

CAP. 3 NUMERI:

3.1 IL PRINCIPIO DI INDUZIONE:

ci sono 3 modi per dimostrare
che $A \rightarrow B$:

I) DIMOSTRAZIONE DIRETTA:

un ragionamento che mostra
che se A è vero allora B

E' PURE NECESSARIAMENTE VERO.

2) DIMOSTRAZIONE PER ASSURDO:

UN RAGIONAMENTO CHE ASSUME
CHE A e $\neg B$ SIANO ENTRAMBE VERE
E DEDUCE UNA CONTRADDIZIONE.

3) IL PRINCIPIO DI INDUZIONE MATEMATICA:

Sia $P(m)$ un predicato (dove $m \in \mathbb{P}$) tale che:

i) $P(1)$ è vero;

ii) $P(m) \Rightarrow P(m+1)$ per $\forall m \in \mathbb{P}$.

Allora $P(m)$ è vera per $\forall m \in \mathbb{P}$.

PRINCIPIO DI INDUZIONE COMPLETA:

SIA $P(n)$ UN PREDICATO (DOVE
 $n \in \mathbb{P}$) TALE CHE:

- 1) $P(1)$ È VERO
- 2) $P(1) \wedge P(2) \wedge \dots \wedge P(n) \Rightarrow P(n+1)$

PER OGNI $n \in \mathbb{P}$.

ALLORA $P(n)$ È VERA PER $\forall n \in \mathbb{P}$.

NOTAZIONE: Sia $\{\alpha_i\}_{i=1,2,\dots} \subset \mathbb{R}$.

SCRIVIAMO

$$\sum_{i=1}^m \alpha_i$$

PER DIRE

$$\alpha_1 + \alpha_2 + \dots + \alpha_m$$

E.g. DIMOSTRARE CHE:

$$\sum_{i=1}^m i = \frac{m(m+1)}{2} \quad (\mathbb{P}(m))$$

$\forall m \in \mathbb{P}$.

i) $\mathbb{P}(i)$ È VERA?

$$\sum_{i=1}^l i = l = \frac{l(l+1)}{2} \Rightarrow \text{Si}$$

2) E' VERO CHE $P(m) \Rightarrow P(m+1)$?

SIA $P(m)$ VERA. ALLORA

$$\sum_{i=1}^m i = \frac{m(m+1)}{2}$$

MA ALLORA

$$\begin{aligned}\sum_{i=1}^{m+1} i &= \sum_{i=1}^m i + (m+1) \stackrel{(P(m))}{=} \frac{m(m+1)}{2} + (m+1) \\ &= (m+1)\left(\frac{m}{2} + 1\right) = \frac{(m+1)(m+2)}{2}\end{aligned}$$

$\Rightarrow P(m+1)$ È VERO. QUINDI $P(m)$ È VERO
PER OGNI $m \in \mathbb{P}$. \square

ES. [1]: DIMOSTRARE CHE

$$\sum_{i=1}^m (2i-1) = m^2$$

per $\forall m \in \mathbb{P}$.

(PER ES., $m=3 \Rightarrow 1+3+5=3^2$)

3.2 IL PRINCIPIO DEL BUON

ORDINAMENTO:

PRINCIPIO DEL BUON ORDINAMENTO (WOP)
(WELL ORDERING PRINCIPLE):

Sia $S \subseteq P \Rightarrow \exists m \in S$ TALE CHE

$x \in S \Rightarrow x \geq m$.

OSS. FALSO PER \mathbb{Z} . ($S = \{-1, -2, -3, \dots\}$
NON HA UN MINIMO).

OSS. WOP NON VALE PER $\mathbb{Q}_{>0}$ ($\stackrel{\text{def}}{=} \{x \in \mathbb{Q} : x > 0\}$). PER ES. $S = \{1, \frac{1}{2}, \frac{1}{3}, \dots\}$ NON HA UN MINIMO.

TEO:

WOP \Leftrightarrow INDUZIONE

DIM: OMESSA. \square

ES. [1+]: DIMOSTRARE PER INDUZIONE CHE

$$\sum_{i=1}^m \frac{i(i-1)}{2} = \frac{(m+1) \cdot m \cdot (m-1)}{6} \quad \forall m \in \mathbb{P}.$$

ES. [1+]: DIMOSTRARE PER ASSURDO CHE

α irrazionale $\Rightarrow \sqrt[5]{\alpha}$ irrazionale.

("irrazionale" significa $\notin \mathbb{Q}$).

3.3 NUMERI NATURALI, INTERI E

RAZIONALI

i numeri NATURALI (\circ positivi) sono

$$P \stackrel{\text{def}}{=} \{1, 2, 3, \dots\}$$

i NUMERI INTERI SONO

$$\mathbb{Z} \stackrel{\text{def}}{=} \{0, 1, -1, 2, -2, \dots\}$$

i NUMERI RAZIONALI SONO

$$\mathbb{Q} \stackrel{\text{def}}{=} \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

FORMALMENTE i NUMERI RAZIONALI SONO
LE CLASSI DI EQUIVALENZA DI
 $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ RISPETTO ALLA REL.

DI EQUIV. STUDIATA IN UN ESERCIZIO
PRECEDENTE

(IN EFFETTI $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \frac{-1}{-2} = \dots$)

3.4 NUMERI REALI

SI INDICANO CON \mathbb{R} , PER LA DEF.
VEDI IL CORSO DI ANALISI.
INTUITIVAMENTE: UN NUMERO REALE
E' LA LUNGHEZZA DI UN SEGMENTO.

3.5 NUMERI COMPLESSI

i NUMERI COMPLESSI SONO

$$\mathbb{C} \stackrel{\text{def}}{=} \left\{ \alpha + i\beta : \alpha, \beta \in \mathbb{R} \right\}$$

DOVE

$$i \stackrel{\text{def}}{=} \sqrt{-1}.$$

Si A $z \in \mathbb{C}$, $z = \alpha + i\beta$ ($\alpha, \beta \in \mathbb{R}$).

DEF. α si dice la PARTE REALE di z .

β " " " " " PARTE IMMAGINARIA di z .

DEF. $i (= \sqrt{-1})$ si dice l'UNITÀ IMMAGINARIA (o CONIUGATO)

DEF. il COMPLESSO CONIUGATO di z è

$$\bar{z} \stackrel{\text{def}}{=} \alpha - i\beta$$

SIANO $z, w \in \mathbb{C}$, $z = \alpha + i\beta$, $w = c + id$ ($\alpha, \beta, c, d \in \mathbb{R}$). ALLORA LA SOMMA di z e w è

$$z + w \stackrel{\text{def}}{=} (\alpha + c) + i(\beta + d)$$

il PRODOTTO di w e z è

$$z \cdot w = (a+ib)(c+id)$$

$$= a \cdot c + iad + ibc + i^2 \cdot bd$$

$$(i^2 = -1) \rightarrow \stackrel{\cong}{=} (ac - bd) + i(ad + bc).$$

E.g. $z = 2-i$, $w = 3+4i$. ALLORA

$$z+w = 5+3i$$

$$z \cdot w = (2-i) \cdot (3+4i) = 6+8i-3i-4i^2$$

$$= 10 + 5i$$

\uparrow
 $(i^2 = -1)$

COME SI DIVIDONO 2 NUMERI COMPLESSI
 Si z, w (CON $w \neq 0$)?

"RAZIONALIZZANDO"

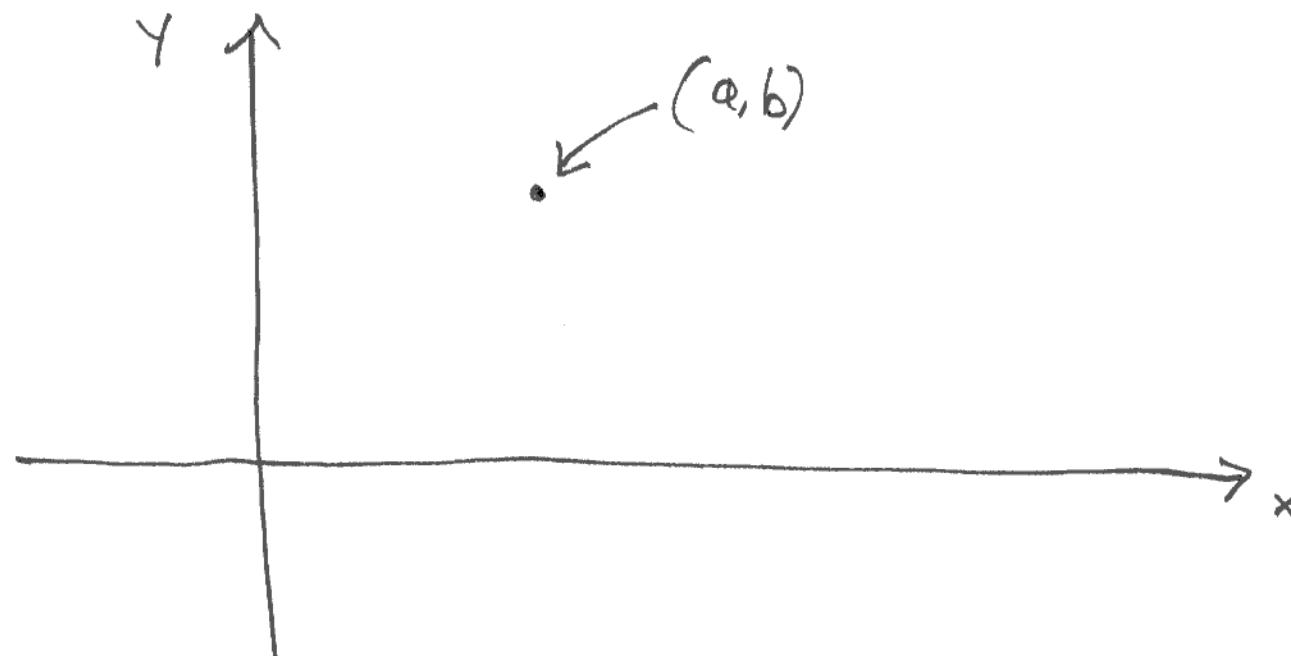
E.g. $z = 2 - i$, $w = 3 + 4i$. ALLORA

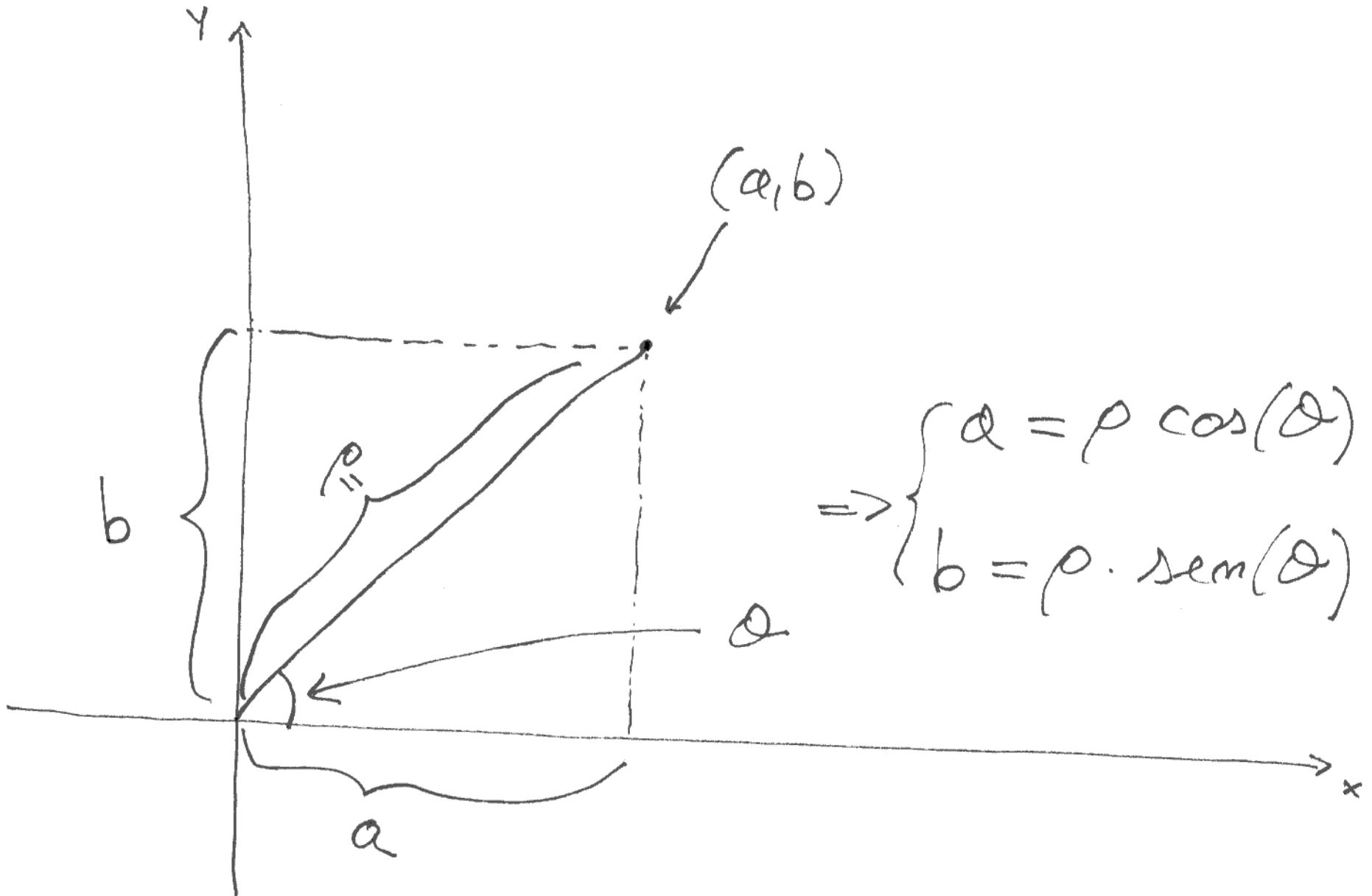
$$\frac{z}{w} = \frac{2-i}{3+4i} = \frac{(2-i)(3-4i)}{(3+4i)(3-4i)} =$$

$$= \frac{6 - 3i - 8i + 4i^2}{9 - 12i + 12i - 16i^2} = \frac{2 - 11i}{25} = \frac{2}{25} - i\left(\frac{-11}{25}\right)$$

$$\left(= \frac{2}{25} + i\left(\frac{-11}{25}\right) \right)$$

SiA $z \in \mathbb{C}$, $z = a + ib$ ($a, b \in \mathbb{R}$).





