- Conversely sps $\exists$ alg. determining if sol'ns in $\mathbb{N}$ and $F(x_1, \ldots, x_k) = 0$ is Dio.
- Let $F' = \prod_{\substack{\text{all } +/- \\ \text{combos}}} F(+/- x_1, \ldots, +/- x_k)$
- Then F has integer sol'ns iff F' has sol'ns in $\mathbb{N}$ (which we can decide)

Both problems 1 and 2 solved by:

<u>Theorem</u> (Matiyasevich, 1970) Sps $R(n_1, \ldots, n_k)$ is r.e. Then there are poly's $G(x_1, \ldots, x_k, y_1, \ldots, y_m)$, $H(x_1, \ldots, x_k, y_1, \ldots, y_m)$ w/ coeffs in $\mathbb{N}$ s.t.

$$R(\vec{n}) \text{ iff } \exists \vec{y}\, [G(\vec{n}, \vec{y}) = H(\vec{n}, \vec{y})]$$

<u>Notes</u>: ① any R defined by such an expression is clearly r.e. (since checking equality of two poly's on a given input is recursive); hence is iff

② "very nice" way to define r.e. sets: $\exists \vec{y}$ (term = term)

③ letting $F = G - H$ can rewrite

$$\exists \vec{y}\, (F(\vec{n}, \vec{y}) = 0)$$ Diophantine

(F coeffs in $\mathbb{Z}$)

<u>Sol'n to problem 1:</u>

<u>Claim</u>: $\exists_1 = \Sigma^0_1$

pf: ①+② shows even better:

every r.e. R defined by
$\exists \vec{y}\,(G = H)$ ... q.f. part is atomic:
no need for $\wedge, \vee, \neg$

now $\forall_1 = \Pi^0_1$, $\exists_2 = \Sigma^0_2$ ... follows
by induction.

<u>Sol'n to problem 2</u>:

- No such algorithm exists
- if it did, then fix $A \in \Sigma^0_1 \setminus \Delta^0_1$
- by theorem there is $F \in \mathbb{Z}[\dots]$

s.t. $\vec{n} \in A$ iff $\exists \vec{y}\,(F(\vec{n}, \vec{y}) = 0)$

- but our algorithm can determine

for all $\vec{n}$ whether $\exists \vec{y}\, F(\vec{n}, \vec{y}) = 0$, i.e.
if $\vec{n} \in A$

$\Rightarrow$ A recursive contradiction

there's not even an algorithm for this particular F ... much less all.

<u>Another nifty consequence</u>:

<u>Corollary</u>: if $A \subseteq \mathbb{N}$ is r.e. then there
is a poly $F(\vec{x}) \in \mathbb{Z}[\vec{x}]$ s.t.

$$A = \{F(\vec{x}) \mid \vec{x} \in \mathbb{N}^k\} \cap \mathbb{N}$$

(i.e. $n \in \mathbb{N}$ iff $\exists \vec{x} \in \mathbb{N}^k$ s.t. $F(\vec{x}) = n$)

<u>Pf</u>: By Matiyasevich there is a
poly G s.t. $R(a)$ iff $\exists \vec{x}\,(G(a, \vec{x}) = 0)$

- Let $F(\vec{x}, y) := (y+1)(1 - G^2(y, \vec{x})) - 1$

observe: $F(\vec{x},y) \geq 0$ (for $y \in \mathbb{N}$) $\Rightarrow G(y,\vec{x}) = 0$ (so $y \in A$) and in this case $F(\vec{x},y) = y$

Conversely if $G(y,\vec{x}) = 0$ (so $y \in A$) then $F(\vec{x},y) = y$ ✓

In particular for e.g. the set of primes P there is a poly $F(\vec{x})$ (w/ coeffs in $\mathbb{Z}$) whose non-negative outputs are exactly the elements of P (i.e. the primes)

Proving Matiyasevich

Def'n $R \subseteq \mathbb{N}^k$ is Diophantine ("Dio") if there is $F \in \mathbb{Z}[\vec{x},\vec{y}]$ s.t.

