

CAP 3: NUMERI

3.1. Il principio di induzione

In matematica ci sono 3 modi per dimostrare un'implicazione
 $A \rightarrow B$

1) Dimostrazione diretta

→ Un ragionamento che mostra che se A è vero allora necessariamente è vero anche B

2) Dimostrazione per assurdo

→ Si suppone vera A e $\neg B$, deducendo una contraddizione

[es. [1+]
Dimostrare che se a è irrazionale allora
sia a è irrazionale
("irrazionale" significa " $\in \mathbb{R} \setminus \mathbb{Q}$ ")]

3) Il principio di induzione matematica

→ Sia $P(n)$ un predicato in cui $n \in \mathbb{N}$.

Supponiamo che:

1) $P(1)$ è vero;

2) Se $n \in \mathbb{N}$ allora $(P(1) \wedge P(2) \wedge \dots \wedge P(n)) \rightarrow P(n+1)$

Allora $P(n)$ è vero per ogni $n \in \mathbb{N}$

PRINCIPIO DI INDUZIONE COMPLETA

Sia $P(n)$ come sopra. Supponiamo che:

1) $P(1)$ è vero;

2) Se $n \in \mathbb{N}$ allora $(P(1) \wedge P(2) \wedge \dots \wedge P(n)) \rightarrow P(n+1)$

Allora $P(n)$ è vero per $\forall n \in \mathbb{N}$

NOTAZIONE : Siano $a_0, \dots, a_n \in \mathbb{R}$ allora

$$\sum_{i=0}^n a_i$$

Significa $a_0 + a_1 + \dots + a_n$

ESEMPIO: Dimostrare che

$$\prod_{i=1}^n i = \frac{n(n+1)}{2} \quad (\mathcal{P}(n))$$

$\forall n \in \mathbb{N}$

Dobbiamo dimostrare che:

- $\mathcal{P}(1)$ è vero?

$$\prod_{i=1}^1 i = 1 = \frac{1(1+1)}{2} \Rightarrow \mathcal{P}(1) \text{ è vero}$$

- $\mathcal{P}(n) \rightarrow \mathcal{P}(n+1)$ è vero per $\forall n \in \mathbb{N}$?

Sia $n \in \mathbb{N}$. Suppongo $\mathcal{P}(n)$ vero. Allora

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

Quindi

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

$\mathcal{P}(n+1)$ è vero \Rightarrow OK

Quindi $\mathcal{P}(n)$ è vero per $\forall n \in \mathbb{N}$

[es [1+3] : Dimostrare che

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

$$\forall n \in \mathbb{N} \quad (\text{es., } n=3 \Rightarrow 1+3+5 = 3^2)$$

3.2 Il principio del buon ordinamento

Principio del buon ordinamento (WOP) (Well ordering principle):

Sia $S \subseteq \mathbb{N}$. Allora $\exists m \in S$ tale che $m \leq x \quad \forall x \in S$
(in ogni sottoinsieme c'è sempre un minimo)

OSS WOP è falso per \mathbb{Z} ($S = \{-1, -2, -3\}$ non ha un minimo)

OSS WOP è falso per $\mathbb{Q}_{>0}$ ($= \{a \in \mathbb{Q} : a > 0\}$)
($S = \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$ non ha un minimo)

TEO. 3.2.1

PRINCIPIO DI INDUZIONE \Leftrightarrow WOP

DIM Omessa. \square

3.3 Numeri ~~primi e composti~~ complessi.

NOTAZIONE :

$$\mathbb{R} := \{ \text{Numeri reali} \}$$

$$\mathbb{C} := \{ \text{Numeri complessi} \}$$

$$\{a+bi : a, b \in \mathbb{R}\}$$

$$(i := \sqrt{-1})$$

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

DEF a si dice la parte reale di z
 b si dice la parte immaginaria di z

DEF i ($\stackrel{\text{def}}{=} \sqrt{-1}$) si dice l'unità immaginaria

Siano $w, z \in \mathbb{C}$, $z = a+ib$, $w = c+id$

($a, b, c, d \in \mathbb{R}$)

DEF la somma di w e z è

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

DEF Il prodotto di w e z è

$$\begin{aligned} w \cdot z &:= \stackrel{\text{def}}{(a+ib) \cdot (c+id)} = \\ &= ac + iad + icb + i^2 bd = \\ &= ac + i(ad + cb) - bd = \\ &= (ac - bd) + i(ad + cb) \end{aligned}$$

DEF Il complesso coniugato (o coniugato) di z è

$$\overline{z} := \stackrel{\text{def}}{a-ib}$$

Possiamo dividere z per w , se $w \neq 0$?

Si, "razionalizzando".

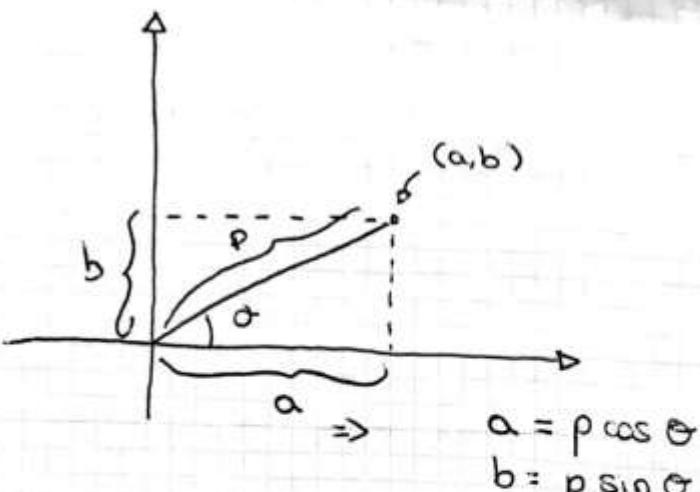
Esempio: $z = 1-4i$, $w = 2+3i$

$$\begin{aligned} \frac{z}{w} &= \frac{1-4i}{2+3i} = \frac{(1-4i)(2-3i)}{(2+3i)(2-3i)} = \\ &= \frac{2-8i-3i+12i^2}{4+6i-6i-9i^2} = \\ &= \frac{2-11i-12}{4+9} = \frac{-10-11i}{13} = -\frac{10}{13} - \frac{11}{13}i \end{aligned}$$

Sia $z = a + bi$

DEF p si dice i.e.
modulo di z .
Scritto $\|z\|$

DEF θ si dice
e' argomento di
 z .



$$\Rightarrow \begin{aligned} a &= p \cos \theta \\ b &= p \sin \theta \end{aligned}$$

Quindi

$$z = p \cos \theta + i p \sin \theta = \underbrace{p(\cos \theta + i \sin \theta)}_{\text{FORMA POLARE di } z}$$

OSS: $\|z\| = \sqrt{a^2 + b^2}$

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

Siano $z, w \in \mathbb{C}$, $z = p \cos \theta + i p \sin \theta$ e
 $w = \varepsilon \cos \varphi + i \varepsilon \sin \varphi$ ($\Rightarrow p, \varepsilon \geq 0$) ($\theta, \varphi \in \mathbb{R}$)

Allora

$$\begin{aligned} z \cdot w &= (p \cos \theta + i p \sin \theta) \cdot (\varepsilon \cos \varphi + i \varepsilon \sin \varphi) = \\ &= \varepsilon p (\cos(\theta + \varphi) + i \sin(\theta + \varphi)) \end{aligned}$$

ES [1+] Sia $z = \frac{1}{2} + i \frac{\sqrt{3}}{2} \in \mathbb{C}$. Calcolare z^{2022}

3.G. NUMERI PRIMI E COMPOSTI

Sono $a, b \in \mathbb{N}^*$

DEF Si dice che a divide b (o che a è multiplo di a) se $\exists k \in \mathbb{Z}$ tale che $b = ak$ (scritto $a|b$)

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

OSS $a|b$ e $b|c \Rightarrow a|c$

OSS $a|b$ e $a|c \Rightarrow a|(ax+by) \quad \forall x, y \in \mathbb{Z}$

DEF Sia $a \in \mathbb{P}$, a si dice PRIMO se $a \geq 2$ e

$b|a \Rightarrow b = \pm 1$ o $b = a$

Altrimenti, a si dice COMPOSTO

TEO 3.G.1 Sia $n \in \mathbb{P}$, $n \geq 2$, Allora n è prodotto di numeri primi

DIH Induzione su $n \geq 2$ se $n=2 \Rightarrow n$ è primo \Rightarrow OK

Sia il teorema vero per tutti i numeri $\leq n$.

