CAP. 3 NUMERI:

3.1 IL PRINCIPIO DI INDUZIONE:

CI SONO 3 MODI PER DIMOSTRARE CHE $A \to B$:

1) DIMOSTRAZIONE DIRETTA:

UN RAGIONAMENTO CHE MOSTRA CHE SE A È VERO ALLORA B

È PURE NECESSARIAMENTE VERO.

2) DIMOSTRAZIONE PER ASSURDO:

UN RAGIONAMENTO CHE ASSUME CHE A e ¬B SIANO ENTRAMBE VERE E DEDUCE UNA CONTRADDIZIONE.

3) IL PRINCIPIO DI INDUZIONE MATEMATICA:

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

1) $P(1)$ È VERO;

2) $P(n) \Rightarrow P(n+1)$ PER $\forall n \in \mathbb{P}$.

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

PRINCIPIO DI INDUZIONE COMPLETA:

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

1) $P(1)$ È VERO

2) $P(1) \wedge P(2) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)$

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

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

<u>NOTAZIONE:</u> SIA $\{a_i\}_{i=1,2,\dots} \subseteq \mathbb{R}$.

SCRIVIAMO

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

PER DIRE

$$a_1 + a_2 + \dots + a_m$$

E.g. DIMOSTRARE CHE:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad (P(n))$$

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

1) $P(1)$ È VERA ?

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

2) È VERO CHE $P(n) \Rightarrow P(n+1)$?

SIA $P(n)$ VERA. ALLORA

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

MA ALLORA

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) \overset{(P(n))}{=} \frac{n(n+1)}{2} + (n+1)$$

$$= (n+1)\left(\frac{n}{2}+1\right) = \frac{(n+1)(n+2)}{2}$$

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

<u>ES. [1]</u>: DIMOSTRARE CHE

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

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

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

3.2 IL PRINCIPIO DEL BUON ORDINAMENTO:

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

SIA $S \subseteq \mathbb{P} \Rightarrow \exists\, m \in S$ 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 $\mathbb{Q}_{>0}$ $\left(\overset{def}{=} \{\alpha \in \mathbb{Q} : \alpha > 0\}\right)$. PER ES. $S = \{1, \frac{1}{2}, \frac{1}{3}, \dots\}$ NON HA UN MINIMO.

TEO:

WOP $\Longleftrightarrow$ INDUZIONE

DIM: OMESSA. $\square$

ES. [1+]: DIMOSTRARE PER INDUZIONE CHE

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

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 (o POSITIVI) SONO

$$\mathbb{P} \overset{def}{=} \{1, 2, 3, \dots\}$$

I NUMERI <u>INTERI</u> SONO

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

I NUMERI <u>RAZIONALI</u> SONO

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

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 È LA LUNGHEZZA DI UN SEGMENTO.

3.5 NUMERI COMPLESSI

I NUMERI <u>COMPLESSI</u> SONO

$$\mathbb{C} \overset{def}{=} \{\alpha + i\beta : \alpha, \beta \in \mathbb{R}\}$$

DOVE

$$i \overset{def}{=} \sqrt{-1}.$$

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

<u>DEF.</u> α SI DICE LA <u>PARTE REALE</u> DI z.

β " " " " <u>PARTE IMMAGINARIA</u> DI z.

DEF. i $(=\sqrt{-1})$ SI DICE L'<u>UNITÀ IMMAGINARIA</u>.

(o <u>CONIUGATO</u>)

DEF. IL <u>COMPLESSO CONIUGATO</u> DI z È

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

SIANO $z, w \in \mathbb{C}$, $z = a + ib$, $w = c + id$ $(a, b, c, d \in \mathbb{R})$. ALLORA LA <u>SOMMA</u> DI z E w È

$$z + w \overset{def}{=} (a + c) + i(b + d)$$

IL <u>PRODOTTO</u> DI w e z È

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

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

$(i^2 = -1)$

$$= (ac - bd) + i(ad + bc).$$

<u>E.g.</u> $z = 2 - i$, $w = 3 + 4i$. ALLORA

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

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

$$= 10 + 5i$$

$$\uparrow$$

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

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

"RAZIONALIZZANDO"

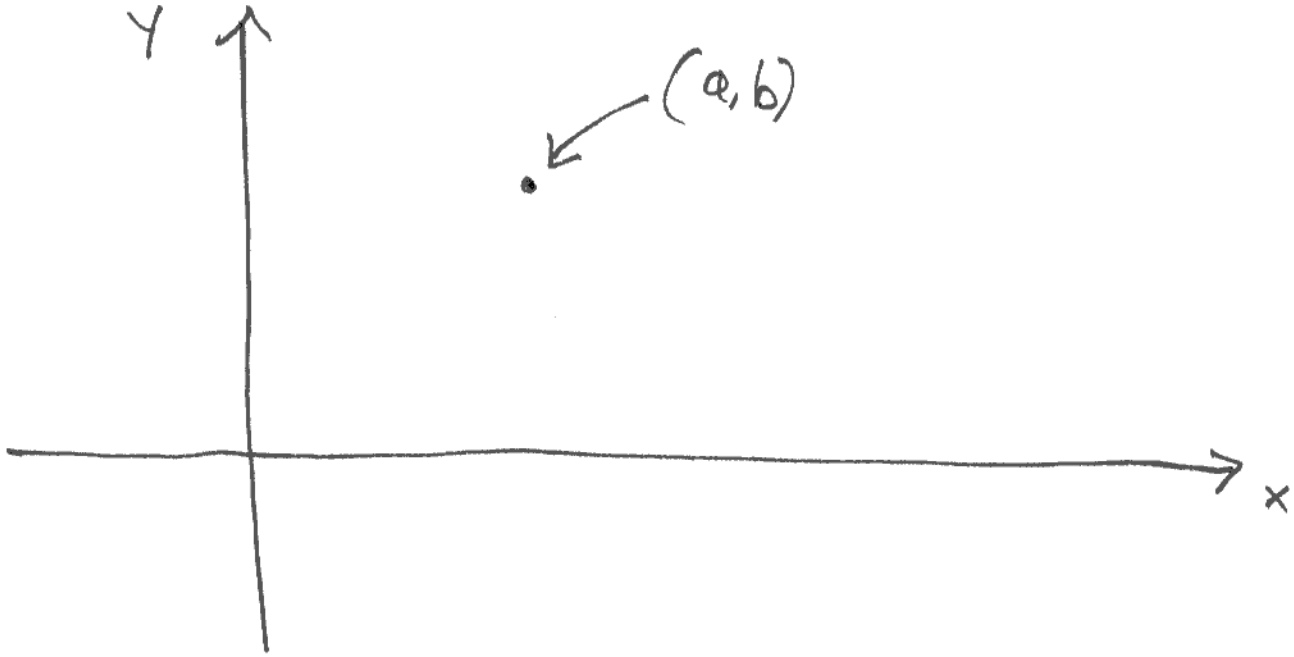
<u>E.g.</u> $z = 2 - i$, $w = 3 + 4i$. ALLORA

