

$a, b \in \mathbb{N}$

interi ≥ 0

divisione di a per b ?

①

\leadsto quoziente q e resto $r \in \mathbb{N}$

1) $a = qb + r$
2) $0 \leq r < b$

Algoritmo di Euclide

$$a, b \rightsquigarrow q, r$$

$$a = bq + r$$
$$0 \leq r < b$$

②

q, r es unicos
mno

$$b \geq 1$$

Se $b=1$
banale

$$b \geq 2$$

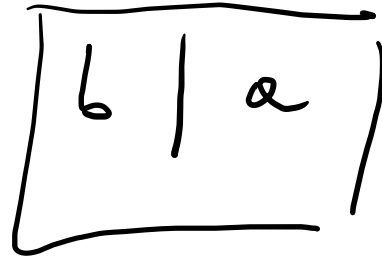
$$a = q, r < 1 \Rightarrow r = 0$$

$$\begin{array}{r|l} 17 & 4 \\ -16 & 4 \\ \hline & 1 \end{array} \quad 17 = \underbrace{4} \cdot 4 + 1$$

$a \quad b \quad q$

Se $a = b \cdot q$ diremo che a è divisibile per b (3)

oppure b divide a



Es $3 \mid 15$, $17 \mid 34$
 $3 \nmid 14$

$$a, b \in \mathbb{N}, b \geq 1$$

4

Massimo comun divisore di a e b

MCD

è il più grande divisore di a e b

$$\text{MCD}(a, b) = \boxed{(a, b)}$$

$$a, b \rightsquigarrow q, r$$

$$a = bq + r, 0 \leq r < b$$

$$k | a, k | b$$

$$(a, b) \rightsquigarrow (b, r) \rightsquigarrow (b_1, r_1) \rightsquigarrow \dots \rightsquigarrow (b_n, r_n)$$

$$\rightsquigarrow (b_{n+1}, 0)$$

$$\boxed{r_n = \text{MCD}(a, b)}$$

MCD
||

(r_n)

Es $MCD(90, 20) = 10$

(5)

$$90 = 20 \cdot 4 + 10$$

$$20 = 10 \cdot 2$$

Minimo comune multiplo (mcm)

mcm(a, b) = minimo multiplo di

$$mcm(a, b) = \frac{a \cdot b}{MCD(a, b)}$$

Es $mcm(12, 9) = \frac{108}{3} = 36$

$$d = MCD(a, b)$$

$$a = kd, \quad b = ld$$

$$(k, l) = 1 \quad (k, l, d \text{ coprimi})$$

$$\frac{a \cdot b}{d} = kld^2$$

$$mcm(a, b) = kld$$

$$\text{MCD}(a, b, c) = \text{MCD}(\text{MCD}(a, b), c)$$

⑥

Numeri primi

Def. $p \in \mathbb{N}$, $p \geq 2$ è detto primo se i divisori di p sono 1 e p

Es: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots$

Scomposizione in primi

T. Ogni numero naturale $a \geq 2$ è prodotto di numeri primi.
 $a = p_1 \dots p_k$, p_i primo $\forall i$. Inoltre questa scomposizione
 è unica a meno dell'ordine dei fattori.

Dim Per induzione su $\underline{a} \geq 2$

1) base dell'induzione: $a = 2$

ovvio

2) Supponiamo che la fattorizzazione $\exists \forall k < a, a > 2$, dimostrando
(ipotesi induttiva) per a .

Se a è primo \checkmark

Se a non è primo: $a = k l$ $k, l \in \mathbb{N}$, $k, l \neq 1$
 $k, l \neq a$

$$1 < k < a$$

$$k = p_1 \cdots p_n$$

p_i primo

$$1 < l < a$$

$$l = p_{n+1} \cdots p_m$$

$$a = k l = p_1 \cdots p_m \quad \square$$

Teorema di Eudossio. Esistono infiniti numeri primi.

Dim Per assurdo: i numeri primi sono finiti

$P = \{p_1, \dots, p_n\}$ insieme dei numeri primi

Proviamo

$$q = p_1 \dots p_n + 1 > p_i \quad \forall i = 1, \dots, n$$

1) q non è primo

2) $q = t_1 \dots t_k$, $t_i \in P$

→ q è divisibile per un primo t_1

→ q diviso un primo t_1 ha come resto 1

Contraddizione