ES.: CONSIDERIAMO IL SEGUENTE

"TEOREMA": SIA $a \in \mathbb{R} \setminus \{0\}$ E SIA $n \in \mathbb{N}$ $(= \{0, 1, \dots\})$.

ALLORA

$$a^n = 1 .$$

"DIM." INDUZIONE SU $n = 0, 1, \dots$. SE $n = 0$

$$\Rightarrow \quad a^n = a^0 = 1 \Rightarrow \text{O.K.}$$

SIA IL TEOREMA VERO PER OGNI $m \leq n-1$. ALLORA

$$a^n = \frac{a^{n-1} \cdot a^{n-1}}{a^{n-2}} = \frac{a^{2n-2}}{a^{n-2}} = \frac{1 \cdot 1}{1} = 1 \Rightarrow \text{O.K.} \ \square$$

(INDUZIONE)

DOV'È L'ERRORE?

ES.: CALCOLARE

$$MCD\left(\underbrace{17^{88}\cdot 31^{5}\cdot 37^{2}\cdot 59^{1000}}_{a},\ \underbrace{19^{(9^{22})}\cdot 37^{12}\cdot 53^{3678}}_{b}\right)$$

POICHÈ 17, 31, 37, 19, 53, E 59 SONO TUTTI NUMERI PRIMI ABBIAMO CHE

$$MCD = 37^{2}.$$

(SE $p \in \mathbb{P}$, p primo, È TALE CHE

$p \mid a$ E $p \mid b \Rightarrow (p \mid 17$ o $p \mid 31$ o $p \mid 37$

$\circ\ p \mid 59)\ E\ (\ p \mid 19 \circ p \mid 37 \circ p \mid 53)$. MA p È

PRIMO $\Rightarrow$ $(\circ\ p=17 \circ p=31 \circ p=37 \circ p=59)$

E $(\circ\ p=19 \circ p=37 \circ p=53) \Rightarrow p=37)$.

MA $37^2 \mid a$ E $37^2 \mid b$ MENTRE $37^3 \nmid a$

$\Rightarrow MCD = 37^2$.

ES.: CALCOLARE $MCD(389, 167)$ E LA CORRISPONDENTE IDENTITÀ DI BEZOÚT.

USIAMO A.E.:

$$389 = 2 \cdot 167 + 55 \qquad (1)$$

$$167 = 3 \cdot 55 + 2 \qquad (2)$$

$$55 = 2 \cdot 27 + \boxed{1} \qquad (3)$$

$$2 = 2 \cdot 1 + 0$$

$\Rightarrow MCD = 1.$

PER CALCOLARE L'IDENTITÀ DI BEZOÚT SVOLGO A.E. A RITROSO, ESPLICITANDO i RESTI:

$$1 = 55 + 2(-27)$$

(3) ↗

$$= 55 + \left(167 + 55(-3)\right)(-27)$$

(2) ↗

$$= 167(-27) + 55 \cdot (82)$$

(1) ↗

$$= 167(-27) + \left(389 + 167(-2)\right)(82)$$

$$= 389 \cdot (82) + 167(-191)$$

QUINDI L'ID. DI BEZOÚT E

$$1 = \underset{a}{389} \cdot \underset{x}{(82)} + \underset{b}{167} \underset{y}{(-191)}$$

SONDAGGIO: L'INVERSA DELLA PERMUTAZIONE

$$81357246 \quad (\in S_8)$$

È

a) 64275318 9%

b) 26374851 ~~81%~~ 80% ✓

c) 18642753 2%

d) 26374815 0%

e) NESSUNA DI QUESTE. 9%

(56)

ES.: CALCOLARE MCD(1137, 419) E LA CORRISPONDENTE ID. DI BEZOUT.

USIAMO A.E.

$1137 = 2 \cdot 419 + 299$ (1)

$419 = 1 \cdot 299 + 120$ (2)

$299 = 2 \cdot 120 + 59$ (3)

$120 = 2 \cdot 59 + 2$ (4)

$59 = 29 \cdot 2 + \boxed{1}$ (5) $\quad 2 = 2 \cdot 1 + 0$

PERTANTO $MCD(1137, 419) = 1$. CALCOLIAMO L'ID. DI BEZOÚT SVOLGENDO A.E. A RITROSO:

$$1 = 59 + 2(-29)$$

(5)

$$= 59 + \left(120 + 59(-2)\right)(-29)$$

(4)

$$= 59\left(1 + (-2)(-29)\right) + 120(-29)$$

$$= 59(59) + 120(-29)$$

(3)

$$= \left(299 + 120 \cdot (-2)\right) \cdot (59) + 120(-29)$$

$$= 299(59) + 120(-147)$$

(2) ↓

$$= 299(59) + \big(419 + 299(-1)\big) \cdot (-147)$$

$$= 299(206) + 419(-147)$$

(1) ↓

$$= \big(1137 + 419(-2)\big) \cdot (206) + 419 \cdot (-147)$$

$$= 1137 \cdot (206) + 419(-559)$$

QUINDI L'ID. DI BEZOÚT È

$$\underline{1} = 1137.(206) + 419(-559).$$

" " " " "

(a,b) a x b y

ES.: DIMOSTRARE CHE L'A.E. SU a, b COMPIE AL PIÙ

$$2 \cdot \log_2(b)$$

ITERAZIONI $(a \geq b \geq 2)$.

