Chapter 6

Listable Sets and Diophantine Sets; Hilbert's Tenth Problem

6.1 Diophantine Equations and Hilbert's Tenth Problem

There is a deep and a priori unexpected connection between the theory of computable and listable sets and the solutions of polynomial equations involving polynomials in several variables with integer coefficients.

These are polynomials in $n \geq 1$ variables $x_1, \ldots, x_n$ which are finite sums of *monomials* of the form

$$ax_1^{k_1} \cdots x_n^{k_n},$$

where $k_1, \ldots, k_n \in \mathbb{N}$ are nonnegative integers, and $a \in \mathbb{Z}$ is an integer (possibly negative).

The natural number $k_1 + \cdots + k_n$ is called the *degree* of the monomial $ax_1^{k_1} \cdots x_n^{k_n}$.

For example, if $n = 3$, then

1. $5, \ -7$, are monomials of degree 0.
2. $3x_1, \ -2x_2$, are monomials of degree 1.
3. $x_1x_2, \ 2x_1^2, \ 3x_1x_3, \ -5x_2^2$, are monomials of degree 2.
4. $x_1x_2x_3, \ x_1^2x_3, \ -x_2^3$, are monomials of degree 3.
5. $x_1^4, \ -x_1^2x_3^2, \ x_1x_2^2x_3$, are monomials of degree 4.

Definition 6.1. A *polynomial* $P(x_1, \ldots, x_n)$ in the variables $x_1, \ldots, x_n$ with integer coefficients is a finite sum of monomials of the form $ax_1^{k_1} \cdots x_n^{k_n}$. The maximum of the degrees $k_1 + \cdots + k_n$ of the monomials $ax_1^{k_1} \cdots x_n^{k_n}$. is called the *total degree* of the polynomial $P(x_1, \ldots, x_n)$. The set of all such polynomials is denoted by $\mathbb{Z}[x_1, \ldots, x_n]$.

Sometimes, we write P instead of $P(x_1, \ldots, x_n)$. We also use variables x, y, z *etc.* instead of $x_1, x_2, x_3, \ldots$.

For example, $2x - 3y - 1$ is a polynomial of total degree 1, $x^2 + y^2 - z^2$ is a polynomial of total degree 2, and $x^3 + y^3 + z^3 - 29$ is a polynomial of total degree 3.

Mathematicians have been interested for a long time in the problem of solving equations of the form

$$P(x_1, \ldots, x_n) = 0,$$

with $P \in \mathbb{Z}[x_1, \ldots, x_n]$, seeking only *integer solutions* for $x_1, \ldots, x_n$.

What this means is that we try to find n-tuples of integers $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ such that when we assign the value a_i to the variable x_i for $i = 1, \ldots, n$ in the polynomial $P(x_1, \ldots, x_n)$ and evaluate $P(a_1, \ldots, a_n)$ we obtain $P(a_1, \ldots, a_n) = 0$.

Diophantus of Alexandria, a Greek mathematician of the 3rd century, was one of the first to investigate such equations.

For this reason, seeking integer solutions of polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ is referred to as *solving Diophantine equations*.

This problem is not as simple as it looks. The equation

$$2x - 3y - 1 = 0$$

obviously has the solution $x = 2, y = 1$, and more generally $x = -1 + 3a$, $y = -1 + 2a$, for any integer $a \in \mathbb{Z}$.

The equation

$$x^2 + y^2 - z^2 = 0$$

has the solution $x = 3$, $y = 4$, $z = 5$, since $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

More generally, the reader should check that

$$x = t^2 - 1,\ y = 2t,\ z = t^2 + 1$$

is a solution for all $t \in \mathbb{Z}$.

The equation

$$x^3 + y^3 + z^3 - 29 = 0$$

has the solution $x = 3$, $y = 1$, $z = 1$.

What about the equation

$$x^3 + y^3 + z^3 - 30 = 0?$$

Amazingly, the only known integer solution is

$$(x, y, z) = (-283059965, -2218888517, 2220422932),$$

discovered in 1999 by E. Pine, K. Yarbrough, W. Tarrant, and M. Beck, following an approach suggested by N. Elkies.