Se $n+1$ è primo \Rightarrow OK. Se $n+1$ non è primo

$\Rightarrow \exists a, b \in \mathbb{P}$ tali che

$$n+1 = ab \quad (*)$$

$2 \leq a \leq n, 2 \leq b \leq n$.

Poiché $a \leq n$ e $b \leq n \Rightarrow$ il teorema vale

per a e $b \Rightarrow a$ e b sono prodotto di

primi $\Rightarrow n+1$ è prodotto di primi

(*)

ES è vero che
 $((A \vee B) \wedge (A \rightarrow B)) \rightarrow A$?

A	B	$A \vee B$	$A \rightarrow B$	$(A \vee B) \wedge (A \rightarrow B)$
0	0	0	v	f
0	1	1	v	v
1	0	1	f	f
1	1	1	v	v

$((A \vee B) \wedge (A \rightarrow B)) \rightarrow A$

v
v
f
v

(Da riscrivere)

ES è vero* che
 $((A \rightarrow B) \wedge (A \times B)) \rightarrow A$?

A	B	$A \rightarrow B$	$A \times B$	$(A \rightarrow B) \wedge (A \times B)$
v	v	v	f	f
v	f	f	v	f
f	v	v	v	v
f	f	v	f	f

$((A \rightarrow B) \wedge (A \times B)) \rightarrow A$

v
v
f
v

No, non è sempre vera

ES esprimere la seguente affermazione
"Ci sono studenti che hanno seguito MD
e hanno preso 30"

Come un predicato, usando i predicati:

$$S(x) = "x \text{ ha seguito MD}"$$

$$L(x) = "x \text{ ha preso } 30"$$

(x è nell'universo degli studenti)

$$\exists x. (S(x) \wedge L(x)) \leftarrow \text{Possiamo scrivere}$$

ES Consideriamo l'affermazione
"Tutti i tutori di MD che hanno seguito MD
hanno preso 30"

Scrivere un predicato che esprima questa affermazione,
usando i predicati, $S(x)$, $L(x)$ e $T(x) = "x \text{ è tutore
di MD}"$

Potremo scrivere

$$\forall x. (T(x) \wedge S(x) \rightarrow L(x))$$

PERCHÉ NON

$$\forall x. (T(x) \wedge S(x) \wedge L(x)) ?$$

(Significa "è tutore di MD, ha seguito MD e
ha preso 30")

ES consideriamo l'affermazione

"Esiste uno studente che ha spedito una posta elettronica ad esattamente due studenti, tranne forse a se' stessa"

Scriuire un predicato equivalente usando i.e. predicato:

$E(x, y) \stackrel{\text{def}}{=} "x \text{ ha spedito una e-mail ad } y"$

Potremmo scrivere:

$$\exists x. \exists y. \exists z. ((x \neq y) \wedge (x \neq z) \wedge (y \neq z) \wedge (E(x, y) \wedge E(x, z)) \\ \vee (E(x, y) \wedge E(x, z) \wedge E(x, x))) \wedge (\forall w. ((w \neq x) \wedge \\ \wedge (w \neq y) \wedge (w \neq z)) \rightarrow \neg E(x, w)))$$

Siano $a, b \in \mathbb{P}$

DEF a e b sono COPRIMI (o primi tra loro) se

$$c|a \text{ e } c|b \Rightarrow c=1$$

OSS Siano $p, q \in \mathbb{P}$, $p \neq q$ e, p e q primi.
 \Rightarrow allora p e q sono coprimi.

Sia $n \in \mathbb{P}$

DEF n si dice PERFETTO se è uguale alla somma
dei suoi divisori $\neq n$.

esempio: $n=6$ è PERFETTO ($1+2+3$)

esempio: $n=8$ non è PERFETTO ($1+3 \neq 8$)

PROBLEMA APERTO: esistono numeri perfetti dispari

[ES [2-]: Siano p, q primi, $p > 2$, $q > 2$. Dimostrare
che $p \cdot q$ è non è perfetto.]

TEO. 3.4.2 Esistono infiniti numeri primi.

DIM:

Per assurdo, : Siano $\{p_1, p_2, \dots, p_n\}$ tutti i
numeri primi. Sia

$$N := p_1 \cdot \dots \cdot p_n + 1$$

Per 3.4.1 $\Rightarrow N$ è prodotto di primi $\Rightarrow \exists q \in \mathbb{P}, q$ PRIMO
tale che $q|N$.

Allora $q \neq p_i$.

Se $q = p_i \Rightarrow q|N$ e $q|p_1 \cdot \dots \cdot p_n \Rightarrow q|(N - p_1 \cdot \dots \cdot p_n) \Rightarrow$
 $\Rightarrow q|1 \Rightarrow q \leq 1$, ASSURDO!

Similmente $q \neq p_2$, etc. Quindi $q \notin \{p_1, \dots, p_n\}$ ASSURDO

Sia $n \in \mathbb{N}$. Poniamo

$$\pi(n) := \left| \left\{ m \in \mathbb{P} : m \leq n, m \text{ è primo} \right\} \right|$$

esempio:

$$\pi(8) = \left| \left\{ 2, 3, 5, 7 \right\} \right| = 4$$

(N. B. : $|A| \stackrel{\text{def}}{=} \text{Numero di elementi di } A$)

TEOREMA DEI NUMERI PRIMI,

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

3.5 ALGORITMO EUCLIDEO

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

DEF Il MASSIMO COMUNE DIVISORE tra a e b è

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

(si scrive anche (a, b) o $\text{GCD}(a, b)$)

Come calcolare $\text{MCD}(a, b)$?

PROP 3.5.1 : Siano $a, b \in \mathbb{N}$, $a \geq b$. Allora esistono $q, r \in \mathbb{Z}$ tali che

$$a = b \cdot q + r \quad \text{e } 0 < r < b \quad (\text{N. B. } q = \text{quoziente} \\ r = \text{resto})$$

D.M. è uota.

ALGORITMO EUCLideo:

Siamo $a, b \in \mathbb{N}^*$, $a \geq b$. Ricorda $\exists q, r \in \mathbb{Z}$ tali che

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

e $0 \leq r < b$. - Se $r=0 \Rightarrow \text{HCD}(a,b)=b$
(~~esso~~ vedremo)

- Se $r>0 \Rightarrow \exists q_1, r_1 \in \mathbb{Z}$ tali che
 $b = r \cdot q_1 + r_1$, $0 \leq r_1 < r$



Se $r_1 = 0 \Rightarrow \text{HCD}(a,b) = r$

Se $r_1 > 0 \Rightarrow \exists q_2, r_2 \in \mathbb{Z}$ tali che
 $r = r_1 \cdot q_2 + r_2$, $0 \leq r_2 < r_1$

Se $r_2 = 0 \Rightarrow \text{HCD}(a,b) = r_1$

Se $r_2 > 0 \Rightarrow \exists q_3, r_3 \in \mathbb{Z}$ tali che
 $r_1 = r_2 \cdot q_3 + r_3$, $0 \leq r_3 < r_2$

Ottieniamo quindi due sequenze di ~~nessun~~ numeri

q_1, q_2, \dots e r_1, r_2, \dots tali che

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

Quindi $\exists k \in \mathbb{N}$ tale che $r_k = 0 \Rightarrow \text{HCD}(a,b) = r_{k-1}$

[es [2-]: Fino A ≈ 25 anni fa il numero primo più grande
~~esso~~ conosciuto era

$$p := \frac{2^{16082}-1}{3}$$

Dimostrare che p ha 65050 cifre, e che le ultime 3 sono 447

es. comporre un predicato $P(n)$ che esprime l'affermazione
"n è primo" usando i simboli $<$, \leq , $+$, $-$, ma non
costanti ($1, 2, 3, \dots$) ($n \in \mathbb{N}$)

(per esempio, se $E(n) = "n \text{ è pari}"$, allora posso
scrivere

$$E(n) = \exists m : (n = m + m)$$

Cavriene definire prima il predicato

$$D(n, m) = "n \text{ divide } m"$$

Potremmo scrivere

$$D(n, m) = \exists k : (m = n \cdot k)$$

Abbiamo bisogno di un pred. $\{U(n)\} = "n=1"$.