SIANO $r, r_1, r_2, \ldots, q, q_1, q_2, \ldots$ COME IN A.E. ALLORA

$$r_1 \leq \frac{b}{2}.$$

INFATTI. ABBIAMO CHE

$$a = b \cdot q + r \qquad 0 \leq r < b$$

$$b = q_1 \cdot r + r_1 \qquad 0 \leq r_1 < r .$$

SE $r \leq \frac{b}{2} \Rightarrow r_1 < \frac{b}{2} \Rightarrow$ O.K.

SE $r > \frac{b}{2} \Rightarrow 2 \cdot r > b \Rightarrow q_1 = 1 \Rightarrow$

$r_1 = b - r \Rightarrow r_1 = b - r \leq \frac{b}{2} \Rightarrow$ O.K.

DIMOSTRIAMO L'ESERCIZIO PER INDUZIONE SU $b \geq 2$.

SE $b = 2$ ALLORA

$$a = 2 \cdot q + r \quad , \quad 0 \leq r < 2 .$$

SE $r = 0 \Rightarrow$ 1 ITERAZIONE $\Rightarrow$ O.K.

SE $r = 1 \Rightarrow$

$$\underset{\text{"}}{\underset{b}{2}} = q_1 \cdot \overset{\text{"}}{\underset{r}{1}} + r_1 \quad , \quad 0 \leq r_1 < \overset{\text{"}}{\underset{r}{1}}$$

QUINDI $r_1 = 0 \Rightarrow$ 2 ITERAZIONI $\Rightarrow$ O.K.

SUPPONIAMO L'ESERCIZIO VERO PER TUTTI i NUMERI $< b$. SAPPIAMO CHE

$$(a,b) = (b,r) = (r,r_1).$$

MA $r_1 \leq \frac{b}{2} \Rightarrow$ PER INDUZIONE, L'A.E. SU r, r_1 COMPIE AL PIÚ

$2 \cdot \log_2(r_1)$ ITERAZIONI $\Rightarrow$ L'A.E.

SU a, b COMPIE AL PIÙ

$$2 \cdot \log_2(r_1) + 2$$

ITERAZIONI. MA $r_1 \leq \frac{b}{2}$, QUINDI

$$2 \cdot \log_2(r_1) + 2 \leq 2 \cdot \log_2\left(\frac{b}{2}\right) + 2$$

$$= 2\left(\log_2(b) - \log_2(2)\right) + 2$$

$\left(\log_2(2) = 1\right)$

$$\equiv 2 \cdot \log_2(b).$$

ES.: SIANO $a, b \in \mathbb{P}$.

$$(a+1, b+1) \stackrel{?}{=} (a, b) + 1 \quad ?$$

SE $b = 1$ ALLORA AVREI

$$(a+1, 2) = (a, 1) + 1 = 1 + 1 = 2$$

MA È VERO CHE $(a+1, 2) = 2$ PER $\forall\, a \in \mathbb{P}$? NO, PER ES., $(4+1, 2) = 1 \neq 2$

QUINDI, NO (E.g. $a = 4, b = 1$).

ES.: SIANO $a, b \in \mathbb{P}$. DIMOSTRARE CHE

$$(a, b) = 1 \Rightarrow (a^2, b) = 1.$$

PER ASSURDO. SIA $(a^2, b) \geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid (a^2, b) \Rightarrow p \mid a^2$ E $p \mid b \Rightarrow p \mid a$ E $p \mid b \Rightarrow$ ASSURDO PERCHE' $(a, b) = 1$. PERTANTO $(a^2, b) = 1$.

ES. : SIANO $a, b, c \in \mathbb{P}$. DIMOSTRARE CHE

$$\begin{cases} (a,c) = 1 \\ (b,c) = 1 \end{cases} \Rightarrow (ab, c) = 1.$$

PER ASSURDO. SIA $(ab, c) \geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid (ab, c) \Rightarrow p \mid ab$ E $p \mid c \Rightarrow (\sigma\ p \mid a\ \sigma\ p \mid b)$ E $p \mid c$

$\Rightarrow \sigma\,(p \mid a$ E $p \mid c)\ \sigma\,(p \mid b$ E $p \mid c) \Rightarrow$

σ (ASSURDO PERCHE' $(a,c)=1$) σ

(ASSURDO PERCHE' $(b,c)=1$) $\Rightarrow$ ASSURDO.

PERTANTO $(ab,c)=1$.

ES.: SIANO $a, b \in \mathbb{P}$.

$$(a,b) = 1 \overset{?}{\Rightarrow} (a^2, b^2) = 1 \quad ?$$

PER ASSURDO. SIA $(a^2, b^2) \geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid a^2$ E $p \mid b^2 \Rightarrow$ $p \mid a$ E $p \mid b \Rightarrow$ ASSURDO PERCHÈ $(a,b) = 1$. QUINDI, SÌ, È SEMPRE VERO.

SONDAGGIO: UNA PROPOSIZIONE LOGICAMENTE EQUIVALENTE A

$$P \to Q$$

È: (66)

a) $(\neg Q) \to P$ 1%

b) $(\neg Q) \to (\neg P)$ 85% ✓

c) $Q \to (\neg P)$ 7%

d) $Q \to P$ 1%

e) NDQ. 4%