And what about solutions of the equation

$$x^3 + y^3 + z^3 - 33 = 0?$$

Until 2019 it was still an open problem but Andrew Booker found the following amazing solution:

$$(8,866,128,975,287,528)^3 + (-8,778,405,442,862,239)^3 + (-2,736,111,468,807,040)^3 = 33.$$

In 1900, at the International Congress of Mathematicians held in Paris, the famous mathematician David Hilbert presented a list of ten open mathematical problems.

Soon after, Hilbert published a list of 23 problems. The tenth problem is this:

Hilbert's tenth problem (H10)

Find an algorithm that solves the following problem:

Given as input a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ with integer coefficients, return YES or NO, according to whether there exist integers $a_1, \ldots, a_n \in \mathbb{Z}$ so that $P(a_1, \ldots, a_n) = 0$; that is, the Diophantine equation $P(x_1, \ldots, x_n) = 0$ has a solution.

It is important to note that at the time Hilbert proposed his tenth problem, a rigorous mathematical definition of the notion of algorithm did not exist.

In fact, the machinery needed to even define the notion of algorithm did not exist.

It is only around 1930 that precise definitions of the notion of computability due to Turing, Church, and Kleene, were formulated, and soon after shown to be all equivalent.

So to be precise, the above statement of Hilbert's tenth should say: find a RAM program (or equivalently a Turing machine) that solves the following problem: ...

In 1970, the following somewhat surprising resolution of Hilbert's tenth problem was reached:

Theorem (Davis-Putnam-Robinson-Matiyasevich)

Hilbert's tenth problem is undecidable; that is, there is no algorithm for solving Hilbert's tenth problem.

Even though Hilbert's tenth problem turned out to have a negative solution, the knowledge gained in developing the methods to prove this result is very significant.

What was revealed is that polynomials have considerable expressive powers.

6.2 Diophantine Sets and Listable Sets

We begin by showing that if we can prove that the version of Hilbert's tenth problem *with solutions restricted to belong to* $\mathbb{N}$ is undecidable, then Hilbert's tenth problem (with solutions in $\mathbb{Z}$ is undecidable).

Proposition 6.1. *If we had an algorithm for solving Hilbert's tenth problem (with solutions in* $\mathbb{Z}$*), then we would have an algorithm for solving Hilbert's tenth problem with solutions restricted to belong to* $\mathbb{N}$ *(that is, nonnegative integers).*

The above statement is not at all obvious, although its proof is short with the help of some number theory.

Indeed, by a theorem of Lagrange (Lagrange's four square theorem), *every* natural number m can be represented as the sum of four squares. This is what is used in the proof of Proposition 6.1.

In fact, the Davis-Putnam-Robinson-Matiyasevich theorem establishes the undecidability of the version of Hilbert's tenth problem restricted to solutions in $\mathbb{N}$.

From now on, we restrict our attention to this version of Hilbert's tenth problem.

A key idea is to use Diophantine equations with parameters, to *define* sets of numbers.

For example, consider the polynomial

$$P_1(a, y, z) = (y + 2)(z + 2) - a.$$

For $a \in \mathbb{N}$ fixed, the equation

$$a = (y + 2)(z + 2)$$

has a solution with $y, z \in \mathbb{N}$ iff a is composite.

If we now consider the polynomial

$$P_2(a, y, z) = y(2z + 3) - a,$$

for $a \in \mathbb{N}$ fixed, the equation

$$a = y(2z + 3)$$

has a solution with $y, z \in \mathbb{N}$ iff a is not a power of 2.

For a slightly more complicated example, consider the polynomial

$$P_3(a, y) = 3y + 1 - a^2.$$

We leave it as an exercise to show that the natural numbers a that satisfy the equation

$$a^2 = 3y + 1$$

are of the form $a = 3k + 1$ or $a = 3k + 2$, for any $k \in \mathbb{N}$.