Possiamo scrivere

$$U(n) = \neg(n \cdot n = n)$$

Possiamo allora scrivere

$$P(n) = \forall m ((D(m, n) \wedge (m < n)) \rightarrow U(m))$$

es. scrivere un predicato $G(n)$ che esprima la

CONGETTURA DI GOLDBACK \rightarrow Dato $n \in \mathbb{N}$, $n > 2$, n
Pari, allora esistono
 q, p primi tali che
 $n = p + q$

(es. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, ...)

Potremmo scrivere prima un pred. $F(n)$ che esprima " $m=2$ ",
per es.

$$F(n) = (n \cdot n = \cancel{n} + n)$$

e poi potremmo avere

$$\forall n ((E(n) \wedge (\forall m. (F(m) \rightarrow n > m))) \rightarrow \exists p. \exists q. (P(p) \wedge P(q) \wedge (n = p + q)))$$

Esempio: $a = 375$ $b = 45$

$$375 = \underbrace{8 \cdot 45 + 15}_{\downarrow q} \quad \Rightarrow \text{MCD}(375, 45) = 15$$

$$45 = 3 \cdot 15 + 0$$

Siano $a, b \in \mathbb{P}$, $a \geq b$, e siano r_1, r_2, \dots e
 q_1, q_2, \dots come in A.E.. Allora

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

$$b = q_1 \cdot r + r_1$$

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

$$r_1 = q_3 \cdot r_2 + r_3$$

$$\boxed{r_i = q_{i+2} \cdot r_{i+1} + r_{i+2}}$$

Sia $k \in \mathbb{P}$ tale che $r_{k+1} = 0$. Allora

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

$$\begin{array}{c} \Downarrow \\ r_k \mid r_{k+1} \end{array}$$

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

$$\Downarrow$$

$$r_k \mid r_{k-2}$$

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

$$\Downarrow$$

$$r_k \mid r_{k-3} \cdot$$

~~vediamo come~~

$$r_k | r_{k-1}, \quad r_k | r_{k-2}, \quad r_k | r_{k-3}, \quad r_k | r;$$

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

↓

$$r_k | r_1$$

ua

$$b = q_1 \cdot v + r_1$$

$$\begin{array}{c} \downarrow \\ r_k | b \end{array}$$

ua

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

↓

$$r_k | a$$

Pertanto $r_k | a$ e $r_k | b$

Sia $c \in \mathbb{P}$ tale che $c | a$ e $c | b$.

$$a = b \cdot q + r \Rightarrow c | r \quad (\text{perche' } r = a - bq)$$

$$b = q_1 r + r_1 \Rightarrow c | r_1 \quad (" r_1 = b - q_1 \cdot r)$$

$$r = q_2 r_1 + r_2 \Rightarrow c | r_2 \quad (r_2 = r_1 - q_2 \cdot r_1)$$

$$r_1 = q_3 r_2 + r_3 \Rightarrow c | r_3 \quad (r_3 = r_2 - q_3 \cdot r_2)$$

Pertanto $c | r_k \Rightarrow c \leq r_k$. Quindi

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

3.6 CONSEGUENZE DELL'A.E.

OSS. Siano $a, b, q, r \in \mathbb{N}$ tali che

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

e $r > 0$. Allora

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

PROP. 3.6.1

Siano $a, b \in \mathbb{N}$. Allora $\exists x, y \in \mathbb{Z}$ tali che

$$\boxed{\begin{aligned} \text{MCD}(a, b) &= ax + by \\ (\text{IDENTITÀ DI BÉZOUT}) \end{aligned}}$$

DIM Sia ~~sia~~ $a \geq b$. Utilizziamo la dim. per induzione su $b \geq 1$.

Se $b=1 \Rightarrow b|a \Rightarrow \text{MCD}(a, b) = 1 = a \cdot 1 + b \cdot (-1)$

Se $b \geq 2 \Rightarrow \exists q, r \in \mathbb{N}$ tali che

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

Se $r=0 \Rightarrow b|a \Rightarrow \text{MCD}(a, b) = b = a \cdot 1 + b \cdot 0$

Se $r > 0 \Rightarrow \text{MCD}(a, b) = \text{MCD}(b, r)$

Ma $r < 0$

↓

Per induzione $\exists \alpha, \beta \in \mathbb{Z}$
tali che

$$\begin{aligned}
 \text{MCD}(b, r) &= b \cdot \alpha + r \cdot \beta = \\
 &= b \cdot \alpha + \underbrace{(a - b \cdot q)}_{r = a - b \cdot q} \cdot \beta = \\
 &= a \cdot \beta + b(\alpha - q \cdot \beta) \\
 &\Downarrow \\
 \text{MCD}(a, b) &= a \cdot \beta + b(\alpha - q \cdot \beta)
 \end{aligned}$$

PROP. 3.6.2

Siano $a, b \in \mathbb{P}$. Allora

$$\text{MCD}(a, b) = \min(\{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{P})$$

DIM OMESSA.

PROP. 3.6.3

Siano $a, b, p \in \mathbb{P}$ tali che

$$p | a \cdot b \quad \text{e} \quad p \text{ è primo}$$

Allora $p | a$ oppure $p | b$

DIM

Se $p | a \Rightarrow$ OK. Se $p \nmid a \Rightarrow \text{MCD}(a, p) = 1$
(se $c | a$ e $c | p \Rightarrow c = 1$ e $c = p \Rightarrow c = 1$)

\Rightarrow per la teoria di Bezout $\exists x, y \in \mathbb{Z}$ tali che

$$1 = (a, p) = ax + py$$

Se mettiamo $x \cdot b$:

$$b = ab \cdot x + pby$$

ma $p | ab \Rightarrow p | b$

es Sia $a \in \mathbb{Q}$. Dimostra, usando il WOP, che esistono $a, b \in \mathbb{Z}$, tali che $b > 0$, $a = \frac{a}{b}$, e $(a, b) = 1$

$$\text{Sia } S := \left\{ d \in \mathbb{P} : \exists c, z \in \mathbb{Z} \text{ per cui } d = \frac{c}{z} \right\}$$

Allora $S \subseteq \mathbb{P}$ e $S \neq \emptyset$ (perché $a \in \mathbb{Q}$)

Per il principio del buon ordinamento

$\exists b \in \mathbb{P}$ tale che $b \leq d$ per ogni $d \in S$. (*)

Poiché $b \in S \Rightarrow \exists a \in \mathbb{Z}$ per cui $a = \frac{a}{b}$.

Allora $(a, b) = 1$. Infatti, sia $c \in \mathbb{P}$ tale che $c | a$ e $c | b \Rightarrow \exists k, e \in \mathbb{Z}$ tali che $a = ck$ e $b = ce \Rightarrow c | b \Rightarrow e < b$.

Ma allora

$$d = \frac{a}{b} = \frac{ck}{ce} = \frac{k}{e} \Rightarrow e \in S \text{ e } e < b, \text{ ASSURDO per (*)}$$

es Consideriamo un torneo all'italiana tra n squadre ($1, 2, \dots, n$). Una classifica ~~qualsiasi~~ è ragionevole se $\tau = \tau(1) \tau(2) \dots \tau(n) \in S_n$ e' ragionevole se $\tau(i)$ ha battuto $\tau(i+1)$ per $\forall 1 \leq i \leq n-1$. Dimostrare che esiste sempre una classifica ragionevole.

Induzione su $n \geq 1$

Chiaro che se $n=1$ e $n=2$.

Se $n \geq 3$. Sia

$$A := \left\{ i \in [n-1] : i \text{ ha battuto } 1 \right\} \setminus \{1\}$$

$$B := \left\{ j \in [n-1] : 1 \text{ ha battuto } j \right\} \setminus \{1\}$$

Allora $|A| \leq n-1$ e $|B| \leq n-1$.

