

[https://open.spotify.com/playlist/3zMsGGKjUNIx3DFJ133ex?  
si=rGWujY5LSLy7B1vKdUTHnA&pi=e-SkW9gkIWTLG5](https://open.spotify.com/playlist/3zMsGGKjUNIx3DFJ133ex?si=rGWujY5LSLy7B1vKdUTHnA&pi=e-SkW9gkIWTLG5)



Si vuole creare una teoria generale che contenga come esempio  $\mathbb{Z}$  e le sue operazioni

$$\mathbb{Z} \xrightarrow{-} \mathbb{Z} \quad \text{opposto}, \quad \mathbb{Z} \times \mathbb{Z} \xrightarrow{+} \mathbb{Z} \quad \text{somma e prodotto (binarie)}$$

l'altro modo di esprimere l'addizione



Ci sono diverse condizioni di compatibilità tra le operazioni:

$$\Delta(b+c) = ab+ac, \Delta+b = b+\Delta, \Delta+(b+c) = (\Delta+b)+c$$

def ANELLO es.  $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$

poi lo chiameremo solo A

Un anello (commutativo unitario) è il dato di una SESTUPLA  $(A, +, -, \cdot, 0_A, 1_A)$

dove:

- $A \longrightarrow$  insieme non vuoto
- $+, - : A \times A \longrightarrow A$  operazioni binarie
- $- : A \longrightarrow A$  opposto
- $0_A \in A$  elemento neutro addizione
- $1_A \in A$  elemento neutro moltiplicazione

questi dati devono soddisfare 8 proprietà:

4 sull'addizione  $(A, +, -, 0_A, 1_A)$

- ①  $\forall a, b \in A, a+b = b+a$  COMMUTATIVITÀ
- ②  $\forall a, b, c \in A, (a+b)+c = a+(b+c)$  ASSOCIAZIATIVITÀ DELLA SOMMA
- ③  $\forall a \in A, a+0_A = 0_A+a = a$  EL NEUTRO SOMMA
- ④  $\forall a \in A, a+(-a) = 0_A$  (OPPOSTO)



queste 4 proprietà indicano che  $(A, +, -, 0_A)$  è un GRUPPO ABELIANO in notazione additiva

$\exists e \in A : \forall a \in A, e+a = a+e = a$   
An identity element  
 $\forall a \in A, \exists b \in A : a+b = b+a = e$   
Inverse elements  
 $\forall a, b \in A, a+b = b+a$  That's not your girl, that's an Abelian group!  
and Commutativity

$\forall a, b, c \in A, (a+b)+c = a+(b+c)$   
ASSOCIATIVITÀ  
 $\forall a, b \in A, a \oplus b \in A$  Closure

Fellas, if your girl  
 $(A, \oplus)$   
is a set together with  
a well-defined binary  
operation, with  
 $\forall a, b \in A, a \oplus b \in A$

(grazie Pinterest)

4 sul prodotto  $(A, +, -, \cdot, 0_A, 1_A)$ :

- ⑤  $\forall a, b, c \in A, a(b \cdot c) = (a \cdot b)c = abc$  ASSOCIAZIATIVITÀ DEL PRODOTTO
- ⑥  $\forall a, b, c \in A, a(b+c) = ab+ac$  DISTRIBUTIVITÀ  
 $(a+b)c = ac+bc$
- ⑦  $\forall a \in A, a \cdot 1_A = 1_A \cdot a = a$  EL NEUTRO DEL PRODOTTO  
rende l'anello "UNITARIO"
- ⑧  $\forall a, b \in A, a \cdot b = b \cdot a$ , COMMUTATIVITÀ DEL PRODOTTO  
rende l'anello "COMMUTATIVO"

l'anello  $A = \mathbb{Z}$  ha proprietà più specifiche:

#### BUON ORDINAMENTO E ORDINE TOTALE

- esiste il sottoinsieme  $\mathbb{N}^* = \mathbb{N} \setminus \{0\} \subset \mathbb{Z}$  che permette di definire una relazione su  $\mathbb{Z}$ :

si scrive  $a > b \iff a - b \in \mathbb{N}^*$

$$\forall a \in \mathbb{Z} \text{ si ha: } \begin{cases} a \in \mathbb{N}^* & \text{è positivo} \\ a = 0 & \text{è nullo} \\ -a \in \mathbb{N}^* & \text{è negativo} \end{cases} \quad (\text{proprietà di tricotomia})$$

- Ogni sottoinsieme  $E \subset \mathbb{N}^*$  non vuoto possiede un più piccolo elemento per

$\langle \exists c \in E \text{ tc. } \forall e \in E \setminus \{c\} \text{ si ha } e > c \rangle \text{ BUON ORDINAMENTO}$

un anello commutativo e unitario che soddisfa le proprietà di tricotomia e buon ordinamento "è essenzialmente"  $\mathbb{Z}$

- se  $a < b \quad c < d$  allora  $a+c < b+d$  e  $-a > -b$  allora l'operazione + e > sono compatibili in modo simile, c'è compatibilità tra  $\circ$  e  $>$

#### legge di cancellazione in $\mathbb{Z}$

Se  $ab = ac$  con  $a \neq 0$  allora  $b=c$ .

altrimenti basta mult per -1 entrambi le parti

Infatti, supponendo  $a > 0$

Induzione su  $a \geq 1$

•  $a=1$  è chiaro perché 1 è l'el. neutro

• Supponiamo per ip. induttiva che  $a > 1$  e  $(a-1)b = (a-1)c$

Supponiamo x ass. che  $b \neq c$ . Allora  $\circ b > c \circ b < c$ . Supponiamo  $b > c \implies (a-1)b + b > (a-1)c + c$

tricotomia

premessa  $ab = ac$

$\circ b > ac$ , che è impossibile  
quindi necessariamente  $b=c$

def ELEMENTI INVERTIBILI dato  $A$  anello  $1_A \neq 0_A$

$a \in A$  t.c.  $\exists b \in A : ab = ba = 1_A$  ( $a$ ) è detto elemento invertibile.

(si dice che  $b$  è inverso di  $a$  e si scrive  $b = a^{-1}$ )

es. se  $a$  è invertibile allora  $a^{-1}$  è unicamente determinato

inverso di  $a$ : el che, moltiplicato per  $a$ , dà  $1_A$

es.  $1_A$  è invertibile di inverso  $1_A^{-1} = 1_A$

$$a \cdot b = a \cdot b' = 1 \text{ con } b, b' \in A$$

deve essere =

$$\begin{aligned} \text{allora } (a \cdot b) b' &= 1_A \cdot b' = b' \\ \text{quindi } \textcircled{3} &\rightarrow \text{uguali} \\ (a \cdot b') b &= 1_A \cdot b = b \\ \text{quindi } \textcircled{2} &\rightarrow \text{uguali} \\ (a \cdot b) b' &= a(b \cdot b') = a(b' \cdot b) = ab' \cdot b \\ \text{quindi } \textcircled{1} &\rightarrow \text{uguali} \end{aligned}$$

Si pone  $A^x = \{ \alpha \in A \text{ t.c. } \alpha \text{ è invertibile} \}$   $A^x$  è un gruppo

verificare ①  $A^x$  è non vuoto ② se  $\alpha \in A^x$  allora  $\alpha^{-1} \in A^x$

③ se  $a, b \in A^x$  sono invertibili, allora  $(ab)^{-1} = a^{-1}b^{-1}$

④  $\mathbb{Z}^x = \{1, -1\}$

esercizio  $(\mathbb{Q}, +, -, \cdot, 0, 1)$  è un anello (cu). Calcolare l'insieme degli elementi invertibili

risposta:  $\mathbb{Q}^x = \{r \in \mathbb{Q}; r \neq 0\}$   $[1] = [1_A]$

PICCOLI ESEMPI

①  $\forall \alpha \in A, \alpha \cdot 0_A = 0_A$

$$\begin{aligned} \alpha \cdot 0_A &= \underbrace{\alpha \cdot (0_A + (-0_A))}_{0_A \text{ (assioma)}} = \alpha \cdot 0_A + \alpha \cdot (-0_A) \\ &= \alpha \cdot 0_A + (-(\alpha \cdot 0_A)) \text{ elemento} + \text{il suo opposto quindi } \alpha \cdot 0_A = 0_A \\ &= 0_A \times \text{assioma} \end{aligned}$$

② Supponiamo  $0_A = 1_A$ .

Mostriamo che  $\forall \alpha \in A, \alpha = 0_A = 1_A$  ( $A = \{0_A\}$ )

$$\alpha \in A : 1_A = 0_A \implies \underbrace{\alpha \cdot 1_A}_{=\alpha} = \underbrace{\alpha \cdot 0_A}_{0_A} \text{ quindi, } \forall \alpha, \alpha = 0_A$$

③ se  $1_A \neq 0_A$  allora  $0_A \notin A^x$ .

Supponiamo per assurdo  $\exists x \in A^x$  t.c.  $1_A = x \cdot 0_A = 0_A$  contraddizione

gli assiomi implicano che  $0_A$  non è mai invertibile

Si pone  $A^\times = \{a \in A \text{ t.c. } a \text{ è invertibile}\}$   $A^\times$  è un gruppo

verificare ①  $A^\times$  è non vuoto ② se  $a \in A^\times$  allora  $a^{-1} \in A^\times$

③ se  $a, b \in A^\times$  sono invertibili, allora  $(ab)^{-1} = a^{-1}b^{-1}$

④  $\mathbb{Z}^\times = \{1, -1\}$

①  $A^\times$  non è vuoto.

Abbiamo visto che  $1_A$  è sempre invertibile e  $1_A \in A$  per def. di omessa comm. un. (semplice)

quindi,  $1_A \in A \Rightarrow A \neq \emptyset$

② se  $a \in A^\times$  allora  $a^{-1} \in A^\times$

se  $a \in A^\times$ , vuol dire che  $\exists$  vista in classe unicamente determinato  $b \in A : ab = ba = 1_A$ .

Supponiamo per assurdo che  $b \notin A^\times$ .

se  $b \notin A^\times$ ,  $\nexists x \in A$  t.c.  $bx = xb = 1_A$ . ma questo è falso, esiste ed è  $a$ .

