

### TEOREMA DI EUCLIDE

Esistono infiniti numeri primi.

DIM

Per assurdo, supponiamo che  $P = \{\text{insieme dei numeri primi}\}$  sia finito.

E supponiamo che  $|P| = t$ ,  $P = \{p_1, \dots, p_t\}$ .

Sia  $n = p_1 \cdot \dots \cdot p_t$  e  $n+1 = p_1 \cdot \dots \cdot p_t + 1$

Dato  $q \in P$ ,  $q | n$ . Osserviamo anche che  $n+1$  non è primo perché ha  $p_i < n+1 \forall i=1, \dots, t$  (per come ho definito  $n+1$ )

Allora esiste  $r \in P$  tale che  $r | n+1$  (perché  $n+1$  si scomponne in fattori primi). Quindi ho  $r | n+1$  e  $r | n$  (perché ogni primo divide  $n$ )

$\Rightarrow r | 1$  e questo è assurdo perché 1 non è divisibile da niente.  $\square$

$$\boxed{1 = (n+1) - n \quad \begin{matrix} \uparrow & \uparrow \\ n+1 = rh & n = rk \end{matrix} \quad \Rightarrow 1 = (h-k)r}$$

### CRIVELLO DI ERATOSTENE

sd

Sia  $n \geq 2$ . Allora  $n$  è primo se non ammette divisori primi  $p$  con  $p^2 \leq n$ .

ESEMPIO: 151 è un numero primo

$$\begin{array}{lll} 2 \rightarrow 2^2 = 4 \leq 151 & \text{ma } 2 \nmid 151 \\ 3 \rightarrow 3^2 = 9 \leq 151 & \text{ma } 3 \nmid 151 \\ 5 \rightarrow 5^2 = 25 \leq 151 & \text{ma } 5 \nmid 151 \\ 7 \rightarrow 7^2 = 49 \leq 151 & \text{ma } 7 \nmid 151 & (151 = 7 \cdot 21 + 4) \\ 11 \rightarrow 11^2 = 121 \leq 151 & \text{ma } 11 \nmid 151 & (151 = 13 \cdot 11 + 8) \\ 13 \rightarrow 13^2 = 169 \not\leq 151 & & \end{array}$$

$\Rightarrow 151$  è primo perché tutti i primi con un quadrato  $\leq 151$  non dividono 151.

### RAPPRESENTAZIONE DI UN NUMERO NATURALE IN UN BASE FISSATA

$$1739 = 9 \cdot 10^0 + 3 \cdot 10^1 + 7 \cdot 10^2 + 1 \cdot 10^3 \rightarrow 1739 = (1739)_{10}$$

Sia  $b \geq 2$ . Ogni  $n \in \mathbb{N}$  ha una scrittura

$$n = c_0 + c_1 b + c_2 b^2 + \dots + c_s b^s$$

con  $s \geq 0$ ,  $c_0, c_1, \dots, c_s \in \{0, 1, 2, \dots, b-1\}$  e  $c_s \neq 0$

Si dice che  $n = (c_s c_{s-1} \dots c_0)_b$  rappresentazione in base  $b$ .

DIM

Dati  $n \in \mathbb{N}$  e  $b \geq 2$ , esistono  $q_0 \in \mathbb{N}_0$  tali che

$$n = (q_0)b + c_0, \quad q_0 \in \mathbb{N}_0 \quad 0 \leq c_0 \leq b-1 \quad (c_0 < b)$$

$$q_0 = (q_1)b + c_1, \quad q_1 \in \mathbb{N}_0 \quad 0 \leq c_1 \leq b-1$$

$$q_1 = \dots$$

;

$$q_{s-1} = q_s b + c_s \rightarrow \text{Mi ferma quando } q_{s-1} < b - \text{In questo caso ho } q_s = 0 \text{ e } q_{s-1} = c_s$$

Questo succede perché  $q_0 > q_1 > q_2 > \dots > q_s$  e quindi ad un certo punto

il quoziente  $q_s$  sarà minore di  $b$ .

$$n = q_0 b + c_0 =$$

$$= (q_1 b + c_1)b + c_0 = q_1 b^2 + c_1 b + c_0$$

$$= (q_2 b + c_2)b^2 + c_1 b + c_0 = q_2 b^3 + c_2 b^2 + c_1 b + c_0$$

;

$$= (\cancel{b} \cancel{q_s} + c_s)b^s + \dots \rightarrow c_s b^s + c_1 b + c_0$$

$$= c_s b^s + c_{s-1} b^{s-1} + \dots + c_1 b + c_0 \quad \square$$

ESEMPIO

277 in base 8 = ?

$$277 = \underline{34} \cdot 8 + 5$$

$\frac{q_0}{q_1} \frac{b}{b} \frac{c_0}{c_1}$

$$\begin{array}{r|l} 277 & 8 \\ \hline 34 & \\ 32 & \\ \hline 5 & \end{array}$$

$$277 = (34) \cdot 8 + 5$$

$$34 = (4) \cdot 8 + 2$$

$$4 = 0 \cdot 8 + 4$$

$$(277)_{10} = (425)_8$$

$$\frac{32}{5} \Big|$$

$$4 \cdot 8^2 + 2 \cdot 8 + 5 = 277 \quad \text{OK!}$$

□

### ALGORITMO DELLA DIVISIONE EUCLIDEA (in $\mathbb{Z}$ ) (Sd)

Dati  $a, b \in \mathbb{Z}$  con  $b \neq 0$   $\exists!$   $q, r \in \mathbb{Z}$  tali che  $a = qb+r$  con  $0 \leq r < |b|$