Quindi per induzione $\exists p \in \sigma$ classifica ragionevole
di A e B. Ma allora

$$p \perp \sigma \rightarrow p(1) p(2) \dots \perp \sigma(1) \sigma(2) \dots$$

è una classifica ragionevole (perché $p(1)$ ha battuto
 $\sigma(2)$ (p è ragionevole))

$$p(2) \perp \perp \perp p(3)$$

$$p(1a) \perp \perp \perp \perp \quad (\text{def di A})$$

$$\perp \perp \perp \perp \sigma(1) \quad (\text{def di B})$$

$$\sigma(1) \perp \perp \perp \sigma(2) \quad (\sigma \text{ è ragionevole})$$

es Sia $n \in \mathbb{N}$. Abbiamo una piazza $2^n \times 2^n$.

Vogliamo mettere una statua al "centro" della
piazza e pavimentare il resto con mattonelle
della forma $\begin{cases} \square \\ \square \\ \square \end{cases}$

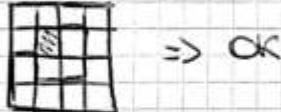
È sempre possibile questo?

Vediamo.

Se $n=1$

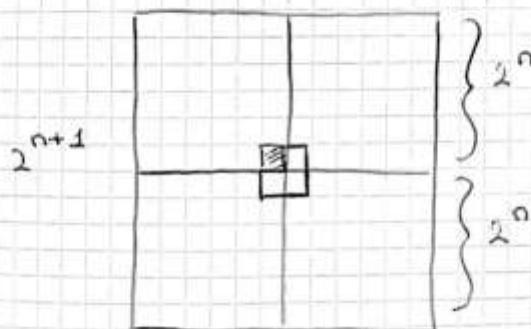


Se $n=2$



Dim per II.

$$2^{\frac{n+1}{2}}$$



OSS Se si puo' fare $\Rightarrow 2^n$ diviso per 3 deve dare resto 1 (se viceversa pero' potrebbe non essere vero, non posso pavimentare \square con $\square\Box$)

RAFFORZAMENTO DELL' IPOTESI:

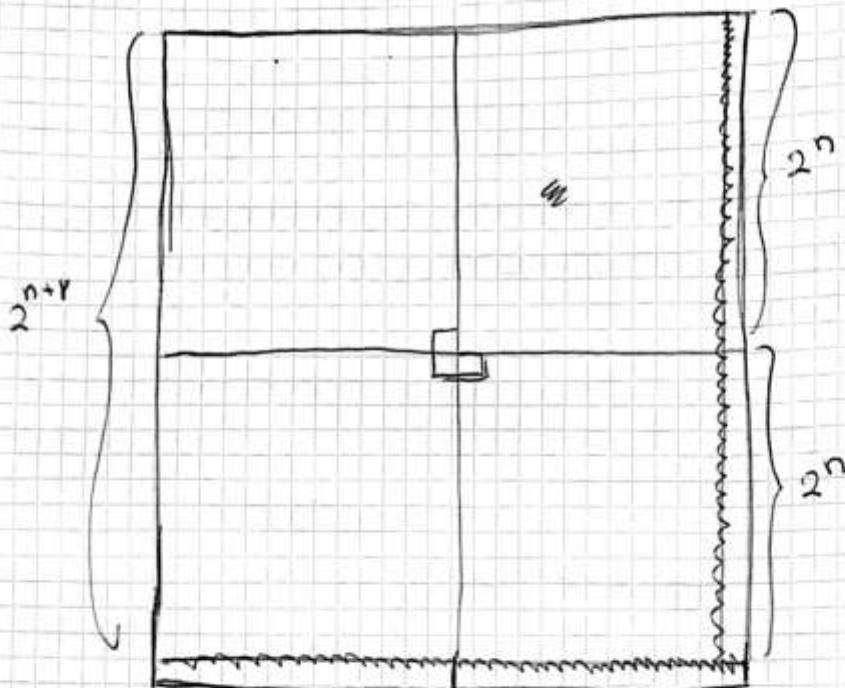
Dimostriamo che possiamo pavimentare una piazza $2^n \times 2^n$ con mattonelle del tipo $\square\Box$, detta doublé.
Mettiamo la statua.

Se $n=1$



OK

Intuizione



\Rightarrow OK

es Consideriamo il seguente "Teorema":
Sia $a \in \mathbb{Z}$, $a \neq 0$, e sia $n \in \mathbb{N}$. Allora

$$a^n = 1 \quad (*)$$

DIH Induzione su $n \geq 0$.

Se $n=0 \Rightarrow a^n = a^0 = 1 \Rightarrow \text{OK}$

~~se necessario~~

Supponiamo (*) vero per $\forall m \in \mathbb{N}$ tale che $m \leq n$.

Allora

$$a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1$$

Dove è l'errore?

OSS 3.6.3. è falso, più generale, se p non è primo

es.: $(4|6 \cdot 2 \text{ ma } 4\nmid 6 \text{ e } 4\nmid 2)$

OSS Se similmente a 3.6.3 si dimostra quanto segue:

$$m|a \cdot b \text{ e } (m,a)=1 \Rightarrow m|b$$

TEO 3.6.4 (TEOREMA FONDAMENTALE DELL'ARITMETICA)

Sia $n \in \mathbb{P}$, $n \geq 2$. Allora

n è prodotto di numeri primi,
in uno ed un solo modo,
a parte l'ordine dei fattori

DIM. Sappiamo già l'esistenza (3.4.1).

Vediamo l'unicità attraverso induz. completa
su $n \geq 2$.

Sia $n=2$. Siano $p_1, \dots, p_n \in \mathbb{P}$, p_1, \dots, p_n primi,
tali che

$$2 = p_1 \cdot \dots \cdot p_n$$

Allora $p_1|2 \Rightarrow p_1 \leq 2 \Rightarrow p_1 = 2$

Similmente $p_2 = 2, \dots, p_n = 2$. Quindi $2 = 2^r \Rightarrow$
 $\Rightarrow r = 1 \Rightarrow \text{OK}$

Sia ora $n \geq 3$ e supponiamo il teorema vero per
tutti gli interi $m \in \mathbb{P}$, $m \leq n-1$.

Siano $p_1, \dots, p_{n-1}, q_1, \dots, q_n \in \mathbb{P}$, p_1, \dots, p_{n-1} e
 q_1, \dots, q_n primi tali che:

$$n = p_1 \cdot \dots \cdot p_{n-1} = q_1 \cdot \dots \cdot q_n \quad (\square)$$

Affora $p_i | q_1 \dots q_s \Rightarrow \exists 1 \leq i \leq s$ tali che $p_i | q_i$
 $\Rightarrow p_i = q_i$. Ma allora

$$\frac{n}{p_i} = p_2 \dots p_r = q_1 \dots q_{i-1} \cdot q_{i+1} \dots q_s \quad (*)$$

e $\frac{n}{p_i} < n \Rightarrow$ per induzione, le due decomposizioni in
(*) coincidono a meno dell'ordine dei fattori \Rightarrow le due
decomposizioni in (*) coincidono a meno dell'ordine
dei fattori }

ESEMPIO: $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$

3.7 EQUAZIONI DIOFANTEE LINEARI

TEO. 3.7.1: Siano $a, b, n \in \mathbb{N}$. Allora $\exists x, y \in \mathbb{Z}$
tali che

$$ax + by = n \quad (*)$$

Se e solo se $(a, b) | n$

DIH

Siano $x, y \in \mathbb{Z}$ tali che (*) vale. Allora $(a, b) | a$ e
 $(a, b) | b \Rightarrow (a, b) | n$.
(*)

Viceversa.

Supponiamo che $(a, b) | n \Rightarrow \exists k \in \mathbb{Z}$ tali che
 $n = (a, b) \cdot k$.