$R(\vec{n})$ iff $\exists \vec{y}\,(F(\vec{n},\vec{y}) = 0)$

Matiy thm says: R is r.e. iff Dio

$\Rightarrow$ is hard direction

Def'n $f: \mathbb{N}^k \to \mathbb{N}$ is Diophantine ("Dio") if its graph is, i.e. "$f(\vec{x}) = y$" is Dio

to prove Matiy: enough to prove every recursive f is Dio

Why: if R is r.e. then $R = dom(f)$ for some rec. f

so then: $\vec{a} \in R$ iff $\exists y\, f(\vec{a}) = y$

iff $\exists y \exists \vec{z}\, F(\vec{a}, y, \vec{z})$
where $F(\vec{x}, y, \vec{z})$ is poly s.t.
$f(\vec{x}) = y$ iff $\exists \vec{z}\, F(\vec{x}, y, \vec{z})$
but then R also defined by Dio eq'n (hence is Dio)

Outline of pf of Matiy:

- we induct on construction of recursive f's to reduce problem to showing Diophantine-ness is closed under certain quantifiers, connectives, etc.

① Basic functions are Dio:

C_n's, π_i^n, s defined by:

$$y = 0$$
$$y - x_i = 0$$
$$y - (x+1) = 0$$

- these of the form $F(\vec{x}, y) = 0$
- can make them "look more Dio" (i.e. of form $\exists \vec{z}(F(\vec{x}, y, \vec{z}) = 0)$) by adding dummy variables

e.g. $\exists z\,(y - (x+1) = 0)$ defines successor.

② <u>Compositions</u> of Dio functions are Dio:

if $f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$

where h, g_i all Dio we have

$f(\vec{x}) = y$ iff $\exists y_1 \ldots \exists y_m [g_1(\vec{x}) = y_1 \wedge$

$g_2(\vec{x}) = y_2 \wedge$

defined by Dio eq'ns

$\vdots$

$g_m(\vec{x}) = y_m$

$\wedge\, h(y_1, \ldots, y_m) = y]$

so would be done if we can show Dio rel'ns closed under $\wedge$ and $\exists$.

③ <u>minimalization</u>: if $f(\vec{x}) = \mu y [g(\vec{x}, y) = 0]$ and g is Dio then:

$f(\vec{x}) = y$ iff $g(\vec{x}, y) = 0 \wedge \forall z < y\, \exists w$

$[w > 0 \wedge g(\vec{x}, z) = w]$

So sufficient to moreover show: "$w > 0$" is Diophantine and Dio rel'ns closed under bdd quantification $\forall x < y$

④ <u>primitive recursion</u>: if f defined by:

$f(0, \vec{x}) = g(\vec{x})$

$f(n+1, \vec{x}) = h(f(n, \vec{x}), n, \vec{x})$

and g, h Dio then:

$$f(i,\vec{x}) = y \text{ iff } [i=0 \wedge g(\vec{x}) = y] \vee [i>0 \wedge \exists a \exists b\, (g(\vec{x}) = \beta(a,b,0) \wedge \forall j<i\, (\beta(a,b,j+1) = h(\beta(a,b,j), j, \vec{x})) \wedge \beta(a,b,i) = y]$$

So done w/ 4 if moreover can show: β is D_ω and D_ω rel'ns closed under $\vee$ and substitution by D_ω functions.

Thus we'll be done if we can prove:

Crucial Lemma: The collection of Diophantine relations:
1 contains the relations $x<y$ and $\beta(a,b,i)=z$, and
2 is closed under substitution by Diophantine functions, $\exists$ quantification, bdd $\forall x<y$ quantification, and the connectives $\wedge$ and $\vee$

→ most of these straightforward
→ hardest by far is bdd $\forall x<y$ quantification
- relies on some real number theory
- boils down partly to showing $x^y = z$ is D_ω.