Dim. dell'esistenza della β: cerco una coppia (c,d) t.c. b_i è la classe di resto di c modulo $i \cdot d+1$.

Prendo d in modo che:

1) $p \mid d$ per ogni primo $\leq n$;
2) $d \geq b_1, \dots, b_n$.

Ad esempio, $d = b_1 \cdot \ldots \cdot b_n \cdot (n!)$.

Allora i numeri $d+1, 2d+1, \dots, nd+1$ sono coprimi.

Per il TCR esiste c t.c. $c \equiv b_i \ (i \cdot d+1)$ per ogni $i=1,\dots,n$.

Infine notiamo che $b_i \leq d$ (per 2)) e quindi $b_i < i \cdot d+1$.

La funzione "$\beta(c,d,i)=r$" è definita dalla proprietà "r è il resto della divisione euclidea di c per $i \cdot d+1$", che può essere espressa da una formula Δ_0. □

Ex.: usando la β, mostrare che "$x^y = z$" è definibile da una formula Σ_1.

Dim. (di ($\Leftarrow$) del teo. della volta scorsa): bisogna vedere che tutti gli insiemi definiti da formule Σ_1 sono semidecidibili.

A questo scopo, notiamo che tutti gli insiemi definiti da formule Δ_0 sono PR perché ottenuti a partire da grafici di $+$ e $\cdot$, che sono PR usando connettivi booleani e quantificatori ristretti. □

Teo.: ogni enunciato σ nel linguaggio dell'aritmetica di classe Δ_0 è "deciso" da Q, cioè $Q \vdash \sigma$ o $Q \vdash \neg\sigma$.

Dim.: dopo (forse). □

Cor.: se σ è di classe Δ_0, allora

1) $\mathbb{N} \models \sigma$ ("vero in $\mathbb{N}$") $\iff Q \vdash \sigma$;
2) $\mathbb{N} \not\models \sigma$ ("falso in $\mathbb{N}$") $\iff Q \vdash \neg\sigma$.

Es.: $Q \nvdash$ "commutatività di $+$". Tuttavia, per ogni termine chiuso t $Q \vdash \forall x,y \leq t \ \ x+y=y+x$ perché quella formula Δ_0 è vera in $\mathbb{N}$.

Teo.: tutti gli enunciati σ nel linguaggio dell'aritmetica di classe Σ_1 che sono "veri" in $\mathbb{N}$ sono dimostrati da Q, cioè

$$\mathbb{N} \models \sigma \iff Q \vdash \sigma.$$

⚠ Non vale $\mathbb{N} \models \neg\sigma \Rightarrow Q \vdash \neg\sigma$ per enunciati Σ_1.

Es.: "$\exists x,y \ \ x+y \neq y+x$".

Dim.: ($\Leftarrow$) ovvia. ($\Rightarrow$) Induzione sulla costruzione di σ.

- σ è Δ_0 $\rightsquigarrow$ teo. sopra.
- σ è uguale a $\exists x \psi(x)$ dove $\psi(t)$ soddisfa l'ipotesi induttiva. (per ogni termine chiuso) $\mathbb{N} \models \sigma \iff$ esiste $m \in \mathbb{N}$ t.c. $\mathbb{N} \models \psi(\bar{m})$ $(\bar{m} = S^{(m)}(\bar{0}))$. Ip. induttiva $\Rightarrow Q \vdash \psi(\bar{m}) \Rightarrow Q \vdash \exists x \psi(x)$.
- Quantificatori ristretti: ad esempio sia σ: "$\forall x \leq t \ \exists y \leq x \ \ \psi(x,y)$" dove t termine chiuso e dove $\psi(t,s)$ soddisfa l'ipotesi induttiva per tutti i termini chiusi t,s.
  Lemma: se t è un termine chiuso, allora $\exists\, n \in \mathbb{N}$ t.c. $Q \vdash t = \bar{n}$. Dim.: dopo (forse). □
  Prendo $n \in \mathbb{N}$ t.c. $Q \vdash t = \bar{n}$. Allora
  $\mathbb{N} \models \forall x \leq \bar{n} \ \exists y \leq x \ \ \psi(x,y)$, quindi
  $\mathbb{N} \models \bigwedge_{k=0}^{n} \bigvee_{i=0}^{k} \psi(\bar{k}, \bar{i})$. Da $\mathbb{N} \models \bigvee_{i=0}^{k} \psi(\bar{k}, \bar{i})$ per ogni k, segue per ip. induttiva che $Q \vdash$ " " " ", perciò $Q \vdash \bigwedge_{k=0}^{n} \bigvee_{i=0}^{k} \psi(\bar{k}, \bar{i})$, cioè $Q \vdash \sigma$.
- Connettivi booleani: ex. □