$\circ \forall x \in A, bx = xb \neq 1_A$  falso per  $a$

③ se  $a, b \in A^\times$ , allora  $(ab)^{-1} = a^{-1}b^{-1}$

$$(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow a^{-1}b^{-1} \cdot ab = 1_A \quad \text{per definizione.}$$

$$\Leftrightarrow a^{-1} \cdot b^{-1} \cdot a \cdot b = 1_A \quad \text{se } a^{-1}b^{-1} \cdot ab = 1_A \text{ (e, poiché unicamente determinato,}$$

$a^{-1}b^{-1} \cdot ab = 1_A$

e  $(a \cdot b)^{-1} \cdot ab = 1_A$  allora  $(ab)^{-1} = a^{-1}b^{-1}$ )

visto che  $a^{-1} \cdot a = 1_A$  e  $b^{-1} \cdot b = 1_A$

$$a^{-1} \cdot b^{-1} \cdot a \cdot b \quad \begin{matrix} \text{commutatività} \\ \text{e associtività} \end{matrix} \quad (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1_A$$

$1_A \cdot 1_A = 1_A$  vero perché  $1_A$  il.

neutro della mult.

quindi  $x \cdot 1_A = 1_A$

④  $\mathbb{Z}^\times = \{1, -1\}$

• dimostriamo  $1, -1 \in \mathbb{Z}^\times$

① su  $\mathbb{Z}$ ,  $1_A = 1$ . Visto che  $1_A$  è sempre invertibile,  $1 \in \mathbb{Z}^\times$

②  $-1 = -(-1)$  se  $-1^{-1} = 1$ , allora  $-(-1^{-1}) = -(-1)$  moltiplica per  $-1$  da entrambe le parti  
quindi  $-1 \in \mathbb{Z}^\times$  e  $-1^{-1} = -1$

③ dimostriamo che  $\forall x \in \mathbb{Z}, x \notin \{1, -1\} \Rightarrow x \notin \mathbb{Z}^\times$

Supponiamo per assurdo  $x \in \mathbb{Z}, x \notin \{1, -1\}, x \in \mathbb{Z}^\times$

Allora  $x \cdot y = 1_A$ . su  $\mathbb{Z}$ ,  $1_A = 1$ , quindi  $x \cdot y = 1$

Ma, su  $\mathbb{Z}$ , le uniche coppie che moltiplicate danno 1 sono  $(-1, -1)$  e  $(1, 1)$

Per ipotesi,  $x \notin \{1, -1\}$ , quindi CONTRADDIZIONE

esercizio  $(\mathbb{Q}, +, -, \cdot, 0, 1)$  è un anello (cu). Calcolare  $\mathbb{Q}^{\times} = \{x \in \mathbb{Q} : x \text{ è invertibile}\}$

- invertibili:  $\exists x \in \mathbb{Q} \text{ t.c. } \exists y \in \mathbb{Q} \text{ t.c. } xy = 1$

- in  $\mathbb{Q}^{\times}$ ,  $1_A = 1$ .

quindi  $\exists x \in \mathbb{Q} \text{ t.c. } \exists y \in \mathbb{Q} \text{ t.c. } xy = 1$

① dimostriamo che  $0 \notin \mathbb{Q}^{\times} \rightarrow 0 = 0_A \in \mathbb{Q}_A \text{ e } 0_A \text{ non è invertibile per definizione}$   
(ma, comunque, basta fare:  $0 \cdot y = 1$  impossibile perché  $0 \cdot y = 0$ )

② dimostriamo che  $\forall q \in \mathbb{Q}, q \neq 0, q \in \mathbb{Q}^{\times}$

$qx = 1 \iff x = \frac{1}{q} \text{ e } \frac{1}{q} \in \mathbb{Q}$ . Trovato  $x$  t.c.  $qx = 1$  (per vedere inviamente che  $x \neq 0$  non va)  
perché  $\frac{1}{0}$  impossibile  
(non sono sicura che questo basti, ngl.)

esercizio: c'è un unico elemento neutro

Siamo  $v, v'$  due elementi neutri per la moltiplicazione

$$\begin{array}{lll} \forall a \in A \quad av = ua = a & \text{con } a = v & vv' = v'u = v \\ \quad av' = u'a = a & \text{con } a = v' & v'u \cancel{=} vv' = v' \end{array} \quad \text{quindi } v = v'$$

Dedurre che anche l'elemento neutro per l'addizione è unicamente determinato

## Relazione di divisibilità

Introduciamo la relazione:  $a, b \in A : a|b \iff \exists c \in A \text{ t.c. } b = a \cdot c$ .

$$2|6 : 6 = 2 \cdot 3$$

• è una relazione **riflessiva**:  $\forall a \in A, a = a \cdot 1_A$

• è una relazione **transitiva**:  $a, b, c \in A$  supponiamo  $a|b \iff b = a \cdot a' \exists a' \in A$

• Non è simmetrica né antisimmetrica  
ma su  $N^*$  è antisimmetrica

$$b|c \iff c = b \cdot b' \exists b' \in A$$

$$\Rightarrow c = a \cdot a' \cdot b' = a(\underbrace{a' \cdot b'}_{a''}) \Rightarrow c = a \cdot a'' \iff a|c$$

• se  $a|b \wedge a|c$  allora  $a|b+c$  (compatibilità)

$$a|b \iff \exists a' \text{ t.c. } b = a \cdot a' \quad a|c \iff \exists a'' \in A \text{ t.c. } c = a \cdot a''$$

$$b+c = a \cdot a' + a \cdot a'' = a \underbrace{(a'+a'')}_{a'''} \iff a|b+c$$

più generalmente, se  $\alpha, \beta \in A$ ,  $\alpha|b, \alpha|c \Rightarrow \alpha|b+\beta c$  (la dimostrazione è banale)

$$\alpha b + \beta c = \alpha \cdot a \cdot a' + \beta \cdot a \cdot a'' = a \underbrace{(\alpha a' + \beta a'')}_{a'''}$$

dim.  $\alpha, \beta \in A$

$$a|b, a|c \Rightarrow a|\alpha b + \beta c$$

$\cdot \alpha|b \Rightarrow \alpha|\alpha b$  per def. di moltiplicazione

$\cdot \alpha|c \Rightarrow \alpha|\beta c$

per la dim. d. compatibilità,  $\alpha|\alpha b + \beta c$

In  $\mathbb{Z}$  la relazione di divisibilità è quasi antisimmetrica:

ignoriamo il caso  $0$

$$a, b \in \mathbb{Z} \quad a|b \wedge b|a \Rightarrow \exists c \in \mathbb{Z}^* \text{ t.c. } a = bc \quad (\text{ovvero } a \in \{b, -b\} \circ \{a, -a\} = \{b, -b\})$$

$$\textcircled{1} \mid 1 \Rightarrow 1 = \textcircled{0} \cdot b \quad \textcircled{0} \text{ non divide mai un el. non nullo} \quad \text{quindi possiamo supporre } a, b \neq \textcircled{0}$$

$$a|b, b|a \Rightarrow b = a \cdot a', a = b \cdot b' \exists a, b \in \mathbb{Z}$$

$$b = b \cdot a' \cdot b' \quad \text{con } b \neq \textcircled{0}, \text{ legge di cancellazione} \quad b' = b \cdot a' \cdot b' \Rightarrow 1 = a' \cdot b' \Rightarrow a' \cdot b' \in \{1, -1\}$$

$$\Rightarrow \{a, -a\} = \{b, -b\}$$

• non è simmetrica  $\rightarrow$  supponiamo  $a|b$  simmetrica. Allora  $a|b$  ( $\exists c \text{ t.c. } b = a \cdot c$ )  $\Rightarrow b|a$  ( $\exists c' \text{ t.c. } a = b \cdot c'$ )

$$\text{quindi, } b = b \cdot c' \cdot c \quad \text{con } b \neq \textcircled{0} \quad b = b \cdot c' \cdot c \iff 1 = c \cdot c' \iff (c, c') \in \{(1, 1), (-1, -1)\}$$

oppure, con esempio:  $2|4$  ma  $4 \not| 2$

• non è antisimmetrica: se fosse antisimmetrica,  $a|b \wedge b|a \Rightarrow a = b$

ma (ragionamento di prima)  $1 = c \cdot c \iff (c, c) \in \{(1, 1), (-1, -1)\}$

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

def elemento irriducibile

invertibili

$\alpha \in A \setminus A^\times$  è detto irriducibile se

$\forall b, c \in A, \alpha = bc \Rightarrow b \in A^\times \text{ o } c \in A^\times$

es.  $A = \mathbb{Z}$   $12 = 4 \cdot 3$  ma  $4, 3 \notin \mathbb{Z}^\times \Rightarrow 12$  non è irr.

$$7 = 1 \cdot 7 = 7 \cdot 1 = -1 \cdot -7 = -7 \cdot -1 \quad 7 \text{ è irriducibile}$$

$1 \in \mathbb{Z}$  non è irriducibile perché abbiamo definito  $\alpha \in A \setminus A^\times$

def numero primo

invertibili

$\alpha \in A \setminus A^\times, \alpha \neq 0$  è detto primo se

$\forall b, c \in A, \text{ se } \alpha | bc \Rightarrow \alpha | b \text{ oppure } \alpha | c$

Supponiamo  $A = \mathbb{Z}$

lemma  $p \in \mathbb{Z}$  primo  $\Rightarrow p$  è irriducibile

dim  $p$  primo, siano  $a, b \in \mathbb{Z}$  t.c.  $p = ab \Rightarrow p | a \cdot b$

$$ab = p \cdot 1$$

Supponiamo senza perdita di generalità  $p | a$

$$\text{sost. } a = p a'$$

$$p | a \Rightarrow a = p a' \exists a' \in \mathbb{Z} \Rightarrow p = p a' b \quad \begin{matrix} \text{legge di} \\ \text{concessione} \end{matrix} \quad p = p(a'b) \Leftrightarrow 1 = a'b \Rightarrow a', b \in \{+1, -1\} = \mathbb{Z}^\times$$

Se  $a' = 1$  allora  $a = p \Rightarrow p = pb \Rightarrow b = 1$

Se  $a' = -1$  allora  $a = -p \Rightarrow p = p - b \Rightarrow -b = 1 \Rightarrow b = -1 \Rightarrow p$  è irriducibile