NOTAZIONE :  $\text{rest}(a, b) = r$

#### PROPRIETÀ del RESTO

①  $\text{rest}(a, b) = \text{rest}(a, -b)$

$$a = qb + r \Rightarrow a = (-q)(-b) + r$$

②  $\text{rest}(-a, b) = \begin{cases} 0 & \text{se } \text{rest}(a, b) = 0 \\ b - \text{rest}(a, b) & \text{se } \text{rest}(a, b) \neq 0 \end{cases}$

Se  $a = qb \Rightarrow -a = (-q)b$

Se  $a = qb + r \Rightarrow -a = (-q)b - r$

$$-a = \underline{\underline{(-q)b}} - r + \underline{\underline{b - b}}$$

$$-a = (-q-1)b + \underbrace{(b-r)}$$

$$0 \leq b-r < |b|$$

③ Se  $x \mid y \Rightarrow \text{rest}(x, y) = 0$

ESEMPIO :  $\text{rest}(19, 3) = 1$   $19 = 6 \cdot 3 + 1$

$$\text{rest}(-19, 3) = 3 - 1 = 2$$

$$(-6) \cdot 3 + (-1) \cdot 3 = (-6-1) \cdot 3$$

$$19 = 6 \cdot 3 + 1 \rightarrow -19 = (-6) \cdot 3 - 1 = \underline{\underline{(-6) \cdot 3 - 3 + 3 - 1}} =$$

$$= (-7) \cdot 3 + 2$$

$$= \text{EF} 3+2$$

Esercizi: 231 in base 3  
27 in base 2

Esercizi

①  $\forall n \in \mathbb{N}$ , " $2+4+6+\dots+2n = n(n+1)$ " P(n)

BASE:  $n=1$        $2 = 1(1+1) \Rightarrow 2=2 \quad \checkmark$

PASSO:  $(n \rightarrow n+1)$       P(n+1) è       $2+4+\dots+2n + 2(n+1) = (n+1)(n+1+1)$

$2+4+\dots+2n = n(n+1)$  per ipotesi di induzione

Allora      P(n+1) diventa       $\underbrace{n(n+1)+2(n+1)}_{n^2+n+2n+2} = \underbrace{(n+1)(n+2)}_{n^2+n+2n+2} \quad \checkmark$

② Stabilire per quali  $n \in \mathbb{N}$  si ha che  $n(n+1)-11$  è dispari

$$n=1 \quad 1(1+1)-11 = -9 \notin \mathbb{N}$$

$$n=2 \quad 2(2+1)-11 = 6-11 = -5 \notin \mathbb{N}$$

$$n=3 \quad 3(3+1)-11 = 12-11 = 1 \in \mathbb{N}$$

$$\forall n \geq 3 \quad \underbrace{n(n+1)-11}_{\text{è pari perché uno tra } n \text{ e } n+1 \text{ è pari}} \geq 3 \cdot 4 - 11 = 1 \in \mathbb{N}$$

è pari perché uno tra  $n$  e  $n+1$  è pari

$\Rightarrow \forall n \geq 3 \quad n(n+1)-11$  è positivo e dispari

Per induzione

$$n=3 \text{ base } 34-11=23 \text{ dispari}$$

$n=n+2$  Sia  $n(n+1)-11$  sia dispari e dimostriamo che  $(n+1)(n+1+1)-11$  è dispari.

Poiché  $n(n+1) - 11$  è dispari esiste  $k \in \mathbb{N}$  t.c.  $n(n+1) - 11 = 2k + 1$

Osserviamo che  $n(n+1) = n^2 + n$

$$(n+1)(n+2) = n^2 + n + 2n + 2 = \underline{n^2 + n} + \underline{2(n+1)}$$

$$(n+1)(n+2) - 11 = n^2 + n + 2(n+1) - 11 = \underline{n^2 + n - 11} + \underline{2(n+1)} = \text{DISPARI} + \text{PARI}$$

$n(n+1) - 11 \Rightarrow$  è dispari per i passi  
di sostituzione

$\Rightarrow (n+1)(n+2) - 11$  è dispari

### Esercizio

$$\forall n \in \mathbb{N}, 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$n=1 \quad 1 = \frac{1(1+1)(2 \cdot 1 + 1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1 \quad \checkmark$$

$$n \rightarrow n+1 \quad 1^2 + 2^2 + \dots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6} \quad P(n+1)$$

$$\begin{aligned} & \underbrace{\frac{n(n+1)(2n+1)}{6}}_{\text{hp d: induzione}} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n^2 + 2n + 1)}{6} = \\ &= \frac{(n^2+n)(2n+1) + 6n^2 + 12n + 6}{6} = \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \end{aligned}$$

$$\begin{aligned} & \frac{(n^2 + 3n + 2)(2n+3)}{6} \\ &= \frac{2n^3 + 3n^2 + 6n^2 + 9n + 6n + 6}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \end{aligned}$$

Sono uguali  $\Rightarrow$  abbiamo finito

□