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

interi ≥ 0

divisione di a per b ?

$\rightsquigarrow$ quoziente e resto

q $\quad r \in \mathbb{N}$

1) $a = qb + r$

2) $0 \leq r < b$

Algoritmo di Euclide

$a, b \rightsquigarrow q, r$ $\quad a = bq + r$

$0 \leq r < b$

q, r esistono unici

$b \geq 1$

Se $b = 1$

banale

$b \geq 2$

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

17	4
-16	4
1	

$17 = 4 \cdot 4 + 1$

$a \quad b \quad q$

Se $a = bq$ diremo che a è divisibile per b

oppure b divide a : $\boxed{b \mid a}$

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

$3 \nmid 14$

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

Massimo comun divisore di a, b

MCD

è il più grande divisore di a e b

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

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

$k \mid a$, $k \mid b$

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

$MCD = r_n$

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

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

Es $MCD(90, 20) = 10$

$90 = 20 \cdot 4 + 10$

$20 = 10 \cdot 2$

Minimo comune multiplo (mcm)

$mcm(a,b)$ = minimo multiplo di a e b

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

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

$d = MCD(a,b)$

$a = k\,d$, $b = l\,d$

$(k,l) = 1$ (k, l, d coprimi)

$\frac{a\,b}{d} = k\,l\,d^2$

$mcm(a,b) = k\,l\,d$

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

Numeri primi

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

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

Scomposizione in primi

T. Ogni numero naturale $a \geq 2$ è prodotto di numeri primi.

$a = p_1 \cdots p_k$, p_i primo $\forall i$. Inoltre questa scomposizione è unica a meno dell'ordine dei fattori.

Dim Per induzione su $a \geq 2$

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

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

Se a è primo ✓

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

$1 < k < a$ $k = p_1 \cdots p_n$ p_i primi

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

$a = kl = p_1 \cdots p_m$ $\square$

Teorema di Euclide. Esistono infiniti numeri primi.

Dim Per assurdo: i numeri primi sono finiti

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

Poniamo $\boxed{q = p_1 \cdots p_n + 1} > p_i \quad \forall i = 1, \dots, n$

1) q non è primo
2) $q = t_1 \cdots t_k$, $t_j \in P$

$\longrightarrow$ q è divisibile per un primo t_1

$\longrightarrow$ q diviso un primo t_1 ha come resto 1

Contraddizione