In the first case, if we let S_1 be the set of composite natural numbers, then we can write

$$S_1 = \{a \in \mathbb{N} \mid (\exists y, z)((y + 2)(z + 2) - a = 0)\},$$

where it is understood that the existentially quantified variables y, z take their values in $\mathbb{N}$.

In the second case, if we let S_2 be the set of natural numbers that are not powers of 2, then we can write

$$S_2 = \{a \in \mathbb{N} \mid (\exists y, z)(y(2z + 3) - a = 0)\}.$$

In the third case, if we let S_3 be the set of natural numbers that are congruent to 1 or 2 modulo 3, then we can write

$$S_3 = \{a \in \mathbb{N} \mid (\exists y)(3y + 1 - a^2 = 0)\}.$$

A more explicit Diophantine definition for S_3 is

$$S_3 = \{a \in \mathbb{N} \mid (\exists y)((a - 3y - 1)(a - 3y - 2) = 0)\}.$$

The natural generalization is as follows.

Definition 6.2. A set $S \subseteq \mathbb{N}$ of natural numbers is *Diophantine* (or *Diophantine definable*) if there is a polynomial $P(x, y_1, \ldots, y_n) \in \mathbb{Z}[x, y_1, \ldots, y_n]$, with $n \geq 0$[1] such that

$$S = \{a \in \mathbb{N} \mid (\exists y_1, \ldots, y_n)(P(a, y_1, \ldots, y_n) = 0)\},$$

where it is understood that the existentially quantified variables $y_1, \ldots, y_n$ take their values in $\mathbb{N}$. Thus $a \in S$ iff there exist some natural numbers $(b_1, \ldots, b_n) \in \mathbb{N}^n$ such that $P(a, b_1, \ldots, b_n) = 0$.

More generally, a relation $R \subseteq \mathbb{N}^m$ is *Diophantine* ($m \geq 2$) if there is a polynomial $P(x_1, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_m, y_1, \ldots, y_n]$, with $n \geq 0$, such that

$$R = \{(a_1, \ldots, a_m) \in \mathbb{N}^m \mid \\ (\exists y_1, \ldots, y_n)(P(a_1, \ldots, a_m, y_1, \ldots, y_n) = 0)\},$$

where it is understood that the existentially quantified variables $y_1, \ldots, y_n$ take their values in $\mathbb{N}$.

Thus $(a_1, \ldots a_m) \in R$ iff there exist some natural numbers $(b_1, \ldots, b_n) \in \mathbb{N}^n$ such that
$P(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0$.

[1] We have to allow $n = 0$. Otherwise singleton sets would not be Diophantine.

At first glance it is not obvious how to "convert" a conjunction of Diophantine definitions into a single Diophantine definition, but we can do this using the following trick: given any finite number of Diophantine equations in the variables $x_1, \ldots, x_n$,

$$P_1 = 0, \ P_2 = 0, \ \ldots, \ P_m = 0, \qquad (*)$$

observe that $(*)$ has a solution $(a_1, \ldots, a_n)$, which means that $P_i(a_1, \ldots, a_n) = 0$ for $i = 1, \ldots, m$, iff the single equation

$$P_1^2 + P_2^2 + \cdots + P_m^2 = 0 \qquad (**)$$

also has the solution $(a_1, \ldots, a_n)$.

Definition 6.3. A (partial) function $f\colon \mathbb{N}^n \to \mathbb{N}$ is *Diophantine* iff its graph $\{(a_1, \ldots, a_n, \, a_{n+1}) \subseteq \mathbb{N}^{n+1} \mid a_{n+1} = f(a_1, \ldots, a_n)\}$ is Diophantine. This means that there is a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_{n+1}, y_1, \ldots, y_p]$, with $p \geq 0$, such that $a_{n+1} = f(a_1, \ldots, a_n)$ iff there exist some natural numbers $(b_1, \ldots, b_p) \in \mathbb{N}^p$ such that $P(a_1, \ldots, a_{n+1}, \, b_1, \ldots, b_p) = 0$. A function $f\colon \mathbb{N}^n \to \mathbb{N}$ is *Diophantine* iff it is Diophantine as a partial function and if it is total. This means that for all $(a_1, \ldots, a_n) \in \mathbb{N}^n$, if $a_{n+1} = f(a_1, \ldots, a_n)$, then the equation $P(a_1, \ldots, a_{n+1}, y_1, \ldots, y_p) = 0$ has a solution (in the variables $y_1, \ldots, y_p$).