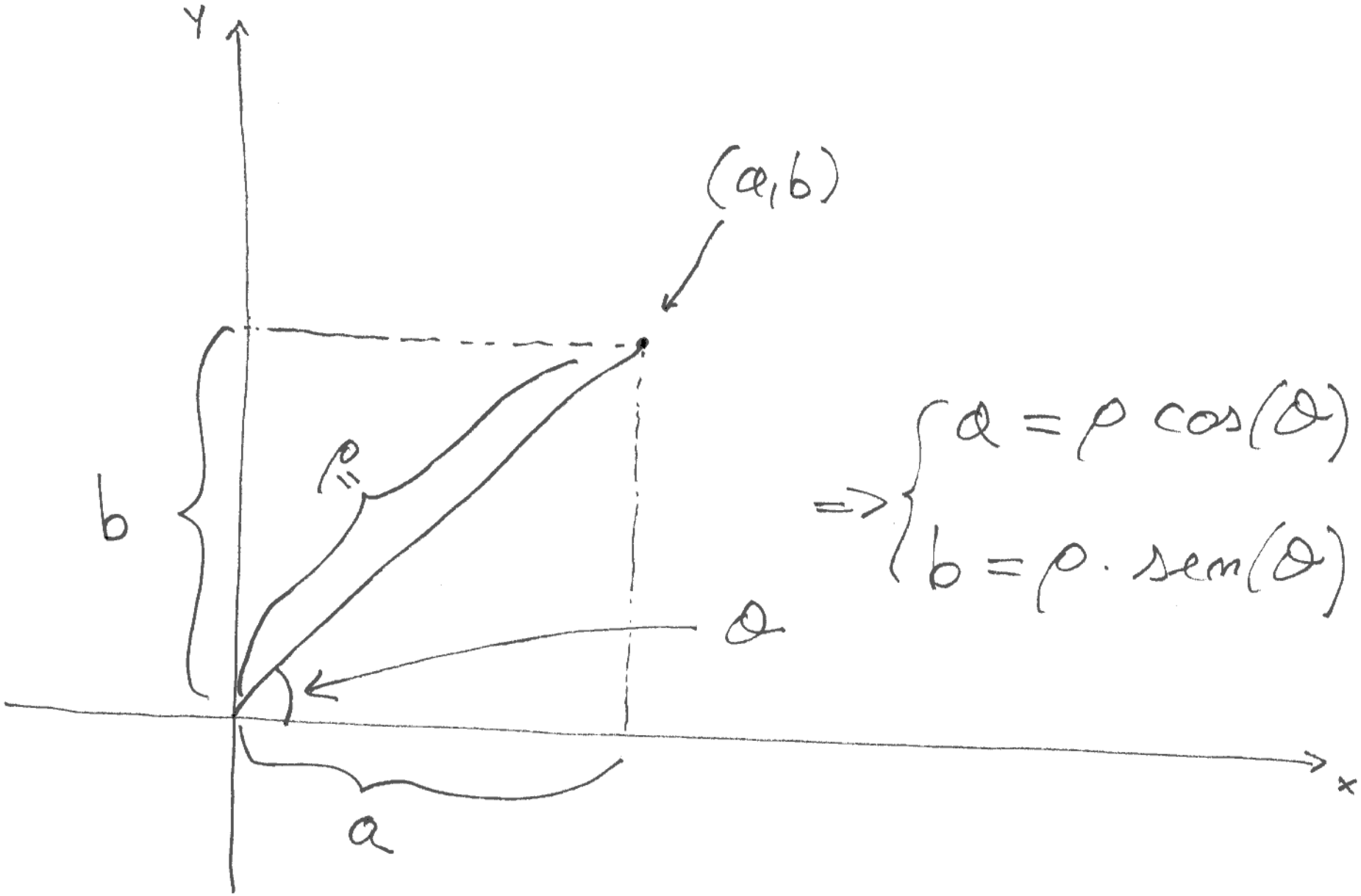
$$\frac{z}{w} = \frac{2-i}{3+4i} = \frac{(2-i)(3-4i)}{(3+4i)(3-4i)} =$$

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

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

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





$$\Rightarrow \begin{cases} a = \rho \cos(\theta) \\ b = \rho \cdot \operatorname{sen}(\theta) \end{cases}$$

QUINDI

$$z = \rho \cos(\theta) + i \rho \operatorname{sen}(\theta)$$

$$= \rho \left(\cos(\theta) + i \operatorname{sen}(\theta) \right)$$

QUESTA È LA <u>FORMA POLARE</u> DI z

ρ SI DICE IL <u>MODULO</u> DI z

θ " " L'<u>ARGOMENTO</u> DI z

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

SIA $z = a + ib$. ALLORA

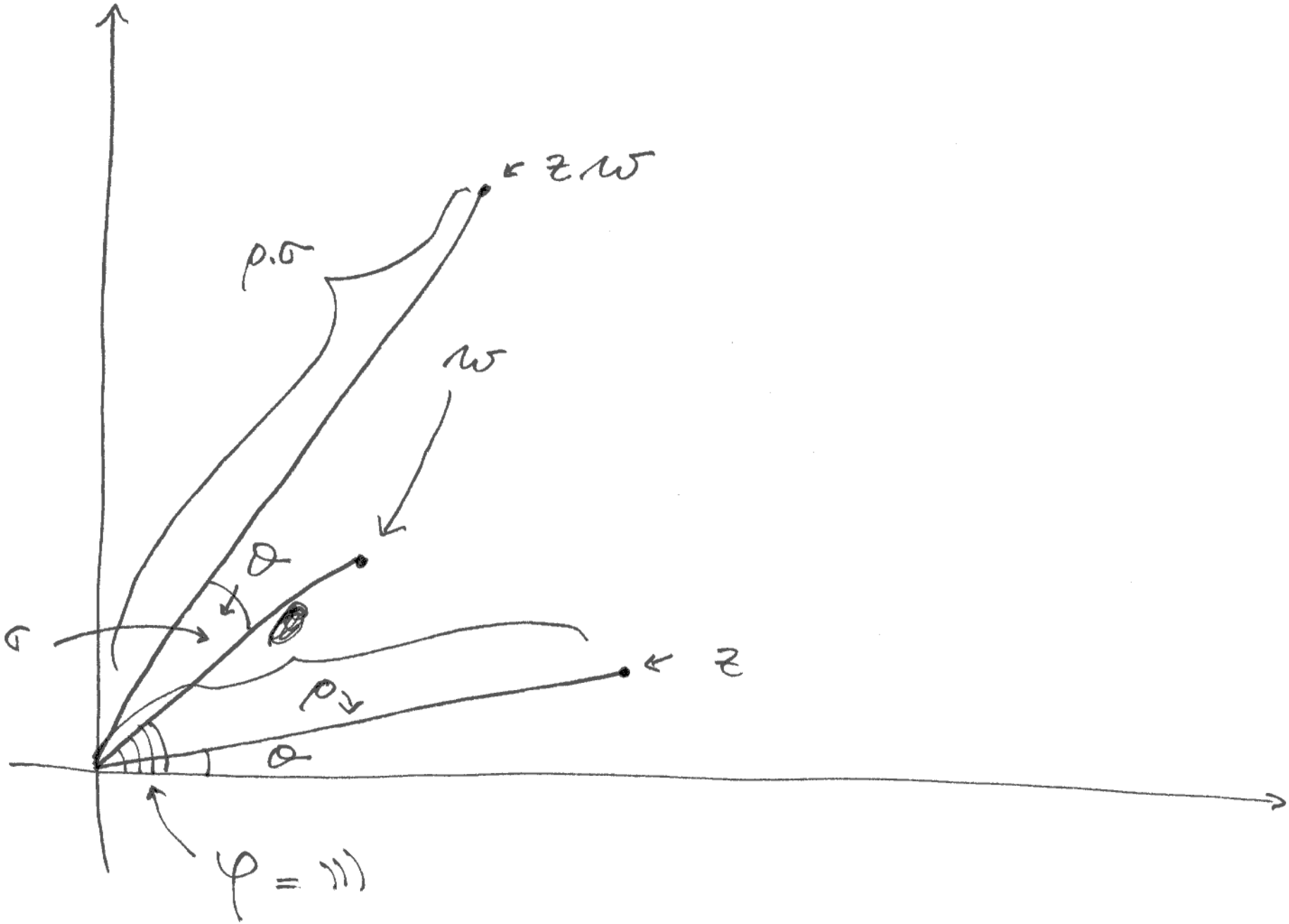
$$\|z\|^2 = \rho^2 = a^2 + b^2 \quad \left(\Rightarrow \|z\| = \sqrt{a^2+b^2} \right)$$

e

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

$$\left(z \cdot \overline{z} = (a+ib)\cdot(a-ib) = a^2 + \overset{iab}{\overset{\shortparallel}{\cancel{iab}}} - \cancel{iab} - b^2 \cdot i^2 \right)$$

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


$z w$
$\rho \cdot \sigma$
w
θ
σ
z
ρ
θ
$\varphi = \dots$

$$w \cdot z = \left(\rho \cos(\theta) + i \rho \operatorname{sen}(\theta)\right) \cdot \left(\sigma \cos(\varphi) + i \sigma \cdot \operatorname{sen}(\varphi)\right)$$

$$= \cdots$$

$$= \rho\sigma\left(\cos(\theta+\varphi) + i \operatorname{sen}(\theta+\varphi)\right).$$

<u>ES. [1]</u>: SIA $z = 1+i$. CALCOLARE

$$z^{1970}.$$

3.6 NUMERI PRIMI E COMPOSTI

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

<u>DEF.</u> SI DICE CHE a <u>DIVIDE</u> b (O CHE b È UN <u>MULTIPLO</u> DI a), SCRITTO $a \mid b$ SE $\exists\, k \in \mathbb{Z}$ TALE CHE

$$b = k \cdot a$$

<u>OSS.</u> $a \mid b \Rightarrow a \leq b$.