QUINDI

$$\begin{aligned}\cancel{z} &= \rho \cos(\theta) + i \rho \sin(\theta) \\ &= \rho (\cos(\theta) + i \sin(\theta))\end{aligned}$$

QUESTA È LA FORMA POLARE DI z

ρ SI DICE IL MODULO DI z

θ " " L' ARGOMENTO DI z

SI SCRIVE $\|z\| \stackrel{\text{def}}{=} \rho (o |z|)$.

SIA $z = \alpha + ib$. ALLORA

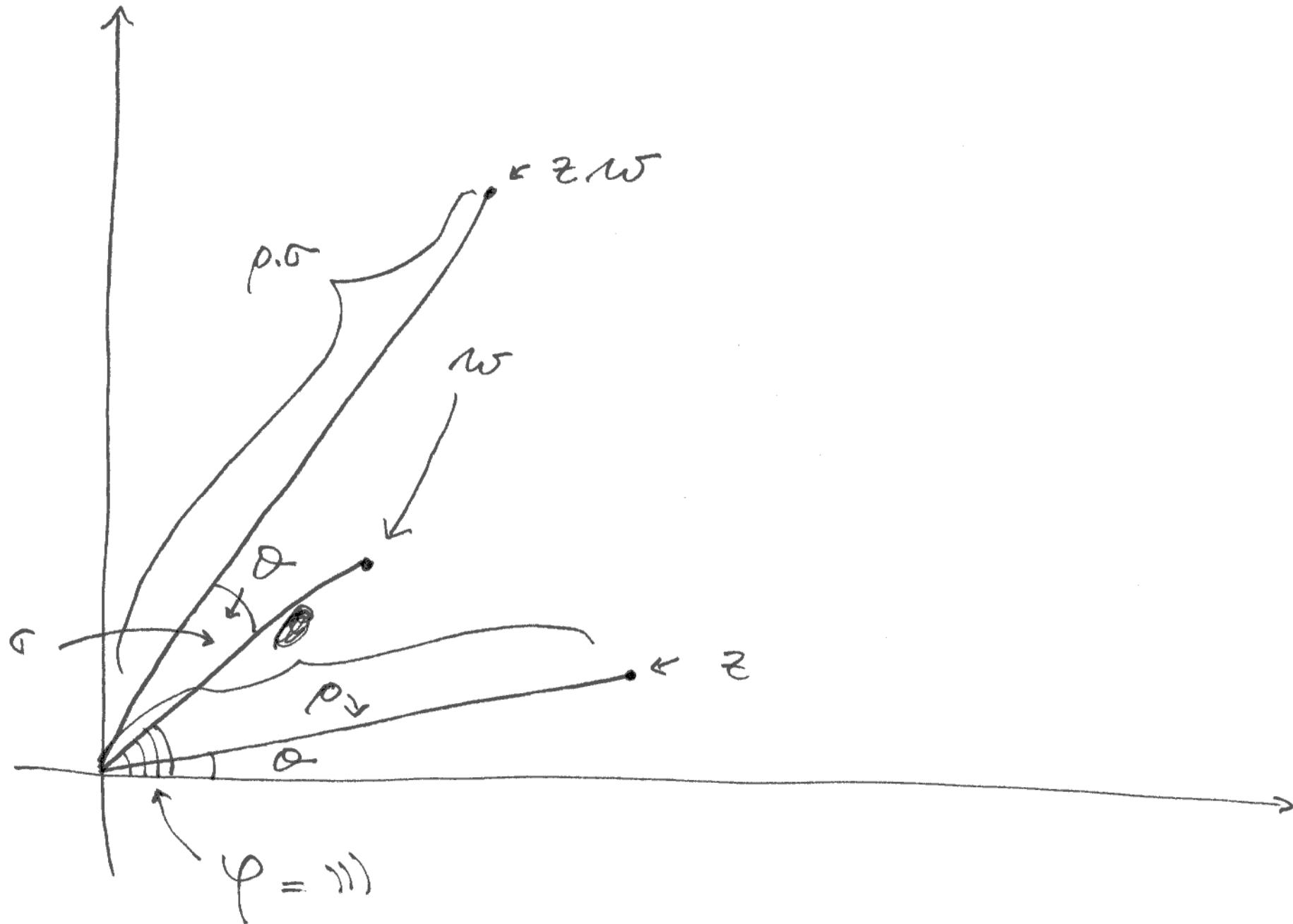
$$\|z\|^2 = \rho^2 = \alpha^2 + b^2 \quad (\Rightarrow \|z\| = \sqrt{\alpha^2 + b^2})$$

e

$$\|z\|^2 = z \cdot \bar{z}$$

$$(z \cdot \bar{z} = (\alpha + ib) \cdot (\alpha - ib) = \alpha^2 + i\cancel{\alpha}b - i\cancel{\alpha}b - b^2 \cdot i^2)$$

SIANO $z, w \in \mathbb{C}$, SIANO $z = \rho(\cos(\theta) + i \sin(\theta)) \in w = \sigma \cdot (\cos(\varphi) + i \sin(\varphi))$ LE
LORO FORME POLARI. ALLORA



$$w \cdot z = (\rho \cos(\theta) + i \rho \sin(\theta)) \cdot (r \cos(\varphi) + i r \sin(\varphi))$$

= ---

$$= \rho r (\cos(\theta + \varphi) + i \sin(\theta + \varphi)).$$

ES. [1]: Sia $z = 1+i$. CALCOLARE

$$\bar{z}^{1970}$$

3.6 NUMERI PRIMI E COMPOSTI

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

DEF. SI DICE CHE a DIVIDE b (a CHE
 b È UN MULTIPLo DI a), SCRITTO

$a | b$ SE $\exists k \in \mathbb{Z}$ TALE CHE

$$b = k \cdot a$$

OSS. $a | b \Rightarrow a \leq b$.

OSS. $a|b \wedge b|c \Rightarrow a|c$

OSS. $a|b \wedge a|c \Rightarrow a|(xb+yc)$

PER OGNI $x, y \in \mathbb{Z}$)

SIA $a \in \mathbb{P}$.

DEF. a È UN NUMERO PRIMO SE

$b|a \Rightarrow b=1 \sigma b=a,$

e $a \geq 2$.

IN CASO CONTRARIO a E' UN NUMERO
COMPOSTO.

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

DEF. a E b SI DICONO COPRIMI SE
(o PRIMI TRA LORO) SE

$$\begin{matrix} c | a \\ c | b \end{matrix} \Rightarrow c = \pm 1.$$

OSS. $a \in P \Rightarrow a | a$.
 $(p \neq q)$



OSS. $p, q \in P, p \neq q$ PRIMI $\Rightarrow p \neq q$ SONO
COPRIMI.



TEO 3.6.1: SIA $n \in P$, $n \geq 2$. ALLORA
 n E' PRODOTTO DI NUMERI PRIMI.

DIM. INDUZIONE. SE $n=2 \Rightarrow 2=2$
E 2 E' PRIMO \Rightarrow O.K.

SUPPONIAMO IL TEOREMA VERO PER

$\forall m \in \mathbb{P}, m \leq m$. SE $m+1$ E' PRIMO

$\Rightarrow m+1 = m+1 \Rightarrow$ O.K. SE $m+1$ NON E'

PRIMO $\Rightarrow \exists a, b \in \mathbb{P}$ TALI CHE $1 < a$

$< m+1, 1 < b < m+1, E$

$$m+1 = a \cdot b. \quad (*)$$

MA, POICHE' $a \leq m$ E $b \leq m$, \Rightarrow
PER INDUZIONE IL TEOREMA

VALE PER $a \in$ PER $b \Rightarrow a \in b$ SONO
PRODOTTO DI NUMERI PRIMI \Leftrightarrow_{m+1}
E' PRODOTTO DI NUMERI PRIMI. □

SIA $m \in \mathbb{P}$.

DEF. m SI DICE PERFETTO SE m
E' LA SOMMA DEI SUOI DIVISORI
 $< m$.

E.g. 6 E' PERFETTO, PERCHE' $1+2+3=6$

E.g. 8 NON È PERFETTO (PERCHE'
 $1+2+4 \neq 8$)

~~PRO*~~

OSS. p PRIMO $\Rightarrow p$ NON È PERFETTO

PROBLEMA APERTO: ESISTONO NUMERI
PERFETTI DISPARI ?

TEO 3.6.2: CI SONO INFINTI NUMERI PRIMI.

DIM. PER ASSURDO, SUPPONIAMO CHE

$\{p_1, p_2, \dots, p_m\}$ SIANO TUTTI I NUMERI

PRIMI. SIA

$$N \stackrel{\text{def}}{=} p_1 \cdot p_2 \cdot \dots \cdot p_m + 1.$$

ALLORA, PER 3.6.1, N E' PRODOTTO
DI NUMERI PRIMI $\Rightarrow \exists q \in P, q$ PRIMO

TALE CHE $q \mid N$. QUINDI $q \mid (p_1 \cdots p_m + 1)$.

ALLORA $q \notin \{p_1, p_2, \dots, p_m\}$. INFATTI, SE $q = p_i$

$$\Rightarrow q \mid N \text{ e } q \mid p_1 \cdots p_m \Rightarrow q \mid (N - p_1 \cdots p_m)$$

$$\Rightarrow q \mid 1 \Rightarrow q \leq 1, \text{ ASSURDO PERCHE'}$$

q E' PRIMO. SIMILMENTE $q = p_2$ E'

ASSURDO, ETC... QUINDI CI SONO
INFINITI NUMERI PRIMI. \square

QUANTO SONO FREQUENTI i NUMERI PRIMI?

SIA, PER $m \in \mathbb{P}$, PONIAMO

$$\pi(n) \stackrel{\text{def}}{=} |\{m \leq n : m \text{ è PRIMO}\}|.$$

($|A| \stackrel{\text{def}}{=} \text{NUMERO DI ELEMENTI DI } A$).

E.g. $\pi(10) = |\{2, 3, 5, 7\}| = 4$.

TEO:

$$\lim_{n \rightarrow +\infty} \frac{\pi(n)}{\left(\frac{n}{\ln(n)}\right)} = 1 .$$

ES. [2+]: DIMOSTRARE CHE ESISTONO
INFINITI $k \in \mathbb{P}$ TALI CHE

$$6 \cdot k + 5$$

E' PRIMO.

ES. [2-]: FINO A \approx 25 ANNI FA IL
NUMERO PRIMO PIÙ GRANDE CONO-
SCIUTO ERA

$$P \stackrel{\text{def}}{=} 2^{216091} - 1.$$

DIMOSTRARE CHE p HA 65050
CIFRE, E CHE LE ULTIME 3 SONO
447.

3.7 ALGORITMO EUCLIDEO

SI ANO $a, b \in \mathbb{P}$.

DEF. IL MASSIMO COMUN DIVISORE

DI $a \in b$, (SCRITTO $\text{MCD}(a, b)$, o
 (a, b) , o $\text{GCD}(a, b)$) E'

$$\text{MCD}(a, b) \stackrel{\text{def}}{=} \max \{ c \in \mathbb{P} : c | a \wedge c | b \}.$$

COME CALCOLARE $\text{MCD}(a, b)$?

RICORDIAMO CHE:

PROP. 3.7.1: SIANO $a, b \in \mathbb{P}$, $a \geq b$.

ALLORA $\exists q, r \in \mathbb{Z}$ TALI CHE

$$a = b \cdot q + r$$

E

$$0 \leq r < b.$$

DIM. E' NOTA. \square

ALGORITMO EUCLIDEO:

SIANO $a, b \in \mathbb{R}$. SIA $a \geq b$. ALLORA

$\exists q, r \in \mathbb{Z}$ TALI CHE

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

SE $r=0 \Rightarrow \text{MCD} = b$ (LO VEDREMO).

SE $r>0 \Rightarrow \exists q_1, r_1 \in \mathbb{Z}$ TALI CHE

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

SE $r_1 = 0 \Rightarrow \text{MCD} = r_1$ (LO VEDREMO).

SE $r_1 > 0 \Rightarrow \exists q_2, r_2 \in \mathbb{Z}$ TALI CHE

$$r_1 = r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

SE $r_2 = 0 \Rightarrow \text{MCD} = r_1$ (LO VEDREMO).