How extensive is the family of Diophantine sets?

The remarkable fact proved by Davis-Putnam-Robinson-Matiyasevich is that they coincide with the listable sets (the recursively enumerable sets). This is a highly nontrivial result.

Actually, *the crucial result is that a total function is computable iff it is Diophantine*.

The "easy" direction is the following result.

Proposition 6.2. *Every Diophantine function is (total) computable. Every Diophantine set is listable (recursively enumerable).*

The main theorem of the theory of Diophantine sets is the following deep result.

Theorem 6.3. *(Davis-Putnam-Robinson-Matiyasevich, 1970) Every (total) computable function is Diophantine. Every listable subset of $\mathbb{N}$ is Diophantine.*

Theorem 6.3 is often referred to as the *DPRM theorem.*

As noted by Martin Davis, although the proof is certainly long and nontrivial, it only uses elementary facts of number theory, nothing more sophisticated than the Chinese remainder theorem.

Nevetherless, the proof is a tour de force.

Using some results from the theory of computation it is now easy to deduce that Hilbert's tenth problem is undecidable.

To achieve this, recall that there are listable sets that are not computable.

For example, it is shown in Section 2.5 that
$K = \{x \in \mathbb{N} \mid \varphi_x(x) \text{ is defined}\}$ is listable but not computable.

Since K is listable, by Theorem 6.3, it is defined by some Diophantine equation

$$P(a, x_1, \ldots, x_n) = 0,$$

which means that

$$K = \{a \in \mathbb{N} \mid (\exists x_1 \ldots, x_n)(P(a, x_1, \ldots, x_n) = 0)\}.$$

We have the following strong form of the undecidability of Hilbert's tenth problem, in the sense that it shows that Hilbert's tenth problem is already undecidable for a fixed Diophantine equation in one parameter.

Theorem 6.4. *There is no algorithm which takes as input the polynomial $P(a, x_1, \ldots, x_n)$ defining K and any natural number $a \in \mathbb{N}$ and decides whether*

$$P(a, x_1, \ldots, x_n) = 0.$$

Consequently, Hilbert's tenth problem is undecidable.

It is an open problem whether Hilbert's tenth problem is undecidable if we allow *rational solutions* (that is, $x_1, \ldots, x_n \in \mathbb{Q}$).

6.3 Some Applications of the DPRM Theorem

The first application of the DRPM theorem is a particularly striking way of defining the listable subsets of $\mathbb{N}$ as the nonnegative ranges of polynomials with integer coefficients.

This result is due to Hilary Putnam.

Theorem 6.5. *For every listable subset S of $\mathbb{N}$, there is some polynomial $Q(x, x_1, \ldots, x_n)$ with integer coefficients such that*

$$S = \{Q(a, b_1, \ldots, b_n) \mid Q(a, b_1, \ldots, b_n) \in \mathbb{N},\\ a, b_1, \ldots, b_n \in \mathbb{N}\}.$$

Proof idea. By the DPRM theorem (Theorem 6.3), there is some polynomial $P(x, x_1, \ldots, x_n)$ with integer coefficients such that

$$S = \{a \in \mathbb{N} \mid (\exists x_1, \ldots, x_n)(P(a, x_1, \ldots, x_n) = 0)\}.$$

Let $Q(x, x_1, \ldots, x_n)$ be given by

$$Q(x, x_1, \ldots, x_n) = (x+1)(1 - P^2(x, x_1, \ldots, x_n)) - 1.$$

We claim that Q satisfies the statement of the theorem. $\square$

Remark: It should be noted that in general, the polynomials Q arising in Theorem 6.5 may take on negative integer values, and to obtain all listable sets, we must restrict ourself to their nonnegative range.