!! ogni modo di scriverlo come  
 $p = ab$  porta ad  $a, b \in \{-1, 1\}$   
 $A^\times \text{ in } \mathbb{Z}$

def valore assoluto

$$\mathbb{Z} \xrightarrow{\text{1.1}} \mathbb{N} \quad a \in \mathbb{Z} \quad \bullet \text{ se } a = 0 \quad |a| = 0$$

• se  $a \neq 0, |a| =$  l'unico elemento di  $\mathbb{N}$  contenuto nell'insieme  
di due elementi  $\{a, -a\}$

## ALGORITMO DELLA DIVISIONE EUCLIDEA

$a, n \in \mathbb{Z}, n \neq 0$  allora esistono unicamente determinati

$q \in \mathbb{Z}, r \in \{0, \dots, |n|-1\}$  t.c.  $a = nq + r$

resto  
quoziente

è una riformulazione  
del principio del minimo su  $\mathbb{N}$

## def CONGRUENZA

b è il resto di  $\frac{2}{\sqrt{n}}$

$$a \equiv b \pmod{n} \iff n \mid a - b$$

(n divide  $a - b$ )

$$\iff \exists q \in \mathbb{Z} \text{ t.c. } d-b = qn$$

ovvero, il resto della divisione escluse di  $a - b$  per  $n$  è 0

- La congruenza modulo  $n$  è di equivalenza

④ Transitivität:  $a \equiv b \pmod{n}$  und  $b \equiv c \pmod{n} \iff n \mid b-a$  und  $n \mid c-b$

$$n|\alpha: n|\beta \Rightarrow n|\alpha+\beta \quad n|c-b+b-a \Rightarrow n|c-a \Leftrightarrow a \equiv c \pmod{n}$$

Scw. rifl. e simm.

$$\mathbb{Z}_{\equiv \text{mod } n} = \left\{ \begin{matrix} n\mathbb{Z}, & n\mathbb{Z}+1, & \dots, & n\mathbb{Z}+n-1 \\ [0] & [1] & & [n-1] \\ & & & [n-1] \end{matrix} \right\}$$

② riflessiva :  $\delta = \delta \bmod n$        $n \mid \delta - \delta$  vero perché  $\forall x \in \mathbb{Z}, x \neq 0, x \mid 0$

$$\textcircled{3} \text{ simmetrico: } a \equiv_n b \implies b \equiv_n a \quad n | a - b \implies n | b - a$$

$$n > -b \iff a - b = qn \iff -(a - b) = -(qn) \iff b - a = -qn \quad \text{quindi } n | b - a$$

Esempi: congruenze modulo 2

$$\mathbb{Z} = \underbrace{2\mathbb{Z}}_{[0]} \sqcup \underbrace{2\mathbb{Z} + 1}_{[1]} \quad \mathbb{Z}/\equiv_{\text{mod}_2} = \{2\mathbb{Z}, 2\mathbb{Z} + 1\}$$

congruenza mod. 3

$$\mathbb{Z}_{\equiv_{\text{mod } 3}} = \{ [3]_3, [1]_3, [2]_3 \}$$

$$\mathbb{Z}/\equiv_n = \mathbb{Z}_{n\mathbb{Z}} \quad n > 0 \quad \text{insieme quoziente}$$

di  $\mathbb{Z}$  su congr. modulo  $n$

l'componente  
mod.  $n$

quindi  $\mathbb{Z}_{2\mathbb{Z}} = \{[0], [1]\}$   $\mathbb{Z}_{3\mathbb{Z}} = \{[0], [1], [2]\}$   $\mathbb{Z}_{1\mathbb{Z}} = \{[0]\}$

tutti gli interi

$[2]_3 = \{m \in \mathbb{Z} : m \equiv 2 \pmod{3}\} = \{m \in \mathbb{Z} : 3 | m - 2\}$

Le operazioni: + · - di  $\mathbb{Z}$  sono compatibili con  $\equiv_n$  ( $n > 0$ )

①  $\forall \alpha, \alpha' \in \mathbb{Z}, \alpha \equiv \alpha' \pmod{n} \iff -\alpha \equiv -\alpha' \pmod{n}$  compatibilità con opposto

②  $\forall \alpha, \alpha', b, b' \in \mathbb{Z}, \alpha \equiv_n \alpha', b \equiv_n b' \Rightarrow \alpha + b \equiv_n \alpha' + b'$  comp. con somma

③  $\forall \alpha, \alpha', b, b' \in \mathbb{Z}, \alpha \equiv_n \alpha', b \equiv_n b' \Rightarrow \alpha b \equiv_n \alpha' b'$  comp. con prodotto

dim. ②

$$2 \mid 5-1 \quad \text{e} \quad 2 \mid 1-5$$

$$\alpha \equiv_n \alpha' \iff n \mid \alpha - \alpha' \quad \text{e} \quad n \mid \alpha' - \alpha$$

$$n \mid b' - b \iff \exists k \in \mathbb{Z} \text{ t.c. } \underline{\alpha'} - \underline{\alpha} = nk$$

$$n \mid b' - b \iff \exists k' \in \mathbb{Z} \text{ t.c. } \underline{b'} - \underline{b} = nk'$$

Dove ottenere  $\alpha + b \equiv_n \alpha' + b'$

sommare le due formule

$$\Rightarrow \underline{\alpha'} + \underline{b'} - (\underline{\alpha} + \underline{b}) = n(k + k') \iff \alpha' + b' \equiv_n \alpha + b$$

quindi  $n(\alpha' + b') - \alpha + b$   
(perché  $n \cdot \text{qualcosa} = \text{quello}$ )

dim. ①

$$\forall \alpha, \alpha' \in \mathbb{Z}, \alpha \equiv_n \alpha' \iff -\alpha \equiv_n -\alpha'$$

$$\alpha \equiv_n \alpha' \iff n \mid \alpha - \alpha' \iff \alpha - \alpha' = qn \iff -\alpha + \alpha' = -qn$$

dim. ③

$$\forall \alpha, \alpha', b, b' \in \mathbb{Z}, \alpha \equiv_n \alpha', b \equiv_n b' \Rightarrow \alpha b \equiv_n \alpha' b'$$

ovvero  $\alpha b - \alpha' b' = kn \quad \text{o} \quad \alpha b = kn + \alpha' b'$

$$\alpha = qn + \alpha' \quad \text{e} \quad b = q'n + b' \quad \text{quindi } \alpha b = (\alpha' + qn)(b' + q'n) = \alpha' b' + n(q'b' + \alpha' q' + qq'n)$$

$kn$

$\alpha b = \alpha' b' + n(k)$

### OPERATORI

$\mathbb{Z}/n\mathbb{Z}$  definiamo  $[a] \in \mathbb{Z}/n\mathbb{Z}$   $[a] = a + n\mathbb{Z}$  insieme degli interi che si esprimono come  $a +$  multiplo di  $n$  (interi che hanno come resto  $a$ )

-  $[a] := [-a]$  questa funz.  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  è ben definita: opposto in  $\mathbb{Z}/n\mathbb{Z}$

definiamo

•  $[a] + [b] := [a+b]$  ben definito (ovvero indipendente dalla scelta di rapp. di  $[a] \in [b]$ )

$$\text{scelgiamo } a' \in [a] \quad \text{e } b' \in [b] \quad \text{e calcoliamo } [a'+b'] = \left\{ m : n \mid m - a' - b' \right\} = \left\{ m : n \mid m - (a+b) \right\}$$

per (2), perché  $[a] = [a']$   
quindi  $a \equiv a'$   
e stessa cosa per  $b$

$\Leftrightarrow [a+b] = [a'+b']$  l'operazione + introdotta su  $\mathbb{Z}/n\mathbb{Z}$  è ben definita

$$\text{esempi: } [1]_3, [2]_3 \in \mathbb{Z}/3\mathbb{Z} \quad [1] + [2] = [3] = [0]$$

$$\text{altri rapp. } [1] = [4] \quad [2] = [-4]$$

$$\text{quindi } [4 + -4] = [0]$$

• definiamo inoltre  $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$   $[a] \cdot [b] = [ab]$  ben definito

$$\text{scelgiamo } a' \in [a] \quad \text{e } b' \in [b], [ab] = \left\{ m : n \mid m - a'b' \right\} \quad \begin{aligned} \text{ma } a' &= na \\ &\text{e } b' = nb \\ &\text{quindi, per (3)} \end{aligned} = \left\{ m : n \mid m - ab \right\}$$

$$\text{esempi: } [1]_3, [2]_3 \in \mathbb{Z}/3\mathbb{Z} \quad [1] \cdot [2] = [2]$$

$$\text{e } [4 \cdot -4] = [-16] = [2] \quad \begin{aligned} \text{perché } \frac{2}{3} &= 0 \text{ resto } 2 \\ &\text{e } \frac{-16}{3} = -6 \text{ resto } 2 \end{aligned}$$

### TEOREMA

$(\mathbb{Z}/n\mathbb{Z}, +, -, \cdot, [0], [1])$  è un ANELLO (comm. un.)

alcuni sottoinsiemi di  $\mathbb{Z}$

•  $n\mathbb{Z} = \{m \in \mathbb{Z} \text{ t.c. } \exists k \in \mathbb{Z} \text{ con } m = kn\}$  multipli di  $n$

•  $\mathbb{Z} \setminus \{0\} = \mathbb{Z}^*$

•  $a\mathbb{Z} + b\mathbb{Z} := \{m \in \mathbb{Z} : \exists k, k' \in \mathbb{Z} \text{ con } m = ka + kb\}$  multipli di  $a +$  multipli di  $b$

$$2\mathbb{Z} + 3\mathbb{Z} = \left\{ 0, 2, 4, \frac{8}{3}, 6, \frac{9}{3}, 5, \frac{10}{3}, 8, \frac{14}{3}, 7, \frac{16}{3}, -1, \frac{-10}{3}, 1, \frac{2}{3} \right\} = \mathbb{Z}$$

mod. 2      mod. 3       $2+3$        $2+6$

vedremo  $a\mathbb{Z} + b\mathbb{Z} = \text{MCD}(a, b)\mathbb{Z}$

in particolare  $\text{MCD}(2, 3) = 1 \quad 2\mathbb{Z} + 3\mathbb{Z} = 1\mathbb{Z}$