Es.: se Goldbach è consistente in Q, allora è vera in $\mathbb{N}$.

Teo. (RAPPRESENTABILITÀ): ogni funzione calcolabile $f : \mathbb{N}^k \to \mathbb{N}$ totale è RAPPRESENTABILE in Q, cioè esiste una formula $\varphi(x_1, \dots, x_k, y)$ di classe Σ_1 t.c. se $f(a_1, \dots, a_k) = b$ allora $Q \vdash \varphi(\bar{a}_1, \dots, \bar{a}_k, y) \leftrightarrow y = \bar{b}$.

Dim.: abbiamo visto che f è definibile da una formula Σ_1 $\varphi(x_1, \dots, x_k, y)$. Inoltre, abbiamo visto prima che gli enunciati Σ_1 "veri" in $\mathbb{N}$ sono dimostrati da Q. Quindi $f(a_1, \dots, a_k) = b \iff \mathbb{N} \models \varphi(\bar{a}_1, \dots, \bar{a}_k, \bar{b}) \Rightarrow Q \vdash \varphi(\bar{a}_1, \dots, \bar{a}_k, \bar{b})$.
Di più: se f è totale, si può mostrare che $Q \vdash \varphi(\bar{a}_1, \dots, \bar{a}_k, y) \leftrightarrow y = \bar{b}$. □

Teo.: esiste una funzione $\mathrm{Sub} : \mathbb{N}^3 \to \mathbb{N}$ PR t.c. per ogni formula φ dell'aritmetica, per ogni variabile x e per ogni termine t sostituibile a x in φ, si ha

$$\mathrm{Sub} : (\ulcorner \varphi \urcorner, \ulcorner x \urcorner, \ulcorner t \urcorner) \mapsto \ulcorner \varphi(t/x) \urcorner$$

(che Sub è calcolabile totale segue dalla tesi di Church).

Inoltre esiste una funzione $\mathrm{Num} : \mathbb{N} \to \mathbb{N}$ PR t.c.
$\mathrm{Num} : n \mapsto \ulcorner S^{(n)}(\bar{0}) \urcorner$, cioè $n \mapsto \ulcorner \bar{n} \urcorner$
(di nuovo tesi di Church).

Idea di Gödel: trovare un enunciato dell'aritmetica che dice "Io non sono un teorema".

Lemma diagonale: per ogni formula $\varphi(x)$ dove x è l'unica variabile libera, esiste un enunciato γ che dice "Io soddisfo φ", cioè t.c. $Q \vdash \gamma \leftrightarrow \varphi(\overline{\ulcorner \gamma \urcorner})$.