As an example, the set S_3 of natural numbers that are congruent to 1 or 2 modulo 3 is given by

$$S_3 = \{a \in \mathbb{N} \mid (\exists y)(3y + 1 - a^2 = 0)\}.$$

so by Theorem 6.5, S_3 is the nonnegative range of the polynomial

$$\begin{aligned} Q(x, y) &= (x+1)(1 - (3y + 1 - x^2)^2)) - 1 \\ &= -(x+1)((3y - x^2)^2 + 2(3y - x^2))) - 1 \\ &= (x+1)(x^2 - 3y)(2 - (x^2 - 3y)) - 1. \end{aligned}$$

Observe that $Q(x, y)$ takes on negative values. For example, $Q(0, 0) = -1$.

Also, in order for $Q(x, y)$ to be nonnegative, $(x^2 - 3y)(2 - (x^2 - 3y))$ must be positive, but this can only happen if $x^2 - 3y = 1$, that is, $x^2 = 3y + 1$, which is the original equation defining S_3.

There is no miracle. The nonnegativity of $Q(x, x_1, \ldots, x_n)$ must subsume the solvability of the equation $P(x, x_1, \ldots, x_n) = 0$.

A particularly interesting listable set is the set of primes.

By Theorem 6.5, in theory, the set of primes is the positive range of some polynomial with integer coefficients.

Remarkably, some explicit polynomials have been found.

This is a nontrivial task. In particular, the process involves showing that the exponential function is definable, which was the stumbling block of the completion of the DPRM theorem for many years.

To give the reader an idea of how the proof begins, observe by the Bezout identity, if $p = s+1$ and $q = s!$, then we can assert that p and q are relatively prime ($\gcd(p, q) = 1$) as the fact that the Diophantine equation

$$ap - bq = 1$$

is satisfied for some $a, b \in \mathbb{N}$.

Then, it is not hard to see that $p \in \mathbb{N}$ is prime iff the following set of equations has a solution for $a, b, s, r, q \in \mathbb{N}$:

$$\begin{aligned} p &= s + 1 \\ p &= r + 2 \\ q &= s! \\ ap - bq &= 1. \end{aligned}$$

The problem with the above is that the equation $q = s!$ is not Diophantine.

The next step is to show that the factorial function is Diophantine, and this involves a lot of work.

One way to proceed is to show that the above system is equivalent to a system allowing the use of the exponential function.

The final step is to show that the exponential function can be eliminated in favor of polynomial equations.

Here is a polynomial of total degree 25 in 26 variables (due to J. Jones, D. Sato, H. Wada, D. Wiens) which produces the primes as its positive range:

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

Around 2004, Nachi Gupta, an undergraduate student at Penn, and I, tried to produce the prime 2 as one of the values of the positive range of the above polynomial.

It turns out that this leads to values of the variables that are so large that we never succeeded!

6.4 Gödel's Incompleteness Theorem

Gödel published his famous incompleteness theorem in 1931.

At the time, his result rocked the mathematical world, and certainly the community of logicians.

In order to understand why his result had such impact one needs to step back in time.

In the late 1800's, Hilbert had advanced the thesis that it should be possible to completely formalize mathematics in such a way that every true statement should be provable "mechanically."

In modern terminology, Hilbert believed that one could design a theorem prover that should be complete. His quest is known as *Hilbert's program*.

In order to achieve his goal, Hilbert was led to investigate the notion of proof, and with some collaborators including Ackerman, Hilbert developed a significant amount of what is known as *proof theory*.

When the young Gödel announced his incompleteness theorem, Hilbert's program came to an abrupt halt. Even the quest for a complete proof system for arithmetic was impossible.

It should be noted that when Gödel proved his incompleteness theorem, computability theory basically did not exist, so Gödel had to start from scratch. His proof is really a tour de force.

Gödel's theorem also triggered extensive research on the notion of computability and undecidability between 1931 and 1936, the major players being Church, Gödel himself, Herbrand, Kleene, Rosser, Turing, and Post.

In this section we will give a (deceptively) short proof that relies on the DPRM and the existence of universal functions.

The proof is short because the hard work lies in the proof of the DPRM!