2	-7	-4	-1	2	5
0	-9	-6	-3	0	3
-2	-11	-8	-5	-2	1
-4	-13	-10	-7	-4	-1
-6	-15	-12	-9	-6	-3
	-9	-6	-3	0	3

La divisibilità è una relazione di inclusione di sottoinsiemi

$$a, b \in \mathbb{Z}^* \quad a|b \iff b \mathbb{Z} \subset a\mathbb{Z} \quad \text{solo se i multipli di } b \text{ sono un sott. dei multipli di } a$$

• Supponiamo  $a|b$

$$\iff \exists k \in \mathbb{Z} \text{ t.c. } b = ka$$

se  $a|b$ , allora  
ogni multiplo di  $b$  può essere riscritto  
come  $b$ -qualcosa. Ma, per def di  $|$ ,  $b = a$ -qualcosa.  
quindi, un multiplo di  $b$  è un multiplo di  $a$

per definizione,  $b = ka \Rightarrow b' = \underbrace{l}_{l'} \underbrace{ka}_{k'} = l'a \iff b' \in a\mathbb{Z}$

dimostriamo  $b\mathbb{Z} \subset a\mathbb{Z} \Rightarrow a|b$

• Supponiamo  $b\mathbb{Z} \subset a\mathbb{Z}$

Allora  $\forall b' \in b\mathbb{Z}, b' \in a\mathbb{Z}$ . Per definizione,  $b' \in a\mathbb{Z} \iff \exists k \in \mathbb{Z} \text{ t.c. } b' = ka$

ma  $b' = lb$ . Quindi,  $lb = ka \iff b = \underbrace{k}_{k'} \underbrace{l}_{l'} a = k'a$  quindi  $b = ka$  ■

Lemma:  $E = a\mathbb{Z} + b\mathbb{Z}$  con  $a, b \neq 0$ , allora  $\exists! \delta \in \mathbb{N}^*$  t.c.  $E = \delta\mathbb{Z}$

tutte le  
combinazioni sono  
multiple di un certo  
numero unico

dimostrazione

el. d:  $E > 0$

poniamo  $E^* := E \cap \mathbb{N}^* \subset \mathbb{N}^*$

• osserviamo che  $E^* \neq \emptyset$

- infatti, se  $a, b > 0$ , esiste una coppia  $(k, k') \in \mathbb{N}^2$  t.c.  $k_a + k'b > 0$

$\in E^*$

- se invece  $a > 0$  e  $b < 0$ ,  $\exists (k, k') \in \mathbb{N} \times \mathbb{N}$  t.c.  $k_a + k'b > 0$

(e, per  $a < 0$ ,  $b > 0$   $\exists (k, k') \in -\mathbb{N} \times \mathbb{N}$  e per  $a < 0$ ,  $b < 0$   $\exists (k, k') \in -\mathbb{N} \times -\mathbb{N}$ )

• poniamo  $\delta = \min(E^*)$  ben definito in  $\mathbb{N}^*$  (principio del minimo)

• osserviamo che  $\delta \leq |a|$  e  $\delta \leq |b|$

infatti  $|a| \in E^*$  (perché  $E = a\mathbb{Z} + b\mathbb{Z}$ )  $\subset \delta = \min(E^*)$

• per la DIVISIONE EUCLIDEA  $a = q\delta + r$ ,  $r \in \{0, 1, \dots, \delta-1\}$

notiamo che  $r = a - q\delta$

$a \in E$ ,  $\delta \in E^* \subset E \implies \delta = ua + vb$  con  $u, v \in \mathbb{Z}$

sempre per  
 $E = a\mathbb{Z} + b\mathbb{Z}$

quindi  $r = a - q(ua + vb) \iff r = a - qua - qvb \iff r = a(\underbrace{1-qu}_k) + b(\underbrace{-qv}_{k'})$  quindi  $r = \delta k + \delta k' \iff r \in E$

Ci sono 2 opzioni: ①  $r = 0$ ,  $\delta | a$  ( $a = q\delta + r$ ) e abbiamo finito

per  $\delta = \min(E^*)$

② altrimenti,  $r > 0$  e  $r \in E^*$ . Se fosse vero,  $r \geq \delta$ . Ma questo è impossibile per  $a = q\delta + r$  con  $r \in \{0, 1, \dots, \delta-1\}$

$r \neq \delta$

quindi necessariamente  $r = 0$  e  $\delta | a$ . Per la stessa ragione,  $\delta | b$ .

•  $\forall \alpha, \beta \in \mathbb{Z}$ ,  $\delta | \alpha a + \beta b \implies E \subset \delta\mathbb{Z}$  per la dim sopra ( $a | b \iff b\mathbb{Z} \subset a\mathbb{Z}$ )

d'altronde,  $\delta \in E \iff \delta = ka + kb$

$\forall l \in \mathbb{Z}$ ,  $l\delta = lk a + lk' b \implies l\delta \in E$

se i multipli di  $\delta$  sono

elementi di  $E$ , allora  $\Rightarrow \delta\mathbb{Z} \subset E$

$\delta\mathbb{Z}$  è contenuto in  $E$

(per def  $=$ )

QUINDI, visto che  $E \subset \delta\mathbb{Z}$  e  $E \supset \delta\mathbb{Z}$ ,  $E = \delta\mathbb{Z}$

cosa abbiamo fatto? POSTI:  $E = a\mathbb{Z} + b\mathbb{Z}$  con  $a, b \neq 0$  •  $E^* = E \cap \mathbb{N}^*$  (dimostrato  $E \neq \emptyset$ ) •  $\delta = \min(E^*)$

notiamo che

•  $a$  e  $b$  si può riscrivere come  $a = q\delta + r$ . Questo implica che  $r < \delta-1$  (per questioni resto)

• e che  $r \in E$ , perché  $\delta = ua + vb$  e  $r = a - q\delta \iff r = a - (ua + vb)$  che porta a  $r = a(1-qu) + b(-qv)$

•  $r$  può essere  $0 > 0 = 0$ . Ma se fosse  $> 0$ , dovrebbe essere anche  $< \delta-1$  per def resto e  $\delta = \min$ , il che è IMPOSSIBILE

quindi,  $r = 0 \Rightarrow$  abbiamo dimostrato che  $\delta | a$  (e  $\delta | b$ )

$\delta$  divide i numeri di  $E$   $\iff$  formato da  $\alpha a + \beta b$

ora: visto che  $\delta | a$  e  $\delta | b$ ,  $\delta | a+b$  e  $\delta | \alpha a + \beta b$ . Questo implica  $\delta\mathbb{Z} \supset E$

e, visto che  $\delta \in E$  allora i suoi multipli  $\in E$ . Questo implica  $\delta\mathbb{Z} \subset E$

quindi,  $\delta\mathbb{Z} \subset E$  e  $\delta\mathbb{Z} \supset E \iff \delta\mathbb{Z} = E$

## MASSIMO COMUN DIVISORE

data  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$  con  $(a, b) \neq (0, 0)$

def  $d \in \mathbb{N}$  è MCD di  $a$  e  $b$  se:

$$\textcircled{1} \quad d | a \text{ e } d | b$$

\textcircled{2} se  $d' \in \mathbb{N}$  t.c.  $d'|a$  e  $d'|b$ , allora  $d'|d$  ogni divisore di  $a$  e  $b$   
divide anche  $d$

lemma:

se  $d$  soddisfa \textcircled{1} e \textcircled{2}, allora è unico.

dim.

Supponiamo che  $d_1, d_2$  soddisfano \textcircled{1} e \textcircled{2}. Mostriamo che  $d_1 = d_2$ .

$d_2 = k \cdot d_1 \text{ e } d_1 = l \cdot d_2$  quindi  $d_1$  e  $d_2$  devono essere uguali o opposti

$$\text{Si ha } d_2 | d_1 \text{ e } d_1 | d_2 \Rightarrow \{d_1, -d_1\} = \{d_2, -d_2\} \Rightarrow d_1 = d_2$$

• Si scrive  $d = \text{MCD}(a, b)$

def COPRIMI  $\rightarrow$  Se  $\text{MCD}(a, b) = 1$ , si dice che  $a$  e  $b$  sono primi tra loro o coprimi

lemma

$$d = \text{MCD}(a, b) \quad a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \quad d > 0, a, b \neq 0$$

$$\left( \begin{array}{l} \cdot \text{ se } a=0, b \neq 0 \text{ allora } d = |b| > 0 \\ \cdot \text{ se } a \neq 0, b=0 \text{ allora } d = |a| > 0 \end{array} \right)$$

dim.

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \quad \begin{array}{l} \textcircled{1} \quad d \mid a \rightarrow d | a \\ d \mid b \rightarrow d | b \end{array} \quad \begin{array}{l} \text{condizione } \textcircled{1} \\ \text{verificata} \end{array}$$

$$\textcircled{2} \quad (\text{mostro } d' | d \Leftrightarrow d\mathbb{Z} \subset d'\mathbb{Z})$$

Ogni divisore di  
 $a$  e  $b$  divide il MCD

per la cond. \textcircled{2}: sia  $d' \in \mathbb{N}$  t.c.  $d' | a \text{ e } d' | b$

$$d' | a \Leftrightarrow a\mathbb{Z} \subset d'\mathbb{Z} \quad \cdot \quad d' | b \Leftrightarrow b\mathbb{Z} \subset d'\mathbb{Z}$$

$$\text{quindi } \underbrace{a\mathbb{Z} + b\mathbb{Z}}_{= d\mathbb{Z}} \subset \overbrace{d'\mathbb{Z} + d'\mathbb{Z}}^{= 2d'\mathbb{Z}} = d'\mathbb{Z}$$

$$d\mathbb{Z} \subset d'\mathbb{Z} \Leftrightarrow d' | d \quad \text{cond. } \textcircled{2} \text{ verificata}$$

## ALGORITMO DI EUCLIDE x MCD

dati:  $a, b > 0$   $\delta = \text{MCD}(a, b)$

comincia con la divisione euclidea  $a, b$  ( $\circ$   $b, a - \text{è uguale}$ )

$$a = q_0 b + r_0 \quad (0 \leq r_0 < b) - x \text{ def. resto}$$

$$b = q_1 r_0 + r_1 \quad (0 \leq r_1 < r_0)$$

$$r_0 = q_2 r_1 + r_2 \quad (0 \leq r_2 < r_1)$$

$\therefore r_0, r_1, r_2 \dots$  decrescono - arriveranno  $\geq 0$

$$r_{n-2} = q_n r_{n-1} + r_n \quad (0 \leq r_n < r_{n-1})$$

$$r_{n-1} = q_n r_n + 0$$

$\delta !!$  (MCD)