<u>OSS.</u> $a \mid b$ E $b \mid c \Rightarrow a \mid c$

<u>OSS.</u> $a \mid b$ E $a \mid c \Rightarrow a \mid (xb + yc)$

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

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

<u>DEF.</u> a È UN <u>NUMERO PRIMO</u> SE

$b \mid a \Rightarrow b = 1$ o $b = a$,

e $a \geq 2$.

IN CASO CONTRARIO a È UN <u>NUMERO COMPOSTO</u>.

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

<u>DEF.</u> a E b SI DICONO <u>COPRIMI</u> ~~SE~~ (O <u>PRIMI TRA LORO</u>) SE

$$\left.\begin{array}{l} c \mid a \\ \text{e} \\ c \mid b \end{array}\right. \Rightarrow c = \pm 1 .$$

<u>OSS.</u> $a \in \mathbb{P} \Rightarrow a \mid a$.

<u>OSS.</u> $p, q \in \mathbb{P}$, $(p \neq q)$ p E q PRIMI $\Rightarrow$ p E q SONO COPRIMI.

<u>TEO 3.6.1</u>: SIA $m \in \mathbb{P}$, $m \geq 2$. ALLORA m È PRODOTTO DI NUMERI PRIMI.

<u>DIM.</u> INDUZIONE. SE $m = 2 \Rightarrow 2 = 2$ E 2 È PRIMO $\Rightarrow$ O.K.

SUPPONIAMO IL TEOREMA VERO PER $\forall\, m \in \mathbb{P},\ m \leq n$. SE $n+1$ È PRIMO $\Rightarrow n+1 = n+1 \Rightarrow$ O.K. SE $n+1$ NON È PRIMO $\Rightarrow \exists\, a, b \in \mathbb{P}$ TALI CHE $1 < a < n+1$, $1 < b < n+1$, E

$$n+1 = a \cdot b. \qquad (*)$$

MA, POICHÈ $a \leq n$ E $b \leq n$, $\Rightarrow$ PER INDUZIONE IL TEOREMA

VALE PER a E PER b $\Rightarrow$ a E b SONO PRODOTTO DI NUMERI PRIMI $\overset{(*)}{\Rightarrow}$ $m+1$ È PRODOTTO DI NUMERI PRIMI. $\square$

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

<u>DEF.</u> m SI DICE <u>PERFETTO</u> SE m È LA SOMMA DEI SUOI DIVISORI $< m$.

<u>E.g.</u> 6 È PERFETTO, PERCHÉ $1+2+3=6$

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

~~PROP~~

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

PROBLEMA APERTO: ESISTONO NUMERI PERFETTI DISPARI?

<u>TEO 3.6.2</u>: CI SONO INFINITI NUMERI PRIMI.

<u>DIM</u>. PER ASSURDO, SUPPONIAMO CHE $\{p_1, p_2, \dots, p_m\}$ SIANO TUTTI I NUMERI PRIMI. SIA

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

ALLORA, PER 3.6.1, N È PRODOTTO DI NUMERI PRIMI $\Rightarrow \exists\, q \in \mathbb{P}$, q PRIMO

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

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

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

$\Rightarrow q \mid 1 \Rightarrow q \leq 1$, ASSURDO PERCHÈ

q È PRIMO. SIMILMENTE $q = p_2$ È

ASSURDO, ETC.... QUINDI CI SONO

INFINITI NUMERI PRIMI. $\square$

QUANTO SONO FREQUENTI I NUMERI PRIMI?

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

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

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

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

TEO:

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

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

$$6 \cdot k + 5$$

È PRIMO.

ES. [2-]: FINO A $\cong 25$ ANNI FA IL NUMERO PRIMO PIÙ GRANDE CONOSCIUTO ERA

$$p \overset{def}{=} 2^{216091} - 1.$$

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

3.7 ALGORITMO EUCLIDEO

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

<u>DEF.</u> IL <u>MASSIMO COMUN DIVISORE</u> DI a E b, (SCRITTO $MCD(a,b)$, O (a,b), O $GCD(a,b)$) È

$$MCD(a,b) \overset{def}{=} \max\{c \in \mathbb{P} : c \mid a \text{ E } c \mid b\}.$$

COME CALCOLARE $MCD(a,b)$?

RICORDIAMO CHE:

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

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

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

E

$$0 \leq r < b.$$

<u>DIM.</u> È NOTA. $\square$

ALGORITMO EUCLIDEO:

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

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

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

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

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

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

SE $r_1 = 0 \Rightarrow MCD = r$ (LO VEDREMO).

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

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

SE $r_2 = 0 \Rightarrow MCD = r_1$ (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 $r_3 = 0 \Rightarrow MCD = r_2$ (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

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

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

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

$$\vdots \qquad\qquad \vdots$$

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

$$\vdots$$

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

$\Rightarrow \exists\, k \in \mathbb{P}$ 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

$$(k-1) \qquad r_{k-1} = r_k \cdot q_{k+1} + \underset{\overset{\shortparallel}{0}}{r_{k+1}}$$

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

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

$\Rightarrow r_k \mid r_{k-2}$. MA

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

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

$r_k \mid r_{k-1}$, $r_k \mid r_{k-2}$, ..., $r_k \mid r_1$, $r_k \mid r$

MA

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

$\Rightarrow r_k \mid b$. MA

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

$\Rightarrow r_k \mid a$. QUINDI r_k È UN DIVISORE COMUNE DI a E b.

SIA $c \in \mathbb{P}$ TALE CHE $c \mid a$ E $c \mid b$.

MA

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

$\Rightarrow c \mid r \; (= a - bq)$. MA

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

$\Rightarrow c \mid r_1 \; (= b - r \cdot q)$. MA

$r = r_1 \cdot q_2 + r_2$

$\Rightarrow c \mid r_2 \; (= r - r_1 \cdot q_2)$ ETC... QUINDI

$c \mid r_1, \; c \mid r_2, \ldots, c \mid r_k$

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

$r_k = MCD(a, b)$.

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

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

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

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

OSS. SIANO a, b, q, r, ETC. COME IN A.E., ALLORA

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

3.8 CONSEGUENZE DI A.A.E.

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

$$(a,b) = a \cdot x + b \cdot y \quad \left(\text{IDENTITÀ DI BEZOÚT}\right)$$

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

SE $b = 1 \Rightarrow b \mid a \Rightarrow (a,b) = b = a \cdot 0 + b \cdot 1$

$\Rightarrow$ 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 $r = 0 \Rightarrow$

$b \mid a \Rightarrow (a, b) = b = a \cdot 0 + b \cdot 1 \Rightarrow$ 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

$$(a, b) = b \cdot x + r \cdot y = b \cdot x + (a - b \cdot q) \cdot y$$
$$= b \cdot (x - q \cdot y) + a \cdot y \quad . \square$$

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

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

DIM. OMESSA. $\square$

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

$$MCD(a,b) = 1 \overset{?}{\Longrightarrow} MCD(a+b, a-b) = 1 \ ?$$

<u>PROP. 3.8.3:</u> SIANO $p, a, b \in \mathbb{P}$ TALI CHE $p \mid a \cdot b$ E p È PRIMO. ALLORA O $p \mid a$ O $p \mid b$.

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

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

QUINDI

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

MA $p \mid a \cdot b$ E $p \mid p \cdot b \cdot y \Rightarrow p \mid b$. $\square$

<u>OSS</u>: FALSO, INGENERALE, SE p NON È PRIMO. PER ES.

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

<u>OSS.</u> $m, a, b \in \mathbb{P}$ TALI CHE $m \mid a \cdot b$ E $(m, a) = 1 \Rightarrow m \mid b$.

