is diophantine, which unlocked the ability to show that relations of 1's in binary expansions are diophantine and many other lemmas such as this. The totality of these lemmas allows for showing every polynomial relation is listable.

Theorem 2.4 (Impossibility of Hilbert's 10th Problem)**.** *Take $S\mathbb{Z}^n$ a set which is listable and not recursive. S is Diophantine, so if H held, we would have an algorithm which decided if S has elements.*

3 Solvability Over Fields

There are rings where Hilbert's 10th Problem is solvable! We will use these rings to make statements about solutions over $\mathbb{Q}$.

3.1 $\mathbb{F}_q$

There are only finitely many values to check, so for an algorithm we can simply take evaluating every solution.

3.2 $\mathbb{C}$

In the univariate case, we check if the polynomial degree 0. If not, use the fundamental theorem of algebra! In the multivariable case, we can use tools from Gröbner basis methods seen in 667 - check if the Gröbner basis is (1).

3.3 $\mathbb{R}$

We have the intermediate value theorem and infinite differentiablility, so finding a Liepchitz constant to survey a bounded region containing the zeros will do it. The idea here is to generalize Cauchy's bound to n dimensions. This is my favorite elementary theorem so I'll prove the one dimensional case quickly.

Lemma 3.1 (Cauchy's Bound)**.** *The norm of solutions to a polynomial equation is bounded by the maximum coefficient divided by the leading coefficent plus* 1*.*

Proof. Take $p(x) = a_d x^d + ... + a_0$, and suppose $p(x) = 0$. Then

$$\begin{aligned} |x|^d &\leq \frac{a_{d-1}}{a_d}|x^{d-1}| + ... + \frac{a_0}{a_d} \\ &\leq \max(\frac{a_i}{a_d}) \sum_{i=0}^{d-1} |x|^i \\ &= \max(\frac{a_i}{a_d}) \frac{|x|^d - 1}{|x| - 1} \end{aligned}$$

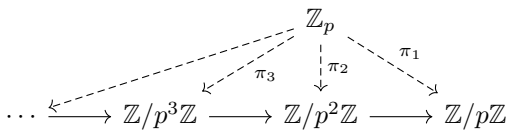
from which the theorem is obvious. □

Note that if there is no solution over $\mathbb{R}$, then there can be no solution over $\mathbb{Q}$.

3.4 $\mathbb{Q}_p$

3.4.1 Review of p-adic numbers

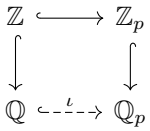
Definition 3.1. Let p be prime. The p-adic integers are defined as $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Explicitly, $\mathbb{Z}_p$ is the limit object making the following diagram commute:



where the horizontal maps are uniquely determined as ring homomorphisms.

The units in $\mathbb{Z}_p$ are those numbers not divisible by p. The natural inclusion of $\mathbb{Z} \mapsto \mathbb{Z}_{\text{ı}}$ works well with taking fraction fields, i.e. the following commutes:

Lemma 3.2. *There exists a ring homomorphism $\iota : \mathbb{Q} \to \mathbb{Q}_p$ making the following diagram commute:*



The image of $\mathbb{Q}_p$ consists of all elements that eventually repeat.

Lemma 3.3. *If there is a point $p \in V(f, \mathbb{Q})$, there is a point $p' \in V(f, \mathbb{Q}_p)$.*

3.4.2 Hensel's Lemma

Lemma 3.4. *Let R be a ring, $f \in R[x]$. Then $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$ for some $g \in R[x,y]$.*

Proof. Let $f(x) = \sum_{j=1}^{n} a_j x^j$. By the binomial theorem, we have

$$(x+y)^j = \sum_{i=0}^{j} \binom{i}{j} x^{j-i} y^i.$$

Combining these we have

$$
\begin{aligned}
f(x+y) &= \sum_{j=1}^{n} a_j \sum_{i=0}^{j} \binom{i}{j} x^{j-i} y^i \\
&= \sum_{j=1}^{n} (a_j x^j + j a_j x^{j-1} y + \sum_{i=2}^{j} \binom{i}{j} x^{j-i} y^i) \\
&= f(x) + y f'(x) + y^2 (\sum_{i=2}^{j} \binom{i}{j} x^{j-i} y^{i-2})) \\
&= f(x) + y f'(x) + y^2 g(x,y)
\end{aligned}
$$

□

Lemma 3.5 (Henel's Lemma, (1908))**.** *If f has a solution over $\mathbb{F}_p$, it has a solution over $\mathbb{Z}_p$.*

Note that this is an if and only if since we have the projection map $\mathbb{Z}_p \to \mathbb{F}_p$ sending $0 \mapsto 0$.