The first step is to translate the fact that there is a universal partial computable function φ_{univ} (see Proposition 2.5), such that for all $x, y \in \mathbb{N}$, if φ_x is the xth partial computable function, then

$$\varphi_x(y) = \varphi_{univ}(x, y).$$

Also recall from Definition 3.6 that for any acceptable indexing of the partial computable functions, the listable (c.e. r.e.) sets W_x are given by

$$W_x = dom(\varphi_x), \quad x \in \mathbb{N}.$$

Since φ_{univ} is a partial computable function, it can be converted into a Diophantine equation so that we have the following result.

Theorem 6.6. *(Universal Equation Theorem) There is a Diophantine equation* $U(m, a, x_1, \ldots x_\nu) = 0$ *such that for every listable (c.e., r.e.) set* W_m *(*$m \in \mathbb{N}$*) we have*

$$a \in W_m \quad \textit{iff} \quad (\exists x_1, \ldots, x_\nu)(U(m, a, x_1, \ldots, x_\nu) = 0).$$

The Diophantine equation $U(m, a, x_1, \ldots x_\nu) = 0$ is called a *universal Diophantine equation*. It is customary to denote $U(m, a, x_1, \ldots x_\nu)$ by $P_m(a, x_1, \ldots, x_\nu)$.

Gödel's incompleteness theorem applies to sets of logical (first-order) formulae of arithmetic built from the mathematical symbols $0, S, +, \cdot, <$ and the logical connectives $\wedge, \vee, \neg, \Rightarrow, =, \forall, \exists$.

Recall that logical equivalence, $\equiv$, is defined by

$$P \equiv Q \quad \text{iff} \quad (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

The term

$$\underbrace{S(S(\cdots(S}_{n}(0))\cdots))$$

is denoted by $S^n(0)$, and represents the natural number n.

For example,

$$\exists x(S(S(S(0))) < (S(S(0)) + x)),$$

$$\exists x \exists y \exists z((0 < x) \land (0 < y) \land (0 < z) \land ((x \cdot x + y \cdot y) = z \cdot z)),$$

and

$$\begin{aligned} &\forall x \forall y \forall z((0 < x) \land (0 < y) \land (0 < z) \Rightarrow \\ &\qquad \neg((x \cdot x \cdot x \cdot x + y \cdot y \cdot y \cdot y) = z \cdot z \cdot z \cdot z)) \end{aligned}$$

are formulae in the language of arithmetic.

All three are true. The first formula is satisfied by $x = S(S(0))$, the second by $x = S^3(0), y = S^4(0)$ and $z = S^5(0)$ (since $3^2 + 4^2 = 9 + 16 = 25 = 5^2$), and the third formula asserts a special case of *Fermat's famous theorem*:

for every $n \geq 3$, the equation $x^n + y^n = z^n$ has *no solution* with $x, y, z \in \mathbb{N}$ and $x > 0, y > 0, z > 0$.

The third formula corrresponds to $n = 4$. Even for this case, the proof is hard.

To be completely rigorous we should explain precisely what is a formal proof.

Roughly speaking, a proof system consists of axioms and inference rule.

A proof is a certain kind of tree whose nodes are labeled with formulae, and this tree is constructed in such a way that for every node some inference rule is applied.

Given a polynomial $P(x_1, \ldots, x_m)$ in $\mathbb{Z}[x_1, \ldots, x_m]$, we need a way to "prove" that some natural numbers $n_1, \ldots,$ $n_m \in \mathbb{N}$ are a solution of the Diophantine equation

$$P(x_1, \ldots, x_m) = 0,$$

which means that we need to have enough formulae of arithmetic to allow us to simplify the expression $P(n_1, \ldots, n_m)$ and check whether or not it is equal to zero.

For example, if $P(x, y) = 2x - 3y - 1$, we have the solution $x = 2$ and $y = 1$.

What we do is to group all monomials with positive signs, $2x$, and all monomials with negative signs, $3y + 1$, plug in the values for x and y, simplify using the arithmetic tables for $+$ and $\cdot$, and then compare the results.

If they are equal, then we proved that the equation has a solution.