<u>TEO 3.8.4:</u> (<u>TEOREMA FONDAMENTALE DELL'ARITMETICA</u>): SIA $n \in \mathbb{P}$, $n \geq 2$. ALLORA n SI ESPRIME COME PRODOTTO DI NUMERI PRIMI IN UNO ED <u>UN SOLO MODO</u>, A PARTE L'ORDINE DEI FATTORI.

(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 $n=2 \Rightarrow 2=2 \Rightarrow$ o.k. SIA $n \geq 3$.
SUPPONIAMO IL TEOREMA VERO PER
$\forall m \in \mathbb{P}$ TALE CHE $m \leq n-1$. VOGLIAMO
DIMOSTRARE IL TEOREMA PER n.

PER ASSURDO, SIANO $p_1, \dots, p_r, q_1, \dots, q_s \in \mathbb{P}$ $(r, s \in \mathbb{P})$ 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 $p_1 \mid n \Rightarrow p_1 \mid (q_1 \cdot q_2 \cdot \dots \cdot q_s) \overset{(3.8.3)}{\Longrightarrow}$

$\exists\ 1 \leq i \leq s$ TALE CHE $p_1 \mid q_i \Rightarrow p_1 = q_i$

(PERCHÈ q_i È PRIMO). MA ALLORA

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

E $\frac{m}{p_1} \in \mathbb{P}$ 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

<u>TEO 3.9.1</u>: 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

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

MA $(a,b) \mid a$ E $(a,b) \mid b \Rightarrow (a,b) \mid m$.

VICEVERSA. SUPPONIAMO CHE $(a,b) \mid m$.

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

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

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

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

QUINDI

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

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

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

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 $d \overset{def}{=} (a, b)$, $t \in \mathbb{Z}$, E $x_0, y_0 \in \mathbb{Z}$ SONO UNA SOLUZIONE PARTICOLARE DI $(\square)$.

<u>DIM.</u> OMESSA. $\square$

<u>OSS.</u> EQUIVALENTEMENTE:

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

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

$$\Updownarrow$$

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

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

E

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

DOVE $d \overset{def}{=} (a, b)$ 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 <u>RELAZIONE DI CONGRUENZA MODULO m</u>.

<u>PROP. 3.10.1</u>: SIA $m \in \mathbb{P}$. ALLORA $\equiv_m$ È UNA RELAZIONE DI EQUIVALENZA, SU $\mathbb{Z}$.

<u>DIM.</u> VEDI SEZ. 1.4 $(m = 3)$. $\square$

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

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

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

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

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

$$(= [0]_2)$$

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

$$[a]_m \overset{def}{=} \{ b \in \mathbb{Z} : a \equiv_m b \}$$

(SI CHIAMA ANCHE <u>CLASSE DI RESTO</u> DI a (MODULO m))

<u>E.g.</u>

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

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

$$\begin{array}{l} a \equiv_n b \\ c \equiv_n d \end{array} \Rightarrow a \cdot c \equiv_n b d \quad (\underline{\text{ES. [1]}})$$

E

$$\begin{array}{l} a \equiv_n b \\ c \equiv_n d \end{array} \Rightarrow a + c \equiv_n b + d \quad (\underline{\text{ES. [1-]}})$$

QUESTO SUGGERISCE LE SEGUENTI DEF.

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

<u>DEF.</u> LA <u>SOMMA</u> DI $[a]_n$ E $[b]_n$ È

$$[a]_n + [b]_n \overset{def}{=} [a+b]_n .$$

IL <u>PRODOTTO</u> DI $[a]_n$ E $[b]_n$ È

$$[a]_n \cdot [b]_n \overset{def}{=} [a \cdot b]_n .$$

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 $\mathbb{Z}_n$ L'INSIEME DELLE CLASSI DI RESTO MODULO n. QUINDI

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}.$$

LE CLASSI DI RESTO DI $\mathbb{Z}_n$ SI COMPORTANO COME I NUMERI. PER ES. SE $[a]_n$, $[b]_n, [c]_n \in \mathbb{Z}_n$, ALLORA

$$[a]_n \cdot \left([b]_n + [c]_n\right) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$$

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

ETC....

MA C'E UNA DIFFERENZA:

$$[k]_n \cdot [a]_n = [k]_n \cdot [b]_n \quad \not\Rightarrow \quad [a]_n = [b]_n.$$

$$[k]_n \neq [0]_n$$

<u>E.g.</u> $n=6$, $k=\overset{3}{\cancel{4}}$, $a=\overset{4}{\cancel{3}}$, $b=2$ ALLORA

$$[3]_6 \cdot [4]_6 = [12]_6 = [6]_6 = [3]_6 \cdot [2]_6$$

MA $[4]_6 \neq [2]_6$.

PROP. 3.10.2: SIANO $a, b, m, k \in \mathbb{P}$ TALI CHE $(k, m) = 1$. ALLORA

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

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

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

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

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

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

(VEDI 3.8)

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

$(k, m) = 1$

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

$$[a]_m = [b]_m . \square$$

SIA $[a]_n \in \mathbb{Z}_n$.

<u>DEF.</u> UN'<u>INVERSA MOLTIPLICATIVA</u> DI $[a]_n$ È UNA CLASSE $[b]_n \in \mathbb{Z}_n$ TALE CHE

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

PROP. 3.10.3: SIANO $a, \overset{n}{\cancel{b}} \in \mathbb{P}$ TALI CHE $(a,n)=1$. ALLORA $\exists!\ [b]_n \in \mathbb{Z}_n$ TALE CHE

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

DIM. POICHÈ $(a,n)=1 \overset{\text{(BEZOUT)}}{\Longrightarrow} \exists\ x, y \in \mathbb{Z}$ TALI CHE

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

$$\Rightarrow \quad n \mid (a \cdot x - 1) \Rightarrow \quad a x \equiv 1 \pmod{n}$$

$$\Rightarrow [a x]_n = [1]_n \Rightarrow [a]_n \cdot [x]_n = [1]_n .$$

VEDIAMO L'UNICITÀ. SIANO $[b]_n, [c]_n \in \mathbb{Z}_n$ TALI CHE $[a]_n \cdot [b]_n = [1]_n$ E $[a]_n \cdot [c]_n = [1]_n$. ALLORA

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

QUINDI $\underset{(3.10.2)}{\Longrightarrow}$ $[b]_m = [c]_m$. $\square$

<u>ES. [1+]</u>: TROVARE IL MINIMO $k \in \mathbb{P}$ TALE CHE

$$\underbrace{[3]_{17} \cdot [3]_{17} \cdot \ldots \cdot [3]_{17}}_{k} = [1]_{17}.$$

<u>E.g.</u> $[3]_{17} \cdot [3]_{17} = [9]_{17} \neq [1]_{17} \Rightarrow k \geq 3$

3.11 LA FUNZIONE DI EULERO

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

DEF. LA FUNZIONE DI EULERO DI n È

$$\Phi(n) \overset{def}{=} \left| \{ 1 \leq i \leq n : (n, i) = 1 \} \right|.$$

E.g.

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

$$\Phi(11) = \left| \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \right| = 10$$

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

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

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

<u>TEO 3.11.1:</u> SIANO $p, q \in \mathbb{P}$, p, q PRIMI, $p \neq q$. ALLORA

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

<u>DIM.</u> 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 $(p\cdot q, i) > 1$

$\Rightarrow (p\cdot q, i) \geq 2 \Rightarrow \exists\, r \in \mathbb{P}$, r PRIMO,

TALE CHE $r \mid (p\cdot q, i) \Rightarrow r \mid p\cdot q$ E

$r \mid i \Rightarrow (r \mid p$ O $r \mid q)$ E $r \mid i$

$$\Rightarrow \left(r = p \quad \text{o} \quad r = q \right) \text{ E } r \mid i \Rightarrow$$

o $p \mid i$ o $q \mid i$. QUINDI $i = p, 2 \cdot p, 3 \cdot p, \ldots, q \cdot p$ OPPURE $i = q, 2 \cdot q, 3 \cdot q, \ldots, p \cdot q$

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

TEO 3.11.2: SIA $n \in \mathbb{P}$ E SIA

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$$

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

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

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

<u>DIM.</u> VEDI CAP. 4. $\square$

<u>COR 3.11.3:</u> SIANO $a, b \in \mathbb{P}$ TALI CHE $(a,b)=1$. ALLORA

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

<u>DIM.</u> SEGUE SUBITO DA 3.11.2. $\square$

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

$$E(n) \overset{def}{=} \{ [a]_n : 1 \leq a \leq n, (a,n) = 1 \}.$$

<u>OSS.</u> $|E(n)| = \Phi(n)$.