SE $r_2 > 0 \Rightarrow \exists q_3, r_3 \in \mathbb{Z}$ TALI CHE

$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

SE $r_3 = 0 \Rightarrow \cancel{\text{MCD}} = r_2$ (LO VEDREMO)

SE $r_3 > 0 \Rightarrow \exists q_4, r_4 \in \mathbb{Z}$ ETC...

IN GENERALE OTTENIAMO DUE SEQUENZE DI NUMERI TALI CHE

$$\alpha = b \cdot q + r, \quad 0 \leq r < b$$

$$b = r_1 \cdot q_1 + r_1, \quad 0 \leq r_1 < r$$

$$r_1 = r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1$$

:

:

$$r_i = r_{i+1} \cdot q_{i+2} + r_{i+2}, \quad 0 \leq r_{i+2} < r_{i+1}$$

:

Poiché $b > r > r_1 > r_2 > \dots \geq 0$

$\Rightarrow \exists k \in \mathbb{P}$ TALE CHE $r_k = 0 \Rightarrow$

L'A.E. TERMINA (E MCD = r_{k-1}).

SIANO $a, b, q_1, q_2, \dots, r_1, r_2, \dots$ COME NEL A.E.

SIA $k \in \mathbb{P}$ TALE CHE $r_{k+1} = 0$. ALLORA

$$(k-1) \quad r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$$

\Downarrow
 0

$$\Rightarrow r_k \mid r_{k-1} \text{ MA}$$

$$(k-2) \quad r_{k-2} = r_{k-1} \cdot q_k + r_k$$

$\Rightarrow r_k | r_{k-1} \cdot MA$

(k-3) $r_{k-3} = r_{k-2} \cdot q + r_{k-1}$

$\Rightarrow r_k | r_{k-3} \cdot MA$ ETC... QUINDI

$r_k | r_{k-1}, r_k | r_{k-2}, \dots, r_k | r_1, r_k | r$
MA

$$(2) \quad b = r \cdot q_1 + r_1$$

$$\Rightarrow r_k | b. \text{ MA}$$

$$(1) \quad a = b \cdot q + r$$

$\Rightarrow r_k | a$. QUINDI r_k E' UN DIVISORE
COMUNE DI $a \in b$.

SIA $c \in P$ TALE CHE $c | a \in b$.

MA

$$(1) \quad a = b \cdot q + r$$

$$\Rightarrow c | r \quad (= a - b \cdot q). \text{MA}$$

$$(2) \quad b = r \cdot q_1 + r_1$$

$$\Rightarrow c | r_1 \quad (= b - r \cdot q). \text{MA}$$

$$r = r_1 \cdot q_2 + r_2$$

$\Rightarrow c | r_2 \left(= r - r_1 q_2 \right)$ ETC.. QUINDI

$c | r_1, c | r_2, \dots, c | r_k$

$\Rightarrow c | r_k \Rightarrow c \leq r_k$. PERTANTO

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

E.g. CALCOLARE $\text{MCD}(78, 18)$. ABBIAMO
" " "
 a b

$$78 = 18 \cdot 4 + \boxed{6} \leftarrow$$

$$18 = 6 \cdot 3 + 0$$

$$\Rightarrow \text{MCD}(78, 18) = 6.$$

OSS. SIANO $a, b, q, r, \text{ETC.}$ COME IN

A.E., ALLORA

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

3.8 CONSEGUENZE DI A. GE.

PROP. 3.8.1: SIANO $a, b \in \mathbb{P}$. ALLORA $\exists x, y \in \mathbb{Z}$ TALI CHE

$$(a, b) = a \cdot x + b \cdot y \quad \begin{array}{l} \text{(IDENTITÀ DI} \\ \text{BEZOÚT)} \end{array}$$

DIM. SIA $a \geq b$. INDUZIONE SU $b \in \mathbb{P}$.

SE $b=1 \Rightarrow b | a \Rightarrow (a, b) = b = a \cdot 0 + b \cdot 1$
 \Rightarrow O. K.

SIA $b \geq 2$. ALLORA $\exists q, r \in \mathbb{Z}$ TALI CHE

$a = b \cdot q + r$, CON $0 \leq r < b$. SE $r = 0 \Rightarrow$

$b | a \Rightarrow (a, b) = b = a \cdot 0 + b \cdot 1 \Rightarrow$ O.K. SE

$r > 0 \Rightarrow (a, b) = (b, r) \Rightarrow$ PER INDUZIONE

$\exists x, y \in \mathbb{Z}$ TALI CHE $(b, r) = b \cdot x + r \cdot y$

QUINDI

$$\begin{aligned} (a, b) &= b \cdot x + r \cdot y = b \cdot x + (a - b \cdot q) \cdot y \\ &= b \cdot (x - q \cdot y) + a \cdot y \end{aligned} \quad \square$$

PROP. 3.8.2: SIANO $a, b \in \mathbb{P}$. ALLORA

$$\text{MCD}(a, b) = \min \left(\left\{ a \cdot x + b \cdot y : x, y \in \frac{\mathbb{R}}{\mathbb{Z}} \right\} \cap \mathbb{P} \right).$$

DIM. OMESSA. \square

ES. [1+]: SIANO $a, b \in \mathbb{P}$. E' VERO

CHE

$$\text{MCD}(a, b) = 1 \stackrel{?}{\Rightarrow} \text{MCD}(a+b, a-b) = 1 ?$$

PROP. 3.8.3: SIANO $p, \alpha, b \in \mathbb{P}$ TALI CHE
 $p \mid \alpha \cdot b$ E $p \in \mathbb{P}$ PRIMO. ALLORA O $p \mid \alpha$
O $p \mid b$.

DIM. SE $p \mid \alpha \Rightarrow$ O.K. SE $p \nmid \alpha \Rightarrow$
 $(\alpha, p) = 1$ (SE $c \mid \alpha \in c \mid p \Rightarrow c = 1$
O $c = p \Rightarrow c = 1$). QUINDI, PER 3.8.1
 $\Rightarrow \exists x, y \in \mathbb{Z}$ TALI CHE

$$1 = (\alpha, p) = \alpha \cdot x + p \cdot y.$$

QUINDI

$$b = \alpha \cdot b \cdot x + p \cdot b \cdot y.$$

$$\text{MA } p \mid \alpha \cdot b \text{ E } p \mid p \cdot b \cdot y \Rightarrow p \mid b. \square$$

OSS: FALSO, IN GENERALE, SE P NON
E' PRIMO. PER ES.

$$4 \mid 6 \cdot 2 \text{ MA } 4 \nmid 6 \text{ E } 4 \nmid 2.$$

OSS. $m, a, b \in \mathbb{P}$ TALI CHE $m | a \cdot b$
 $E(m, a) = 1 \Rightarrow m | b.$

TEO 3.8.4: (TEOREMA FONDAMENTALE

DELL' ARITMETICA): SIA $n \in \mathbb{P}$, $n \geq 2$.

ALLORA n SI ESPRIME COME
PRODOTTO DI NUMERI PRIMI IN
UNO ED UN SOLO MODO, A PARTE
L'ORDINE DEI FATTOREI.

(E.g.: $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$)

DIM. SAPPIAMO GIÀ L'ESISTENZA (3.6.1).

VEDIAMO L'UNICITÀ. INDUZIONE COMPLETA.

SE $m=2 \Rightarrow 2=2 \Rightarrow$ o.k. SIA $m \geq 3$.

SUPPONIAMO IL TEOREMA VERO PER

$\forall m \in \mathbb{P}$ TALE CHE $m \leq m-1$. VOGLIAMO

DIMOSTRARE IL TEOREMA PER m .

PER ASSURDO, SIANO $p_1, \dots, p_r, q_1, \dots, q_s \in P$
 $(r, s \in \mathbb{N})$ TALI CHE $p_1, \dots, p_r, q_1, \dots, q_s$
 SONO PRIMI E

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s. \quad (*)$$

ALLORA $p_1 \mid n \Rightarrow p_1 \mid (q_1 \cdot q_2 \cdot \dots \cdot q_s) \stackrel{(3.8.3)}{\Rightarrow}$
 $\exists 1 \leq i \leq s$ TALE CHE $p_1 \mid q_i \Rightarrow p_1 = q_i$.
 (PERCHE' q_i E' PRIMO). MA ALLORA

$$\frac{m}{p_1} = p_2 \cdots p_n = q_1 \cdots q_{i-1} \cdot q_{i+1} \cdots q_s \quad (**)$$

E $\frac{m}{p_1} \in P$ E $\frac{m}{p_1} < m \Rightarrow$ INDUZIONE

\Rightarrow LE DUE ESPRESSIONI IN $(**)$

COINCIDONO A MENO DELL'ORDINE

DEI FATTORI \Rightarrow ANCHE QUELLE IN

$(*)$ COINCIDONO. \square

3.9 EQUAZIONI DIOFANTEE LINEARI

TEO 3.9.1: SIANO $a, b, m \in \mathbb{P}$. ALLORA

ESISTONO $x, y \in \mathbb{Z}$ TALI CHE

$$a \cdot x + b \cdot y = m$$

SE E SOLO SE

$$(a, b) \mid m.$$

DIM. SIANO $x, y \in \mathbb{Z}$ TALI CHE

$$\underline{a} \cdot x + b \cdot y = n.$$

MA $(a, b) | a \wedge (a, b) | b \Rightarrow (a, b) | n$.

VICEVERSA. SUPPONIAMO CHE $(a, b) | n$.

ALLORA $\exists k \in \mathbb{Z}$ TALE CHE

$$n = (a, b) \cdot k.$$

MA, PER 3.8.1, $\Rightarrow \exists x, y \in \mathbb{Z}$ TALI CHE

$$(a, b) = a \cdot x + b \cdot y$$

QUINDI

$$m = (a, b) \cdot k = a \cdot (x \cdot k) + b \cdot (y \cdot k). \square$$

TEO 3.9.2: SIANO $a, b, m \in \mathbb{P}$ TALI CHE
 $(a, b) \mid m$. ALLORA TUTTE LE
SOLUZIONI DI

$$a \cdot x + b \cdot y = m \quad (\square)$$

SONO DELLA FORMA

$$\begin{cases} x = x_0 - \left(\frac{b}{d}\right)t \\ y = y_0 + \left(\frac{a}{d}\right)t \end{cases}$$

DOVE $d \stackrel{\text{def}}{=} (a, b)$, $t \in \mathbb{Z}$, E $x_0, y_0 \in \mathbb{Z}$

SONO UNA SOLUZIONE PARTICOLARE

Di (□).

DIM. OMESSA. □

OSS. EQUIVALENTEMENTE:

ABBIAMO CHE, DATI $x, y \in \mathbb{Z}$,

$$a \cdot x + b \cdot y = m$$



$\exists t \in \mathbb{Z}$ TALE CHE

$$x = x_0 - \left(\frac{b}{d}\right) \cdot t$$

$$E \quad y = y_0 + \left(\frac{a}{d}\right) \cdot t$$

DOVE $d \stackrel{\text{df}}{=} (a, b)$ E $x_0, y_0 \in \mathbb{Z}$ SODDISFANO \square .

3.10 LE CLASSI DI RESTO

2 COLORI

... -5 -4 -3 -2 -1 0 1 2 3 4 5 ...

... 1 0 1 0 1 0 1 0 1 0 1 ...

3 COLORI

... -4 -3 -2 -1 0 1 2 3 4 5 ...

... 2 0 1 2 0 1 2 0 1 2 ...

m COLORI

SIA $m \in \mathbb{P}$. DEFINIAMO UNA RELAZIONE \equiv_m
SU \mathbb{Z} PONENDO

$$a \equiv_m b \iff m \mid (b-a)$$

$\forall a, b \in \mathbb{Z}$. LA RELAZIONE \equiv_m SI CHIAMA
RELAZIONE DI CONGRUENZA MODULO m .

PROP. 3.10.1: SIA $m \in \mathbb{P}$. ALLORA \equiv_m È
UNA RELAZIONE DI EQUIVALENZA, SU \mathbb{Z} .
DIM. VEDI SEZ. 1.4 ($m=3$). \square

$$[0]_2 = \{0, 2, -2, 4, -4, \dots\}$$

$$[1]_2 = \{1, 3, -1, 5, -3, \dots\}$$

$$[1]_6 = \{1, 7, -5, 13, -11, \dots\}$$

$$\left(\Rightarrow [1]_6 \subseteq [1]_3 \right)$$

$$[6]_2 = \{6, 8, 4, 10, 2, 12, 0, 14, -2, \dots\}$$

$$\left(= [0]_2 \right)$$

SIA $m \in \mathbb{P}$ E SIA $a \in \mathbb{Z}$. LA CLASSE DI EQUIVALENZA DI a (MODULO m) È LA CLASSE DI EQUIVALENZA DI a RISPETTO A \equiv_m . QUINDI

$$[a]_m \stackrel{\text{df}}{=} \{b \in \mathbb{Z} : a \equiv_m b\}$$

E.g. (SI CHIAMA ANCHE CLASSE DI RESTO DI a (MODULO m))

$$[1]_3 = \{1, 4, -2, 7, -5, \dots\}$$

OSS. SIANO $a, b, c, d \in \mathbb{Z}$. ALLORA

$$\begin{array}{l} a \equiv_m b \\ c \equiv_m d \end{array} \Rightarrow a \cdot c \equiv_m b \cdot d \quad (\underline{\text{ES. [I]}})$$

E

$$\begin{array}{l} a \equiv_m b \\ c \equiv_m d \end{array} \Rightarrow a + c \equiv_m b + d \quad (\underline{\text{ES. [I-]}})$$

QUESTO SUGGERISCE LE SEGUENTI DEF.

