More on Hilbert's Tenth Problem

Recall Hilbert's Tenth Problem

Hilbert's 10th problem (in modern language) Give an algorithm that will, given $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Recall Hilbert's Tenth Problem

Hilbert's 10th problem (in modern language) Give an algorithm that will, given $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

By the combined efforts of Davis-Putnam-Robinson (1959) and Matiyasevich (1970) showed the following:

Recall Hilbert's Tenth Problem

Hilbert's 10th problem (in modern language) Give an algorithm that will, given $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

By the combined efforts of Davis-Putnam-Robinson (1959) and Matiyasevich (1970) showed the following:

Thm There is no such algorithm.

Beginning of the Proof that H10 is Undecidable

The proof consists of

Beginning of the Proof that H10 is Undecidable

The proof consists of

1. Show that many sets can be expressed using polynomials.

Beginning of the Proof that H10 is Undecidable

The proof consists of

1. Show that many sets can be expressed using polynomials.
2. Show that HALT can be expressed using polynomials.

Beginning of the Proof that H10 is Undecidable

The proof consists of

1. Show that many sets can be expressed using polynomials.
2. Show that HALT can be expressed using polynomials.

We will discuss expressing sets using polynomials.

Diophantine Sets

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[(a \geq 0) \wedge (p(a_1, \ldots, a_n, a) = 0)].$$

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[(a \geq 0) \wedge (p(a_1, \ldots, a_n, a) = 0)].$$

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[(a \geq 0) \wedge (p(a_1, \ldots, a_n, a) = 0)].$$

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = a].$$

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[(a \geq 0) \wedge (p(a_1, \ldots, a_n, a) = 0)].$$

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = a].$$

The definitions are equivalent.

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[(a \geq 0) \wedge (p(a_1, \ldots, a_n, a) = 0)].$$

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = a].$$

The definitions are equivalent.

We use the first one on slides. We may use second on HW.

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \land (x - 3y = 0)]\}$$

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \pmod 3\}$.

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \pmod 3\}$. Try with neighbor.

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \ (\text{mod } 3)\}$. Try with neighbor.

$$\{x : x \not\equiv 0 \pmod 3\} = \{x : x \equiv 1 \pmod 3\} \cup \{x : x \equiv 2 \pmod 3\}$$

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \pmod 3\}$. Try with neighbor.

$$\{x : x \not\equiv 0 \pmod 3\} = \{x : x \equiv 1 \pmod 3\} \cup \{x : x \equiv 2 \pmod 3\}$$

$$\{x : x \equiv 1 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 1 = 0)]\}$$

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \ (\text{mod } 3)\}$. Try with neighbor.

$$\{x : x \not\equiv 0 \pmod 3\} = \{x : x \equiv 1 \pmod 3\} \cup \{x : x \equiv 2 \pmod 3\}$$

$$\{x : x \equiv 1 \ (\text{mod } 3)\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 1 = 0)]\}$$
$$\{x : x \equiv 2 \ (\text{mod } 3)\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 2 = 0)]\}$$

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \land (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \ (\text{mod } 3)\}$. Try with neighbor.

$$\{x : x \not\equiv 0 \pmod 3\} = \{x : x \equiv 1 \pmod 3\} \cup \{x : x \equiv 2 \pmod 3\}$$

$$\{x : x \equiv 1 \ (\text{mod } 3)\} = \{x : (\exists y)[(x \geq 0) \land (x - 3y - 1 = 0)]\}$$
$$\{x : x \equiv 2 \ (\text{mod } 3)\} = \{x : (\exists y)[(x \geq 0) \land (x - 3y - 2 = 0)]\}$$

Is there a way to combine these? Yes!

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \pmod 3\}$. Try with neighbor.

$$\{x : x \not\equiv 0 \pmod 3\} = \{x : x \equiv 1 \pmod 3\} \cup \{x : x \equiv 2 \pmod 3\}$$

$\{x : x \equiv 1 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 1 = 0)]\}$
$\{x : x \equiv 2 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 2 = 0)]\}$

Is there a way to combine these? Yes!
$\{x : x \not\equiv 0 \pmod 3\} =$

Examples of Dio Sets

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \not\equiv 0 \ (\text{mod } 3)\}$. Try with neighbor.

$$\{x : x \not\equiv 0 \pmod 3\} = \{x : x \equiv 1 \pmod 3\} \cup \{x : x \equiv 2 \pmod 3\}$$

$\{x : x \equiv 1 \ (\text{mod } 3)\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 1 = 0)]\}$
$\{x : x \equiv 2 \ (\text{mod } 3)\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y - 2 = 0)]\}$

Is there a way to combine these? Yes!