D'altra parte, per 3.6.1 $\Rightarrow \exists \alpha, \beta \in \mathbb{Z}$ tali che
 $a \cdot \alpha + b \cdot \beta = (a, b)$ (Bezout)

$$\alpha(\alpha \cdot k) + \beta(\beta \cdot k) \stackrel{!}{=} (a, b) \cdot k = n$$

TEO 3 f. 2 : Siano $a, b, n \in \mathbb{N}$, tali che $(a, b) | n$. Trova tutte le soluzioni $x, y \in \mathbb{Z}$ di $ax + by = n$ sono della forma (*)

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

Dove $b \in \mathbb{Z}$ e $x_0, y_0 \in \mathbb{Z}$ è una soluzione di (*)

DIH omessa

3.8 LE CLASSI DI RESTO

~~... 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...~~

0 1 2

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

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

dividiamo i numeri con 3 colonne

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

dividiamo in n colonne ...

LE CLASSI DI RESTO sono i numeri che hanno lo stesso colore.

es calcolare $\text{MCD}(389, 167)$ e la corrispondente identità di Bezout.

Usiamo A.E., abbiamo:

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

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

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

$$2 = 2 \cdot 1 + 0 \quad \cancel{\cancel{\cancel{\quad}}}$$

$$\Rightarrow \text{MCD}(389, 167) = 1$$

Per calcolare Bezout sugliamo A.E. dccontrario.

Abbiamo

$$1 = 55 + (-27 \cdot 2) \quad (3)$$

$$\text{Ora si moltiplica per } 167 \quad (4)$$

$$= 55 + (-27)(167 + (-3) \cdot 55) \quad (2)$$

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

$$= (-27) \cdot 167 + (82)(389 + (-2) \cdot 167) \quad (1)$$

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

Quindi l'identità di Bezout è

$$1 = (82) \cdot 389 + (-191) \cdot 167$$

ES calcolare

$$\text{NCD} \left(\underbrace{17^{88} \cdot 31^5 \cdot 37^2 \cdot 59^{100}}_c, \underbrace{19^{(9^{22})} \cdot 37^4 \cdot 53^{36+8}}_b \right)$$

notiamo che $17, 31, 37, 59, 19, 53$ sono tutti numeri primi, quindi

$$\text{NCD}(a, b) = 37^2$$

Infatti, sia $p \in \mathbb{P}$, p primo, tale che $p|a$ e $p|b \Rightarrow (p|17 \circ p|31 \circ p|37 \circ p|59)$
 $\quad \quad \quad (3.6.3)$

$$e(p|19 \circ p|37^3 \circ p|53) \Rightarrow \quad \quad \quad (p \text{ primo}) \\ \Rightarrow (p=17 \circ p=31 \circ p=37 \circ p=59) \text{ e } (p=19 \circ p=37 \circ p=53) = p=37 \text{ - ma } 37^2|a \text{ e } 37^2|b$$

mentre

$$37^3 \nmid a$$

Sia $n \in \mathbb{P}$ definiamo la relazione \equiv_n su \mathbb{Z} ponendo
 $a \equiv_n b \iff n \mid (b - a)$

$\forall a, b \in \mathbb{Z}$. \equiv_n si dice RELAZIONE DI CONGRUENZA
MODULO n

PROP. 3.8.1 Sia $n \in \mathbb{P}$. Allora \equiv_n è di equivalenza
su \mathbb{Z} .

DIM Vedi 1.4 ($n=3$)

Sia $a \in \mathbb{Z}$. La classe di congruenza di a modulo n
è la classe di equivalenza di a rispetto a \equiv_n .

Quindi

$$[a]_n := \{b \in \mathbb{Z} : a \equiv_n b\}$$

(si chiama anche classe di resto di a modulo n)

esempio:

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

(divisi per 2
danno resto 0)

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

(divisi per
due
danno
resto 1)

$$[0]_6 = \{0, 6, -6, 12, \dots\}$$

(divisi per 6
danno resto 0)

$$(\Rightarrow [0]_6 \subseteq [0]_2)$$

$$[3]_6 = \{3, 9, -3, 15, -\cancel{9}, \dots\}$$

~~$[8]_4 = \{8, 9, 12, 0, 16, -4, \dots\}$~~

$$[8]_4 = \{8, 9, 12, 0, 16, -4, \dots\}$$

$$\begin{aligned}
 (\text{perche } [8]_4 &= \{b \in \mathbb{Z} : b \equiv_4 8\} = \\
 &= \{b \in \mathbb{Z} : 4 \mid (b-8)\} = \{b \in \mathbb{Z} : \exists k \in \mathbb{Z} \\
 &\quad \text{per cui } b-8 = 4k\} = \{4k+8 : k \in \mathbb{Z}\} = \\
 &= \{4k : k \in \mathbb{Z}\})
 \end{aligned}$$

$$\{8, 8+4, 8-4, 8+4 \cdot 2, 8-4 \cdot 2, \dots\}$$

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

$$\begin{array}{ll}
 a \equiv_n c & a+b \equiv_n c+d \quad (\text{es. } [I-I]) \\
 \begin{matrix} e \\ b \equiv_n d \end{matrix} & \Rightarrow \quad a \cdot b \equiv_n c \cdot d \quad (\text{es. } [I+I])
 \end{array}$$

$(n \in \mathbb{P})$

Questo suggerisce e permette di definire le seguenti definizioni:

Sia $a, b \in \mathbb{Z}$ e $n \in \mathbb{P}$. La somma di $[a]_n$ e $[b]_n$ e'

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

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

Il prodotto e'

$$[a]_n \cdot [b]_n \stackrel{\text{def}}{=} [ab]_n$$

esempio

$$[3]_6 + [3]_6 = [3+3]_6 = [6]_6 = [0]_6$$

$$[4]_6 \cdot [3]_6 = [4 \cdot 3]_6 = [12]_6 = [0]_6$$

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

$$[2]_6 \cdot [5]_6 = [10]_6 = [4]_6$$

Sia $n \in \mathbb{N}$. Si pone \mathbb{Z}_n come l'insieme delle classi di resto modulo n .

Quindi:

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

Somma e prodotto tra classi di resto si comportano come le operazioni tra numeri.

esempio:

$$[a]_n \cdot ([b]_n + [c]_n) = [ab]_n + [ac]_n$$

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

etc...

c'e' pero' una differenza:

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

e

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

\Downarrow

$$[a]_n = [b]_n$$

esempio

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

$$\in [3]_6 \neq [0]_6 \text{ ma } [4]_6 \neq [2]_6.$$

oss : $[a]_n \cdot [0]_n = [a \cdot 0]_n = [0]_n$

$$\forall a \in \mathbb{Z} \quad (n \in \mathbb{P})$$

esercizio: Calcolare $\text{MCD}(1137, 419)$ e la corrispondente identità di Bezout.

Usiamo A.E.:

$$\begin{aligned}1137 &= 2 \cdot 419 + 299 \\419 &= 1 \cdot 299 + 120 \\299 &= 2 \cdot 120 + 59 \\120 &= 2 \cdot 59 + 2 \\59 &= 2 \cdot 2 + \underline{1} \\2 &= 2 \cdot 1 + 0\end{aligned}$$

$$\text{MCD}(1137, 419) = 1$$

Identità di Bezout

(A.E. al contrario)

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

$$\begin{aligned}1 &= 59 + (-29)(120 + (-2) \cdot 59) \\&= (59) \cdot (59) + (-29) \cdot 120 \\&= (59) \cdot (299 + (-2) \cdot 120) + (-29) \cdot 120 \\&= (59) \cdot 299 + (-147) \cdot 120 \\&= (59) \cdot 299 + (-147) \cdot (419 - 299) \\&= (206) \cdot 299 + (-147) \cdot 419 \\&= (206) \cdot (1137 + (-2) \cdot 419) + (-147) \cdot 419 \\&= (206) \cdot 1137 + (-559) \cdot 419\end{aligned}$$

Pertanto l'identità di Bezout è

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

x a y b

esercizio: Siamo $a, b \in \mathbb{N}$, $a \geq b$, $b \geq 2$.
 Dimostrare che e' A.E. termina
 in al più

$$2\log_2(b)$$

Iterazioni

Dimostrazione per induzione su $b \geq 2$.

Se $b = 2 \rightarrow$ e' A.E. termina in al più 2 iterazioni (1 se a è pari,
 2 se a è dispari) e
 $2\log_2(b) = 2\log_2(2) = 2 \Rightarrow \text{OK}$

Se $b \geq 3 \rightarrow$ Abbiamo che

$$\begin{aligned} a &= b \cdot q + r & 0 \leq r < b \\ b &= q_1 \cdot r + r_1 & 0 \leq r_1 < r \end{aligned}$$

Notiamo che $r_1 \leq \frac{r}{2}$.