### esercizio d'esempio

$$a = 3522, b = 321$$

$$3522 = 10 \cdot 321 + 312$$

$$321 = 1 \cdot 312 + 9$$

$$312 = 34 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

$$3522 = 10 \cdot 321 + 312$$

$$321 = 1 \cdot 312 + 9$$

$$312 = 34 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

$$3 = \text{MCD}(3522, 321)$$

ma, da qui, sappiamo che vale  $\delta \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

$$\Rightarrow \exists u, v \in \mathbb{Z} \text{ t.c. } 3 = 3522u + 321v$$

Come calcolare  $u$  e  $v$ ? IDENTITÀ DI BÉZOUT

Solviamo tra le  $\longrightarrow 3 = 9 - 1 \cdot 6$

iterazioni di euclide

e prendiamo

il resto

$$6 = 312 - 34 \cdot 9$$

$$3 = 9 - 1(312 - 34 \cdot 9) = 9 - 312 + 9 \cdot 34$$

$$3 = -312 + 35 \cdot 9$$

$$9 = 321 - 1 \cdot 312$$

$$3 = -312 + 35 \cdot (321 - 312) = 35 \cdot 321 - 312 \cdot 35$$

$$3 = 35 \cdot 321 - 312 \cdot 35$$

$$312 = 3522 - 10 \cdot 321$$

$$3 = 35 \cdot 321 - (3522 - 10 \cdot 321) \cdot 36 = 35 \cdot 321 - 3522 \cdot 36 + 321 \cdot 36 \cdot 10 \\ = 321(35 + 360) - 3522 \cdot 36$$

$$3 = 321 \cdot 395 - 36 \cdot 3522$$

abbiamo trovato  $v$  e  $u$  !! (bravi tutti)

Lemma di Gauss se  $a, b \in \mathbb{Z}^*$  e  $c \in \mathbb{Z}$  e se  $\text{MCD}(a, b) = 1$  allora  $a|bc \Rightarrow a|c$

dim.

$$\text{MCD}(a, b) = 1 \iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$$

Sono primi tra loro ( $\text{MCD}=1$ )

$$\text{quindi } \exists u, v \in \mathbb{Z} \text{ t.c. } au + bv = 1$$

$$au + bv = 1$$

$$\text{moltiplico tutto per } c \quad acu + bcv = c$$

$a|bc$  per ipotesi, quindi  $bc = ka$

$$acu + bcv = c \iff a(\underbrace{uc + bv}_{\exists 1 \text{ t.c. } c=1}) = c \quad \text{quindi } a|c \quad \blacksquare$$

Lemma  $p \in \mathbb{N}, p > 1$ , allora  $p$  irriducibile  $\Rightarrow p$  primo

dimostrazione + claim se  $p$  è irriducibile e  $p \nmid a$ , allora  $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$

infatti, altrimenti  $\exists \delta > 1$  t.c.  $\delta | a$ ,  $\delta | p$

ma visto che  $p$  irr.,  $\delta = p \Rightarrow p | a$  CONTRADDIZIONE

Supponiamo  $p | ab$  con  $p$  irriducibile. (Devo dim. che  $p | a$  o  $p | b$ )

Se  $p \nmid a$ , ho finito  $\rightarrow$  suppongo  $p \nmid b$ .

Ma allora  $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$ . Moltiplico tutto per  $b$   $\rightarrow \underbrace{ab\mathbb{Z}}_{\text{div per } p} + \underbrace{pb\mathbb{Z}}_{\text{div per } p} = b\mathbb{Z}$  quindi  $b\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p | b$  (perché  $\subset$  è una rel. di  $\subset$ )

fun fact del collega di Pellorin.

James P Jones, Daishachiro Sato, Hideo Wada, Douglas Wiens

$f(a, b, c, \dots, z)$  sostituendo le lettere (variabili) con elementi di  $\mathbb{N}$  ottengo elementi di  $\mathbb{Z}$

$$\mathbb{N}^{26} \xrightarrow{f} \mathbb{Z}$$

$$f(\mathbb{N}^{26}) \subset \mathbb{Z} \quad \text{il teorema dice che } f(\mathbb{N}^{26}) \cap \mathbb{N}^* = \{x : x \text{ primo}\} = \{2, 3, 5, 7, \dots\} = \mathbb{P}$$

$$\text{per esempio } f^{-1}(\{13\}) = \emptyset$$

⑤ per ogni intero  $n$ ,  $2n^{17} + 2n^{15} + 3n^3 + 3n$  è divisibile per 5

• la classe mod 5 ( $\mathbb{Z}/5\mathbb{Z}$ ) ha le stesse operazioni di  $\mathbb{Z}$

$$\left[ 2n^{17} + 2n^{15} + 3n^3 + 3n \right]_5 \text{ deve essere } [0]$$

oper. in  $\mathbb{Z}/5\mathbb{Z}$

$$= [2] \cdot [n]^{17} + [2] \cdot [n]^{15} + [3] \cdot [n]^3 + [3] \cdot [n] = [0]$$

un intero  $n \pmod{5}$  ha resto da 1 a 4 (quindi mi basta verificare queste classi)

• se  $n \equiv_5 0 \iff [n] = [0]$  allora è chiaramente verificato

altr: così:

$\bar{n}$	$[n]^3$	$[n]^{15}$	$[n]^{17}$	$3[n]$	$3[n]^3$	$2[n]^{15}$	$2[n]^{17}$	$3[n] + 3$
$n \equiv 1$	$[1]$	$[1]$	$[1]$	$[3]$	$[3]$	$[2]$	$[2]$	$[0]$
	$[1] \cdot [1] \cdot [1] = [1]$	$[1] \cdot [1] \cdot [1] = [1]$	$[1] \cdot [1] \cdot [1] = [1]$	$[3] \cdot [3] \cdot [3] = [3]$	$[3] \cdot [3] \cdot [3] = [3]$	$[2] \cdot [2] \cdot [2] = [2]$	$[2] \cdot [2] \cdot [2] = [2]$	$[3] + 3 = [0]$
$n \equiv 2$	$[2]$	$[3]$	$[3]$	$[1]$	$[1]$	$[4]$	$[1]$	$[0]$
	$[2] \cdot [3] \cdot [3] = [2]$	$[3] \cdot [2] \cdot [2] = [3]$	$[3] \cdot [3] \cdot [3] = [2]$	$[1] \cdot [1] \cdot [1] = [1]$	$[1] \cdot [1] \cdot [1] = [1]$	$[4] \cdot [4] \cdot [4] = [4]$	$[1] \cdot [1] \cdot [1] = [1]$	$[0] + 3 = [3]$
$n \equiv 3$	$[3]$	$[2]$	$[2]$	$[3]$	$[4]$	$[1]$	$[4]$	$[0]$
	$[3] \cdot [2] \cdot [2] = [3]$	$[2] \cdot [3] \cdot [3] = [2]$	$[2] \cdot [2] \cdot [2] = [2]$	$[3] \cdot [3] \cdot [3] = [3]$	$[4] \cdot [4] \cdot [4] = [4]$	$[1] \cdot [1] \cdot [1] = [1]$	$[4] \cdot [4] \cdot [4] = [4]$	$[0] + 3 = [3]$
$n \equiv 4$	$[4]$	$[4]$	$[4]$	$[4]$	$[2]$	$[2]$	$[3]$	$[0]$
	$[4] \cdot [4] \cdot [4] = [2]$	$[4] \cdot [4] \cdot [4] = [2]$	$[4] \cdot [4] \cdot [4] = [2]$	$[2] \cdot [2] \cdot [2] = [2]$	$[2] \cdot [2] \cdot [2] = [2]$	$[3] \cdot [3] \cdot [3] = [3]$	$[2] \cdot [2] \cdot [2] = [2]$	$[0] + 3 = [3]$

divisibile per  
5 in tutti i casi

Studiamo le potenze 2 mod 5

$$[2]^0 = [1] \quad [2]^1 = [2] \quad [2]^2 = [4] \quad [2]^3 = [3] \quad [2]^4 = [1]$$

è ciclico:

$$[2]^5 = [2] \cdot [2]^4 = [2] \cdot [1] = [2] \quad \text{il ciclo è lungo 4, quindi } [2]^m = [2]^{\frac{m}{4} \cdot 4 + r} = [2]^{\frac{m}{4} \cdot 4} \cdot [2]^r = [2]^r$$

$$[2]^6 = [2] \cdot [2]^5 = [4]$$

quando per calcolare  $[2]^n$  basta calcolare  $[2]^r$  resto div. per 4

potenze 3 mod 5:

$$[3]^0 = [1] \quad [3]^1 = [3] \quad [3]^2 = [4] \quad [3]^3 = [2] \quad [3]^4 = [1]$$

potenze 4 mod 5

$$[4]^0 = [1] \quad [4]^1 = [4] \quad [4]^2 = [1] \quad [4]^3 = [4] \quad [4]^4 = [1]$$

④ Calcolare  $(\mathbb{Z}/N\mathbb{Z})^\times$  con  $N \in \mathbb{N}$

$$\cdot A = \mathbb{Z}/N\mathbb{Z} = \mathbb{Z}_{\equiv_N}$$

$$\cdot [a] + [b] = [a+b] \quad e \quad [a] \cdot [b] = [ab] \quad (\text{premesse})$$

• con l'elemento  $[0]$  ( $= N\mathbb{Z}$ ) per l'elemento neutro per + e con l'elemento  $[1]$  ( $= N\mathbb{Z}+1$ ) per il neutro di  $\cdot$ , si ottiene che  $A$  è un anello unitario commutativo.