SIANO $a, b \in \mathbb{Z}$

DEF. LA SOMMA DI $[a]_m$ E $[b]_m$ E'

$$[a]_m + [b]_m \stackrel{\text{def}}{=} [a+b]_m.$$

IL PRODOTTO DI $[a]_m$ E $[b]_m$ E'

$$[a]_m \cdot [b]_m \stackrel{\text{def}}{=} [a \cdot b]_m.$$

E.g.

$$[2]_6 + [3]_6 = [5]_6$$

$$[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$$

$$[2]_6 + [5]_6 = [7]_6 = [1]_6$$

$$[3]_6 \cdot [3]_6 = [9]_6 = [3]_6$$

PONIAMO \mathbb{Z}_m L'INSIEME DELLE CLASSI DI RESTO MODULO m. QUINDI

$$\mathbb{Z}_m = \left\{ [0]_m, [1]_m, \dots, [m-1]_m \right\}.$$

LE CLASSI DI RESTO DI \mathbb{Z}_m SI COMPORENTANO COME I NUMERI. PER ES. SE $[a]_m$,

$[b]_m, [c]_m \in \mathbb{Z}_m$, ALLORA

$$[a]_m \cdot ([b]_m + [c]_m) = [a]_m \cdot [b]_m + [a]_m \cdot [c]_m$$

$$[a]_m \cdot [b]_m = [b]_m \cdot [a]_m$$

ETC...

MA C'E UNA DIFFERENZA:

$$\left[\begin{smallmatrix} k \\ m \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} a \\ m \end{smallmatrix} \right] = \left[\begin{smallmatrix} k \\ m \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} b \\ m \end{smallmatrix} \right] \nRightarrow \left[\begin{smallmatrix} a \\ m \end{smallmatrix} \right] = \left[\begin{smallmatrix} b \\ m \end{smallmatrix} \right]$$
$$\left[\begin{smallmatrix} k \\ m \end{smallmatrix} \right] \neq \left[\begin{smallmatrix} 0 \\ m \end{smallmatrix} \right]$$

E.g. $m=6$, $k=\frac{3}{4}$, $a=\frac{3}{8}$, $b=2$ ALLORA

$$\left[\begin{smallmatrix} 3 \\ 6 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 4 \\ 6 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 12 \\ 6 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 6 \\ 6 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 3 \\ 6 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 2 \\ 6 \end{smallmatrix} \right]$$

MA $\left[\begin{smallmatrix} 4 \\ 6 \end{smallmatrix} \right] \neq \left[\begin{smallmatrix} 2 \\ 6 \end{smallmatrix} \right]$.

PROP. 3.10.2: SIANO $a, b, m, k \in \mathbb{P}$ TALI CHE

$(k, m) = 1$. ALLORA

$$[k]_m \cdot [a]_m = [k]_m \cdot [b]_m \Leftrightarrow [a]_m = [b]_m.$$

DIM. SE $[a]_m = [b]_m \Rightarrow a \equiv b \pmod{m}$

$$\Rightarrow m | (b - a) \Rightarrow m | k(b - a) \Rightarrow m | kb - ka$$

$$\Rightarrow [kb]_m = [ka]_m \Rightarrow [k]_m \cdot [a]_m = [k]_m \cdot [b]_m$$

VICEVERSA. SE $\left[k \right]_m \cdot \left[a \right]_m = \left[k \right]_m \cdot \left[b \right]_m \Rightarrow$

$$\left[k \cdot a \right]_m = \left[k \cdot b \right]_m \Rightarrow ka \equiv kb \pmod{n}$$

(VEDI 3.8)

$$\Rightarrow m \mid (kb - ka) \Rightarrow m \mid k(b-a) \Rightarrow$$

$(k, m) = 1$

$$m \mid (b-a) \Rightarrow a \equiv b \pmod{n} \Rightarrow$$

$$\left[a \right]_m = \left[b \right]_m \cdot \square$$

Sia $[a]_m \in \mathbb{Z}_m$.

DEF. UN'INVERSA MOLTIPLICATIVA DI

$[a]_m$ E' UNA CLASSE $[b]_m \in \mathbb{Z}_m$ TALE

CHE

$$[a]_m \cdot [b]_m = [1]_m$$

PROP. 3.10.3: SIANO $a, b \in \mathbb{P}$ TALI CHE

$(a, m) = 1$. ALLORA $\exists! [b]_m \in \mathbb{Z}_m$ TALE
CHE

$$[a]_m \cdot [b]_m = [1]_m.$$

DIM. POICHÉ $(a, m) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$
TALI CHE

$$a \cdot x + m \cdot y = 1$$

$$\Rightarrow m \mid (a \cdot x - 1) \Rightarrow ax \equiv 1 \pmod{m}$$

$$\Rightarrow [ax]_m = [1]_m \Rightarrow [a]_m \cdot [x]_m = [1]_m.$$

VEDIAMO L'UNICITÀ. SIANO $[b]_m, [c]_m$

$$\in \mathbb{Z}_m \text{ TALI CHE } [a]_m \cdot [b]_m = [1]_m \text{ E }$$

$$[a]_m \cdot [c]_m = [1]_m. \text{ ALLORA}$$

$$[a]_m \cdot [b]_m = [a]_m \cdot [c]_m$$

QUINDI $\stackrel{\uparrow}{\Rightarrow} \begin{bmatrix} b \\ m \end{bmatrix} = \begin{bmatrix} c \\ m \end{bmatrix}$. \square
 $(3.10.2)$

ES. [1+]: TROVARE IL MINIMO $k \in \mathbb{P}$

TALE CHE

$$\underbrace{\begin{bmatrix} 3 \\ 17 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 17 \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 3 \\ 17 \end{bmatrix}}_k = \begin{bmatrix} 1 \\ 17 \end{bmatrix}.$$

E.p. $\begin{bmatrix} 3 \\ 17 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 17 \end{bmatrix} = \begin{bmatrix} 9 \\ 17 \end{bmatrix} \neq \begin{bmatrix} 1 \\ 17 \end{bmatrix} \Rightarrow k \geq 3$

3.11 LA FUNZIONE DI EULERO

Sia $m \in \mathbb{P}$.

DEF. LA FUNZIONE DI EULERO di m è

$$\Phi(m) \stackrel{\text{def}}{=} |\{1 \leq i \leq m : (m, i) = 1\}|.$$

E.g.

$$\Phi(6) = |\{1, 5\}| = 2$$

$$\Phi(10) = |\{1, 3, 7, 9\}| = 4$$

$$\Phi(8) = \left| \{1, 3, 5, 7\} \right| = 4.$$

$$\Phi(10) = \left| \{1, 3, 7, 9\} \right| = 4$$

OSS. $p \in \mathbb{P}$, p PRIMO, $\Rightarrow \Phi(p) = p-1$.

TEO 3.II.1: SIANO $p, q \in \mathbb{P}$, p, q PRIMI,

$p \neq q$. ALLORA

$$\Phi(p \cdot q) = (p-1) \cdot (q-1).$$

DIM. ABBIAMO CHE

$$\Phi(p \cdot q) = p \cdot q - \left| \left\{ 1 \leq i \leq p \cdot q : (p \cdot q, i) > 1 \right\} \right|.$$

SIA $1 \leq i \leq p \cdot q$ TALE CHE $(p \cdot q, i) > 1$

$\Rightarrow (p \cdot q, i) \geq 2 \Rightarrow \exists \pi \in P, \pi$ PRIMO,

TALE CHE $\pi | (p \cdot q, i) \Rightarrow \pi | p \cdot q \in$

$\pi | i \Rightarrow (\pi | p \sigma \pi | q) \in \pi | i$

$\Rightarrow (r=p \quad \sigma \quad \overset{r=9}{\cancel{\sigma}}) \in r|i \Rightarrow$

$\sigma \mid i \quad \sigma \mid 9 \mid i$. QUINDI $i=p, 2 \cdot p,$

$3 \cdot p, \dots, q \cdot p$ OPPURE $i = 9, 2 \cdot 9, 3 \cdot 9, \dots, p \cdot 9$

$\Rightarrow 9+p-1. \square$

TEO 3.11.2: SiA $m \in \mathbb{P}$ E SiA

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

LA SUA DECOMPOSIZIONE IN NUMERI PRIMI (p_1, \dots, p_r PRIMI DISTINTI,
 $a_1, \dots, a_r \in \mathbb{P}$). ALLORA

$$\Phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

$$\Phi(10) = 10 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$$

DIM. VEDI CAP. 4. □

COR 3.11.3: SIANO $a, b \in P$ TALI CHE
 $(a, b) = 1$. ALLORA

$$\Phi(ab) = \Phi(a) \cdot \Phi(b).$$

DIM. SEGUE SUBITO DA 3.11.2. □

SIA $n \in \mathbb{P}$. PONIAMO

$$E(n) \stackrel{\text{def}}{=} \left\{ [a]_n : 1 \leq a \leq n, (a, n) = 1 \right\}.$$

OSS. $|E(n)| = \varphi(n)$.

PROP. 3.11.4: SIANO $n, k \in \mathbb{P}$ TALI CHE
 $(k, n) = 1$. ALLORA LA FUNZIONE

$$[a]_n \mapsto [k]_n \cdot [a]_n$$

E' DA $E(n)$ IN $E(n)$ ED E' UNA
BIEZIONE.

DIM. SIA $[a]_n \in E(n) \Rightarrow (a, n) = 1$.

MA $[k]_m \cdot [a]_n = [k \cdot a]_n \quad E \quad (k \cdot a, n) = 1$

(VEDI UN ESERCIZIO FATTO). QUINDI
(PERCHE' $(a, n) = (k, n) = 1$)

$[k \cdot a]_n \in E(n)$.

SIANO $[a]_m, [b]_m \in E(n)$ TALI CHE

$$[\kappa]_m \cdot [a]_m = [\kappa]_m \cdot [b]_m \stackrel{(3.10.2)}{\Rightarrow} [a]_m = [b]_m.$$

INFINE, SIA $[b]_m \in E(n)$. SIA $[\kappa']_m \in$

\mathbb{Z}_m L'INVERSA MOLTIPLICATIVA

DI $[\kappa]_m$ ($[\kappa']_m$ ESISTE ED E'

UNICA PER 3.10.3). ALLORA

$$[\underline{k'}]_m [\underline{b}]_m \mapsto [\underline{k}]_m \cdot [\underline{k'}]_m \cdot [\underline{b}]_m = [\underline{1}]_m \cdot [\underline{b}]_m$$

$$= [\underline{b}]_m$$

QUINDI E' SURIETTIVA. \square

TEO 3.11.5: (TEOREMA DI EULERO): SIANO

$k, n \in \mathbb{P}$, TALI CHE $(k, n) = 1$. ALLORA

$$k^{\Phi(n)} \equiv 1 \pmod{n}.$$

DIM. SIA

$$E(n) = \left\{ [k]_n, [k_2]_n, \dots, [k_r]_n \right\}.$$

$(\Rightarrow r = \Phi(n))$. ALLORA, PER 3.11.4,

$$E(n) = \left\{ \left[k \right]_n \left[k \right]_n, \dots, \left[k \right]_n \cdot \left[k_r \right]_n \right\}.$$

QUINDI

$$\left[k_1 \right]_n \cdot \dots \cdot \left[k_r \right]_n = \left[k \right]_n \left[k_1 \right]_n \cdot \dots \cdot \left[k \right]_n \cdot \left[k_r \right]_n$$

\Leftarrow

$$\left[k_1 \right]_n \cdot \dots \cdot \left[k_r \right]_n = \left(\left[k \right]_n \right)^r \cdot \left[k_1 \right]_n \cdot \dots \cdot \left[k_r \right]_n$$

$$\left((k_i, m) = 1 \right) \rightarrow \Downarrow \quad (3.10.2)$$

$$[k_1]_m \cdot \dots \cdot [k_r]_m = \left([k]_m \right)^r [k_1]_m \cdot \dots \cdot [k_r]_m$$



⋮



$$[1]_m = \left([k]_m \right)^r = [k^r]_m$$



$$l \equiv k^r \pmod{n}. \square$$

COR. 3.11.6: SIANO $k, p \in \mathbb{P}$, p PRIMO,

$p \nmid k$. ALLORA

$$k^{p-1} \equiv l \pmod{p}.$$

DIM. BASTA PORRE $n=p$ in 3.11.5. \square

3.12 IL CODICE RSA

PROBLEMA FONDAMENTALE DELLA CRITTOGRAFIA:

SPEDIRE UN MESSAGGIO DA A A B
IN MODO CHE SOLO B POSSA LEGGERLO
(DECIFRARLO).

CODICE RSA:

PREPARAZIONE: B SCEGLIE DUE NUMERI

PRIMI $p, q \in \mathbb{P}$, $p \neq q$ E CALCOLA

$$m \stackrel{\text{def}}{=} p \cdot q$$

QUINDI TROVA $e \in \mathbb{P}$ TALE CHE

$$\text{MCD}(e, (p-1) \cdot (q-1)) = 1$$

INFINE B CALCOLA L'INVERSA MOLTI₌

MPLICATIVA $[d]_{(p-1)(q-1)}$ DI $[e]_{(p-1)(q-1)}$

(ESISTE ED E` UNICA). QUINDI B

PUBBLICA

n ED e

E TIENE SEGRETI

p, q , ED d .