Inoltre, se $r \leq \frac{b}{2} \Rightarrow r_1 < r \leq \frac{b}{2} \Rightarrow \text{OK}$

Se $r > \frac{b}{2} \Rightarrow 2r > b > r \Rightarrow q_1 = 1$ e

$$r_1 = b - r < b - \frac{b}{2} = \frac{b}{2} \Rightarrow \text{OK}.$$

ma $\text{MCD}(a, b) = \text{MCD}(b, r) = \text{MCD}(r, r_1)$

Poiché $r_1 \leq \frac{b}{2} \Rightarrow$ e' A.E. per $\text{MCD}(r, r_1)$

Induzione

Termina in al più $2\log_2(r_1)$ iterazioni.

~~Quindi e' A.E. per $\text{MCD}(a, b)$ termina
 in al più~~

Quindi e' A.E. per $\text{MCD}(a, b)$ termina e' in al più

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

Iterazioni. ma $r_1 \leq \frac{b}{2}$, pertanto

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

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

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

esercizio : Siano $a, b \in \mathbb{P}$. E' vero che
 $\text{MCD}(a+1, b+1) = \text{MCD}(a, b) + 1$?

Se fosse vero $\Rightarrow \text{MCD}(a+1, b+1) \geq 2$ per $\forall a, b \in \mathbb{P}$.

Strano...

$\text{MCD}(17, 11) = 1 \Rightarrow$ se $a = 17$ e $b = 11 \Rightarrow \text{MCD}(a+1, b+1)$
 $= 1$, ma $\text{MCD}(a, b) + 1 = 2 + 1 = 3 \neq 1 \Rightarrow \underline{\text{NO}}$

PROP. 3.8.2: Siano $a, b, k \in \mathbb{Z}$ e $n \in \mathbb{P}$ tali che
 $(k, n) = 1$. Allora

$$\left[k \right]_n \cdot \left[a \right]_n = \left[k \right]_n \cdot \left[b \right]_n$$

\Updownarrow

$$\left[a \right]_n = \left[b \right]_n$$

DIM. Se $\left[a \right]_n = \left[b \right]_n \Rightarrow a \equiv b \pmod{n} \Rightarrow$
 $\Rightarrow n \mid (b-a) \Rightarrow n \mid k(b-a) \Rightarrow n \mid (kb - ka) \Rightarrow$
 $\Rightarrow kb \equiv ka \pmod{n} \Rightarrow \left[ka \right]_n = \left[kb \right]_n \Rightarrow$
 $\Rightarrow \left[k \right]_n \cdot \left[a \right]_n = \left[k \right]_n \cdot \left[b \right]_n$

VICEVERSA

Se $\left[k \right]_n \cdot \left[a \right]_n = \left[k \right]_n \cdot \left[b \right]_n \Rightarrow$
 $\Rightarrow \left[ka \right]_n = \left[kb \right]_n \Rightarrow ka \equiv kb \pmod{n} \Rightarrow$
 $\qquad\qquad\qquad \text{(sino congrui)}$
 $\Rightarrow n \mid (kb - ka) \Rightarrow n \mid k(b-a) \Rightarrow$
 $\stackrel{(3.6)}{\Rightarrow} n \mid b(b-a) \Rightarrow b \equiv a \pmod{n} \Rightarrow$
 $\qquad\qquad\qquad ((k, n) = 1)$
 $\Rightarrow \left[b \right]_n = \left[a \right]_n$

Sia $a \in \mathbb{Z}$ e sia $n \in \mathbb{P}$.

DEF Un'INVERSA MOLTIPLICATIVA di $\left[a \right]_n$ e'
 un'altra classe $\left[b \right]_n$ tale che

$$\left[a \right]_n \cdot \left[b \right]_n = \left[1 \right]_n \cdot *$$

PROP. 3.8.3: Siano $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ tali che
 $(a, n) = 1$. Allora esiste una unica
 inversa moltiplicativa di $[a]_n$.

DIM.

(3.6.1)

Poiché $(a, n) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ tali che

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

↓

$$a \cdot x - 1 = n \cdot (-y)$$

↪ n divide la prima parte

$$\Rightarrow n \mid (ax - 1) \Rightarrow ax \equiv 1 \pmod{n} \Rightarrow$$

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

(Sabbiamo trovato
 e' inversa moltiplicativa

Siano $[b]_n, [c]_n \in \mathbb{Z}_n$ tali che :

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

$$\text{ma } (a, n) = 1 \Rightarrow [b]_n = [c]_n$$

(3.8.2)

3.9 LA FUNZIONE DI EULERO

Sia $n \in \mathbb{N}$.

DEF. La funzione di Eulero di n è

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

esempio:

(questi numeri ~~danno resto~~
danno resto)

$$\Phi(9) = |\{1, 2, 3, 4, 5, 6, 7, 8\}| = 6.$$

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

PROP. 3.9.1: Siano $p, q \in \mathbb{P}$, p, q primi, $p \neq q$.
Allora

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

DIH

Abbiamo che

$$\Phi(p \cdot q) = p \cdot q - |\{1 \leq i \leq p \cdot q : (i, pq) \geq 2\}|$$

Se $(i, pq) \geq 2 \Rightarrow \exists r \in \mathbb{P}$, r primo tale che $r | (i, pq)$

$$\Rightarrow r | i \text{ e } r | (p \cdot q) \Rightarrow$$

$$\Rightarrow r | i \text{ e } (r | p \text{ o } r | q) \Rightarrow$$

4
(3.6.2)

$$\Rightarrow r | i \text{ e } (r = p \text{ o } r = q) \Rightarrow$$

$$\Rightarrow (r | i \text{ e } r | p) \text{ o } (r | i \text{ e } r | q) \Rightarrow$$

$$\Rightarrow r | i \text{ e } q | i \Rightarrow$$

$$\Rightarrow r | i \in \{p, 2 \cdot p, \dots, q \cdot p\} \text{ e}$$

 $i \in \{q, 2q, \dots, p \cdot q\} \Rightarrow$

$$\Rightarrow i \in \{p, 2p, \dots, qp, q, 2q, \dots, (p-1)q\} \Rightarrow$$

\Rightarrow ci sono $q + p - 1$ possibilità per i .

PERTANTO

$$\Psi(p, q) = p \cdot q - (p + q - 1)$$

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 $p | (a^2, b) \Rightarrow p | a^2$ e $p | b \Rightarrow$
 $\Rightarrow p | a$ e $p | b \Rightarrow p | (a, b) \Rightarrow p | 1$, ASSURDO.
(3.6.2)

Poi in generale

$$(a, b) = 1 \Rightarrow (a^n, b^m) = 1 \text{ per } \forall n, m \in \mathbb{P}$$

es Siano $a, b, c \in \mathbb{Z}$. Dimostrare che

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

Per assurdo, sia $(ab, c) \geq 2 \Rightarrow$

$$\begin{aligned} &\Rightarrow \exists p \in \mathbb{P}, \text{ } p \text{ primo, tale che } p | ab \text{ e } p | c \Rightarrow \\ &\Rightarrow (\cancel{\circ} p | a \circ p | b) \text{ e } p | c \Rightarrow \quad (3.6.2) \\ &\Rightarrow (\cancel{\circ} p | a \text{ e } p | c) \circ (p | b \text{ e } p | c) \Rightarrow \text{ASSURDO} \end{aligned}$$

[es [1+]: calcolare il minimo $k \in \mathbb{P}$ tale che

$$\underbrace{[3]_{17} \cdot [3]_{17} \cdots [3]_{17}}_k = [1]_{17}$$

es Trovare tutti i numeri $x, y \in \mathbb{Z}$ tali che

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

Sappiamo dalla teoria che esistono tali $x, y \in \mathbb{Z}$ se e solo se $(89, 43) | 1$.