In our language, $x = S^2(0)$, $2x = S^2(0) \cdot x$, and $y = S^1(0)$, $3y + 1 = S^3(0) \cdot y + S(0)$. We need to simplify the expressions

$$2x = S^2(0) \cdot S^2(0) \quad \text{and} \quad 3y + 1 = S^3(0) \cdot S(0) + S(0).$$

Using the formulae

$$\begin{aligned} S^m(0) + S^n(0) &= S^{m+n}(0) \\ S^m(0) \cdot S^n(0) &= S^{mn}(0) \\ S^m(0) < S^n(0) &\quad \text{iff} \quad m < n, \end{aligned}$$

with $m, n \in \mathbb{N}$, we simplify $S^2(0) \cdot S^2(0)$ to $S^4(0)$, $S^3(0) \cdot S(0) + S(0)$ to $S^4(0)$, and we see that the results are equal.

In general, given a polynomial $P(x_1, \ldots, x_m)$ in $\mathbb{Z}[x_1, \ldots, x_m]$, we write it as

$$P(x_1, \ldots, x_m) = P_{\text{pos}}(x_1, \ldots, x_m) - P_{\text{neg}}(x_1, \ldots, x_m),$$

where $P_{\text{pos}}(x_1, \ldots, x_m)$ consists of the monomials with positive coefficients, and $-P_{\text{neg}}(x_1, \ldots, x_m)$ consists of the monomials with negative coefficients.

Next we plug in $S^{n_1}(0)$, ..., $S^{n_m}(0)$ in $P_{\mathrm{pos}}(x_1, \ldots, x_m)$, and evaluate using the formulae for the addition and multiplication tables obtaining a term of the form $S^p(0)$.

Similarly, we plug in $S^{n_1}(0), \ldots, S^{n_m}(0)$ in $P_{\mathrm{neg}}(x_1, \ldots, x_m)$, and evaluate using the formulae for the addition and multiplication tables obtaining a term of the form $S^q(0)$.

Then, since exactly one of the formulae

$$S^p(0) = S^q(0), \quad \text{or} \quad S^p(0) < S^q(0), \quad \text{or} \quad S^q(0) < S^p(0)$$

is true, we obtain a proof that either $P(n_1, \ldots, n_m) = 0$ or $P(n_1, \ldots, n_m) \neq 0$.

A more economical way that does use not an infinite number of formulae expressing the addition and multiplication tables is to use various axiomatizations of arithmetic.

One axiomatization known as *Robinson arithmetic* (R. M. Robinson (1950)) consists of the following seven axioms:

$$\begin{aligned}
&\forall x \neg (S(x) = 0)\\
&\forall x \forall y ((S(x) = S(y)) \Rightarrow (x = y))\\
&\forall y ((y = 0) \lor \exists x (S(x) = y))\\
&\forall x (x + 0 = x)\\
&\forall x \forall y (x + S(y) = S(x + y))\\
&\forall x (x \cdot 0 = 0)\\
&\forall x \forall y (x \cdot S(y) = x \cdot y + x).
\end{aligned}$$

Peano arithmetic is obtained from Robinson arithmetic by adding a rule schema expressing induction:

$$[\varphi(0) \land \forall n(\varphi(n) \Rightarrow \varphi(n+1))] \Rightarrow \forall m\varphi(m),$$

where $\varphi(x)$ is any (first-order) formula of arithmetic. To deal with $<$, we also have the axiom

$$\forall x \forall y(x < y \equiv \exists z(S(z) + x = y)).$$

It is easy to prove that the formulae

$$\begin{aligned} S^m(0) + S^n(0) &= S^{m+n}(0) \\ S^m(0) \cdot S^n(0) &= S^{mn}(0) \\ S^m(0) < S^n(0) &\quad \text{iff} \quad m < n, \end{aligned}$$

are provable in Robinson arithmetic, and thus in Peano arithmetic (with $m, n \in \mathbb{N}$).

Gödel's incompleteness applies to sets $\mathcal{A}$ of formulae of arithmetic that are "nice" and strong enough.