Proof. We proceed by induction to construct a sequence $a' = (a_i)$ explicitly. In the case $n = 1$, take $a_1 = a$ which is uniquely determined. Suppose we can find unique a_i for all $i \leq n-1$. Suppose $a_n = a_{n-1} + p\epsilon$ for some ϵ that we must find and show uniqueness for.

We have $f(a_n) = f(a_{n-1} + p\epsilon) = f(a_{n-1}) + (p\epsilon) f'(a_{n-1}) + \epsilon^2 g(\epsilon)$, and we know $f(a_{n-1}) = 0 \mod p^{n-1}$, so $f(a_{n-1}) = a p^{n-1} \mod p^n$. We also have that $f'(a_{n-1}) \neq 0$ because f has no repeated factors, so this suggests choosing $\epsilon = -a p^{n-2} f'(a_{n_1})^{-1}$. □

3.4.3 Solutions over *all* $\mathbb{F}_p$ are computable

Theorem 3.1 (Lang, Weil (1954))**.** *Suppose V is a variety in $\mathbb{P}^n$ of dimension r, degree d. Then there exists a constant P depending on n, r, d such that*

$$
|\#V(\mathbb{F}_p) - p^r| \leq (d-1)(d-2) p^{r-1/2} + A(n,d,r) p^{r-1}.
$$

In particular, we can use this to bound the size of p we need to check as supposing $\#V(\mathbb{F}_p) = 0$ for all p and taking a limit as $p \to \infty$ gives a suggestive contradiction. This proves the following:

Theorem 3.2. *It is possible to compute if a polynomial has solutions over $\mathbb{Q}_p$ for all p.*

4 Rational Points Over $\mathbb{Q}$

Notice we have maps $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $\mathbb{Q} \hookrightarrow \mathbb{R}$, so if we can find solutions over $\mathbb{Q}$ we can find solutions over $\mathbb{Q}_p$ for all p and over $\mathbb{R}$. It therefore suffices to show that there are no solutions over any of these fields to see there are no solutions over $\mathbb{Q}$. The other direction for $\mathbb{R}$ is clearly false, take $x^2 - 2$, yet the situation over $\mathbb{Q}_p$ can tell us considerable information about solutions over $\mathbb{Q}$.

4.1 Hasse Principle for Quadratic Forms

Note that in the projective case we're looking for nonzero solutions.

Theorem 4.1 (Hasse-Minkowski)**.** *A quadratic form $f(\underline{x})$ has $f(\underline{x}) - a$ a solution for $a \in \mathbb{Q}$ if and only if it has a solution for all $\mathbb{Q}_p$.*

Proof. See Serre 1973 □

Example 4.1. $x^2 + y^2 - 3$ has no solutions over $\mathbb{F}_5$, so no solutions over $\mathbb{Q}_5$ and no solutions over $\mathbb{Q}$.

This theorem fails for higher degree varieties.

Example 4.2. First, notice $\mathbb{F}_p^\times$ cyclic gives $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$, so $3, -3$, or -1 is square mod $p \geq 5$.

Take $p(x) = (x^2-3)(x^2+1)(x^2+11)$, it has a solution mod $p \geq 5$ by the lemma and the first two factors. It has a solution mod 2 taking $x = 1$, and mod 3 taking $x = 1$ and considering the last term. Yet we see there are no solutions over $\mathbb{Q}$.

4.2 Manin's Obstruction to the Hasse Principle

Let $\mathbb{A} = \mathbb{R} \times \prod_p \mathbb{Q}_\text{ı}$. We've just seen that knowing if there are points over $X(\mathbb{A})$there need not be points over $V(\mathbb{Q})$. Manin found a closed intermediate group which closes in on $V(\mathbb{Q})$, but it was proven by Skorobogatov that this group too is too lax.

$$V(\mathbb{Q}) \subseteq V(\mathbb{A})^{\text{Br}} \subseteq V(\mathbb{A})$$

The Brauer Manin obstruction to the Hasse principle occurs when $V(\mathbb{A})^{\text{Br}} \neq \emptyset$ but $V(\mathbb{A}) = \emptyset$.

Definition 4.1. $\text{Br}(V) := H^2_{et}(V, \mathbb{G}_m)$

Definition 4.2. The Brauer Manin set $V(\mathbb{A})^{\text{Br}}$