CODIFICA: A PRENDE UN MESSAGGIO m ,

$1 \leq m \leq n$ E SPEDISCE

$$[\tilde{m}]_n^{\text{def}} = [m^e]_n,$$

(DOVE $(m, n) = 1$).

DECODIFICA: B RICEVE \tilde{m} E DECO₌

DIFICA CALCOLANDO

$$[\tilde{m}^d]_n.$$

PERCHE` FUNZIONA ?

PERCHE` $[d]_{(p-1)(q-1)}$ E $[e]_{(p-1)(q-1)}$ SONO

INVERSI MOLTIPLICATIVI, QUINDI

$$[d]_{(p-1)(q-1)} \cdot [e]_{(p-1) \cdot (q-1)} = [1]_{(p-1) \cdot (q-1)}$$

PERTANTO $\exists k \in \mathbb{P}$ TALE CHE

$$d \cdot e = k \cdot (p-1) \cdot (q-1) + 1$$

QUINDI

$$\left[\hat{m}^d \right]_m = \left(\left[m^e \right]_m \right)^d = \left[m^{e \cdot d} \right]_m$$

$$= \left[m^{k(p-1)(q-1)+1} \right]_m$$

$$= \left[m^{k(p-1)(q-1)} \right]_m \cdot \left[m \right]_m$$

$$= \left(\left[m^{(p-1)(q-1)} \right]_m \right)^k \cdot \left[m \right]_m$$

$$= \left(\left[m^{\Phi(n)} \right]_m \right)^k \cdot [m]_m$$

$$\xrightarrow{\text{(TEO. DI EULERO)}} = \left([1]_m \right)^k \cdot [m]_m$$

$$= [m]_m.$$

OSS. A E B NON SI SCAMBIANO NIENTE

PERCHE' PENSO CHE SIA DIFFICILE
ROMPERE RSA ?

PER ROMPERE RSA DOVREI O

FATTORIZZARE n

(IMPOSSIBILE SE n E' GRANDE) O

RISOLVERE $\left([x]_m \right)^e = [\tilde{m}]_m$

(SE $\ell = 2 \Rightarrow$ RECIPROCITÀ QUADRATICA
(GAUSS ≈ 1810), SE $\ell \geq 3 \Rightarrow$ RICERCHE
ATTUALI)

COSA VUOL DIRE "GRANDE" ?

ATTUALMENTE $\approx 10^{1000}$ (cioè \geq
1000 CIFRE)

ES. [1-]: SIANO $p, q \in \mathbb{P}$ DUE NUMERI DI
1000 CIFRE DECIMALI OGNIUNO. QUANTE
CIFRE DECIMALI HA, ALL'INCIRCA, $p \cdot q$?

ES. : DIMOSTRARE, USANDO IL WOP, CHE
SE $\alpha \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}$ TALI CHE $\alpha = \frac{a}{b}$
 $\text{E } (a, b) = 1$.

SIA

$$S \stackrel{\text{def}}{=} \left\{ b \in \mathbb{P} : \exists a \in \mathbb{Z} \text{ PER CUI } \alpha = \frac{a}{b} \right\}.$$

ALLORA $S \subseteq \mathbb{P}$ E $S \neq \emptyset$ (PERCHE' $\alpha \in \mathbb{Q}$)
 \Rightarrow PER WOP $\Rightarrow S$ HA UN MINIMO.

SIA $b \stackrel{\text{def}}{=} \min(S)$. QUINDI $\exists a \in \mathbb{Z}$ PER CUI
 $\alpha = \frac{a}{b}$. VOGLIAMO DIMOSTRARE CHE $(\alpha, b) = 1$.

PER ASSURDO, SIA $(\alpha, b) > 1$. SIA $c \in \mathbb{P}$ TALE
CHE $c \mid a$ E $c \mid b$ E $c \geq 2$. ALLORA

$$\alpha = \frac{a}{b} = \frac{(c \mid a)}{(c \mid b)}$$

e $\frac{b}{c} \in \mathbb{N} \setminus S$ E $\frac{b}{c} < b$, ASSURDO. QUINDI
 $(\alpha, b) = 1$.

ES. : SIA $m \in \mathbb{P}$ E SIA T_m UN TORNEO
COMPLETO SU $[m]$. UNA CLASSIFICA $\sigma \in$
 S_m E' RAGIONEVOLE SE $\sigma(i)$ HA BATTUTO
 $\sigma(i+1)$ PER OGNI $i = 1, \dots, m-1$. DIMOSTRARE
CHE ESISTE SEMPRE UNA CLASSIFICA
RAGIONEVOLE.

INDUZIONE SU m . Ovvio SE $m=1$,
FACILE SE $m=2$. SUPPONIAMO $m \geq 3$.

SIANO

$$A \stackrel{\text{def}}{=} \left\{ i \in \overline{[m]}^{2,m} : i \text{ HA BATTUTO } 1 \right\}$$

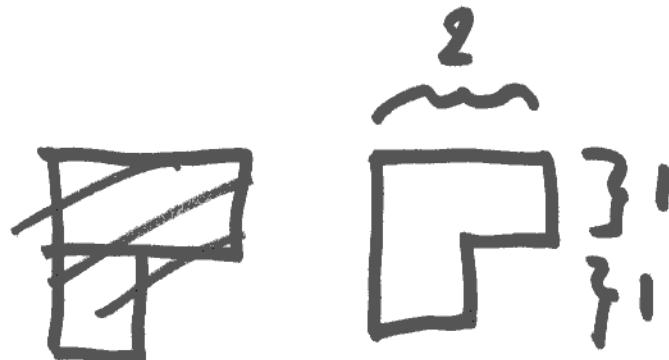
$$B \stackrel{\text{def}}{=} \left\{ j \in \overline{[m]}^{2,m} : 1 \text{ HA BATTUTO } j \right\}.$$

ALLORA $|A| \leq m-1$ E $|B| \leq m-1 \Rightarrow$ PER
INDUZIONE ESISTONO DUE CLASSIFICHE
RAGIONEVOLI τ E ρ PER A E B,
RISPECTIVAMENTE. MA ALLORA

$$\tau \neq \rho$$

E` UNA CLASSIFICA RAGIONEVOLE PER
 T_m .

ES. : SIA $m \in \mathbb{P}$. VOGLIAMO ERIGERE
UNA STATUA AL CENTRO DI UNA
PIAZZA $2^m \times 2^m$, E PAVIMENTARE
IL RESTO CON MATTONEILLE
DELLA FORMA

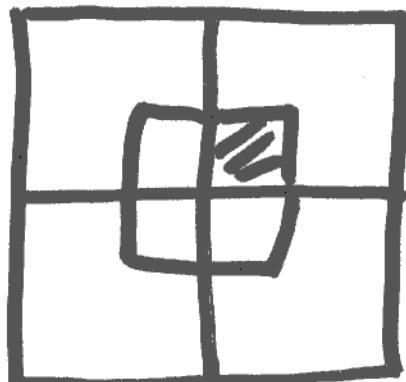


DIMOSTRARE CHE QUESTO È SEMPRE
POSSIBILE.

E.g. $m = \frac{1}{2}$



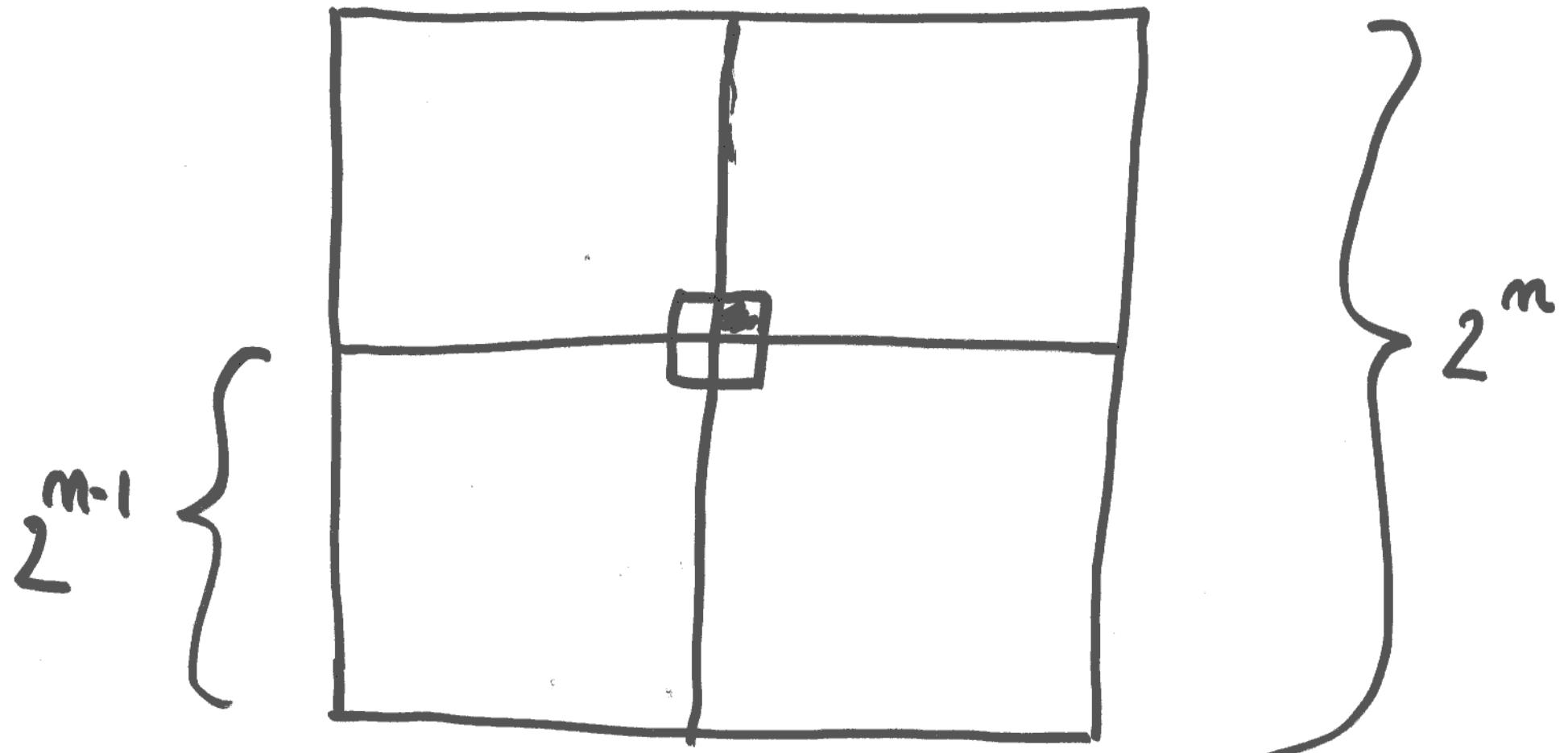
$m = 2$



}

4

INDUZIONE SU $m \in \mathbb{P}$. SI A $m \geq 3$



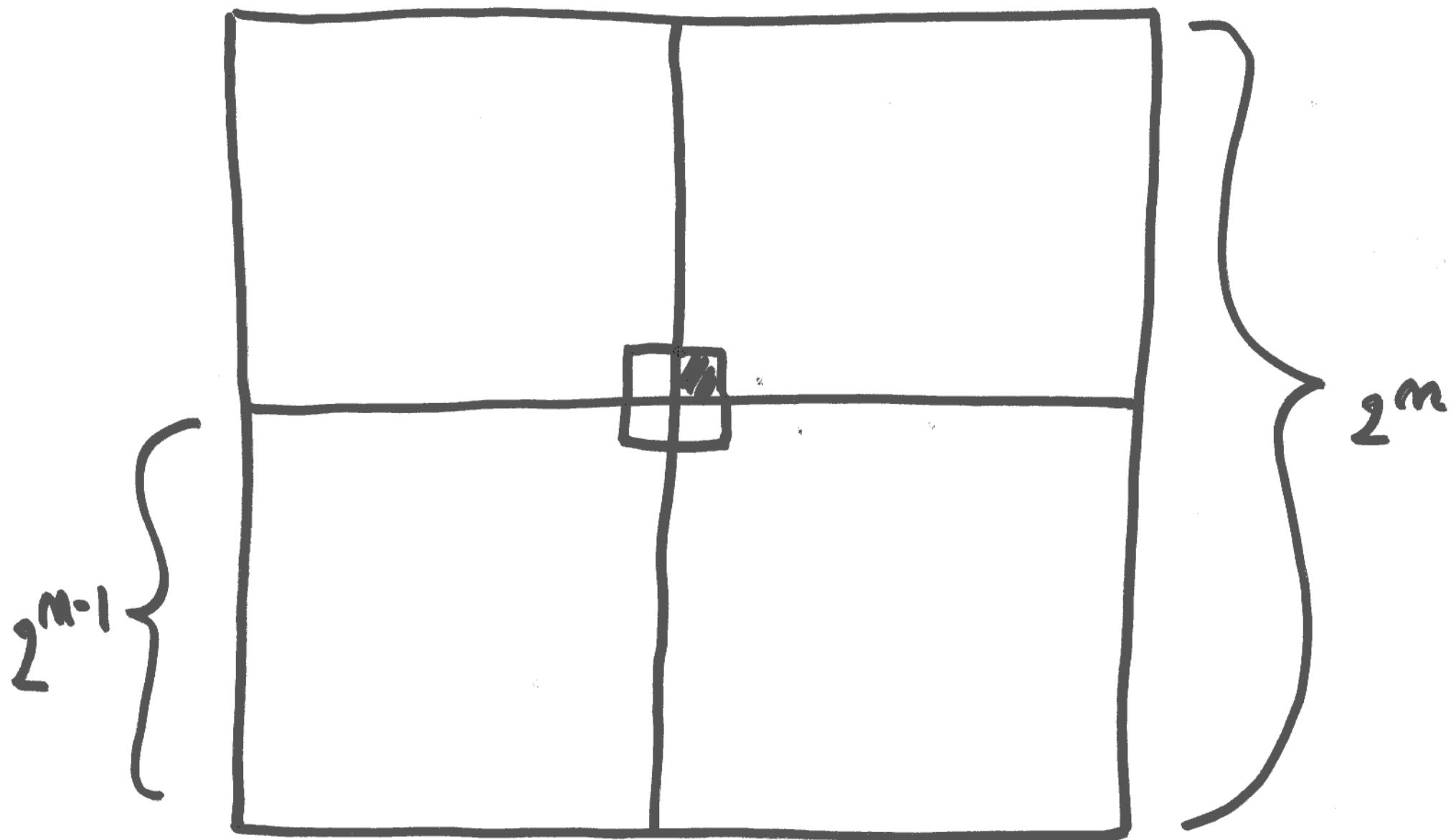
=> ?