$\{x : x \not\equiv 0 \ (\text{mod } 3)\} =$

$$\{x : (\exists y)[(x \geq 0) \wedge ((x - 3y - 1)(x - 3y - 2) = 0)]\}.$$

Dio Sets are Closed Under Union

Let A, B be Dio Sets.

Dio Sets are Closed Under Union

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$

Dio Sets are Closed Under Union

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$
$B = \{x : (\exists z_1, \ldots, z_n)[(x \geq 0) \wedge (p_B(z_1, \ldots, z_n, x) = 0)]\}$

Dio Sets are Closed Under Union

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$
$B = \{x : (\exists z_1, \ldots, z_n)[(x \geq 0) \wedge (p_B(z_1, \ldots, z_n, x) = 0)]\}$

$A \cup B =$
$\{x : (\exists y_1, \ldots, y_n, z_1, \ldots, z_n)$

$$[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) p_B(z_1, \ldots, z_n, x) = 0)]\}.$$

More Examples of Dio Sets

$$\{x : x \text{ is a square }\} = \{x : (\exists y)[(x \geq 0) \wedge (x - y^2 = 0)]\}$$

More Examples of Dio Sets

$$\{x : x \text{ is a square }\} = \{x : (\exists y)[(x \geq 0) \wedge (x - y^2 = 0)]\}$$

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

More Examples of Dio Sets

$$\{x : x \text{ is a square } \} = \{x : (\exists y)[(x \geq 0) \wedge (x - y^2 = 0)]\}$$

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \text{ is a square} \wedge x \equiv 0 \pmod 3\}$.

More Examples of Dio Sets

$$\{x : x \text{ is a square }\} = \{x : (\exists y)[(x \geq 0) \wedge (x - y^2 = 0)]\}$$

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \text{ is a square} \wedge x \equiv 0 \pmod 3\}$. Try with neighbor.

More Examples of Dio Sets

$$\{x : x \text{ is a square }\} = \{x : (\exists y)[(x \geq 0) \wedge (x - y^2 = 0)]\}$$

$$\{x : x \equiv 0 \pmod 3\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 3y = 0)]\}$$

$\{x : x \text{ is a square} \wedge x \equiv 0 \pmod 3\}$. Try with neighbor.

$$= \{x : (\exists y_1, y_2)[(x \geq 0) \wedge ((x - y_1^2)^2 + (x - 3y_2)^2 = 0)]\}.$$

Dio Sets are Closed Under Intersection

Let A, B be Dio Sets.

Dio Sets are Closed Under Intersection

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$

Dio Sets are Closed Under Intersection

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$
$B = \{x : (\exists z_1, \ldots, z_n)[(x \geq 0) \wedge (p_B(z_1, \ldots, z_n, x) = 0)]\}$

Dio Sets are Closed Under Intersection

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$
$B = \{x : (\exists z_1, \ldots, z_n)[(x \geq 0) \wedge (p_B(z_1, \ldots, z_n, x) = 0)]\}$

$A \cap B = \{x : (\exists y_1, \ldots, y_n, z_1, \ldots, z_n)$

$$[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x)^2 + p_B(z_1, \ldots, z_n, x)^2 = 0)]\}.$$

COMP is a Dio Sets

COMP is the set of composites. We show this is Dio.

COMP is a Dio Sets

COMP is the set of composites. We show this is Dio.

$$\mathrm{COMP} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge ((y_1 + 2)(y_2 + 2) - x = 0)]\}.$$

COMP is a Dio Sets

COMP is the set of composites. We show this is Dio.

$$\mathrm{COMP} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge ((y_1 + 2)(y_2 + 2) - x = 0)]\}.$$

PRIMES is the set of primes (duh). Is PRIMES Dio?

COMP is a Dio Sets

COMP is the set of composites. We show this is Dio.

$$\mathrm{COMP} = \{x : (\exists y_1, y_2)[(x \ge 0) \wedge ((y_1 + 2)(y_2 + 2) - x = 0)]\}.$$

PRIMES is the set of primes (duh). Is PRIMES Dio?
No but Yes.