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

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

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

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

MA $[k]_n \cdot [a]_n = [k \cdot a]_n$ E $(k \cdot a, n) = 1$ (VEDI UN ESERCIZIO FATTO). QUINDI

(PERCHÈ $(a,n)=(k,n)=1$)

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

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

$$[k]_n \cdot [a]_n = [k]_n \cdot [b]_n \overset{(3.10.2)}{\Longrightarrow} [a]_n = [b]_n.$$

INFINE, SIA $[b]_n \in E(n)$. SIA $[k']_n \in \mathbb{Z}_n$ L'INVERSA MOLTIPLICATIVA DI $[k]_n$ ($[k']_n$ ESISTE ED È UNICA PER 3.10.3). ALLORA

$$[k']_n [b]_n \mapsto [k]_n \cdot [k']_n \cdot [b]_n = [1]_n \cdot [b]_n$$

$$= [b]_n$$

QUINDI È SURIETTIVA. $\square$

<u>TEO 3.11.5</u>: (TEOREMA DI EULERO): SIANO $k, n \in \mathbb{P}$, TALI CHE $(k, n) = 1$. ALLORA

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

<u>DIM.</u> SIA

$$E(n) = \{[k_1]_n, [k_2]_n, \dots, [k_r]_n\}.$$

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

$$E(n) = \left\{ [k]_n [k_1]_n, \dots, [k]_n \cdot [k_r]_n \right\}.$$

QUINDI

$$[k_1]_n \cdot \ldots \cdot [k_r]_n = [k]_n [k_1]_n \cdot \ldots \cdot [k]_n \cdot [k_r]_n$$

$$\Downarrow$$

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

$$\left((k_1, m) = 1 \right) \rightarrow \Downarrow \quad (3.10.2)$$

$$[k_2]_m \cdot \ldots \cdot [k_r]_m = \left([k]_m \right)^r [k_2]_m \cdot \ldots \cdot [k_r]_m$$

$$\Downarrow$$

$$\vdots$$

$$\Downarrow$$

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

$$\Downarrow$$

$$1 \equiv k^r \pmod{m}. \square$$

<u>COR. 3.11.6</u>: SIANO $k, p \in \mathbb{P}$, p PRIMO, $p \nmid k$. ALLORA

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

<u>DIM.</u> BASTA PORRE $m = p$ 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

$$n \overset{def}{=} p \cdot q$$

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

$$MCD\big(e, (p-1)\cdot(q-1)\big) = 1$$

INFINE B CALCOLA L'INVERSA MOLTIPLICATIVA $[d]_{(p-1)(q-1)}$ DI $[e]_{(p-1)(q-1)}$ (ESISTE ED È UNICA). QUINDI B PUBBLICA

n ED e

E TIENE SEGRETI

p, q, ED d.

<u>CODIFICA:</u> A PRENDE UN MESSAGGIO m, $1 \leq m \leq n$ E SPEDISCE

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

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

<u>DECODIFICA:</u> B RICEVE $\tilde{m}$ E DECODIFICA CALCOLANDO

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

PERCHÈ FUNZIONA?

PERCHÈ $[d]_{(p-1)(q-1)}$ 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

$$\left[\tilde{m}^{d}\right]_{n} = \left(\left[m^{e}\right]_{n}\right)^{d} = \left[m^{e\cdot d}\right]_{n}$$

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

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

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

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

$$= \left([1]_n \right)^k \cdot [m]_n$$

(TEO. DI EULERO)

$$= [m]_n .$$

OSS. A E B NON SI SCAMBIANO NIENTE

PERCHÈ PENSO CHE SIA DIFFICILE ROMPERE RSA ?

PER ROMPERE RSA DOVREI O

FATTORIZZARE n

(IMPOSSIBILE SE n È GRANDE) O

RISOLVERE $([x]_n)^e = [\tilde{m}]_n$

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

<u>COSA VUOL DIRE "GRANDE"?</u>

ATTUALMENTE $\cong 10^{1000}$ (CIOÈ $\geq$ 1000 CIFRE)

ES. [1-]: SIANO $p, q \in \mathbb{P}$ DUE NUMERI DI 1000 CIFRE DECIMALI OGNUNO. 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 $\alpha = \frac{a}{b}$

E $(a, b) = 1$.

SIA

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

ALLORA $S \subseteq \mathbb{P}$ E $S \neq \emptyset$ (PERCHÈ $\alpha \in \mathbb{Q}$)

$\Rightarrow$ PER WOP $\Rightarrow$ S HA UN MINIMO.

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

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

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

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

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

INDUZIONE SU n. OVVIO SE $n=1$, FACILE SE $n=2$. SUPPONIAMO $n \geq 3$.

SIANO

$$A \overset{def}{=} \{ i \in [\cancel{n}\ 2, m] : i \text{ HA BATTUTO } 1 \}$$

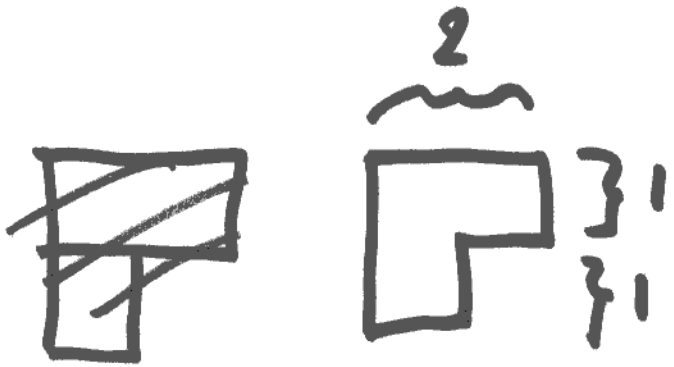
$$B \overset{def}{=} \{ j \in [\cancel{n}\ 2, m] : 1 \text{ HA BATTUTO } j \}.$$

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

$$\tau \perp \rho$$

È UNA CLASSIFICA RAGIONEVOLE PER T_n.

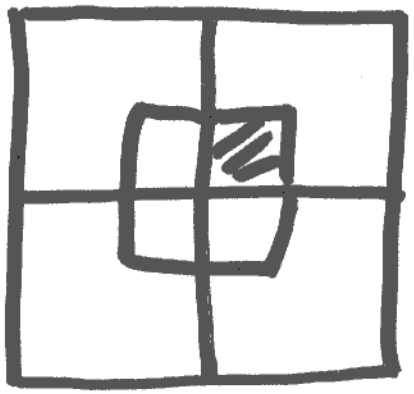
<u>ES.</u> : SIA $n \in \mathbb{P}$. VOGLIAMO ERIGERE UNA STATUA AL CENTRO DI UNA PIAZZA $2^n \times 2^n$, E PAVIMENTARE IL RESTO CON MATTONELLE DELLA FORMA



DIMOSTRARE CHE QUESTO È SEMPRE POSSIBILE.