RAFFORZAMENTO DELL' IPOTESI:

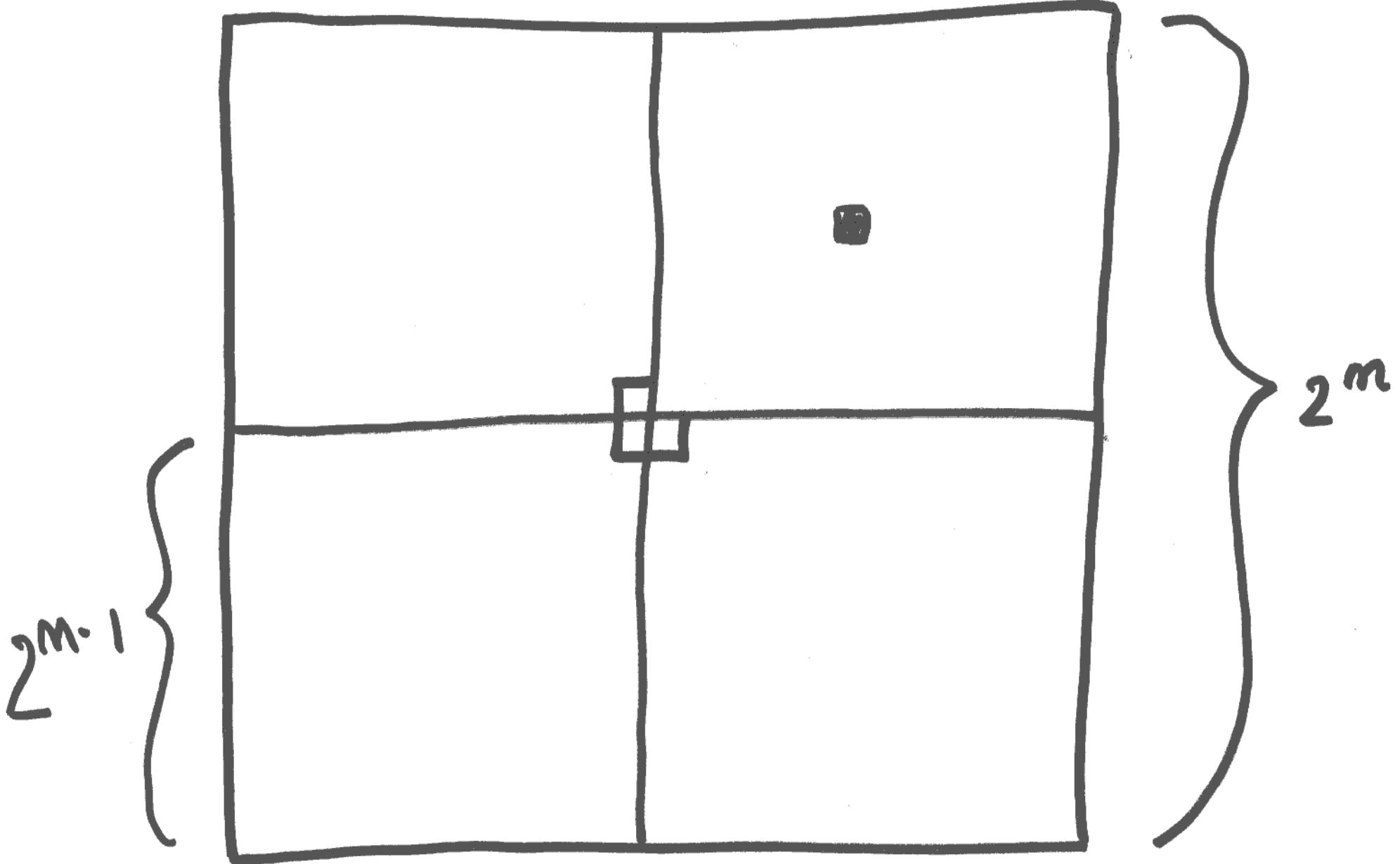
DIMOSTRARE CHE OVUNQUE METTO
LA STATUA => POSSO PAVIMENTARE
IL RESTO CON .

INDUZIONE:

$$2^{m-1} + 2^{m-1} = 2^{m-1}(1+1) = 2^m$$



=> a.k.



=> O.K.

ES.: CONSIDERIAMO IL SEGUENTE

"TEOREMA": SIA $a \in \mathbb{R} \setminus \{0\}$ E SIA $m \in \mathbb{N}^* (= \{q_1, \dots\})$.

ALLORA

$$a^m = 1.$$

"DIM." INDUZIONE SU $m = q_1, \dots$. SE $m=0$

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

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

$$a^m = \frac{a^{m-1} \cdot a^{m-1}}{a^{m-2}} \stackrel{\begin{array}{c} = \frac{a^{2m-2}}{a^{m-2}} \\ \uparrow \quad \uparrow \\ 1 \cdot 1 \end{array}}{=} 1 \Rightarrow \text{o.k. } \square$$

(INDUZIONE)

DOV'E' L'ERRORE ?

ES. : CALCOLARE

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

Poiché $17, 31, 37, 19, 53$, e 59 sono tutti numeri primi abbiamo che

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

(Se $p \in \mathbb{P}$, p primo, è tale che
 $p|a$ e $p|b \Rightarrow (p|17 \circ p|31 \circ p|37)$

$\circ p \mid 59 \Rightarrow E(p \mid 19 \circ p \mid 37 \circ p \mid 53) \cdot MA \ p \in$

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

$\Rightarrow MCD = 37^2$.

ES. : CALCOLARE $\text{MCD}(389, 167)$ E LA CORRISPONDENTE IDENTITÀ DI BEZOUT.

USIAMO A.E.:

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

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

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

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

$$\Rightarrow \text{MCD} = 1.$$

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

$$1 \xrightarrow{(3)} = 55 + 2(-27)$$

$$\begin{aligned} (2) \xrightarrow{\quad} &= 55 + (167 + 55(-3))(-27) \\ &= 167(-27) + 55 \cdot (82) \end{aligned}$$

$$\begin{aligned} (1) \xrightarrow{\quad} &= 167(-27) + (389 + 167(-2))(82) \\ &= 389 \cdot (82) + 167(-191) \end{aligned}$$

QUINDI L'ID. DI BEZOUT E

$$1 = 389 \cdot (82) + 167 (-191)$$
$$\begin{matrix} " & " & " & " \\ a & x & b & y \end{matrix}$$

SONDAGGIO: L'INVERSA DELLA PERMUTAZIONE

NE

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

E'

- a) 64275318 9%
- b) 26374851 ~~80%~~ ✓
- c) 18642753 2%
- d) 26374815 0% 9%
- e) NESSUNA DI QUESTE. (56)

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

USIAMO A.E.

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

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

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

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

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

PERTANTO $\text{MCD}(1137, 419) = 1$. CALCOLIAMO
L'ID. DI BEZOUT SVOLGENDO A.E. A
RITROSO:

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

(5)

$$\begin{aligned} &= 59 + (120 + 59(-2))(-29) \\ (4) \quad &<= 59(1 + (-2)(-29)) + 120(-29) \end{aligned}$$

$$\begin{aligned} &= 59(59) + 120(-29) \\ (3) \downarrow &\equiv (299 + 120 \cdot (-2))(59) + 120(-29) \end{aligned}$$

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

$$\stackrel{(2)}{=} 299(59) + (419 + 299(-1)) \cdot (-147)$$

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

$$\stackrel{(1)}{=} (1137 + 419(-2)) \cdot (206) + 419 \cdot (-147)$$

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

QUINDI L'ID. DI BEZOUT E'

$$1 = 1137 \cdot (206) + 419 \cdot (-559).$$

" " " "

(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 $r, r_1, r_2, \dots, q, q_1, q_2, \dots$ COME IN
A.E. ALLORA

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

INFATTI. ABBIAMO CHE

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

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

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.

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

SE $b=2$ ALLORA

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

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

SE $r=1 \Rightarrow$

$$\frac{a}{b} = q_1 \cdot 1 + r_1 , \quad 0 \leq r_1 < 1$$

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 $r_1 < \frac{b}{2} \Rightarrow$ PER INDUZIONE, L'A.E.

SU r, r_1 COMPIE AL PIÙ

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

SU a, b COMPIE AL PIÙ

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

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

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

$$\begin{aligned} (\log_2(2)=1) &= 2 \left(\log_2(b) - \log_2(2) \right) + 2 \\ &\cong 2 \cdot \log_2(b). \end{aligned}$$

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

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

SE $b=1$ ALLORA AVREI

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

MA E` 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 $p | (a^2, b) \Rightarrow p | a^2$
 $\wedge p | b \Rightarrow p | a \wedge p | b \Rightarrow$ ASSURDO

PERCHE' $(a, b) = 1$. PERTANTO $(a^2, b) = 1$.

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

$$(a, c) = 1$$

$$(b, c) = 1 \Rightarrow (ab, c) = 1.$$

PER ASSURDO. SIA $(ab, c) \geq 2 \Rightarrow \exists p \in \mathbb{P}$,

p PRIMO, TALE CHE $p | (ab, c) \Rightarrow p | ab$

$\Rightarrow p | c \Rightarrow (p | a \vee p | b) \wedge p | c$

$\Rightarrow \sigma(p | a \wedge p | c) \wedge \sigma(p | b \wedge p | c) \Rightarrow$

σ (ASSURDO PERCHE' $(a,c)=1$) σ

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

PERTANTO $(ab,c)=1$.

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

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

PER ASSURDO. SIA $(a^2, b^2) \geq 2 \Rightarrow \exists p \in \mathbb{P}$,
p PRIMO, TALE CHE $p | a^2 \wedge p | b^2 \Rightarrow$
 $p | a \wedge p | b \Rightarrow$ ASSURDO PERCHE' $(a, b) = 1$. QUINDI, SI, E' SEMPRE VERO.

SONDAGGIO: UNA PROPOSIZIONE LOGICAMENTE
EQUIVALENTE A

$$P \rightarrow Q$$

E':

(66)

- a) $(\neg Q) \rightarrow P$ 1%
- b) $(\neg Q) \rightarrow (\neg P)$ 85% ✓
- c) $Q \rightarrow (\neg P)$ 7%
- d) $Q \rightarrow P$ 1%
- e) NDQ. 4%

ES. : CALCOLARE L'INVERSA MOLTIPLICATIVA DI

$$[28]_{125}$$

DOBBIAMO CALCOLARE L'ID. DI
BEZOUT. CALCOLIAMO A.E. :

$$125 = 4 \cdot 28 + 13$$

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

$$28 = 2 \cdot 13 + 2$$

$$13 = 6 \cdot 2 + \boxed{1}$$

QUINDI $(125, 28) = 1$ (\Rightarrow L'INVERSA
MOLTIPLICATIVA ESISTE ED È UNICA).

CALCOLIAMO BEZOUT:

$$1 = 13 + 2(-6)$$

$$= 13 + (28 + 13(-2)) \cdot (-6)$$

$$= 13 \cdot (13) + 28 \cdot (-6)$$

$$= (125 + 28 \cdot (-4)) \cdot (13) + 28 \cdot (-6)$$

$$= 125 \cdot (13) + 28 \cdot (-58)$$

QUINDI L'ID. DI BEZOUT È

$$1 = 125 \cdot (13) + 28 \cdot (-58)$$

PERTANTO L'INVERSA MOLTIPLICATI-

VA DI $[28]_{125}$ È

$$[-58]_{125} = [67]_{125}.$$

ES. : CALCOLARE LE INVERSE MOLTIPLI
CATIVE DI

$$\begin{bmatrix} 172 \\ 221 \end{bmatrix} \quad E \quad \begin{bmatrix} 221 \\ 172 \end{bmatrix}$$

RISPETTIVAMENTE.