Si cerca

$$A^\times = \{[n] \text{ t.c. } \exists [m] \text{ con } [m] \cdot [n] = [1]\} \quad ("insieme delle unità")$$

③ Si  $\exists [a] \in (\mathbb{Z}/N\mathbb{Z})^\times$ : esiste  $b \in \mathbb{Z}/N\mathbb{Z}$  t.c.  $[a] \cdot [b] = [1]$

$$[ab] = [1] \iff N \mid ab - 1 \quad \text{è invertibile} \iff \text{esiste un qualsiasi rapp. quando faccio } ab-1, \text{ è div per } N$$

$$\iff \exists k \in \mathbb{Z} \text{ t.c. } kN = ab - 1$$

porta 1 e kn dall'altra parte

$$\iff ab - kN = 1 \quad \text{è un'identità di Bézout per } a, N$$

$\iff a \text{ e } N$  sono primi fra loro!

$$\text{quindi } (\mathbb{Z}/N\mathbb{Z})^\times = \{[a] : a \in \mathbb{Z} \text{ e } \text{MCD}(a, N) = 1\}$$

Esiste quindi un'applicazione biiettiva  $\{r \in \{0, \dots, N-1\} \text{ t.c. } \text{MCD}(r, N) = 1\} \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$

$$r \mapsto [r]$$

$N = 24 = 2^3 \cdot 3$  verificare che  $(\mathbb{Z}/24\mathbb{Z})^\times = \{r : z \mid r, 3 \nmid r\}$  tenendo i coprimi

$$\text{esempio } (\mathbb{Z}/24\mathbb{Z})^\times = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{15}, \bar{16}, \bar{17}, \bar{18}, \bar{19}, \bar{20}, \bar{21}, \bar{22}, \bar{23}\}$$

che cosa si osserva quando  $N$  è primo?

$$\cdot N = p \text{ primo} : \text{ Si } \exists r \in \{\bar{1}, \dots, \bar{p-1}\}$$

$\text{MCD}(p, r) = 1$ . Altrimenti, qualora si avesse  $\delta = \text{MCD}(p, r) > 1$  avrei:  $\delta \mid p$ ,  $\delta \mid r \Rightarrow \delta = p$

e si avrebbe  $p \mid r$ . Ma  $r < p$  (perché è resto)  $\rightarrow$  CONTRADDIZIONE. Quindi  $r$  coprimo  $p$

Si ottiene  $(\mathbb{Z}/p\mathbb{Z})^\times = \{[r] : 1 \leq r \leq p-1\} \quad \forall r \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ ,  $r$  è invertibile

def CAMP

$A$  anello commutativo unitario t.c.  $\forall a \in A \setminus \{0\}$  invertibile  
si dice campo

in particolare,  $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$  è un campo

## PICCOLO TEOREMA DI FERMAT

es. 5 dato  $p$  primo e  $n \in \mathbb{Z}$ ,  $n^p \equiv_p n$

Ricordiamo:

$$\bullet \binom{n}{m} = \frac{n!}{m!(n-m)!} = \#\{U \subset \{1, \dots, n\} : \#U = m\} \quad 0 \leq m \leq n$$

in  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  campo, ovvero  $\mathbb{F}_p^\times = \{[1], [2], \dots, [p-1]\}$   
non vero in  $\mathbb{Z}$

$$\bullet \binom{n}{0} = \binom{n}{n} = 1$$

$$\bullet \binom{n}{m} = \binom{n}{n-m}$$

$$\bullet ([a] + [b])^p = [a]^p + [b]^p \text{ con } [a], [b] \in \mathbb{F}_p$$

Sceglieremo rapp.  $a, b$  per le classi  $[a], [b]$

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-2} a^2 b^{p-2} + \binom{p}{p-1} a b^{p-1} + b^p \quad (\text{NEWTON})$$

$\bullet 0 < i < p$  (non  $\leq \geq$  perché so che la rid. mod.  $p$  di  $0$  è  $0$ )

SCRIVIAMO  $\binom{p}{i} = \frac{p!}{i!(p-i)!} \in \mathbb{N}$ , quindi si ha che  $i!(p-i)! \mid p$  (appunto perché la frazione è  $\mathbb{N}$ )

$\bullet$  SUPPONIAMO  $1 \leq i \leq p-1$  e inoltre  $i! = i(i-1) \dots 3 \cdot 2 \cdot 1$

quindi, siccome  $p > i$ , si ha  $p \nmid i$  (perché i si scompongono in fattori tutti  $< p$  (quindi nessuno di questi è  $p$ ) e  $p$  non può essere il prodotto tra alcuni di questi perché è primo)

Similmente,  $p > p-i$  e quindi  $p \nmid (p-i)!$

$$\text{quindi, ho } p! = \underbrace{k}_{\geq} \cdot \underbrace{i!(p-i)!}_{b} \quad (\text{da qui } *) \quad \exists k \in \mathbb{N}^*$$

(visto che  $p \nmid i!$  e  $p \nmid (p-i)!$ ) ho anche  $p \nmid b$ .

ma  $p \mid ab = p!$  visto che  $p$  primo e  $p \nmid b$ , allora  $p \mid a$  per il lemma di Gauss.  
per def. fattoriale

$$\text{ma } a = k = \binom{p}{i} \quad \text{perché } p! = \frac{p!}{i!(p-i)!} \cdot i!(p-i)!$$

$( \in [0] \text{ mod } p )$

quindi, tutti i coeff. "in mezzo" nello sv. di Newton (nello forma  $\binom{p}{i} \cdot \text{qualcosa}$ ) si riducono a 0 e rimangono solo  $a^p$  e  $b^p$ .

$\bullet$  ho dim. che se  $1 \leq i \leq p-1$  e  $p$  primo, si ha:  $\binom{p}{i} = \binom{p}{p-i} \equiv_p 0$

$$\text{e, riducendo, ottengo } ([a] + [b])^p = [a]^p + \binom{p}{1} [a]^{p-1} [b] + \dots + [b]^p \equiv_p [a]^p + [b]^p$$

TORNIAMO ALLA DIM. PRINCIPALE (PTF)

$$[0]^p = [0] \quad [2]^p = ([1] + [1])^p = [1]^p + [1]^p = [1] + [1] = [2]$$

$$[1]^p = [1] \quad [\bar{2}]^p = ([\bar{2}] + [1])^p = [\bar{2}]^p + [1]^p = [\bar{2}] + [1] = [\bar{2}]$$

quindi, per induzione (ipotesi: fino a  $n-1$ ,  $[n-1]^p = [n-1]$ )

$$[n]^p = ([n-1] + [1])^p = [n-1]^p + [1]^p = [n-1] + [1] = [n]$$

which is very cool

if you ask me!!

quindi,  $\forall n \in \mathbb{Z}, n^p \equiv_p n$  (con  $p$  primo)



$$(x+y)^n = x^n + y^n$$



$$(x+y)^n \neq x^n + y^n$$



for a prime number  $n$ , if  $x$  and  $y$  are members of a commutative ring of characteristic  $n$  then  
 $(x+y)^n = x^n + y^n$

## PRECISAZIONE

Se  $[n] \neq [0]$ , ovvero se  $[n] \in \mathbb{F}_p$

allora  $[n]$  invertibile di inverso  $[n']$ .

$$\text{Per il PTF, so già che } [n] = [n]^p \quad \text{e} \quad [n'] [n^p] = [n'] [n] \stackrel{\substack{= \\ \text{def. inverso}}}{=} 1$$

$p$  primo  $\Rightarrow p \geq 2$  si può decomporre in  $p-1 \geq 1 + p$

$$[n'] [n]^p = [n'] [n] = [1]$$

$$\begin{array}{c} \text{Il } [n]^p \\ \text{è } \\ [n'] \cdot \underbrace{[n] [n]^{p-1}}_{\substack{\text{sono} \\ \text{inversi} \\ \text{quindi} = [1]}} = [n'] [n] = [1] \end{array}$$

$$\text{quindi } [1] [n]^{p-1} = [1] \quad \text{se } [n] \neq [0]$$

(il PTF ha dei difetti.)

- se  $[\alpha] \in \mathbb{F}_p^\times$ , calcolare  $[\alpha]^{-1}$  usando il PTF

$$\text{So che } [\alpha]^{p-1} = [1] \quad (\text{PTF}).$$

$$\begin{array}{c} \text{Scrivendo } [\alpha]^{p-1} = [\alpha]^{p-2} \cdot [\alpha] \\ \text{(quindi } [1] = \underbrace{[\alpha]^{p-2} \cdot [\alpha]}_{\text{inversi}}) \end{array}$$

$$\text{Dunque } [\alpha]^{-1} = [\alpha]^{p-2}$$

$$\text{es. } p = 689 \quad (\text{primo})$$

Voglio calcolare  $[2]^{-1}$ . "Basta" calcolare  $[2]^{p-2}$ , ovvero  $[2]^{689}$ .