COMP is a Dio Sets

COMP is the set of composites. We show this is Dio.

$$\mathrm{COMP} = \{x : (\exists y_1, y_2)[(x \ge 0) \wedge ((y_1 + 2)(y_2 + 2) - x = 0)]\}.$$

PRIMES is the set of primes (duh). Is PRIMES Dio?
No but Yes. Really **Yes** but its complicated. Uses 26 variables.

COMP is a Dio Sets

COMP is the set of composites. We show this is Dio.

$$\mathrm{COMP} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge ((y_1 + 2)(y_2 + 2) - x = 0)]\}.$$

PRIMES is the set of primes (duh). Is PRIMES Dio?
No but Yes. Really **Yes** but its complicated. Uses 26 variables.
See `https://www.cs.umd.edu/~gasarch/BLOGPAPERS/BurkesMax.pdf`

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two. We show this is Dio

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$$

NOTPOWtwo is a Dio Sets

NOTPOW2 is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$$

POW2 is the set of powers of 2 (duh). Is POW2 Dio?

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \ge 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$

$\mathrm{POW2}$ is the set of powers of 2 (duh). Is $\mathrm{POW2}$ Dio?
No but Yes.

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$

$\mathrm{POW2}$ is the set of powers of 2 (duh). Is $\mathrm{POW2}$ Dio?
No but Yes. Really **yes** but its complicated.

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \ge 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$

$\mathrm{POW2}$ is the set of powers of 2 (duh). Is $\mathrm{POW2}$ Dio?
No but Yes. Really **yes** but its complicated.
This was the reason DPR didn't show H10 undecidable.

NOTPOWtwo is a Dio Sets

$\mathrm{NOTPOW2}$ is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \ge 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$

$\mathrm{POW2}$ is the set of powers of 2 (duh). Is $\mathrm{POW2}$ Dio?
No but Yes. Really **yes** but its complicated.
This was the reason DPR didn't show H10 undecidable.
They were unable to prove this.

NOTPOWtwo is a Dio Sets

NOTPOW2 is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$$

POW2 is the set of powers of 2 (duh). Is POW2 Dio?
No but Yes. Really **yes** but its complicated.
This was the reason DPR didn't show H10 undecidable.
They were unable to prove this.
Why was Matiyasevich able to solve it when DPR were not?

NOTPOWtwo is a Dio Sets

NOTPOW2 is the set of numbers that are NOT powers of two.
We show this is Dio
A number is NOT a power of 2 if it has an odd factor.

$\mathrm{NOTPOW2} = \{x : (\exists y_1, y_2)[(x \geq 0) \wedge (y_1(2y_2 + 3) - x = 0)]\}$

POW2 is the set of powers of 2 (duh). Is POW2 Dio?
No but Yes. Really **yes** but its complicated.
This was the reason DPR didn't show H10 undecidable.
They were unable to prove this.
Why was Matiyasevich able to solve it when DPR were not?

Next Slide

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book
Fibonacci Numbers by Vorobov, third edition.

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book
Fibonacci Numbers by Vorobov, third edition.
He found the key theorem there:

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book

Fibonacci Numbers by Vorobov, third edition.

He found the key theorem there:

If F_n^2 divides F_m then F_n divides m.

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book
Fibonacci Numbers by Vorobov, third edition.
He found the key theorem there:
If F_n^2 divides F_m then F_n divides m.
Robinson did have the same book (yeah!),

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book
Fibonacci Numbers by Vorobov, third edition.
He found the key theorem there:
If F_n^2 divides F_m then F_n divides m.
Robinson did have the same book (yeah!),
but a different edition which didn't have that thm (boo!).

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book
Fibonacci Numbers by Vorobov, third edition.
He found the key theorem there:
If F_n^2 divides F_m then F_n divides m.
Robinson did have the same book (yeah!),
but a different edition which didn't have that thm (boo!) .

Wow

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book

Fibonacci Numbers by Vorobov, third edition.

He found the key theorem there:

If F_n^2 divides F_m then F_n divides m.

Robinson did have the same book (yeah!),
but a different edition which didn't have that thm (boo!) .

Wow Who discovers what can be arbitrary!

A Short Episode in the History of H10

From **The Honor Class: Hilbert's Problems and their Solvers** by Ben Yandell:

All four of them had been reading up on obscure facts in Number Theory that might help them.
Yuri was looking at the book

Fibonacci Numbers by Vorobov, third edition.