Dim.: $n \overset{D}{\mapsto} \mathrm{Sub}(n, \ulcorner x \urcorner, n)$, cioè $D(\ulcorner \varphi \urcorner) = \ulcorner \varphi(\overline{\ulcorner \varphi \urcorner}) \urcorner$. Questa funzione "diagonale" è PR perché Sub lo è.
Allora, per rappresentabilità esiste una formula $\delta(x,y)$ t.c. se $D(a) = b$ allora $Q \vdash \delta(\bar{a}, y) \leftrightarrow y = \bar{b}$.
Prendiamo la formula $\alpha(x)$: "$\forall y \ \delta(x,y) \to \varphi(y)$".
Informalmente, $\alpha(x)$ dice: "$\varphi(D(x))$".
"Ragioniamo" in Q: per ogni $a \in \mathbb{N}$, $\alpha(\bar{a})$, cioè "$\forall y \ \delta(\bar{a}, y) \to \varphi(y)$", equivale a $\varphi(\overline{D(a)})$, cioè $Q \vdash \alpha(\bar{a}) \leftrightarrow \varphi(\overline{D(a)})$.
Prendiamo $a = \ulcorner \alpha \urcorner$. Abbiamo allora che $D(a) = \ulcorner \alpha(\overline{\ulcorner \alpha \urcorner}) \urcorner = \ulcorner \alpha(\bar{a}) \urcorner$. Quindi se γ è l'enunciato $\alpha(\overline{\ulcorner \alpha \urcorner})$, cioè $\alpha(\bar{a})$, allora $Q \vdash \gamma \leftrightarrow \varphi(\overline{\ulcorner \gamma \urcorner})$. □

Teo. (Tarski, indefinibilità del vero): per ogni formula $\varphi(x)$ dove x unica variabile libera $\mathrm{Def}(\varphi) = \{ n \mid \mathbb{N} \models \varphi(\bar{n}) \} \neq \{ \ulcorner \sigma \urcorner \mid \mathbb{N} \models \sigma \} = TA$ (true arithmetics).

Dim.: applico il lemma diagonale alla formula $\neg\varphi(x)$ ed ottengo l'esistenza di un enunciato γ t.c. $Q \vdash \gamma \leftrightarrow \neg\varphi(\overline{\ulcorner \gamma \urcorner})$. Prendo $k = \ulcorner \gamma \urcorner$. Allora:
$k \in TA \overset{\text{def.}}{\iff} \mathbb{N} \models \gamma \overset{\mathbb{N} \models Q}{\iff} \mathbb{N} \models \neg\varphi(\overline{\ulcorner \gamma \urcorner})$, cioè
$\mathbb{N} \not\models \varphi(\overline{\ulcorner \gamma \urcorner}) \overset{\text{def.}}{\iff} k \notin \mathrm{Def}(\varphi)$. Perciò $TA \neq \mathrm{Def}(\varphi)$. □

TA non è semidec. perche non è definito da alcuna formula, tantomeno Σ_1.

Cor.: PA è incompleto.

Dim.: se PA fosse completo, visto che PA ha un insieme di assiomi decidibile, sarebbe decidibile e $TA = \mathrm{Teor}(PA)$. □

Teo. (incompletezza di Gödel): esiste un enunciato G t.c. $T \nvdash G$ e $T \nvdash \neg G$, $T \supseteq Q$ ricorsivamente assiomatizzata e coerente.

Nota: esiste un predicato $\mathrm{Prov} \subseteq \mathbb{N} \times \mathbb{N}$ decidibile t.c. $\mathrm{Prov}_T(\ulcorner \langle \varphi_1, \dots, \varphi_n \rangle \urcorner, \ulcorner \psi \urcorner)$ vale $\iff \langle \varphi_1, \dots, \varphi_n \rangle$ è una dimostrazione di $T \vdash \psi$, T teoria ricorsivamente assiomatizzabile.

Dim. (del teo.): la formula $\mathrm{Teor}_T(x)$ è la formula che definisce il predicato semidec. "$\exists y \, \mathrm{Prov}_T(y, x)$", cioè il predicato che dice "x è un teorema di T".
Per il lemma diagonale, abbiamo l'esistenza di un enunciato G t.c. $Q \overset{(*)}{\vdash} G \leftrightarrow \neg \mathrm{Teor}_T(\ulcorner G \urcorner)$.