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 333, 666, 641, 591, 491, 291, 582, 473, 255, 510, 329, 658, 625, 5  
 59, 427, 163, 326, 652, 613, 535, 379, 67, 134, 268, 536, 381, 71, 142, 284, 568, 445, 199, 398, 105, 2  
 10, 420, 149, 298, 596, 501, 311, 622, 553, 415, 139, 278, 556, 421, 151, 302, 604, 517, 343, 686, 681,  
 671, 651, 611, 531, 371, 51, 102, 204, 408, 125, 250, 500, 309, 618, 545, 399, 107, 214, 428, 165, 330  
 , 660, 629, 567, 442, 195, 390, 89, 178, 356, 21, 42, 84, 168, 336, 672, 653, 615, 539, 387, 83, 166, 3  
 32, 664, 637, 583, 475, 259, 518, 345, 690, 689, 687, 683, 675, 659, 627, 563, 435, 179, 358, 25, 50, 1  
 00, 200, 400, 109, 218, 436, 181, 362, 33, 66, 132, 264, 528, 365, 39, 78, 156, 312, 624, 557, 423, 155  
 , 310, 620, 549, 407, 123, 246, 492, 293, 586, 481, 271, 542, 393, 95, 190, 380, 69, 138, 276, 552, 413  
 , 135, 270, 540, 389, 87, 174, 348, 5, 10, 20, 40, 80, 160, 320, 640, 589, 487, 283, 566, 441, 191, 382  
 , 73, 146, 292, 584, 477, 263, 526, 361, 31, 62, 124, 248, 496, 301, 602, 513, 335, 670, 649, 607, 523,  
 355, 19, 38, 76, 152, 304, 608, 525, 359, 27, 54, 108, 216, 432, 173, 346, 1, 2, 4, 8, 16, 32, 64, 128  
 , 256, 512, 333, 666, 641, 591, 491, 291, 582, 473, 255, 510, 329, 658, 625, 559, 427, 163, 326, 652, 6  
 13, 535, 379, 67, 134, 268, 536, 381, 71, 142, 284, 568, 445, 199, 398, 105, 210, 420, 149, 298, 596, 5  
 01, 311, 622, 553, 415, 139, 278, 556, 421, 151, 302, 604, 517, 343, 686, 681, 671, 651, 611, 531, 371,  
 51, 102, 204, 408, 125, 250, 500, 309, 618, 545, 399, 107, 214, 428, 165, 330, 660, 629, 567, 443, 195  
 , 390, 89, 178, 356, 21, 42, 84, 168, 336, 672, 653, 615, 539, 387, 83, 166, 332, 664, 637, 583, 475, 2  
 59, 518, 345, 690, 689, 687, 683, 675, 659, 627, 563, 435, 179, 358, 25, 50, 100, 200, 400, 109, 218, 4  
 36, 181, 362, 33, 66, 132, 264, 528, 365, 39, 78, 156, 312, 624, 557, 423, 155, 310, 620, 549, 407, 123  
 , 246, 492, 293, 586, 481, 271, 542, 393, 95, 190, 380, 69, 138, 276, 552, 413, 135, 270, 540, 389, 87,  
 174, 348, 5, 10, 20, 40, 80, 160, 320, 640, 589, 487, 283, 566, 441, 191, 382, 73, 146, 292, 584, 477,  
 263, 526, 361, 31, 62, 124, 248, 496, 301, 602, 513, 335, 670, 649, 607, 523, 355, 19, 38, 76, 152, 30  
 4, 608, 525, 359, 27, 54, 108, 216, 432, 173, 346, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 333, 666, 641  
 , 591, 491, 291, 582, 473, 255, 510, 329, 658, 625, 559, 427, 163, 326, 652, 613, 535, 379, 67, 134, 26  
 8, 536, 381, 71, 142, 284, 568, 445, 199, 398, 105, 210, 420, 149, 298, 596, 501, 311, 622, 553, 415, 1  
 39, 278, 556, 421, 151, 302, 604, 517, 343, 686, 681, 671, 651, 611, 531, 371, 51, 102, 204, 408, 125,  
 250, 500, 309, 618, 545, 399, 107, 214, 428, 165, 330, 660, 629, 567, 443, 195, 390, 89, 178, 356, 21,  
 42, 84, 168, 336, 672, 653, 615, 539, 387, 83, 166, 332, 664, 637, 583, 475, 259, 518, 345, 690, 689, 6  
 87, 683, 675, 659, 627, 563, 435, 179, 358, 25, 50, 100, 200, 400, 109, 218, 436, 181, 362, 33, 66, 132  
 , 264, 528, 365, 39, 78, 156, 312, 624, 557, 423, 155, 310, 620, 549, 407, 123, 246, 492, 293, 586, 481  
 , 271, 542, 393, 95, 190, 380, 69, 138, 276, 552, 413, 135, 270, 540, 389, 87, 174, 348, 5, 10, 20, 40,  
 80, 160, 320, 640, 589, 487, 283, 566, 441, 191, 382, 73, 146, 292, 584, 477, 263, 526, 361, 31, 62, 1  
 08, 216, 432, 173, 346, 1, 689' (689)

ma notiamo che le classi

sono cicliche - possiamo trovare

l'inverso molto prima di 689

- è quello precedente all'1,

perciò sappiamo che  $[n]^{p-1} = [1]$   
(e cerchiamo  $[n]^{p-2}$ )

questo funziona bene con 2, ma, per esempio, non con 3

③ Nessun intero in  $4\mathbb{Z} + 3$

calcoliamo le classi resto modulo 4 dei quadrati

$\bar{n}$	$\bar{n}^2$	la somma dei quadrati mod 4 può essere soltanto
0	0	
1	1	
2	0	
3	1	

	+	$\bar{0} \quad \bar{1}$	in particolare, non è mai $\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0} \quad \bar{1}$	
$\bar{1}$	$\bar{1}$	$\bar{0} \quad \bar{1}$	

no (si può vedere con la riduzione mod 8 e una tabella 3d)

Variante: è vero che ogni intero  $> 0$  è somma di 3 quadrati? Si può dimostrare che ogni intero  $> 0$  è somma di 4 quadrati (Lagrange)

## FIBONACCI

$(F_n)$   $n \geq 0$  definito induttivamente:  $F_0 = 0$ ,  $F_1 = 1$ ,  $F_n = F_{n-1} + F_{n-2}$

proprietà

$$\text{MCD}(F_m, F_n) = F_{\text{MCD}(m, n)}$$

$$\text{in particolare, } \text{MCD}(F_m, F_{m+1}) = F_1 = 1$$

dim. x induzione con algoritmo di Euclideo

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1}$$

$$\text{MCD}(F_n, F_{n+1}) = \delta_n$$

$$\mathbb{Z} F_n + \mathbb{Z} F_{n+1} = \mathbb{Z} \delta_n \quad \text{devo dimostrare} = 1\mathbb{Z}$$

||

$$\left\{ \exists F_n + b F_{n+1} : a, b \in \mathbb{Z} \right\}$$

|| def. Fibonacci

$$\left\{ \exists F_n + b(F_n + F_{n-1}) : a, b \in \mathbb{Z} \right\}$$

ci serve



$$\mathbb{Z} F_{n-1} + \mathbb{Z} F_n$$

così → ipotesi induttiva:  $\mathbb{Z} F_{n-1} + \mathbb{Z} F_n = \mathbb{Z}$

(claim)

17/10

claim: = (serve che la funzione sia suriettiva)

$$\left\{ (\alpha+b) F_n + b F_{n-1} : \alpha, b \in \mathbb{Z} \right\} \subseteq \mathbb{Z} F_{n-1} + \mathbb{Z} F_n = \left\{ u F_{n-1} + v F_n : u, v \in \mathbb{Z} \right\}$$

mi serve dim applicazione biiettiva:

$$f: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$$

$$(\alpha, b) \mapsto (\alpha+b, b) \quad \text{sia } f(\mathbb{Z}^2) \text{ l'immagine} = \{ u F_n, v F_{n-1} : (u, v) \in f(\mathbb{Z}^2) \}$$

se lo dimostro, dimostro che

ogni volta che prendo  $\alpha, b$  posso trovare  $u$  e  $v$  t.c.  $u = \alpha+b$ ,  $v = b$  e viceversa

(basta che sia suriettiva)  
ma dimostriamo biiettiva

Mostriamo  $f$  suriettiva - questo basta per giustificare il claim

Possiamo mostrare che  $f$  biiettiva (+ forse)

Richiamo:  $A \xrightarrow{f} B$   $f$  biiettiva  $\iff \forall b \in B, f^{-1}(\{b\})$  singleton

prop del corso  $\Rightarrow f$  biiett.  $\iff \exists g: B \rightarrow A$  t.c.  $f \circ g = \text{Id}_B$  ( $\forall b \in B, f(g(b)) = b, \forall a \in A, g(f(a)) = a$ )

$$f(a, b) = (a+b, b) =: (u, v)$$

$$\begin{cases} a+b = u \\ b = v \end{cases}$$

unica soluzione (biiettività) (singleton  $f^{-1}$ )

inverso

$$\text{pongo } g: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2, \quad g(u, v) \mapsto (u-v, v)$$

$$\begin{aligned} (f \circ g)(u, v) &= f(g(u, v)) = f(u-v, v) = u-v+v, v = (u, v) \\ (g \circ f)(a, b) &= g(f(a, b)) = g(a+b, b) = (a+b-b, b) = (a, b) \end{aligned} \quad \left. \begin{array}{l} \text{x fibonacchi indice } \geq 0 \\ \text{sono identità:} \\ f \text{ e } g \text{ biiettive} \end{array} \right\}$$

$$\begin{aligned} \text{Abbiamo dimostrato } \forall n > 0 \quad F_{n+1} \mathbb{Z} + F_n \mathbb{Z} &= F_n \mathbb{Z} + F_{n-1} \mathbb{Z} = F_{n-1} \mathbb{Z} + F_{n-2} \mathbb{Z} = \dots = F_1 \mathbb{Z} + F_0 \mathbb{Z} = \\ &= F_1 \mathbb{Z} + \{0\} = \mathbb{Z} \end{aligned}$$

$$\text{ho dim. che } \forall n > 0 \quad F_n \mathbb{Z} + F_{n-1} \mathbb{Z} = \mathbb{Z} \iff \text{MCD}(F_n, F_{n-1}) = 1 \quad \blacksquare$$

Esercizio 5 Dimostrare che  $2^n \not\equiv 1 \pmod{n}$   $\forall n > 1$  x CASA

$$2^n \not\equiv_n 1 \quad \forall n > 1$$

$$n^p \equiv_p n \quad \text{e } n^{p-2} \text{ inverso } n^p$$

$$n^{p-1} \equiv_p 1$$

2 casi:

$$\textcircled{1} \quad n \text{ primo} \rightarrow \text{Fermat: } [2^{n-1}]_n = [1]_n$$

$$[2^n] = [2^{n-1}] \cdot [2] = [1] \cdot [2] = [2]$$

$$\textcircled{2} \quad n \text{ non primo} \rightarrow n = a, b \text{ con } 1 < a < n, \quad 1 < b < n$$

$$\text{sicuramente } n = p \cdot k \text{ con } p \text{ primo e } 2^n = 2^{pk} = (2^p)^k$$

## TEOREMA FONDAMENTALE DELL'ARITMETICA

$$\forall \alpha \in \mathbb{Z}^*$$

① l'insieme  $I = \{ p \text{ primo} : p | \alpha \}$  è finito (il numero di primi che dividono  $\alpha$  è finito)

②  $\alpha = (\pm 1) \cdot \prod_{\substack{p \\ \text{primo}}} p^{v_p(\alpha)}$  dove  $v_p(\alpha) \in \mathbb{N}$  unicamente determinato.

(ogni numero  $\neq 0$  è il prodotto di una certa combinazione di numeri primi elevati a un certo esponente  
- quelli che non vogliono saranno elevati a 0 -)

OSS

si sa che  $P = \{ p \in \mathbb{N}, p \text{ primo} \}$  è infinito.