Calcoliamo $(89, 43)$ con A.E.

$$\begin{aligned} 89 &= 2 \cdot 43 + 3 \\ 43 &= 14 \cdot 3 + \underline{1} \\ 3 &= 3 \cdot 1 + 0 \end{aligned} \Rightarrow (89, 43) = 1$$

poiché $1 | 1 \Rightarrow$ ci sono soluzioni di $(*)$.

Per trovare le soluzioni usiamo Bezout:

$$\begin{aligned} 1 &= 43 + (-14) \cdot 3 \\ &= 43 + (-14) \cdot (89 + (-2) \cdot 43) \\ &= (29) \cdot 43 + (-14) \cdot 89 \end{aligned}$$

Pertanto l'ID. di Bezout è:

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

Pertanto $x_0 = -14, y_0 = 29$ è soluzione di $(*)$

Sappiamo ancora dalla teoria che tutte le soluz.

$x, y \in \mathbb{Z}$ di $(*)$ sono della forma

$$\begin{cases} x = x_0 - \frac{43}{(89, 43)} \cdot t \\ y = y_0 + \frac{89}{(89, 43)} \cdot t \end{cases} \quad (t \in \mathbb{Z})$$

Quindi

$$\begin{cases} x = -14 - 43t \\ y = 29 + 89t \end{cases}$$

esplcitamente

x	y	t
-14	29	0
-57	118	1
29	-60	-1
:	:	:

es Trovare tutte le soluz. $x, y \in \mathbb{Z}$ tali che

$$875 \cdot x + 235 y = 10$$

Sappiamo dalla teoria (3.7.1) che ci sono sol. se e solo se $(875, 235) | 10$.

Calcoliamo $(875, 235)$ con A.E.:

$$875 = 3 \cdot 235 + 170$$

$$235 = 1 \cdot 170 + 65$$

$$170 = 2 \cdot 65 + 40$$

$$65 = 1 \cdot 40 + 25$$

$$40 = 1 \cdot 25 + 15$$

$$25 = 1 \cdot 15 + 10$$

$$15 = 1 \cdot 10 + \underline{\underline{15}}$$

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

$(875, 235) = 5$. Poiché $5 | 10 \Rightarrow$ ci sono soluzioni

TEO. 3.9.2 : Sia $n \in \mathbb{N}$ e sia $n = p_1^{a_1} \cdots p_r^{a_r}$ la sua decomposizione in numeri primi ($\Rightarrow p_1 \cdots p_r \in \mathbb{P}$, $p_1 \cdots p_r$ primi e distinti) ($a_1, \dots, a_r \in \mathbb{N}$).
 Allora:

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

DIH. Vedi cap. 4

PROP. 3.9.3 : Siano $a, b \in \mathbb{N}$, tali che $(a, b) = 1$.
 Allora

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

DIH. Vedi cap. 4

esempio : $n = 100 \Rightarrow n = 2^2 \cdot 5^2$ (dec. in numeri primi)

$$\begin{aligned} \Phi(100) &= 100 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = \\ &= 10 \cdot 4 = 40 \end{aligned}$$

Sia $n \in \mathbb{N}$. Poniamo

$$E(n) := \left\{ [a]_n : (a, n) = 1 \right\}$$

PROP. 3.9.4 : Sia $n \in \mathbb{N}$ e sia $k \in \mathbb{Z}$ tali che $(k, n) = 1$.
 Allora la funzione

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

Per $\forall [a]_n \in E(n)$, è una BIIEZIONE

D14

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

ma $(k, n) = 1 \Rightarrow (ak, n) = 1 \Rightarrow [ak]_n \in E(n) \Rightarrow$
 $\Rightarrow [a]_n \cdot [k]_n \in E(n)$.

DIMOSTRIAMO CHE SIA INIETTIVA

Siano $[a]_n, [b]_n \in E(n)$ tali che $[a]_n \cdot [k]_n =$
 $= [b]_n \cdot [k]_n \Rightarrow$

$$\Rightarrow [a]_n = [b]_n \quad (\text{perche' } (k, n) = 1).$$

(3.8)

Quindi è iniettiva.

DIMOSTRIAMO CHE SIA SURGETTIVA

Sia ora $[b]_n \in E(n)$.

Poiché $(k, n) = 1 \Rightarrow \exists [h]_n \in \mathbb{Z}$ tale che ~~$[hk]_n$~~
 $[k]_n \cdot [h]_n = [1]_n$ (3.8)
(eice' $[h]_n$ è l'inversa moltiplicativa di $[k]_n$).

Ma allora $[bh]_n \in E(n)$ e

$$[bh]_n \cdot [k]_n = [b]_n \cdot [h]_n \cdot [k]_n = [b]_n \cdot [1]_n = [b]_n$$

Quindi è surgettiva.

TEO. 3.9.5 (TEOREMA DI EULERO)

Siano $n \in \mathbb{N}$ e $k \in \mathbb{Z}$ tali che $(k, n) = 1$.

Allora

$$k^{\frac{n}{\varphi(n)}} \equiv 1 \pmod{n}$$

DIM.

$$\text{Sia } \mathcal{E}(n) = \left\{ [k_1]_n, \dots, [k_{\varphi(n)}]_n \right\}$$

Quindi $\mathcal{C} = \mathcal{E}(n)$.

$$\text{Per 3.8.4 : } \mathcal{E}(n) = \left\{ [k_1]_n \cdot [k]_n, \dots, [k_{\varphi(n)}] \cdot [k]_n \right\}$$

Pertanto

$$[k_1]_n \cdot \dots \cdot [k_{\varphi(n)}]_n = [k_1]_n \cdot [k]_n \cdot \dots \cdot [k_{\varphi(n)}]_n \cdot [k]_n$$

\Downarrow

$$[1]_n \cdot [k_1]_n \cdot \dots \cdot [k_{\varphi(n)}]_n = ([k]_n)^{\varphi(n)} \cdot [k_1]_n \cdot \dots \cdot [k_{\varphi(n)}]_n$$

\Downarrow (3.8.2 \rightarrow poiché $(k_1, n) = 1$)

$$[1]_n \cdot [k_2]_n \cdot \dots \cdot [k_{\varphi(n)}]_n = [k^{\varphi(n)}]_n \cdot [k_2]_n \cdot \dots \cdot [k_{\varphi(n)}]_n$$

\Downarrow

$$[1]_n \cdot [k_3]_n \cdot \dots \cdot [k_{\varphi(n)}]_n = [k^{\varphi(n)}]_n \cdot [k_3]_n \cdot \dots \cdot [k_{\varphi(n)}]_n$$

\Downarrow

analogo caso, fino ad arrivare a

$$[1]_n = [k^{\varphi(n)}]_n$$

\Downarrow

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

Esempio: Sia $n = 9$.

Allora

$$E(9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$$

$[10]_9$ non viene ma $= [1]_9$, etc

COR. 3.9.6 : (PICCOLO TEOREMA DI FERMAT)

Siano $k, p \in \mathbb{N}$, p primo, tali che $p \nmid k$.

Allora

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

DIH Segue dal Teorema di Eulero 3.9.5

3.10 IL CODICE RSA

Problema fondamentale della crittografia:

Spedire un messaggio da A a B in modo
che solo B possa leggerlo (decriptarlo)

Il codice RSA ha 3 fasi:

- PREPARAZIONE: B sceglie due primi $p, q > 0$,
 $p \neq q$, e calcola $n \stackrel{\text{def}}{=} p \cdot q$.

Quindi trova $e \in \mathbb{P}$ tale che
 $\text{MCD}(e, (p-1)(q-1)) = 1$.

Infine B calcola l'inversa
moltiplicativa $[d]_{(p-1)(q-1)}$ di
 $[e]_{(p-1)(q-1)}$.
(esiste ed è unica) (vedi 3.8).

B pubblica n, e e
tiene segreti p, q, d .

- CODIFICA : A prende un messaggio $m \in \mathbb{P}$,
 $1 \leq m \leq n$, tale che
 $(m, n) = 1$,
poi calcola
 $[\tilde{m}]_n := [m]^e_n$
e spedisce \tilde{m} .

- DECODIFICA : B riceve \tilde{m} e decodifica calcolando
 $[\tilde{m}^d]_n$

Perché funziona?