He found the key theorem there:

If F_n^2 divides F_m then F_n divides m.

Robinson did have the same book (yeah!),
but a different edition which didn't have that thm (boo!) .

Wow Who discovers what can be arbitrary!

Note I reviewed the book here:
https://www.cs.umd.edu/~gasarch/bookrev/44-4.pdf

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.
Assume BWOC, there's an algorithm. Then we can solve HALT:

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.
Assume BWOC, there's an algorithm. Then we can solve HALT:

1. Input a

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.
Assume BWOC, there's an algorithm. Then we can solve HALT:

1. Input a
2. Form the polynomial $q(x_1, \ldots, x_8) = p(x_1, \ldots, x_8, a)$.

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.
Assume BWOC, there's an algorithm. Then we can solve HALT:

1. Input a
2. Form the polynomial $q(x_1, \ldots, x_8) = p(x_1, \ldots, x_8, a)$.
3. Use the algorithm to determine if there exists $a_1, \ldots, a_8$ such that $q(a_1, \ldots, a_8) = 0$.

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .

Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.

Assume BWOC, there's an algorithm. Then we can solve HALT:

1. Input a
2. Form the polynomial $q(x_1, \ldots, x_8) = p(x_1, \ldots, x_8, a)$.
3. Use the algorithm to determine if there exists $a_1, \ldots, a_8$ such that $q(a_1, \ldots, a_8) = 0$.
   If YES then output YES.

Back to the Proof

The final step of the proof was to show that HALT is **Dio** .
Thm There exists a polynomial $p(x_1, \ldots, x_9)$ over $\mathbb{Z}$ such that $a \in \mathrm{HALT}$ iff $(\exists a_1, \ldots, a_8 \in \mathbb{Z})[p(a_1, \ldots, a_8, a) = 0]$.

Cor There is no algorithm that will, given a polynomial $q(x_1, \ldots, x_8)$ over $\mathbb{Z}$, determine if there exists $a_1, \ldots, a_8 \in \mathbb{Z}$ such that $q(a_1, \ldots, a_8) = 0$.
Assume BWOC, there's an algorithm. Then we can solve HALT:

1. Input a
2. Form the polynomial $q(x_1, \ldots, x_8) = p(x_1, \ldots, x_8, a)$.
3. Use the algorithm to determine if there exists $a_1, \ldots, a_8$ such that $q(a_1, \ldots, a_8) = 0$.
   If YES then output YES.
   If NOT then output NO.

Decidable and Undecidable Theories

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

1. Input a mathematical statement.

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

1. Input a mathematical statement.
   Example $(\forall x, y, z \in \mathbb{N})(\forall n \in \mathbb{N}, n \geq 3)[x^n + y^n \neq z^n]$

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

1. Input a mathematical statement.
   Example $(\forall x, y, z \in \mathbb{N})(\forall n \in \mathbb{N}, n \geq 3)[x^n + y^n \neq z^n]$
   Thats Fermat's last theorem.

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

1. Input a mathematical statement.
   Example $(\forall x, y, z \in \mathbb{N})(\forall n \in \mathbb{N}, n \geq 3)[x^n + y^n \neq z^n]$
   Thats Fermat's last theorem.
   Example Domain is set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.
   $(\forall f)[(f(0) < 0 \wedge f(1) > 0) \rightarrow (\exists 0 < z < 1)[f(z) = 0]]$

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

1. Input a mathematical statement.
   Example $(\forall x, y, z \in \mathbb{N})(\forall n \in \mathbb{N}, n \geq 3)[x^n + y^n \neq z^n]$
   Thats Fermat's last theorem.
   Example Domain is set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.
   $(\forall f)[(f(0) < 0 \wedge f(1) > 0) \rightarrow (\exists 0 < z < 1)[f(z) = 0]]$
   This is the intermediate value theorem.

Decidable and Undecidable Theories

Hilbert wanted to (in modern language) show there was an algorithm that would do the following.

1. Input a mathematical statement.
   Example $(\forall x, y, z \in \mathbb{N})(\forall n \in \mathbb{N}, n \geq 3)[x^n + y^n \neq z^n]$
   Thats Fermat's last theorem.
   Example Domain is set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.
   $(\forall f)[(f(0) < 0 \land f(1) > 0) \rightarrow (\exists 0 < z < 1)[f(z) = 0]]$
   This is the intermediate value theorem.
2. Output if the statement is TRUE or FALSE.

