Teorema $a, b, c \in \mathbb{Z}$ a, b non entrambi nulli. Si considera l'equazione Diofantea:

$$(1) \quad ax + by = c.$$

Si pone $d = M.C.D.(a, b)$ e si pone $\bar{a} = \frac{a}{d}$ $\bar{b} = \frac{b}{d}$.

L'equazione (1) ha soluzioni $\iff d \mid c$.

Se (x_0, y_0) è una soluzione, tutte le soluzioni sono

$$(x_0 + \bar{b}h, y_0 - \bar{a}h), \quad h \in \mathbb{Z}$$

$\Leftarrow)$ ipotesi $d \mid c$ tesi esiste una soluzione $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$ di (1)

Per l'identità di Bezout, esistono $x_0, y_0 \in \mathbb{Z}$ tali che

$$(2) \quad \underbrace{d = ax_0 + by_0}$$

Si pone $\bar{c} = \frac{c}{d}$ e si moltiplica (2) per $\bar{c}$

$$\bar{c}d = \bar{c}ax_0 + \bar{c}by_0$$

$$c = a(\bar{c}x_0) + b(\bar{c}y_0)$$

e quindi, posto $x_1 = \bar{c}x_0$, $y_1 = \bar{c}y_0$, si ha:

$$a x_1 + b y_1 = c$$

ovvero (x_1, y_1) è una soluzione di (1).

$f : \mathbb{N} \to \mathbb{Z}$ $\quad \forall n \in \mathbb{N}$ $\quad f(n) = 3n + 1$

$g : \mathbb{Z} \to \mathbb{Q}$ $\quad \forall x \in \mathbb{Z}$ $\quad g(x) = \frac{1}{3} x + 2$

f è iniettiva? Siano $\underbrace{n, m \in \mathbb{N}}$ tali che sia

$$\underbrace{f(n) = f(m)} \Rightarrow 3n + 1 = 3m + 1 \Rightarrow 3n = 3m \Rightarrow \underbrace{n = m}$$

dunque f è iniettiva

f è surgettiva?. No: $\exists\, -3 \in \mathbb{Z}$ tale che $\forall n \in \mathbb{N}$ $f(n) \neq -3$ perché $\forall n \in \mathbb{N}$ $f(n) > 0$.

f non è bigettiva e quindi non è invertibile.

g è iniettiva? siano $\underbrace{x_1, x_2 \in \mathbb{Z}}$ tali che sia

$$\underbrace{g(x_1) = g(x_2)} \Rightarrow \frac{1}{3} x_1 + 2 = \frac{1}{3} x_2 + 2 \Rightarrow \frac{1}{3} x_1 = \frac{1}{3} x_2 \Rightarrow \underbrace{x_1 = x_2}$$

quindi g è iniettiva.

g è surgettiva? Sia $y \in \mathbb{Q}$ cerchiamo, se esiste, $x \in \mathbb{Z}$ tale che $g(x) = y$, ovvero $\frac{1}{3} x + 2 = y$

$\frac{1}{3}x + 2 = y \Leftrightarrow x + 6 = 3y \Leftrightarrow x = 3y - 6$

in generale $3y-6 \notin \mathbb{Z}$ se $y \in \mathbb{Q}$:

per esempio se $y = \frac{1}{2}$ $\qquad 3y - 6 = \frac{3}{2} - 6 = \frac{3-12}{2} = -\frac{9}{2} \notin \mathbb{Z}$

g non è surgettiva, quindi non è bigettiva e non è invertibile

$$\begin{tikzcd} \mathbb{N} \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & \mathbb{Z} \arrow[r, "g"] & \mathbb{Q} \end{tikzcd} \qquad g \circ f : \mathbb{N} \longrightarrow \mathbb{Q}$$

$$\forall n \in \mathbb{N} \quad (g \circ f)(n) = g(f(n)) = g(3n+1) = \frac{1}{3}(3n+1) + 2 =$$

$$= n + \frac{1}{3} + 2 = n + \frac{7}{3}$$

$$\mathbb{Z} \xrightarrow{g} \mathbb{Q}$$

$$\mathbb{N} \xrightarrow{f} \mathbb{Z}$$

l'insieme di arrivo di g è diverso dall'insieme di partenza di f, per cui non esiste $f \circ g$.

Osserv. Se $a = 0 \wedge b \neq 0$ allora b è massimo comun divisore tra a e b.

1. $b \mid a \quad \wedge \quad b \mid b$

$\Downarrow$

perché ogni numero intero non nullo è divisore di 0

2. Se $d' \in \mathbb{Z}$ tale che $d' \mid a \wedge \underline{d' \mid b} \Rightarrow d' \mid b$.