Poiché $[e]_{(p-1)(q-1)} \cdot [d]_{(p-1)(q-1)} = [1]_{(p-1)(q-1)}$
 $\Rightarrow e \cdot d \equiv 1 \pmod{\Phi(n)} \Rightarrow$
 $\Rightarrow \exists k \in \mathbb{Z} \text{ tale che } e \cdot d = k \cdot \Phi(n) + 1$.

Pertanto

$$\begin{aligned} [\tilde{m}^d]_n &= [(m^e)^d]_n = [m^{ed}]_n = \\ &= [m^{k \cdot \Phi(n) + 1}]_n = [(m^{\Phi(n)})^k]_n \cdot [m]_n = \\ &= ([m^{\Phi(n)}]_n)^k \cdot [m]_n = \\ &= ([1]_n)^k \cdot [m]_n = \\ &\xrightarrow{\text{x teor. di Eulero } ((m, n) = 1)} \\ &= [m]_n \end{aligned}$$

OSS. A e B non si scambiano niente

Perché pensiamo che rompere questo codice sia difficile?

Per romperlo dovremmo o fattorizzare n (Impossibile) se $n \gg 0$ oppure risolvere

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

se $e=2 \Rightarrow$ reciproca quadratica (Gauss, ≈ 1810)

se $e=3 \Rightarrow$ " Cubica (Eisenstein, ≈ 1930)

se $e \geq 4 \Rightarrow$ ricerca attuale

Cosa significa "grande" ?

(Attualmente $\approx 10^{1000}$)

NOTA STORICA:

- Codice Romano : A e B si scambiano una permutazione σ dell'alfabeto (codice di sostituzione)

DEBOLEZZA : un'analisi delle frequenze rivelava la permutazione

ES Siano $p, q \in \mathbb{P}$, $p \neq q$, p, q primi,
 $p \geq 3$, $q \geq 3$.
Dimostrare che $n = p \cdot q$ non è perfetto

I divisori di n sono

$$1, p, q, p \cdot q$$

Per assurdo, sia n perfetto. Allora

$$p \cdot q = 1 + p + q$$

↓↓

$$2 \cdot p \cdot q = (1+p)(1+q)$$

Ma $p \equiv 1 \pmod{2} \Rightarrow \exists k \in \mathbb{Z}$ tale che $p = 2k+1$.

Quindi

$$2 \cdot p \cdot q = 2(k+1)(1+q)$$

↓↓

$$p \cdot q = (k+1)(1+q)$$

Ma $q \equiv 1 \pmod{2} \Rightarrow \exists l \in \mathbb{Z}$ tale che $q = 2l+1$.

Quindi

$$pq = (1+k)(1+l) \cdot 2$$

$$\Rightarrow 2 | pq \Rightarrow \textcircled{e} 2 | p \textcircled{o} 2 | q \Rightarrow \text{assurdo}$$

es [2.] Siano $p_1, \dots, p_r \in \mathbb{P}$, p_1, \dots, p_r primi,
 tali che $p_1 \geq 3, \dots, p_r \geq 3$.
 Dimostrare che
 $n = p_1 \cdot p_2 \cdots p_r$ non è perfetto

es Calcolare le ultime due cifre di 7^{91} .
 Si chiede di calcolare $[7^{91}]_{100}$.

Ma $(7, 100) = 1 \Rightarrow$ per il Teo. di Euler

$$[7^{\varphi(100)}]_{100} = [1]_{100}$$

$$\text{ma } \varphi(100) = \varphi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$$

$$\text{Quindi } [7^{40}]_{100} = [1]_{100}$$

Ma allora

$$\begin{aligned}
 [7^{91}]_{100} &= [(7^{40})^2]_{100} \cdot [7^1]_{100} = \\
 &= ([7^{40}]_{100})^2 \cdot [7^1]_{100} = \\
 &= ([1]_{100})^2 \cdot [7^1]_{100}^* = \\
 &= [7^1]_{100}
 \end{aligned}$$

Ma

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

$$[7^4]_{100} = ([7^2]_{100})^2 = [49^2]_{100} = [2401]_{100} = [1]_{100}$$

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

Pertanto

$$\begin{aligned}
 [7^{11}]_{100} &= [7^{8+2+1}]_{100} = [1]_{100} \cdot [49]_{100} \cdot [7]_{100} = \\
 &= [343]_{100} = [43]_{100}
 \end{aligned}$$

Concludendo

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

\Rightarrow le ultime due cifre di 7^{91} sono 43.

Risposta 3.11 NUMERAZIONI IN BASI DIVERSE

PROP. 3.11.1

Siano $n, b \in \mathbb{N}$, $b \geq 2$. Allora

esistono $b_0, \dots, b_K \in \mathbb{N}$ tali che ~~esse siano uniche~~

$0 \leq b_i \leq b-1$ per $\forall i = 0, \dots, K$ e

$$n = b_K \cdot b^K + b_{K-1} \cdot b^{K-1} + \dots + b_1 \cdot b^1 + b_0 \quad (\square)$$

Dove $K := \max \{i \in \mathbb{N} : b^i \leq n\}$. Tali b_0, \dots, b_K sono uniche.

DIH per induzione su $n \geq 1$

Se $n \leq b-1 \Rightarrow K=0 \Rightarrow b_0=n \Rightarrow \text{OK}$

Se $n \geq b$.

Sia $K = \max \{i \in \mathbb{N} : b^i \leq n\}$. Allora

$$b^K \leq n \leq b^{K+1} \quad (*)$$

Sappiamo che $\exists q, r \in \mathbb{N}$ tali che

$$n = q \cdot b^K + r, \quad 0 \leq r < b^K.$$

(*)

Allora $\Rightarrow q \leq b-1$.

Ma $r < n \Rightarrow$ per induzione $\Rightarrow \exists b_0, \dots, b_{h-1} \in \mathbb{N}$ tali che
 $0 \leq b_0, \dots, b_{h-1} \leq b-1$ e

$$r = b_{h-1} \cdot b^h + b_{h-2} \cdot b^{h-1} + \dots + b_1 \cdot b + b_0$$

Dove $n := \max \{j \in \mathbb{N} : b^j \leq r\}$.

Ma $r < b^K \Rightarrow h \leq K$.

Pertanto

$$\begin{aligned} n &= q \cdot b^K + r \\ &= q \cdot b^K + b_{h-1} \cdot b^h + \dots + b_1 \cdot b + b_0 \\ &= b_K \cdot b^K + b_{K-1} \cdot b^{K-1} + \dots + b_1 \cdot b + b_0 \end{aligned}$$

dove $b_k := q \in \mathbb{N}$ e $b_{k+1} = b_{k+2} = \dots = b_{n+1} := 0$

Siano $b_0, \dots, b_k, c_0, \dots, c_k \in \mathbb{N}$ tali che

$$b_k b^k + \dots + b_1 b + b_0 = n = c_k b^k + \dots + c_1 b + c_0$$

con $0 \leq b_0, \dots, b_k, c_0, \dots, c_k \leq b-1$.

Allora

$$b_0 - c_0 = b \cdot (c_1 - b_1) + b^2 \cdot (c_2 - b_2) + \dots + b^k \cdot (c_k - b_k)$$

$$\Rightarrow b | b_0 - c_0.$$

$$\text{Ma } |b_0 - c_0| \leq b-1$$

$$\Rightarrow b_0 - c_0 = 0 \Rightarrow b_0 = c_0.$$

Quindi

$$b_k b^k + \dots + b_2 b^2 + b_1 b = c_k b^k + \dots + c_2 b^2 + c_1 b$$

↓

$$b_k b^{k-1} + \dots + b_2 b + b_1 = c_k b^{k-1} + \dots + c_2 b + c_1$$

↓

$$b_1 - c_1 = b^{k-1} (c_k - b_k) + \dots + b (c_2 - b_2)$$

Quindi

$$b | (b_1 - c_1). \text{ Ma } |b_1 - c_1| \leq b-1$$

$$\Rightarrow b_1 - c_1 = 0 \Rightarrow b_1 = c_1$$

$$\text{etc } \dots \Rightarrow b_2 = c_2 \Rightarrow \dots \Rightarrow b_k = c_k$$

DEF (ii) si dice e' espressione b-ARIA (σ in base b)
di n .