H10 AS AN UNDEC THEORY

How to Formalize and Refine Hilbert's Goal

How to Formalize and Refine Hilbert's Goal

1. Need a language to make mathematical statements.

How to Formalize and Refine Hilbert's Goal

1. Need a language to make mathematical statements.
2. Need to know the domain of discourse for variables.

How to Formalize and Refine Hilbert's Goal

1. Need a language to make mathematical statements.
2. Need to know the domain of discourse for variables.

Was Hilbert's Goal Achieved?

How to Formalize and Refine Hilbert's Goal

1. Need a language to make mathematical statements.
2. Need to know the domain of discourse for variables.

Was Hilbert's Goal Achieved?

No. Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

How to Formalize and Refine Hilbert's Goal

1. Need a language to make mathematical statements.
2. Need to know the domain of discourse for variables.

Was Hilbert's Goal Achieved?

No. Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

We will derive Godel's Theorem easily from H10 being undecidable.

How to Formalize and Refine Hilbert's Goal

1. Need a language to make mathematical statements.
2. Need to know the domain of discourse for variables.

Was Hilbert's Goal Achieved?

No. Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

We will derive Godel's Theorem easily from H10 being undecidable.

The original proof was much harder.

"Powerful Enough"

“Powerful Enough”

Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

“Powerful Enough”

Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

What about weak languages?

“Powerful Enough”

Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

What about weak languages?

1. In this set of slides we will show a theory that is undecidable.

“Powerful Enough”

Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

What about weak languages?

1. In this set of slides we will show a theory that is undecidable.
2. We will then state it as Godel would have.

"Powerful Enough"

Godel showed that if the language was **powerful enough** then there could be no algorithm to determine truth.

What about weak languages?

1. In this set of slides we will show a theory that is undecidable.
2. We will then state it as Godel would have.
3. Later we will look at theories that are decidable.

Formulas and Sentences

Formulas and Sentences

1. A **Formula** allows variables to not be quantified over. A Formula is neither true or false. Example: $(\exists x)[x + y = 7]$.

Formulas and Sentences

1. A **Formula** allows variables to not be quantified over. A Formula is neither true or false. Example: $(\exists x)[x + y = 7]$.
2. A **Sentence** has all variables quantified over. Example: $(\forall y)(\exists x)[x + y = 7]$. So a Sentence is either true or false.

Formulas and Sentences

1. A **Formula** allows variables to not be quantified over. A Formula is neither true or false. Example: $(\exists x)[x + y = 7]$.
2. A **Sentence** has all variables quantified over. Example: $(\forall y)(\exists x)[x + y = 7]$. So a Sentence is either true or false. **Wrong** –need to also know the domain.
   $(\forall y)(\exists x)[x + y = 7]$— **T** if domain is $\mathbb{Z}$, the integers.

Formulas and Sentences

1. A **Formula** allows variables to not be quantified over. A Formula is neither true or false. Example: $(\exists x)[x + y = 7]$.
2. A **Sentence** has all variables quantified over. Example: $(\forall y)(\exists x)[x + y = 7]$. So a Sentence is either true or false.
   Wrong –need to also know the domain.
   $(\forall y)(\exists x)[x + y = 7]$— **T** if domain is $\mathbb{Z}$, the integers.
   $(\forall y)(\exists x)[x + y = 7]$— **F** if domain is $\mathbb{N}$, the naturals.

Variables and Symbols

We formulate H10 undecidable in these terms. Consider the following language.

Variables and Symbols

We formulate H10 undecidable in these terms. Consider the following language.

1. The logical symbols $\wedge$, $\neg$, $(\exists)$.

Variables and Symbols

We formulate H10 undecidable in these terms. Consider the following language.

1. The logical symbols $\wedge$, $\neg$, $(\exists)$.
2. We use $\vee$ and $\forall$ as shorthand–can be converted to $\wedge$ and $\exists$.

Variables and Symbols

We formulate H10 undecidable in these terms. Consider the following language.

1. The logical symbols $\wedge$, $\neg$, ($\exists$).
2. We use $\vee$ and $\forall$ as shorthand–can be converted to $\wedge$ and $\exists$.
3. Variables $x, y, z, \ldots$ that range over $\mathbb{Z}$.

