Lezione 4

Divisibilità

siano $a, b \in \mathbb{Z}, b \neq 0$ si dice che b divide a se $\exists k \in \mathbb{Z} : a = bk$, $b | a$

Teorema divisibilità in $\mathbb{Z}$

enunciato: siano $a, b \in \mathbb{Z}, b \neq 0$ allora $\exists! q \in \mathbb{Z}, r \in \{0, 1, \dots, |b|-1\} : a = qb + r$

dimostrazione

supponiamo $a \geq 0$, $b > 0$. Unicità

per assurdo $\exists q, q' \in \mathbb{Z}, r, r' \in \{0, 1, \dots, |b|-1\} : a = qb + r, a = q'b + r' \Rightarrow$

$\Rightarrow q'b + r' = qb + r \Rightarrow 0 = qb + r - q'b - r' \Rightarrow 0 = b(q - q') + (r - r')$ ma $0 \leq r < |b|$ e $b > 0 \Rightarrow$

$\Rightarrow q = q'$ e $r = r'$

esistenza (per induzione)

caso base: $a = 0 \Rightarrow 0 = qb + r \Rightarrow q = r = 0$

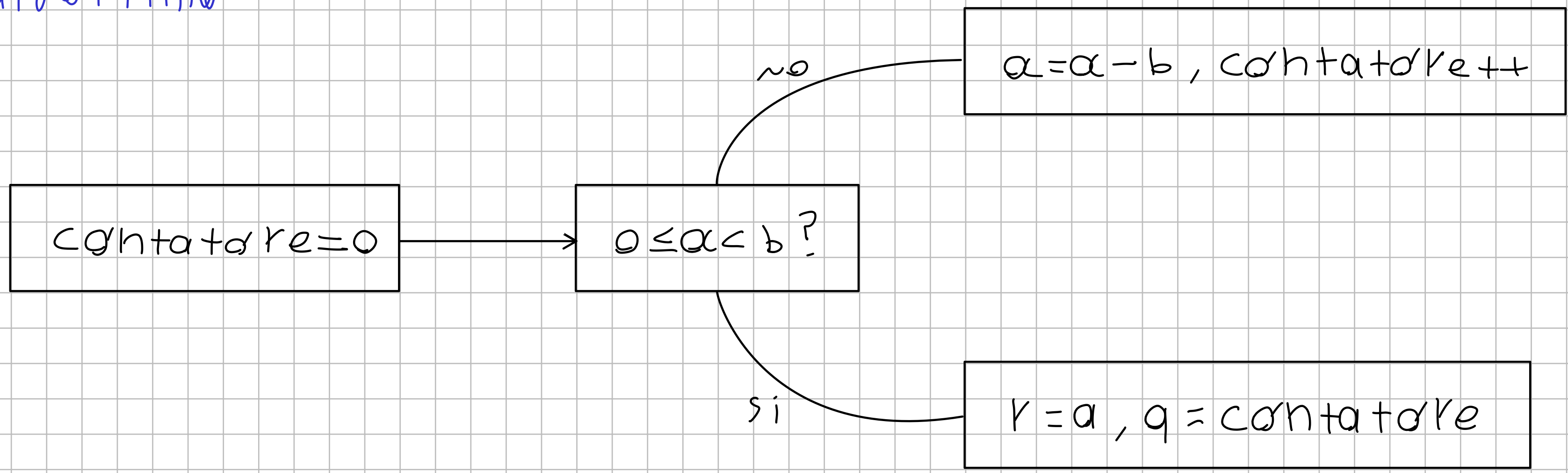
passo induttivo: assumo $a - 1 = q'b + r'$

$a = (a-1) + 1 = (q'b + r') + 1 = q'b + (r' + 1)$, ci sono due casi:

$r' = b - 1 \Rightarrow a = q'b + (b - 1 + 1) = q'b + b = (1 + q')b + 0$

$r' < b - 1 \Rightarrow r' + 1 < b$

algoritmo

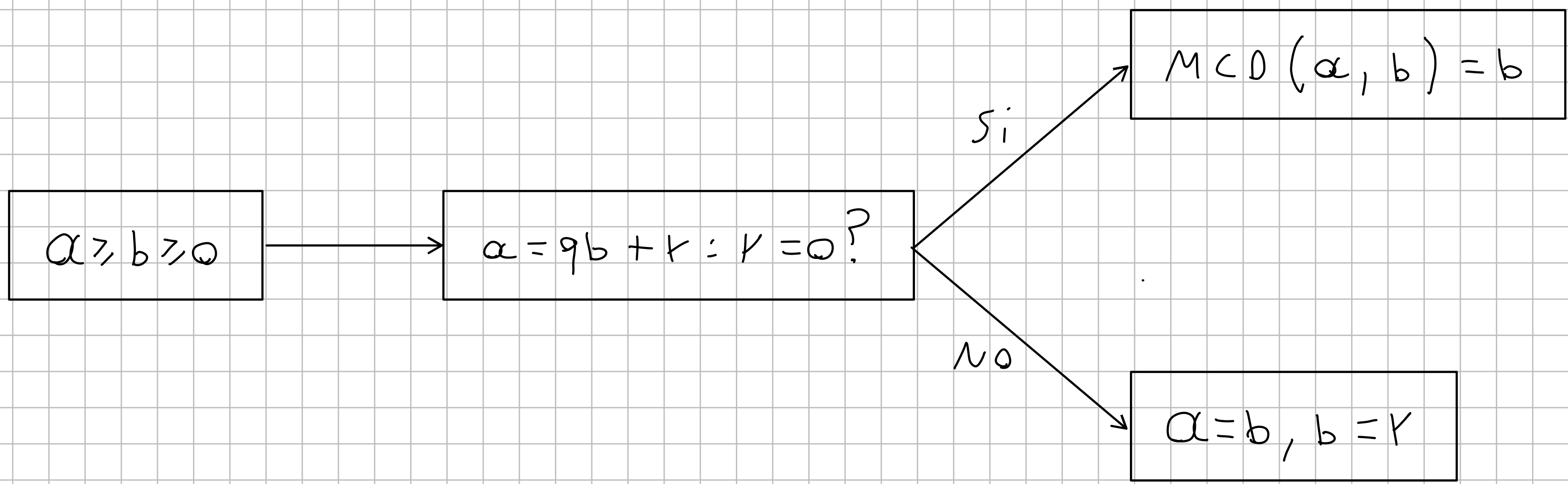


Massimo comun divisore

siano $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$, si definisce massimo comun divisore il più grande $d \in \mathbb{Z}, d > 0 : d \mid a, d \mid b$ si scrive $MCD(a,b) = d$

a e b si dicono relativamente primi se $MCD(a,b) = 1$

algoritmo



Teorema di esistenza del MCD

enunciato

siano $a, b \in \mathbb{Z}$ con $a \neq 0 \vee b \neq 0$ allora:

- $\exists\, MCD(a,b)$
- $\exists\, n,k \in \mathbb{Z} : MCD(a,b) = an + bk$
- $t \in \mathbb{Z} : t \mid a \wedge t \mid b \Rightarrow t \mid MCD(a,b)$

Numeri primi e irriducibili

$p \in \mathbb{Z}$ si dice primo se $p \mid ab \Rightarrow p \mid a$ o $p \mid b \quad \forall a,b \in \mathbb{Z}$

$p \in \mathbb{Z}$ si dice irriducibile se $\exists\, l, m \in \mathbb{Z} : p = l \cdot m \Rightarrow l = \pm 1 \vee m = \pm 1$

negli anelli si parla di elementi primi e irriducibili

Teorema: numeri primi sono irriducibili e viceversa

enunciato: sia $p \in \mathbb{Z}$, allora p è primo $\Longleftrightarrow p$ è irriducibile

Teorema: i numeri primi non sono finiti

enunciato: esistono infiniti numeri primi

dimostrazione

per assurdo sia $P = \{p_1, \dots, p_n\}$ l'insieme dei numeri primi finito

quindi p_n è il massimo di P.

sia $k = p_1 \cdot \ldots \cdot p_n + 1 > p_n \Rightarrow k - 1 = p_1 \cdot \ldots \cdot p_n \Rightarrow p \mid k - 1$

Teorema fondamentale dell'aritmetica

ogni $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ può essere scritto come prodotto di numeri primi $p_i \geq 1$, ovvero $n = p_1 \cdot \ldots \cdot p_n$ se $p_i = p_j$ si può raccogliere e scrivere $n = p_i^{\alpha_i} \cdot \ldots \cdot p_j^{\alpha_j}$ con $p_i \neq p_j$, α_i e α_j sono detti molteplicità di p_i e p_j

Minimo comune multiplo

siano $a, b \in \mathbb{Z}$ con $a \neq 0 \vee b \neq 0$ si dice minimo comune multiplo il più piccolo $n \in \mathbb{Z} : a \mid n \wedge b \mid n$, si scrive $\text{mcm}(a, b) = n$