CALCOLIAMO $(221, 172)$ CON A.E. :

$$221 = 1 \cdot 172 + 49 \quad (1)$$

$$172 = 3 \cdot 49 + 25 \quad (2)$$

$$49 = 1 \cdot 25 + 24 \quad (3)$$

$$25 = 1 \cdot 24 + \boxed{1} \quad (4)$$

$$24 = 24 \cdot 1 + 0$$

$\Rightarrow (221, 172) = 1 \quad (\Rightarrow \text{QUINDI } \exists! \text{ LE INVERSE}).$

CALCOLIAMO BEZOUT

$$1 = 25 + 24 \cdot (-1)$$

$(4) \nearrow$

$$= 25 + (49 + 25 \cdot (-1)) \cdot (-1)$$

(3) \nearrow

$$= 25 \cdot (2) + 49 \cdot (-1)$$

$$= (172 + 49 \cdot (-3)) \cdot (2) + 49 \cdot (-1)$$

(2) \nearrow

$$= 172 \cdot (2) + 49 \cdot (-7)$$

$$(1) \doteq 172 \cdot (2) + (221 + 172 \cdot (-1)) \cdot (-7)$$

$$= 172(9) + 221 \cdot (-7)$$

QUINDI L'ID. DI BEZOUT E'

$$1 = 172 \cdot (9) + 221 \cdot (-7)$$

PERTANTO L'INVERSA MOLTIPLICATIVA

di $\begin{bmatrix} 172 \\ 221 \end{bmatrix}$ E'

$$\begin{bmatrix} 9 \\ 221 \end{bmatrix}$$

QUELLA DI $\begin{bmatrix} 221 \\ 172 \end{bmatrix}$ E'

$$\begin{bmatrix} -7 \\ 172 \end{bmatrix} = \begin{bmatrix} 165 \\ 172 \end{bmatrix}.$$

ES. : CALCOLARE LE ULTIME DUE CIFRE
DECIMALI DI

$$3^{100}$$

SI CHIEDE DI CALCOLARE

$$\left[3^{100} \right]_{100}$$

POICHÉ $(100, 3) = 1 \Rightarrow$ POSSO APPLICARE
IL TEO. DI EULERO ($k=3, m=100$)

\Rightarrow SAPPIAMO CHE

$$\left[3^{\Phi(100)} \right]_{100} = [1]_{100}.$$

DALLA TEORIA SAPPIAMO CHE

$$\begin{aligned}\Phi(100) &= 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \\ (100 &= 2^2 \cdot 5^2) \\ &= 40.\end{aligned}$$

PERTANTO

$$\left[3^{40} \right]_{100} = [1]_{100}.$$

QUINDI

$$\left[3^{100} \right]_{100} = \left[3^{40} \right]_{100} \cdot \left[3^{40} \right]_{100} \cdot \left[3^{20} \right]_{100}$$

$$= \left[1 \right]_{100} \cdot \left[1 \right]_{100} \cdot \left[3^{20} \right]_{100}$$

$$= \left[3^{20} \right]_{100}.$$

CALCOLIAMO $\left[3^{20} \right]_{100}$, ABBIAMO CHE

$$20 = 16 + 4$$

E

$$\left[3^2 \right]_{100} = \left[9 \right]_{100}$$

$$\left[3^4 \right]_{100} = \left(\left[3^2 \right]_{100} \right)^2 = \left(\left[9 \right]_{100} \right)^2 = \left[81 \right]_{100}$$

$$\left[3^8 \right]_{100} = \left(\left[3^4 \right]_{100} \right)^2 = \left(\left[81 \right]_{100} \right)^2 = \left[81^2 \right]_{100}$$

$$= \left[65\cancel{6}1 \right]_{100} = \left[61 \right]_{100}$$

$$\left[3^{16} \right]_{100} = \left(\left[3^8 \right]_{100} \right)^2 = \left(\left[61 \right]_{100} \right)^2 = \left[61^2 \right]_{100}$$

$$= \left[3721 \right]_{100} = \left[21 \right]_{100}.$$

PERTANTO

$$\left[3^{20} \right]_{100} = \left[3^{16} \right]_{100} \cdot \left[3^4 \right]_{100} = \left[21 \right]_{100} \cdot \left[81 \right]_{100}$$

$$= \left[21 \cdot 81 \right]_{100} = \left[1701 \right]_{100} = \left[1 \right]_{100}.$$

CONCLUDENDO

$$\left[3^{100} \right]_{100} = \left[3^{20} \right]_{100} = \left[1 \right]_{100}$$

\Rightarrow ULTIME DUE CIFRE DI 3^{100} SONO
01.

ES. : TROVARE TUTTI GLI $x, y \in \mathbb{Z}$ TALI CHE

$$89 \cdot x + 43 \cdot y = 1. \quad (*)$$

SAPPIAMO DALLA TEORIA CHE ESISTONO TALI $x, y \in \mathbb{Z}$ SE E SOLO SE $\text{MCD}(89, 43) \mid 1$. CALCOLIAMO $(89, 43)$ CON A.E.

$$89 = 2 \cdot 43 + 3$$

$$43 = 14 \cdot 3 + \boxed{1} \leftarrow$$

$$3 = 3 \cdot 1 + 0$$

QUINDI $(89, 43) = 1$. POICHÉ $1|1 \Rightarrow$ CI SONO SOLUZIONI E QUESTE SONO TUTTE DELLA FORMA

$$x = x_0 - \left(\frac{b}{d}\right) \cdot t, \quad y = y_0 + \left(\frac{a}{d}\right) \cdot t$$

CON $t \in \mathbb{Z}$. QUINDI NEL NOSTRO CASO

$$x = x_0 - 43 \cdot t, \quad y = y_0 + 89 \cdot t$$

DOVE x_0, y_0 E' UNA SOLUZIONE PARTICOLARE DI (*). PER TROVARE x_0 E y_0

CALCOLIAMO L'ID. DI BEZOÙT.

SVOLGIAMO A.E. A RIITROSO:

$$1 = 43 + 3(-14)$$

$$= 43 + (89 + 43(-2)) \cdot (-14)$$

$$= 43 \cdot 29 + 89 \cdot (-14)$$

QUINDI L'ID. DI BEZOUT E'

$$1 = 43 \cdot (29) + 89 \cdot (-14)$$

PERTANTO $x_0 = -14$ E $y_0 = 29$ SONO

SOLUZIONE DI (*). QUINDI LE SOL.

Di (*) SONO

$$x = -14 - 43 \cdot t, \quad y = 29 + 89 \cdot t$$

CON $t \in \mathbb{Z}$. PERTANTO PER ES.

$$x = -14, \quad y = 29 \quad E' SOL. (t=0)$$

$$x = -57, \quad y = 118 \quad E' SOL. (t=1)$$

$$x = 29, \quad y = -60 \quad E' SOL. (t=-1)$$

ETC...

ES. : TROVARE TUTTI GLI $x, y \in \mathbb{Z}$ TALI CHE

$$875 \cdot x + 235 \cdot y = 10. \quad (*)$$

SAPPIAMO DALLA TEORIA CHE TALI $x, y \in \mathbb{Z}$ ESISTONO SE E SOLO SE $(875, 235) \mid 10$.
CALCOLIAMO $(875, 235)$ CON A.E:

$$875 = 3 \cdot 235 + 170 \quad (1)$$

$$235 = 1 \cdot 170 + 65 \quad (2)$$

$$170 = 2 \cdot 65 + 40 \quad (3)$$

$$65 = 1 \cdot 40 + 25 \quad (4)$$

$$40 = 1 \cdot 25 + 15 \quad (5)$$

$$25 = 1 \cdot 15 + 10 \quad (6)$$

$$15 = 1 \cdot 10 + \boxed{5} \leftarrow \quad (7)$$

$$10 = 2 \cdot 5 + 0$$

$$\Rightarrow \text{MCD}(875, 235) = 5. \text{ POICHÉ } 5 \mid 10 \Rightarrow$$

\Rightarrow CI SONO SOL. E SONO TUTTE DELLA
FORMA

$$x = x_0 - \left(\frac{235}{5}\right) \cdot t, \quad y = y_0 + \left(\frac{875}{5}\right) \cdot t$$

DOVE $t \in \mathbb{Z}$ E x_0, y_0 È UNA SOLUZIONE
DI (*). PER TROVARE x_0 E y_0 CALCO=
LIAMO L'ID. DI BEZOÚT:

$$5 = 15 + 10 \cdot (-1)$$

$(7) \nearrow$

$$(6) \rightarrow = 15 + (25 + 15(-1)) \cdot (-1)$$

$$= 15 \cdot (2) + 25 \cdot (-1)$$

$$(5) \rightarrow = (40 + 25 \cdot (-1)) \cdot (2) + 25 \cdot (-1)$$

$$= 40 \cdot (2) + 25 \cdot (-3)$$

$$(4) \rightarrow = 40 \cdot (2) + (65 + 40 \cdot (-1)) \cdot (-3)$$

$$= 40 \cdot (5) + 65 \cdot (-3)$$

$$\begin{aligned} &= (170 + 65 \cdot (-2)) \cdot (5) + 65 \cdot (-3) \\ (3) \nearrow &= 170 \cdot (5) + 65 \cdot (-13) \end{aligned}$$

$$\begin{aligned} &= 170 \cdot (5) + (235 + 170 \cdot (-1)) \cdot (-13) \\ (2) \nearrow &= 170 \cdot (18) + 235 \cdot (-13) \end{aligned}$$

$$(1) \rightarrow = (875 + 235 \cdot (-3)) (18) + 235 \cdot (-13)$$

$$= 875 \cdot (18) + 235 \cdot (-67)$$

QUINDI L'ID. DI BEZOUT E'

$$5 = \cancel{875} \cdot (18) + 235 \cdot (-67)$$

MA A NOI INTERESSA 10 \Rightarrow MOLTIPLICÒ
PER 2:

$$10 = 875 \cdot (36) + 235 \cdot (-134)$$

QUINDI $x_0 = 36$ E $y_0 = -134$ È UNA
SOL. DI (*). PERTANTO LE SOL. SONO

$$x = 36 - 47 \cdot t, \quad y = -134 + 175 \cdot t$$

CON $t \in \mathbb{Z}$.

ES. : CALCOLARE LE ULTIME DUE CIFRE DI

$$7^{91}$$

SI CHIEDE DI CALCOLARE

$$\left[7^{91} \right]_{100}.$$

POICHE' $(100, 7) = 1 \Rightarrow$ TEO. DI EULERO \Rightarrow

$$\left[7^{\Phi(100)} \right]_{100} = [1]_{100}.$$

MA $\Phi(100) = 40 \Rightarrow [7^{40}]_{100} = [1]_{100}$. PERTANTO

$$[7^{91}]_{100} = \left([7^{40}]_{100} \right)^2 \cdot [7^{11}]_{100}$$

$$= \left([1]_{100} \right)^2 \cdot [7^{11}]_{100}$$

$$= [7^{11}]_{100}.$$

CALCOLIAMO

$$[7^{11}]_{100}$$

ABBIAMO CHE $11 = 8 + 2 + 1$. MA

$$[7^2]_{100} = [49]_{100}$$

$$\begin{aligned}[7^4]_{100} &= \left([7^2]_{100}\right)^2 = \left([49]_{100}\right)^2 = [49^2]_{100} = \\ &= [2401]_{100} = [1]_{100}\end{aligned}$$

$$\begin{aligned}[7^8]_{100} &= \left([7^4]_{100}\right)^2 = \left([1]_{100}\right)^2 = [1^2]_{100} = [1]_{100}.\end{aligned}$$

PERTANTO

$$\left[\begin{smallmatrix} 7^{11} \\ 100 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 7^8 \\ 100 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 7^2 \\ 100 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 7^1 \\ 100 \end{smallmatrix} \right] =$$

$$= \left[\begin{smallmatrix} 1 \\ 100 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 49 \\ 100 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 7 \\ 100 \end{smallmatrix} \right]$$

$$= \left[\begin{smallmatrix} (49) \cdot 7 \\ 100 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 343 \\ 100 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 43 \\ 100 \end{smallmatrix} \right]$$

CONCLUDENDO

$$\left[7^{91} \right]_{100} = \left[7^{11} \right]_{100} = \left[43 \right]_{100}$$

QUINDI LE ULTIME DUE CIFRE DI 7^{91}
SONO 43.

ES. : Sia $n \in \mathbb{P}$ E Sia

$$n = \alpha_k \cdot 10^k + \alpha_{k-1} \cdot 10^{k-1} + \dots + \alpha_1 \cdot 10 + \alpha_0$$

LA SUA ESPRESSIONE DECIMALE

($0 \leq \alpha_0, \alpha_1, \dots, \alpha_k \leq 9$). DIMOSTRARE CHE

$$3 | n \Leftrightarrow 3 | (\alpha_0 + \alpha_1 + \dots + \alpha_k).$$

Di MOSTRIAMO CHE

$$[n]_3 = [q_0 + q_1 + \dots + q_k]_3.$$

ABBIAMO CHE $[10]_3 = [1]_3$. QUINDI, SE $k \in \mathbb{P}$,

$$[10^k]_3 = ([10]_3)^k = ([1]_3)^k = [1]_3.$$

PERTANTO

$$[n]_3 = [q_k \cdot 10^k + \dots + q_1 \cdot 10 + q_0]_3$$

$$= \left[\alpha_k \right]_3 \cdot \left[10^k \right]_3 + \dots + \left[\alpha_1 \right]_3 \cdot \left[10 \right]_3 + \left[\alpha_0 \right]_3$$

$$= \left[\alpha_k \right]_3 \cdot \left[1 \right]_3 + \dots + \left[\alpha_1 \right]_3 \cdot \left[1 \right]_3 + \left[\alpha_0 \right]_3$$

$$= \left[\alpha_k + \dots + \alpha_1 + \alpha_0 \right]_3.$$

ES.: Sia $n \in \mathbb{P}$, $n \geq 3$. DIMOSTRARE
CHE $\Phi(n)$ È PARI.