Variables and Symbols

We formulate H10 undecidable in these terms. Consider the following language.

1. The logical symbols $\wedge$, $\neg$, $(\exists)$.
2. We use $\vee$ and $\forall$ as shorthand–can be converted to $\wedge$ and $\exists$.
3. Variables $x, y, z, \ldots$ that range over $\mathbb{Z}$.
4. Constants: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$.

Variables and Symbols

We formulate H10 undecidable in these terms. Consider the following language.

1. The logical symbols $\wedge$, $\neg$, $(\exists)$.
2. We use $\vee$ and $\forall$ as shorthand–can be converted to $\wedge$ and $\exists$.
3. Variables $x, y, z, \ldots$ that range over $\mathbb{Z}$.
4. Constants: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$.
5. The symbols $+$, $\times$, and $=$.

Examples of Formulas and Sentences

Formula
$x^2 + 3y - 10xy + z^3 = 0$
NONE of x, y, X are quantified over, so its a formula.

Formula $(\exists x)[x^2 + 3y - 10xy + z^3 = 0]$
There is a var not quantified over.

Examples of Formulas and Sentences

Formula
$x^2 + 3y - 10xy + z^3 = 0$
NONE of x, y, X are quantified over, so its a formula.

Formula $(\exists x)[x^2 + 3y - 10xy + z^3 = 0]$
There is a var not quantified over.

Sentence
$(\exists x, y, z)[x^2 + 3y - 10xy + z^3 = 0]$
ALL of the vars are quantified over.

Atomic Formulas

An **Atomic Formula** is:

Atomic Formulas

An **Atomic Formula** is:

1. For any polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$

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

is an Atomic Formula.

H10 Formulas

A **H10 Formula** is:

H10 Formulas

A **H10 Formula** is:

1. Any Atomic Formula is a H10 Formula.

H10 Formulas

A **H10 Formula** is:

1. Any Atomic Formula is a H10 Formula.
2. If ϕ_1, ϕ_2 are H10 Formulas then so are

H10 Formulas

A **H10 Formula** is:

1. Any Atomic Formula is a H10 Formula.
2. If ϕ_1, ϕ_2 are H10 Formulas then so are
    2.1 $\phi_1 \wedge \phi_2$,

H10 Formulas

A **H10 Formula** is:

1. Any Atomic Formula is a H10 Formula.
2. If ϕ_1, ϕ_2 are H10 Formulas then so are
   2.1 $\phi_1 \wedge \phi_2$,
   2.2 $\phi_1 \vee \phi_2$

H10 Formulas

A **H10 Formula** is:

1. Any Atomic Formula is a H10 Formula.
2. If ϕ_1, ϕ_2 are H10 Formulas then so are
    2.1 $\phi_1 \wedge \phi_2$,
    2.2 $\phi_1 \vee \phi_2$
    2.3 $\neg\phi_1$

H10 Formulas

A **H10 Formula** is:

1. Any Atomic Formula is a H10 Formula.
2. If ϕ_1, ϕ_2 are H10 Formulas then so are
   2.1 $\phi_1 \wedge \phi_2$,
   2.2 $\phi_1 \vee \phi_2$
   2.3 $\neg\phi_1$
3. If $\phi(x_1, \ldots, x_n)$ is a H10 Formula then so is $(\exists x_i)[\phi(x_1, \ldots, x_n)]$

The Poly Theory of the Integers

Is the following problem decidable?

The Poly Theory of the Integers

Is the following problem decidable?

- Input ϕ, a sentence in H10.

The Poly Theory of the Integers

Is the following problem decidable?

- Input ϕ, a sentence in H10.
- Determine if ϕ is TRUE.

The Poly Theory of the Integers

Is the following problem decidable?

- Input ϕ, a sentence in H10.
- Determine if ϕ is TRUE.

Since H10 is undecidable, this problem is NOT decidable.

The Poly Theory of the Integers

Is the following problem decidable?

- Input ϕ, a sentence in H10.
- Determine if ϕ is TRUE.

Since H10 is undecidable, this problem is NOT decidable.

In fact, H10 restricted to just $\exists$-statements is undecidable.

H10 Implies Godel's Inc Theorem

How Godel Would Have Stated It

In the popular press Godel's Inc Theorem is quoted as:

How Godel Would Have Stated It

In the popular press Godel's Inc Theorem is quoted as:
There are statements in Math that are TRUE but not PROVABLE

How Godel Would Have Stated It

In the popular press Godel's Inc Theorem is quoted as:
There are statements in Math that are TRUE but not PROVABLE

Unlike many comments about math in the popular press this one is true.