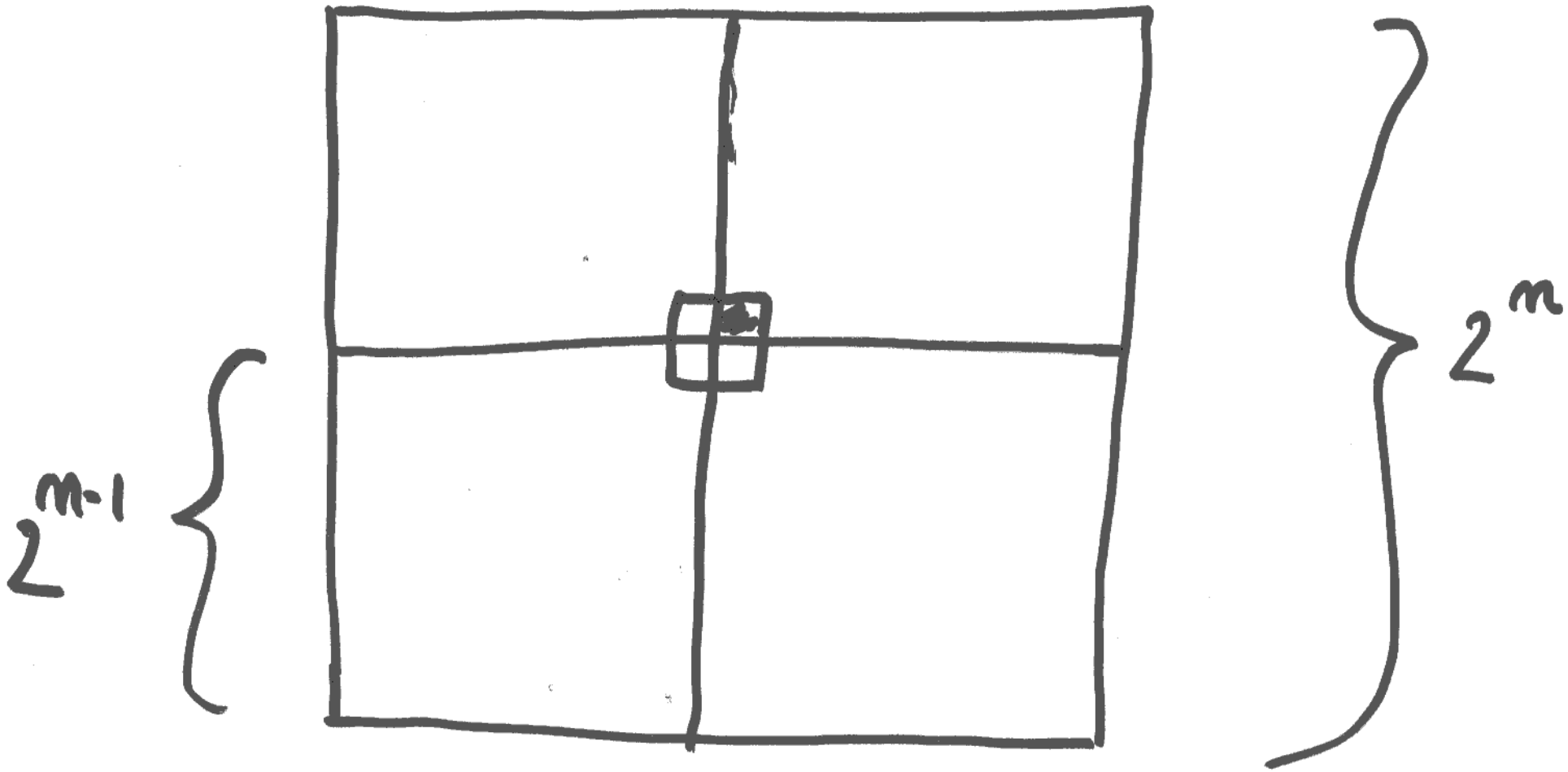
E.g. $n = 1$

$n = 2$



$\Big\}\ 4$

INDUZIONE SU $n \in \mathbb{P}$. SIA $n \geq 3$



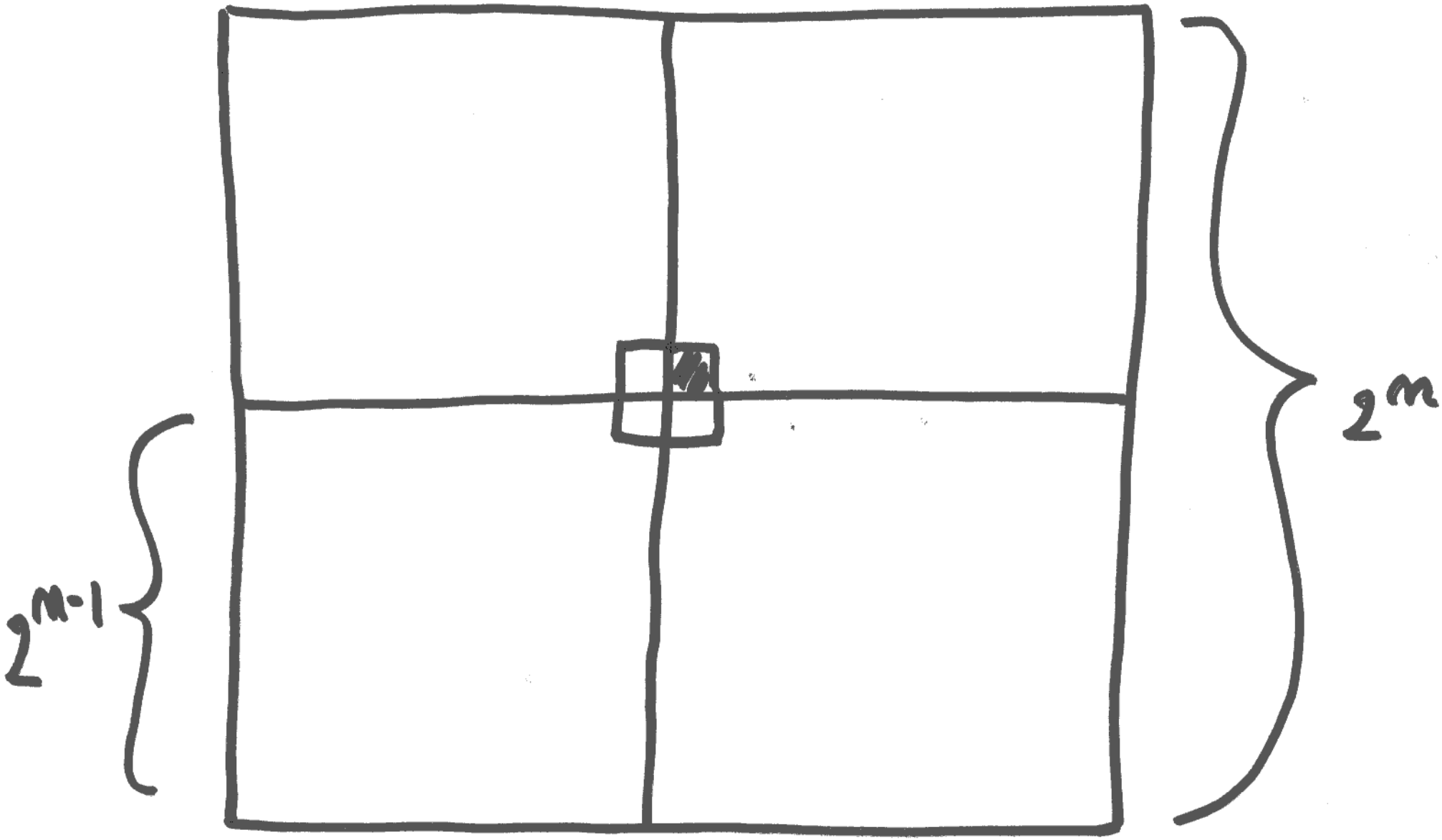
$\Rightarrow$?

RAFFORZAMENTO DELL' IPOTESI:

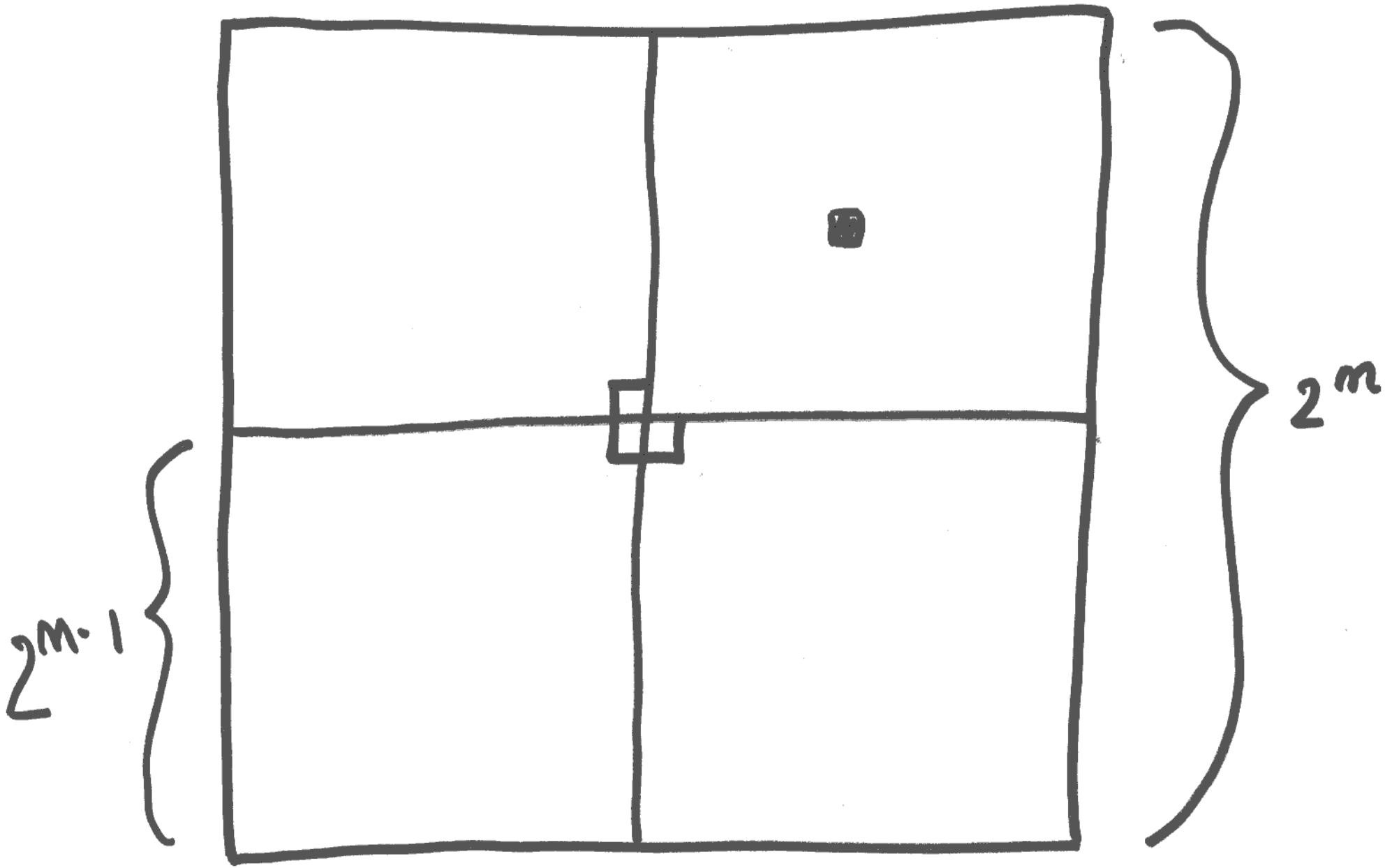
DIMOSTRARE CHE OVUNQUE METTO LA STATUA => POSSO PAVIMENTARE IL RESTO CON .

INDUZIONE:

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



$\Rightarrow$ a.k.



$\Rightarrow$ O.K.

ES.: CONSIDERIAMO IL SEGUENTE

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

ALLORA

$$a^n = 1 .$$

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

$\Rightarrow a^n = a^0 = 1 \Rightarrow$ O.K.

SIA IL TEOREMA VERO PER OGNI

$m \leq n-1$. ALLORA

$$a^n = \frac{a^{n-1} \cdot a^{n-1}}{a^{n-2}} \underset{\substack{\uparrow \\ \text{(INDUZIONE)}}}{=} \frac{\overbrace{1 \cdot 1}^{= \frac{a^{2n-2}}{a^{n-2}}}}{1} = 1 \Rightarrow \text{o.k.} \ \square$$

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 $p \mid 37$

o $p|59$) E ($p|19$ o $p|37$ o $p|53$). MA p È PRIMO $\Rightarrow$ (o $p=17$ o $p=31$ o $p=37$ o $p=59$) E (o $p=19$ o $p=37$ o $p=53$) $\Rightarrow p=37$).

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

$\Rightarrow MCD = 37^2$.

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

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:

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

$$\overset{(2)}{=} 55 + \big(167 + 55(-3)\big)(-27)$$

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

$$\overset{(1)}{=} 167(-27) + \big(389 + 167(-2)\big)(82)$$

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

QUINDI L'ID. DI BEZOÚT E

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

SONDAGGIO: L'INVERSA DELLA PERMUTAZIONE

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

È

a) 64275318 9%

b) 26374851 ~~[illegible]~~ 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.

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

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

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

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

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

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

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

(5)

$$= 59 + \big(120 + 59(-2)\big)(-29)$$

(4)

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

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

(3)

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

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

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

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

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

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

QUINDI L'ID. DI BEZOUT È

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

$$\begin{array}{ccccc} \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel \\ (a,b) & a & x & b & y \end{array}$$

<u>ES.</u> : 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 $r = 1 \Rightarrow$

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

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 PIÙ

$2 \cdot \log_2(r_1)$ 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

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

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

$(\log_2(2) = 1)$ $\rightarrow$ $\cong 2 \cdot \log_2(b)$.

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

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

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 $p \mid c \Rightarrow (\text{o } p \mid a \text{ o } p \mid b)$ E $p \mid c$

$\Rightarrow \text{o } (p \mid a \text{ E } p \mid c) \text{ o } (p \mid b \text{ E } p \mid c) \Rightarrow$

σ (ASSURDO PERCHÈ $(a,c)=1$) σ

(ASSURDO PERCHÈ $(b,c)=1$) $\Rightarrow$ 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%

ES.: CALCOLARE L'INVERSA MOLTIPLICATIVA DI

$$[28]_{125}.$$

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

$125 = 4 \cdot 28 + 13$ $\qquad$ $2 = 2 \cdot 1 + 0$

$28 = 2 \cdot 13 + 2$

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

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

CALCOLIAMO BEZOÚT:

$$
\begin{aligned}
1 &= 13 + 2(-6) \\
&= 13 + \big(28 + 13(-2)\big) \cdot (-6) \\
&= 13 \cdot (13) + 28 \cdot (-6) \\
&= \big(125 + 28 \cdot (-4)\big) \cdot (13) + 28 \cdot (-6)
\end{aligned}
$$

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

QUINDI L'ID. DI BEZOUT È

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

PERTANTO L'INVERSA MOLTIPLICATIVA DI $[28]_{125}$ È

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

ES. : CALCOLARE LE INVERSE MOLTIPLICATIVE DI

$$[172]_{221} \quad E \quad [221]_{172}$$

RISPETTIVAMENTE.

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

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

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

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

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

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

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

CALCOLIAMO BEZOUT

$$1 \underset{(4)}{=} 25 + 24 \cdot (-1)$$

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

(3)

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

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

(2)

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

(1)

$$= 172 \cdot (2) + \left(221 + 172 \cdot (-1)\right) \cdot (-7)$$

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

QUINDI L'ID. DI BEZOUT È

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

PERTANTO L'INVERSA MOLTIPLICATIVA DI $[172]_{221}$ È

$$[9]_{221}$$

QUELLA DI $[221]_{172}$ È

$$[-7]_{172} = [165]_{172}.$$

ES. : CALCOLARE LE ULTIME DUE CIFRE DECIMALI DI

$$3^{100}.$$

SI CHIEDE DI CALCOLARE

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

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

$\Rightarrow$ SAPPIAMO CHE

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

DALLA TEORIA SAPPIAMO CHE

$$\Phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$$

$(100 = 2^2 \cdot 5^2)$

$$= 40.$$

PERTANTO

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

QUINDI

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

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

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

CALCOLIAMO $[3^{20}]_{100}$. ABBIAMO CHE

$$20 = 16 + 4$$

E

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

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

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

$$= [6561]_{100} = [61]_{100}$$

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

$$= [3721]_{100} = [21]_{100}.$$

PERTANTO

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

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

CONCLUDENDO

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

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

01.

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

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

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

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

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

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

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

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

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

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

DOVE x_0, y_0 È UNA SOLUZIONE PARTICOLARE DI (*). PER TROVARE x_0 E y_0 CALCOLIAMO L'ID. DI BEZOÚT.

SVOLGIAMO A.E. A RITROSO:

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

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

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

QUINDI L'ID. DI BEZOÚT È

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

PERTANTO $x_0 = -14$ E $y_0 = 29$ SONO SOLUZIONE DI (*). QUINDI LE SOL.