(PER ES., $\Phi(3)=2$, $\Phi(4)=2$, $\Phi(5)=4$,
 $\Phi(6)=2$, ETC...)

ABBIAMO CHE

$$\Phi(n) = |\{1 \leq i \leq n-1 : (i, n) = 1\}|$$

MA, SE $1 \leq i \leq n-1$, ALLORA

$$(i, m) = 1 \iff (m-i, m) = 1 \quad (*)$$

INFATTI, SIA $(i, m) = 1$. PER ASSURDO,
SIA $(m-i, m) \geq 2 \Rightarrow \exists p \in P$, p PRIMO,
TALE CHE $p | (m-i, m) \Rightarrow p | (m-i) \wedge$
 $p | m \Rightarrow p | (m - (m-i)) \Rightarrow p | i \Rightarrow p | i \wedge$
 $p | m \Rightarrow$ ASSURDO. QUINDI $(m-i, m) = 1$.

VICEVERSA. SIA $(m-i, m) = 1$. PER AS₌
 SURDO, SIA $(i, m) \geq 2 \Rightarrow \exists p \in P, p$ PRIMO,
 TALE CHE $p | i$ E $p | m \Rightarrow p | (m-i) \Rightarrow$
 ASSURDO.

QUESTO DIMOSTRA (*).

PERTANTO

$$\left\lfloor \frac{m}{2} \right\rfloor$$

$$\Phi(m) = \left| \left\{ 1 \leq i \leq \cancel{\frac{m-1}{2}} : (i, m) = 1 \right\} \right| +$$

$$+ \left| \left\{ \lfloor \lceil \frac{m}{2} \rceil \leq i \leq m-1 : (i, m) = 1 \right\} \right|$$

DOVE

$$\lfloor x \rfloor \stackrel{\text{def}}{=} \max \{ i \in \mathbb{P} : i \leq x \}$$

E

$$\lceil x \rceil \stackrel{\text{def}}{=} \min \{ j \in \mathbb{P} : j \geq x \}.$$

(PER ES, $\lfloor \frac{5}{2} \rfloor = 2$, $\lceil \frac{5}{2} \rceil = 3$). MA

$$\left| \left\{ 1 \leq i \leq \left\lfloor \frac{m}{2} \right\rfloor : (i, m) = 1 \right\} \right| =$$

$$\left| \left\{ \lceil \frac{m}{2} \rceil \leq j \leq m-1 : (m, j) = 1 \right\} \right|$$

PER (*) \Rightarrow $\Phi(m) \in \text{PARI}$.

DECODIFICHiamo il messaggio criptato

$$[\tilde{m}]_n = \begin{bmatrix} 1029 \\ 3901 \end{bmatrix} \quad \text{DOBBIAMO CALCOLARE}$$

$$[\tilde{m}^d]_n = \begin{bmatrix} 1029^{503} \\ 3901 \end{bmatrix}.$$

ABBIAMO CHE

$$503 = 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1$$

CALCOLIAMO

$$\left[\begin{smallmatrix} 1029^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 1058841 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 1670 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 1029^4 \\ 3901 \end{smallmatrix} \right] = \left(\left[\begin{smallmatrix} 1029^2 \\ 3901 \end{smallmatrix} \right] \right)^2 = \left[\begin{smallmatrix} 1670^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2788900 \\ 3901 \end{smallmatrix} \right] = \\ = \left[\begin{smallmatrix} 3586 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 1029^8 \\ 3901 \end{smallmatrix} \right] = \left(\left[\begin{smallmatrix} 1029^4 \\ 3901 \end{smallmatrix} \right] \right)^2 = \left[\begin{smallmatrix} 3586^2 \\ 3901 \end{smallmatrix} \right] =$$

$$= \begin{bmatrix} 128 & 5 \\ 39 & 396 \\ 3901 & \end{bmatrix} = \begin{bmatrix} 1700 \\ 3901 \end{bmatrix}$$

$$*\begin{bmatrix} 1029^{16} \\ 3901 \end{bmatrix} = \left(\begin{bmatrix} 1029^8 \\ 3901 \end{bmatrix} \right)^2 = \begin{bmatrix} 1700^2 \\ 3901 \end{bmatrix} = \begin{bmatrix} 3260 \\ 3901 \end{bmatrix}$$

$$\begin{bmatrix} 1029^{32} \\ 3901 \end{bmatrix} = \left(\begin{bmatrix} 1029^{16} \\ 3901 \end{bmatrix} \right)^2 = \begin{bmatrix} 3260^2 \\ 3901 \end{bmatrix} =$$

$$= \begin{bmatrix} 1276 \\ 3901 \end{bmatrix}$$

$$\left[\begin{smallmatrix} 1029^{64} \\ 3901 \end{smallmatrix} \right] = \left(\left[\begin{smallmatrix} 1029^{32} \\ 3901 \end{smallmatrix} \right] \right)^2 = \left[\begin{smallmatrix} 1276^2 \\ 3901 \end{smallmatrix} \right] =$$

$$= \left[\begin{smallmatrix} 1459 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 1029^{128} \\ 3901 \end{smallmatrix} \right] = \left(\left[\begin{smallmatrix} 1029^{64} \\ 3901 \end{smallmatrix} \right] \right)^2 = \left[\begin{smallmatrix} 1459^2 \\ 3901 \end{smallmatrix} \right] =$$

$$= \left[\begin{smallmatrix} 2636 \\ 3901 \end{smallmatrix} \right]$$

$$\begin{bmatrix} 1029^{256} \\ 3901 \end{bmatrix} = \left(\begin{bmatrix} 1029^{128} \\ 3901 \end{bmatrix} \right)^2 = \left(\begin{bmatrix} 2636 \\ 3901 \end{bmatrix} \right)^2$$

$$= \begin{bmatrix} 815 \\ 3901 \end{bmatrix}$$

PERTANTO

$$\begin{bmatrix} 1029^{503} \\ 3901 \end{bmatrix} = \begin{bmatrix} 1029^{256} \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 1029^{128} \\ 3901 \end{bmatrix}.$$

$$\cdot \left[\frac{1029^{64}}{3901} \right] \cdot \left[\frac{1029^{32}}{3901} \right] \cdot \left[\frac{1029^{16}}{3901} \right] \cdot \left[\frac{1029^4}{3901} \right]$$

$$\cdot \left[\frac{1029^2}{3901} \right] \cdot \left[\frac{1029}{3901} \right] =$$

$$= \left[\frac{815}{3901} \right] \cdot \left[\frac{2636}{3901} \right] \cdot \left[\frac{1459}{3901} \right] \cdot \left[\frac{1276}{3901} \right] \cdot$$

$$\cdot \left[\frac{3260}{3901} \right] \cdot \left[\frac{3586}{3901} \right] \cdot \left[\frac{1670}{3901} \right] \cdot \left[\frac{1029}{3901} \right] =$$

$$= \begin{bmatrix} 2790 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 907 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 2964 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 1990 \\ 3901 \end{bmatrix}$$

$$= \begin{bmatrix} 3 \\ 3901 \end{bmatrix}$$

PERTANTO il MESSAGGIO ORIGINALE
ERA

$$\begin{bmatrix} m \\ n \end{bmatrix}_m = \begin{bmatrix} \tilde{m}^d \\ n \end{bmatrix}_m = \begin{bmatrix} 1029^{503} \\ 3901 \end{bmatrix} = \begin{bmatrix} 3 \\ 3901 \end{bmatrix}$$

ES. : SIANO p, q, m, e, d COME IN RSA.

SIA $1 \leq m \leq n$. QUAL'È LA PROBABILITÀ
CHE $(m, n) > 1$?

QUESTA PROBABILITÀ È

$$\frac{n - \Phi(n)}{n} = \frac{p \cdot q - p \cdot q \cdot \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)}{p \cdot q}$$

$$= 1 - \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = \frac{1}{p} + \frac{1}{q} - \frac{1}{p \cdot q}$$

$$SE \quad p, q \approx 10^{1000} \Rightarrow \frac{1}{p}, \frac{1}{q} \approx 10^{-1000}, \frac{1}{p \cdot q} \approx 10^{-2000}$$

$$\Rightarrow \frac{1}{p} + \frac{1}{q} - \frac{1}{p \cdot q} \approx 2 \cdot 10^{-1000} =$$

$$= 0, \underbrace{000 \dots 000}_\text{1000} 2.$$

ES. : COSTRUIRE UN SISTEMA DI COMUNICAZIONE RSA USANDO I PRIMI $p = 47$ E $q = 83$.

INOLTRE CODIFICARE E DECODIFICARE UN MESSAGGIO.

CALCOLIAMO

$$n = p \cdot q = 47 \cdot 83 = 3901$$

QUINDI

$$\Phi(n) = (p-1)(q-1) = 46 \cdot 82 = 3772$$

TROVIAMO $e \in P$ TALE CHE $(e, (p-1) \cdot (q-1)) = 1$.

DOBBIAMO AVERE $(e, 3772) = 1$. PROCEDIAMO

PER TENTATIVI, $e = 15$ FUNZIONA. TROVIAMO

L'INVERSA MOLTIPLICATIVA $[d]$

Di $[e]_{(p-1)(q-1)} = [15]_{3772}$. CALCOLIAMO A.E.: $(p-1)(q-1)$

$$3772 = (200+40+10+1) \cdot 15 + 7$$

$$15 = 2 \cdot 7 + \boxed{1}, \quad 7 = 7 \cdot 1 + 0$$



CALCOLIAMO L'ID. DI BEZOUT:

$$1 = 15 + 7 \cdot (-2)$$

$$= 15 + \left(3772 + 15 \cdot (-251) \right) \cdot (-2)$$

$$= 15 \cdot (503) + 3772 \cdot (-2)$$

QUINDI L'ID. DI BEZOUT E'

$$1 = 15 \cdot (503) + 3772 \cdot (-2)$$

PERTANTO $[d]_{(p-1) \cdot (q-1)} = [503]_{3772}$.

PUBBLICHiamo

$$m = 3901, \ell = 15$$

TENIAMO PRIVATI

$$p = 47, q = 83, d = 503.$$

CODIFICHiamo UN MESSAGGIO $1 \leq m \leq n$

TALE CHE $(m, n) = 1$. PRENDIAMO $m=3$

$((3, 3901) = 1 \Rightarrow \text{o.k.})$, CODIFICHiamo, DOB₌

BIAMO CALCOLARE

$$\left[\begin{smallmatrix} m^e \\ \end{smallmatrix} \right]_n = \left[\begin{smallmatrix} 3^{15} \\ \end{smallmatrix} \right]_{3901}.$$

ABBIAMO CHE

$$15 = 8 + 4 + 2 + 1$$

QUINDI

$$\left[\begin{smallmatrix} 3^2 \\ 3^2 \end{smallmatrix} \right]_{3901} = \left[\begin{smallmatrix} 9 \\ 9 \end{smallmatrix} \right]_{3901}$$

$$\left[\begin{smallmatrix} 3^4 \\ 3^4 \end{smallmatrix} \right]_{3901} = \left(\left[\begin{smallmatrix} 3^2 \\ 3^2 \end{smallmatrix} \right]_{3901} \right)^2 = \left(\left[\begin{smallmatrix} 9 \\ 9 \end{smallmatrix} \right]_{3901} \right)^2 = \left[\begin{smallmatrix} 81 \\ 81 \end{smallmatrix} \right]_{3901}$$

$$\left[\begin{smallmatrix} 3^8 \\ 3^8 \end{smallmatrix} \right]_{3901} = \left(\left[\begin{smallmatrix} 3^4 \\ 3^4 \end{smallmatrix} \right]_{3901} \right)^2 = \left(\left[\begin{smallmatrix} 81 \\ 81 \end{smallmatrix} \right]_{3901} \right)^2 =$$

$$= \begin{bmatrix} 81^2 \\ 3901 \end{bmatrix} = \begin{bmatrix} 6561 \\ " \\ 3901 \end{bmatrix} = \begin{bmatrix} \cancel{2660} \\ 2660 \\ 3901 \end{bmatrix}$$

(3901 + 2660)

PERTANTO

$$\begin{bmatrix} 3^{15} \\ 3901 \end{bmatrix} = \begin{bmatrix} 3^8 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 3^4 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 3^2 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3901 \end{bmatrix}$$

$$= \begin{bmatrix} 2660 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 81 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3901 \end{bmatrix}$$

$$= \begin{bmatrix} 2660 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 81 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 27 \\ 3901 \end{bmatrix}$$

$$= \begin{bmatrix} 2660 \\ 3901 \end{bmatrix} \cdot \begin{bmatrix} 8 & 2187 \\ 3901 \end{bmatrix}$$

$$= \begin{bmatrix} 5817420 \\ 3901 \end{bmatrix}$$

$$= \begin{bmatrix} 1029 \\ 3901 \end{bmatrix}$$

SPEDIAMO QUINDI IL MESSAGGIO
CODIFICATO CHE E'

$$[\tilde{m}]_n = \begin{bmatrix} 1029 \\ 3901 \end{bmatrix}$$

SONDAGGIO: SIANO $a, b \in \mathbb{P}$ TALI CHE

$(a, b) = 1$. ALLORA:

(53)

- a) $(2a, 2b) = 2$ 72% ✓
- b) $(2a, 2b) = 1$ 15%
- c) $(2a, b) = 2$ 6%
- d) $(a, 2b) = 1$ 7%
- e) NDQ. 0%