How Godel Would Have Stated It

In the popular press Godel's Inc Theorem is quoted as:
There are statements in Math that are TRUE but not PROVABLE

Unlike many comments about math in the popular press this one is true.
However, we need to state Godel's inc Thm more carefully.

Peano Arithmetic (PA)

Def Peano Arithmetic (PA) is the following set of axioms and rules of inference

Peano Arithmetic (PA)

Def Peano Arithmetic (PA) is the following set of axioms and rules of inference

We are busy people so we are not going to bother with the particular axioms of PA. We will note that (1) PA has $+$, $\times$, (2) PA allows the use of induction, (3) PA uses domain $\mathbb{N}$ though can be extended to $\mathbb{Z}$, and (4) Virtually every thm in Number Theory can be derived in PA.

Peano Arithmetic (PA)

Def Peano Arithmetic (PA) is the following set of axioms and rules of inference
We are busy people so we are not going to bother with the particular axioms of PA. We will note that (1) PA has $+$, $\times$, (2) PA allows the use of induction, (3) PA uses domain $\mathbb{N}$ though can be extended to $\mathbb{Z}$, and (4) Virtually every thm in Number Theory can be derived in PA.

Godel showed that there is a statement ϕ such that

Peano Arithmetic (PA)

Def Peano Arithmetic (PA) is the following set of axioms and rules of inference

We are busy people so we are not going to bother with the particular axioms of PA. We will note that (1) PA has $+$, $\times$, (2) PA allows the use of induction, (3) PA uses domain $\mathbb{N}$ though can be extended to $\mathbb{Z}$, and (4) Virtually every thm in Number Theory can be derived in PA.

Godel showed that there is a statement ϕ such that

1. ϕ is TRUE.

Peano Arithmetic (PA)

Def Peano Arithmetic (PA) is the following set of axioms and rules of inference

We are busy people so we are not going to bother with the particular axioms of PA. We will note that (1) PA has $+$, $\times$, (2) PA allows the use of induction, (3) PA uses domain $\mathbb{N}$ though can be extended to $\mathbb{Z}$, and (4) Virtually every thm in Number Theory can be derived in PA.

Godel showed that there is a statement ϕ such that

1. ϕ is TRUE.
2. ϕ cannot be derived from PA.

Peano Arithmetic (PA)

Def Peano Arithmetic (PA) is the following set of axioms and rules of inference

We are busy people so we are not going to bother with the particular axioms of PA. We will note that (1) PA has $+$, $\times$, (2) PA allows the use of induction, (3) PA uses domain $\mathbb{N}$ though can be extended to $\mathbb{Z}$, and (4) Virtually every thm in Number Theory can be derived in PA.

Godel showed that there is a statement ϕ such that

1. ϕ is TRUE.
2. ϕ cannot be derived from PA.

This is impressive since almost all of number theory can be derived in PA.

Whats so Special about Peano Arithmetic?

Godel's technique applies to **any** (with caveats) system that has $+$ and $\times$. So its not really about PA.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity
   2.1 Find all statements that can be derived in PA using $\leq s$ steps.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity
   2.1 Find all statements that can be derived in PA using $\leq s$ steps.
   2.2 If one of them is $(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output YES and halt.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity
   2.1 Find all statements that can be derived in PA using $\leq s$ steps.
   2.2 If one of them is $(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output YES and halt.
   2.3 If one of them is $\neg(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output NO and halt.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity
   2.1 Find all statements that can be derived in PA using $\leq s$ steps.
   2.2 If one of them is $(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output YES and halt.
   2.3 If one of them is $\neg(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output NO and halt.
   2.4 If neither of those happens then go to the next s

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity
   2.1 Find all statements that can be derived in PA using $\leq s$ steps.
   2.2 If one of them is $(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output YES and halt.
   2.3 If one of them is $\neg(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output NO and halt.
   2.4 If neither of those happens then go to the next s

Since we are assuming **every** true statement is derivable in PA, then this algorithm must terminate and correctly determine if $p(x_1, \ldots, x_n)$ has an integer solution.

H10 undecidable implies Godel's Inc. Theorem

We will use PA for concreteness.