DI (*) SONO

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

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

$x = -14$, $y = 29$ È SOL. $(t=0)$

$x = -57$, $y = 118$ È SOL. $(t=1)$

$x = 29$, $y = -60$ È SOL. $(t=-1)$

ETC...

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

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

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:

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

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

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

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

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

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

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

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

$\Rightarrow$ MCD$(875, 235) = 5$. POICHÈ $5 \mid 10 \Rightarrow$

$\Rightarrow$ CI SONO SOL. E SONO TUTTE DELLA FORMA

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

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

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

(7)

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

(6)

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

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

(5)

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

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

(4)

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

$$= \big(170 + 65\cdot(-2)\big)\cdot(5) + 65\cdot(-3)$$

(3)

$$= 170\cdot(5) + 65\cdot(-13)$$

$$= 170\cdot(5) + \big(235 + 170(-1)\big)\cdot(-13)$$

(2)

$$= 170\cdot(18) + 235\cdot(-13)$$

$$= \left(875 + 235 \cdot (-3)\right)(18) + 235 \cdot (-13)$$

(1)

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

QUINDI L'ID. DI BEZOUT È

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

MA A NOI INTERESSA 10 => MOLTIPLICO PER 2:

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

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

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

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

ES. : CALCOLARE LE ULTIME DUE CIFRE DI

$$7^{91}.$$

SI CHIEDE DI CALCOLARE

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

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

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

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

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

$$[7^4]_{100} = \left([7^2]_{100}\right)^2 = \left([49]_{100}\right)^2 = [49^2]_{100} =$$

$$= [2401]_{100} = [1]_{100}$$

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

PERTANTO

$$[7^{11}]_{100} = [7^8]_{100} \cdot [7^2]_{100} \cdot [7^1]_{100} =$$

$$= [1]_{100} \cdot [49]_{100} \cdot [7]_{100}$$

$$= [(49) \cdot 7]_{100} = [343]_{100} = [43]_{100}$$

CONCLUDENDO

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

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

ES. : SIA $m \in \mathbb{P}$ E SIA

$$m = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$$

LA SUA ESPRESSIONE DECIMALE ($0 \leq a_0, a_1, \dots, a_k \leq 9$). DIMOSTRARE CHE

$$3 \mid m \iff 3 \mid (a_0 + a_1 + \dots + a_k).$$

DIMOSTRIAMO CHE

$$[n]_3 = [a_0 + a_1 + \dots + a_k]_3 .$$

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

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

PERTANTO

$$[n]_3 = [a_k \cdot 10^k + \dots + a_1 \cdot 10 + a_0]_3$$

$$= [a_k]_3 \cdot [10^k]_3 + \ldots + [a_1]_3 \cdot [10]_3 + [a_0]_3$$

$$= [a_k]_3 \cdot [1]_3 + \ldots + [a_1]_3 \cdot [1]_3 + [a_0]_3$$

$$= [a_k + \ldots + a_1 + a_0]_3 .$$

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

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

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

$$(i, n) = 1 \iff (n-i, n) = 1 \qquad (*)$$

INFATTI, SIA $(i, n) = 1$. PER ASSURDO, SIA $(n-i, n) \geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid (n-i, n) \Rightarrow p \mid (n-i)$ E $p \mid n \Rightarrow p \mid (n-(n-i)) \Rightarrow p \mid i \Rightarrow p \mid i$ E $p \mid n \Rightarrow$ ASSURDO. QUINDI $(n-i, n) = 1$.

VICEVERSA. SIA $(n-i, n)=1$. PER ASSURDO, SIA $(i,n)\geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid i$ E $p \mid n \Rightarrow p \mid (n-i) \Rightarrow$ ASSURDO.

QUESTO DIMOSTRA (*).

PERTANTO

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

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

DOVE

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

E

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

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

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

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

PER $(*)$ $\Rightarrow$ $\Phi(n)$ È PARI.

DECODIFICHIAMO IL MESSAGGIO CRIPTATO

$[\tilde{m}]_n = [1029]_{3901}$. DOBBIAMO CALCOLARE

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

ABBIAMO CHE

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

CALCOLIAMO

$$\left[1029^2\right]_{3901} = \left[1058841\right]_{3901} = \left[1670\right]_{3901}$$

$$\left[1029^4\right]_{3901} = \left(\left[1029^2\right]_{3901}\right)^2 = \left[1670^2\right]_{3901} = \left[2788900\right]_{3901} =$$

$$= \left[3586\right]_{3901}$$

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

$$= \left[128\overset{5}{\cancel{3}}9396 \right]_{3901} = \left[1700 \right]_{3901}$$

$$* \left[1029^{16} \right]_{3901} = \left(\left[1029^{8} \right]_{3901} \right)^{2} = \left[1700^{2} \right]_{3901} = \left[3260 \right]_{3901}$$

$$\left[1029^{32} \right]_{3901} = \left(\left[1029^{16} \right]_{3901} \right)^{2} = \left[3260^{2} \right]_{3901} =$$

$$= \left[1276 \right]_{3901}$$

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

$$= \left[1459\right]_{3901}$$

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

$$= \left[2636\right]_{3901}$$

$$\left[1029^{256}\right]_{3901} = \left(\left[1029^{128}\right]_{3901}\right)^2 = \left(\left[2636\right]_{3901}\right)^2$$

$$= \left[815\right]_{3901}$$

PERTANTO

$$\left[1029^{503}\right]_{3901} = \left[1029^{256}\right]_{3901} \cdot \left[1029^{128}\right]_{3901} \cdot$$

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

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

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

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

$$= [2790]_{3901} \cdot [907]_{3901} \cdot [2964]_{3901} \cdot [1990]_{3901}$$

$$= [3]_{3901}$$

PERTANTO IL MESSAGGIO ORIGINALE ERA

$$[m]_n = [\tilde{m}^d]_n = [1029^{503}]_{3901} = [3]_{3901}.$$

ES.: SIANO p, q, n, 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 $p, q \cong 10^{1000} \Rightarrow \frac{1}{p}, \frac{1}{q} \cong 10^{-1000}, \quad \frac{1}{p \cdot q} \cong 10^{-2000}$

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

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

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

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

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

DOBBIAMO AVERE $(e, 3772) = 1$. PROCEDIAMO PER TENTATIVI, $e = 15$ FUNZIONA. TROVIAMO L'INVERSA MOLTIPLICATIVA $[d]_{(p-1)(q-1)}$ DI $[e]_{(p-1)(q-1)} = [15]_{3772}$. CALCOLIAMO A.E.:

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

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

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 È

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

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

PUBBLICHIAMO

$m = 3901$, $e = 15$

TENIAMO PRIVATI

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

CODIFICHIAMO UN MESSAGGIO $1 \leq m \leq n$ TALE CHE $(m, n) = 1$. PRENDIAMO $m = 3$ $\left((3, 3901) = 1 \Rightarrow \text{o.k.} \right)$. CODIFICHIAMO. DOBBIAMO CALCOLARE

$$[m^e]_n = [3^{15}]_{3901}.$$

ABBIAMO CHE

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

QUINDI

$$[3^2]_{3901} = [9]_{3901}$$

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

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

$$= \left[81^2 \right]_{3901} = \left[\underset{\substack{\parallel \\ (3901+2660)}}{6561} \right]_{3901} = \left[2660 \right]_{3901}$$

PERTANTO

$$\left[3^{15} \right]_{3901} = \left[3^8 \right]_{3901} \cdot \left[3^4 \right]_{3901} \cdot \left[3^2 \right]_{3901} \cdot \left[3 \right]_{3901}$$

$$= \left[2660 \right]_{3901} \cdot \left[81 \right]_{3901} \cdot \left[9 \right]_{3901} \cdot \left[3 \right]_{3901}$$

$$= \left[2660 \right]_{3901} \cdot \left[81 \right]_{3901} \cdot \left[27 \right]_{3901}$$

$$= [2660]_{3901} \cdot [2187]_{3901}$$

$$= [5817420]_{3901}$$

$$= [1029]_{3901}$$

SPEDIAMO QUINDI IL MESSAGGIO CODIFICATO CHE È

$$[\tilde{m}]_n = [1029]_{3901}$$

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%