1) $T \nvdash G$: se per assurdo $T \vdash G$, allora esisterebbe $n \in \mathbb{N}$ che codifica una sua dim., quindi $\mathrm{Prov}_T(n, \ulcorner G \urcorner)$. Per la rappresentabilità di questo predicato ho che esiste una formula $P(x,y)$ t.c. $Q \vdash P(\bar{n}, \overline{\ulcorner G \urcorner}) \Rightarrow$ $\Rightarrow Q \vdash \exists x P(x, \overline{\ulcorner G \urcorner})$, cioè $Q \vdash \mathrm{Teor}_T(\ulcorner G \urcorner)$. Ma allora $Q \vdash \neg G \Rightarrow T \vdash \neg G$ e T sarebbe contraddittoria, assurdo.

2) $T \nvdash \neg G$: usiamo l'ipotesi supplementare che $\mathbb{N} \models T$ (non è necessaria per il teo. di Rosser). Abbiamo visto sopra che $T \nvdash G$, quindi per ogni $n \in \mathbb{N}$ $\neg \mathrm{Prov}_T(n, \ulcorner G \urcorner)$. Per rappresentabilità, $Q \vdash \neg P(\bar{n}, \overline{\ulcorner G \urcorner}) \Rightarrow T \vdash \neg P(\bar{n}, \overline{\ulcorner G \urcorner})$. Ma $\mathbb{N} \models T$, quindi $\mathbb{N} \models \neg P(\bar{n}, \ulcorner G \urcorner)$ per ogni n, quindi $\mathbb{N} \models \forall x \neg P(x, \overline{\ulcorner G \urcorner})$. Visto che $\mathbb{N} \models T$ e T è consistente, $T \nvdash \exists x P(x, \overline{\ulcorner G \urcorner})$, cioè $T \nvdash \mathrm{Teor}_T(\ulcorner G \urcorner)$. Allora $T \nvdash \neg G$, altrimenti da $(*)$ $T \vdash \mathrm{Teor}_T(\ulcorner G \urcorner)$, assurdo. □

G è un esempio di enunciato "vero" in $\mathbb{N}$ ma non dimostrabile. Infatti $PA \nvdash G$, cioè per ogni n $\neg \mathrm{Prov}_{PA}(n, \ulcorner G \urcorner)$. Quindi $\mathbb{N} \models \forall x \neg P(x, \ulcorner G \urcorner)$, cioè $\mathbb{N} \models \neg \mathrm{Teor}_{PA}(\ulcorner G \urcorner)$, cioè $\mathbb{N} \models G$.

Teo.: la teoria pura del 1° ordine nel linguaggio dell'aritmetica (senza assiomi extra-logici) è indecidibile.

Dim.: notiamo che, per ogni enunciato σ, $\ulcorner \sigma \urcorner \in \mathrm{Teor}(Q) \overset{\text{def.}}{\iff}$ $\iff Q \vdash \sigma \iff\ \vdash (Q_1 \wedge \ldots \wedge Q_7) \to \sigma$ dove $Q_1, \dots, Q_7$ sono gli assiomi di Q. Questo $\iff \ulcorner Q_1 \wedge \ldots \wedge Q_7 \to \sigma \urcorner \in \{ \ulcorner \varphi \urcorner \mid \ \vdash \varphi \} =$ $=$ teoria pura. La funzione $g : \ulcorner \sigma \urcorner \mapsto \ulcorner Q_1 \wedge \ldots \wedge Q_7 \to \sigma \urcorner$ è calcolabile totale e quindi $\ulcorner \sigma \urcorner \in \mathrm{Teor}(Q) \iff$ $\iff g(\ulcorner \sigma \urcorner) \in$ teoria pura. Visto che $\mathrm{Teor}(Q)$ non è decidibile, anche teoria pura non è decidibile. □