Assume, BWOC, that every TRUE ϕ was provable in PA.
The following algorithm solves H10, a contradiction.

1. Input $p(x_1, \ldots, x_n)$. So we are asking if $(\exists a_1, \ldots, a_n)[p(a_1, \ldots, a_n) = 0]$ is TRUE.
2. For $s = 1$ to infinity
   2.1 Find all statements that can be derived in PA using $\leq s$ steps.
   2.2 If one of them is $(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output YES and halt.
   2.3 If one of them is $\neg(\exists x_1, \ldots, x_n)[p(x_1, \ldots, x_n) = 0]$ then output NO and halt.
   2.4 If neither of those happens then go to the next s

Since we are assuming **every** true statement is derivable in PA, then this algorithm must terminate and correctly determine if $p(x_1, \ldots, x_n)$ has an integer solution. Contradiction!

Variants of H10

Bound the Degree and the Number of Vars

I covered this last lecture so I will just give the take-away.

Bound the Degree and the Number of Vars

I covered this last lecture so I will just give the take-away.
Let d be the degree and n be the number of variables.
There is a grid of (d, n) where

Bound the Degree and the Number of Vars

I covered this last lecture so I will just give the take-away.
Let d be the degree and n be the number of variables.
There is a grid of (d, n) where

1. For small values of d, n H10 is decidable.

Bound the Degree and the Number of Vars

I covered this last lecture so I will just give the take-away.
Let d be the degree and n be the number of variables.
There is a grid of (d, n) where

1. For small values of d, n H10 is decidable.
2. For large values of d, n H10 is undecidable.

Bound the Degree and the Number of Vars

I covered this last lecture so I will just give the take-away.
Let d be the degree and n be the number of variables.
There is a grid of (d, n) where

1. For small values of d, n H10 is decidable.
2. For large values of d, n H10 is undecidable.
3. There is are many d, n for which this is unknown.

Bound the Degree and the Number of Vars

I covered this last lecture so I will just give the take-away.
Let d be the degree and n be the number of variables.
There is a grid of (d, n) where

1. For small values of d, n H10 is decidable.
2. For large values of d, n H10 is undecidable.
3. There is are many d, n for which this is unknown.
4. Resolving the ones that are unknown seems hard.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$. Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$. **Unknown to Science!** Matiyasevich thinks this may be what Hilbert meant to ask and that it would lead to Number Theory of Interest.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$. **Unknown to Science!** Matiyasevich thinks this may be what Hilbert meant to ask and that it would lead to Number Theory of Interest.
4. $\mathbb{D} = \mathbb{R}$.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$. **Unknown to Science!** Matiyasevich thinks this may be what Hilbert meant to ask and that it would lead to Number Theory of Interest.
4. $\mathbb{D} = \mathbb{R}$. **Decidable** . Tarski-Seidenberg (1974)

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$. **Unknown to Science!** Matiyasevich thinks this may be what Hilbert meant to ask and that it would lead to Number Theory of Interest.
4. $\mathbb{D} = \mathbb{R}$. **Decidable** . Tarski-Seidenberg (1974)
5. $\mathbb{D} = \mathbb{C}$.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$. **Unknown to Science!** Matiyasevich thinks this may be what Hilbert meant to ask and that it would lead to Number Theory of Interest.
4. $\mathbb{D} = \mathbb{R}$. **Decidable** . Tarski-Seidenberg (1974)
5. $\mathbb{D} = \mathbb{C}$. **Decidable** but trivial: always true.

Different Domain For the Solution

We've been talking about H10 where we seek a solution in $\mathbb{Z}$.
Let $\mathbb{D} \subseteq \mathbb{C}$. **H10 for $\mathbb{D}$** is the following problem: Given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathbb{D}$ such that $p(a_1, \ldots, a_n) = 0$?

1. $\mathbb{D} = \mathbb{N}$. **Undecidable**
2. $\mathbb{D} = \mathbb{Z}$. **Undecidable**
3. $\mathbb{D} = \mathbb{Q}$. **Unknown to Science!** Matiyasevich thinks this may be what Hilbert meant to ask and that it would lead to Number Theory of Interest.
4. $\mathbb{D} = \mathbb{R}$. **Decidable** . Tarski-Seidenberg (1974)
5. $\mathbb{D} = \mathbb{C}$. **Decidable** but trivial: always true.
6. Other domains: Mostly unknown.