A set $\mathcal{A}$ of formulae is nice if it is listable and *consistent*, which means that it is impossible to prove φ and $\neg\varphi$ from $\mathcal{A}$ for some formula φ. In other words, $\mathcal{A}$ is free of contradictions.

Since the axioms of Peano arithmetic are obviously true statements about $\mathbb{N}$ and since the induction principle holds for $\mathbb{N}$, the set of all formulae provable in Robinson arithmetic and in Peano arithmetic is consistent.

As in Section 5.3, it is possible to assign a Gödel number $\#(A)$ to every first-order sentence A in the language of arithmetic; see Enderton [**?**] (Chapter III) or Kleene I.M. [**?**] (Chapter X).

With a slight abuse of notation, we say that a set T is sentences of arithmetic is computable (*resp.* listable) iff the set of Gödel numbers $\#(A)$ of sentences A in T is computable (*resp.* listable).

It can be shown that the set of all formulae provable in Robinson arithmetic and in Peano arithmetic are listable.

Here is a rather strong version of Gödel's incompleteness from Davis, Matiyasevich and Robinson [**?**].

Theorem 6.7. *(Gödel's Incompleteness Theorem) Let $\mathcal{A}$ be a set of formulae of arithmetic satisfying the following properties:*

(a) The set $\mathcal{A}$ is consistent.

(b) The set $\mathcal{A}$ is listable (c.e., r.e.)

(c) The set $\mathcal{A}$ is strong enough to prove all formulae

$$\begin{aligned} S^m(0) + S^n(0) &= S^{m+n}(0) \\ S^m(0) \cdot S^n(0) &= S^{mn}(0) \\ S^m(0) < S^n(0) &\quad \textit{iff} \quad m < n, \end{aligned}$$

for all $m, n \in \mathbb{N}$.

Then we can construct a Diophantine equation $F(x_1, \ldots, x_\nu) = 0$ corresponding to $\mathcal{A}$ such that $F(x_1, \ldots, x_\nu) = 0$ has **no** *solution with $x_1, \ldots, x_\nu \in \mathbb{N}$ but the formula*

$$\neg(\exists x_1, \ldots, x_\nu)(F(x_1, \ldots, x_\nu) = 0) \qquad (*)$$

is **not** *provable from $\mathcal{A}$. In other words, there is a true statement of arithmetic not provable from $\mathcal{A}$; that is, $\mathcal{A}$ is incomplete.*

As a corollary of Theorem 6.7, since the theorems provable in Robinson arithmetic satisfy (a), (b), (c), we deduce that there are true theorems of arithmetic not provable in Robinson arithmetic; in short, *Robinson arithmetic is incomplete*.

Since Robinson arithmetic does not have induction axioms, this shows that induction is not the culprit behind incompleteness.

Since Peano arithmetic is an extension (consistent) of Robinson arithmetic, *it is also incomplete*.

This is Gödel's original incompleteness theorem, but Gödel had to develop from scratch the tools needed to prove his result, so his proof is very different (and a tour de force).

But the situation is even more dramatic.

Adding a true unprovable statement to a set $\mathcal{A}$ satisfying (a), (b), (c) preserves properties (a), (b), (c), so there is no escape from incompleteness (unless perhaps we allow unreasonable sets of formulae violating (b)).

Gödel's incomplenetess theorem is a negative result, in the sense that it shows that there is no hope of obtaining proof systems capable of proving all true statements for various mathematical theories such as arithmetic.

We can also view Gödel's incomplenetess theorem positively as evidence that mathematicians will never be replaced by computers! There is always room for creativity.

The true but unprovable formulae arising in Gödel's incompleteness theorem are rather contrived and by no means "natural."

For many years after Gödel's proof was published logicians looked for natural incompleteness phenomena.

In the early 1980's such results were found, starting with a result of Kirby and Paris.

Harvey Friedman then found more spectacular instances of natural incompleteness, one of which involves a finite miniaturization of Kruskal's tree theorem.

The proof of such results uses some deep methods of proof theory involving a tool known as *ordinal notations*.

A survey of such results can be found in Gallier [**?**].