# Hilbert 10th Problem

Thursday, January 14, 2016 4:20 PM

**Def** · A function is computable if $\exists$ algorithm to compute it

· A set $\subset \mathbb{Z}^n$ is computable if its char func is computable

· A set is semi-computable if it's image of a computable set

**Example**: {prime numbers} computable

{numbers = sum of three cubes}

**Thm** $\exists$ semi-comp set that's not computable

**Pf**: $\mathbb{N}$ = {all algorithm}

$X \subset \mathbb{N}$ set of programs such that

**Def** A set $X \subset \mathbb{Z}^n$ is Diophantine if $\exists F$ s.t.

$$X = \{ (x_1, \cdots, x_n) \mid \exists (y_1, \cdots, y_m) \text{ s.t. } F(x_1, \cdots, x_n, y_1, \cdots, y_m) = 0 \}$$

**Thm** Semi-computable $\Leftrightarrow$ Diophantine

If H's 10th were true: Diophantine $\Rightarrow$ computable

Then Semi-comput $\Rightarrow$ comput contradiction!

**Exp**: {even numbers} $\subset \mathbb{Z}$ — Diophantine — $\{x \mid \exists y \text{ s.t. } x - 2y = 0\}$

{positi numbers} $\subset \mathbb{Z}$ — $\{x \mid \exists y_1, \cdots, y_4 \text{ s.t. } x = y_1^2 + \cdots + y_4^2\}$

A binary relation $R$ on $\mathbb{Z}^n$ is Diophantine if

$\{(x, y) \in \mathbb{Z}^n \times \mathbb{Z}^n \mid R(x, y)\}$ is Diaphantine.

**Exp** • $\leq$ on $\mathbb{Z}$ is Diophantine

- divisibility is Diophantine
- Congruence is Diophantine
- $\{(x,y) \mid x \text{ and } y \text{ are coprime}\}$ is Diophantine

A function $f: \mathbb{Z}^n \to \mathbb{Z}^n$ is Diophantine if $\{(x,y) \mid y = f(x)\}$ is

Exp: · The function remainder : $\mathbb{Z}^2 \longrightarrow \mathbb{Z}$ is Diophantine
$(a,b) \longmapsto \text{rem}(a,b)$

· Quo : $\mathbb{Z}^2 \to \mathbb{Z}$
$(a,b) \mapsto [\frac{a}{b}]$

Thm Exp is Diophantine (Matiyasevic)
$\mathbb{Z}^2 \longrightarrow \mathbb{Z}$
$(a,b) \longmapsto a^b$

$d : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$
$(a,b) \longmapsto$ $i^{th}$ digit of $b$-base expansion of $a$
is Diophantine

$$d(a,b) = \text{rem}(\text{quo}(a, b^i), b)$$

The binomial Coefficient is Diophantine

$$\binom{n}{m} = d_m((1+2^n)^n, 2^n)$$

$x \vdash y$ iff $d_i(x,2) \le d_i(y,2)$

$x \vdash y \iff \binom{x}{y} \equiv 1 \pmod 2$

Consider a computer as follows:

- It has $n$ registers $R_1 \cdots R_n$
- It has $m$ lines of code $L_1, \cdots, L_m$

there are 5 instances:

1. GOTO $L_i$
2. If $R_j > 0$, then GOTO $L_i$
3. Inc $R_j$
4. Dec $R_j$

(S) Halt

$R_1$ for Input or Output

$R_i(t)$ = the value in $R_i$ after time $t$

$$L_i(t) = \begin{cases} 1 & \text{if you are at } L_i \text{ at time } t \\ 0 & \text{if not} \end{cases}$$

$0 \leq t \leq S$ note $r_i(t) \leq S + x$

where Input $= x$

Set $q$ = largest power of 2 $> 2(S+X)$

$> m$

$r_i = r_i(S) \cdots r_i(0)$ in base $q$

$l_i = l_i(S) \cdots l_i(0)$

$(x, S, q, r_1, \cdots, r_n, l_1, \cdots, l_m) \in \mathbb{Z}$ proves $\wedge$ is Diophantine

- Each base $q$ digit of $l_i$ must be $0 \sim 1$

  $\nwarrow$ $l_i \vdash \frac{q^S - 1}{q-1}$

- Exact one $l_i$ has $i^{th}$ digit 1

  $\nwarrow$ $l_1 + \cdots + l_n = \frac{q^{S+1} - 1}{q-1}$

- $0^{th}$ digit of $l_1$ is 1

  $\nwarrow$ $1 \vdash l_1$

- Suppose $L_i$ is "GOTO $L_k$"

  $\nwarrow$ $q l_k \vdash l_k$

$\vdots$

Suppose $f: \mathbb{Z} \to \mathbb{Z}$ is computable, then it's Diophantine

Then a subset semicomputable $\Rightarrow$ Diophantine