Siccome

$$\forall \alpha \in \mathbb{Z}, I_\alpha \text{ è finito, } \prod_{\substack{p \\ \text{primo}}} p^{v_p(\alpha)} = \prod_{p \in I_\alpha} p^{v_p(\alpha)} \cdot \prod_{p \notin I_\alpha} p^{v_p(\alpha)}$$

*sarà 0 ("non ci servono")*

posso dividere i primi in divisori di  $\alpha$  e non-divisori di  $\alpha$  e suddividere la produttoria

esempio:

$$\begin{aligned} \alpha = 7! &= 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \\ &= 7 \cdot 5 \cdot 3^2 \cdot 2^4 \end{aligned}$$

$$\text{quindi } v_p(\alpha) = \begin{cases} 1 & p=7 \\ 1 & p=5 \\ 2 & p=3 \\ 4 & p=2 \\ 0 & p>7 \end{cases}$$

OSS: dato  $\alpha = \prod_p p^{v_p(\alpha)}$  e  $b = \prod_p p^{v_p(b)}$

$$\begin{aligned} \alpha = 12 &= 2^2 \cdot 3 \\ b = 15 &= 5 \cdot 3 \end{aligned} \implies \begin{aligned} v_2(\alpha) &= 2 & v_2(b) &= 0 \\ v_3(\alpha) &= 1 & v_3(b) &= 1 \end{aligned}$$

$$\bullet \alpha \cdot b = \prod_p p^{v_p(\alpha)} \prod_p p^{v_p(b)} = \prod_p p^{v_p(\alpha) + v_p(b)}$$

$$v_5(\alpha \cdot b) = 0 \quad v_5(b) = 1$$

$$\bullet p^{v_p(\alpha)} p^{v_p(b)} = p^{v_p(\alpha) + v_p(b)}$$

$$v_p(\alpha \cdot b) = v_p(12 \cdot 15) = v_p(\alpha) + v_p(b)$$

(enunciato)  $\forall \alpha > 0, \exists$  un numero finito di primi distinti  $p_1, \dots, p_r$  t.c.  $\alpha = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$   
e questa fattorizzazione è unicamente determinata.

$$v_2(\alpha \cdot b) = 2 \quad v_3(\alpha \cdot b) = 2 \quad v_5(\alpha \cdot b) = 1 \quad v_p(\alpha \cdot b) = 0 \quad p \geq 7$$

dimostrazione teorema  $\Delta = (\pm 1) \prod_p p^{v_p(\Delta)}$

• posso supporre  $\Delta > 0$  senza perdita di generalità

① Supponiamo per assurdo  $\mathbb{P}_{\Delta}$  infinito - vuol dire che esiste una collezione infinita di primi t.c.  $p \mid \Delta$

ma  $p \mid \Delta \Rightarrow p \leq \Delta$  e impossibile infiniti interi  $\leq \Delta$  contr.

② Procediamo per induzione:

$$\cdot \Delta = 1 \quad V_p(1) = \emptyset \quad \forall p \quad 1 = \prod_p p^0 = 1 \cdot 1 \cdot 1 \cdots 1 = 1$$

• Supponiamo  $\Delta > 1$ .

dove così ①  $\Delta$  primo  $\rightarrow$  allora  $\Delta = \prod_p p^{v_p(\Delta)} \quad V_p(\Delta) = \begin{cases} \emptyset & p \neq \Delta \\ 1 & p = \Delta \end{cases}$

②  $\Delta$  non primo,  $\Delta$  non è irriducibile

si può scrivere in fattori diversi da 1 e  $\Delta$

$$\Rightarrow \Delta = U \cdot V \quad \text{con} \quad 1 < U < \Delta \quad \& \quad 1 < V < \Delta$$

per ipotesi induttiva, visto che  $U, V < \Delta$  posso usare la formula del prodotto

posso scrivere  $U = \prod_p p^{v_p(U)}, \quad V = \prod_p p^{v_p(V)}$

$$\Delta = UV = \prod_p p^{v_p(U) + v_p(V)} \blacksquare$$

altre proprietà (in teoria esercizi ma mi sembrano più proprietà)

①  $a|b \iff \forall p, V_p(a) \leq V_p(b)$

dim • supponiamo  $V_p(a) < V_p(b)$

$$\iff V_p(b) - V_p(a) \geq 0 \in \mathbb{N}$$

poniamo  $k = \prod_p p^{V_p(b) - V_p(a)}$  è quindi un intero

osserviamo che  $V_p(b) - V_p(a) = 0$  per  $p$  abbastanza grande

$$k \cdot a = \prod_p p^{V_p(b) - V_p(a)} \prod_p p^{V_p(a)} = \prod_p p^{V_p(b) - V_p(a) + V_p(a)} = \prod_p p^{V_p(b)} = b$$

quindi  $b = k \cdot a \quad \exists k \in \mathbb{N}$  e quindi  $a|b$

• supponiamo  $a|b$

$$\implies b = k \cdot a \quad \exists k \in \mathbb{N}^*$$

per il teorema fondamentale:

$$\prod_p p^{V_p(b)} = \prod_p p^{V_p(k \cdot a)} = \prod_p p^{V_p(a)}$$

osservo che  
 $\geq 0$  perché  
k intero

quindi  $\prod_p p^{V_p(b)} = \prod_p p^{V_p(k \cdot a) + V_p(a)}$

per unicità della fattorizzazione:  $V_p(b) = \underbrace{V_p(k \cdot a) + V_p(a)}_{\geq 0} \iff V_p(a) = V_p(b) - V_p(k \cdot a)$

$$\forall p, V_p(b) \geq V_p(a) \blacksquare$$

②  $a, b \in \mathbb{N}^*, \quad \text{MCD}(a, b) = \prod_p p^{\min(V_p(a), V_p(b))}$

dim.  $\delta = \text{MCD}(a, b)$  è l'unico intero di  $\mathbb{N}^*$  t.c.

①  $\delta|a \quad e \quad \delta|b$

②  $\forall d' \in \mathbb{N} \quad d'|a \quad e \quad d'|b \implies d'|\delta$

considerando che  $\delta|b \iff \forall p, V_p(\delta) \leq V_p(b)$

③  $\forall p, V_p(\delta) \leq V_p(a) \quad e \quad V_p(\delta) \leq V_p(b)$

② Se  $\exists d' \text{ t.c. } \forall p \quad v_p(d') \leq v_p(a) \leftarrow v_p(d') \leq v_p(b)$

Allora  $\forall p, \quad v_p(d') \leq v_p(\delta)$ :

③  $\iff v_p(\delta) \leq \min(v_p(a), v_p(b))$

④  $\iff$  se  $d'$  è tale che  $v_p(d') \leq \min(v_p(a), v_p(b))$

Allora  $v_p(d') \leq v_p(\delta)$

$\forall p, \quad v_p(\delta)$  è il più grande degli interi  $n$  t.c.  $n \leq \min(v_p(a), v_p(b))$

quindi  $v_p(\delta) = \min(v_p(a), v_p(b))$  (se è il massimo tra  $i \leq, i \neq$ )

esercizio

$$a, b, c \in \mathbb{N}^* \quad \text{MCD}(a, b, c) \mid \text{MCD}(a, c) \cdot \text{MCD}(b, c)$$

pongo  $x, y, z = v_p(a), v_p(b), v_p(c)$  (per comodità)

$$\text{MCD}(a, b, c) \mid \text{MCD}(a, c) \cdot \text{MCD}(b, c) \iff \exists n \text{ t.c. } \text{MCD}(a, c) \cdot \text{MCD}(b, c) = n \cdot \text{MCD}(a, b, c)$$

Come dimostrare la lezione:

$$\bullet \text{MCD}(a, b, c) = \prod_p p^{\min(x, y, z)} \quad \bullet \text{MCD}(a, c) = \prod_p p^{\min(x, z)} \quad \bullet \text{MCD}(b, c) = \prod_p p^{\min(y, z)}$$

$$\bullet \text{MCD}(a, c) \cdot \text{MCD}(b, c) = \prod_p p^{\min(x, z) + \min(y, z)}$$

$$\text{quindi } \text{MCD}(a, b, c) \mid \text{MCD}(a, c) \cdot \text{MCD}(b, c) \iff \prod_p p^{\min(x, z) + \min(y, z)} = \prod_p p^{\min(x, y, z)} \cdot \prod_p p^k$$

$$\iff \min(x, z) + \min(y, z) = \min(x, y, z) + k$$

3 casi:

$$\textcircled{1} \min = z$$

$$\textcircled{2} \min = x$$

$$\textcircled{3} \min = y$$

$$\begin{aligned} \text{qui } \min(x, z) &= z \text{ e } \min(y, z) = z \\ \text{e } \min(x, y, z) &= z \end{aligned}$$

$$\begin{aligned} \text{quindi } z+z &= z+k \\ \text{ovvero } k &= z \end{aligned}$$

$$\begin{aligned} \text{qui } \min(x, z) &= x \\ \text{e } \min(y, z) &= z \circ y \end{aligned}$$

$$\begin{aligned} z &\swarrow \\ x+z &= x+k \\ \text{ovvero } k &= z \end{aligned}$$

$$\begin{aligned} \text{qui } \min(y, z) &= y \\ \text{e } \min(x, z) &= x \circ z \end{aligned}$$

$$\begin{aligned} x &\swarrow \\ x+y &= y+k \\ \text{ovvero } k &= x \end{aligned} \quad \begin{aligned} z &\swarrow \\ z+y &= y+k \\ \text{ovvero } k &= z \end{aligned}$$

$$\text{quindi } n = \prod_p p^k \text{ con } k \text{ definito sopra}$$

## DIVISORI DI ZERO

in  $\mathbb{Z}_{/6\mathbb{Z}}$ ,  $\{[0], [1], [2], [3], [4], [5]\}$ dato  $A$  snello

$[2] \cdot [3] = [0]$  con  $[2], [3] \neq [0]$

ma in  $\mathbb{Z}$  non succededef  $\alpha \in A$  è divisore di zerose  $\exists b \in A \setminus \{0\}$  t.c.  $\alpha b = 0_A$ in  $A$  qualiasi (tranne se  $1_A = 0_A$ ,  $A = \{0\}$ )  $0_A$  è divisore di  $0$ 

- se  $A = K$  CAMPO (es.  $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ )

cioè  $\forall \alpha \in K \setminus \{0\}$ ,  $\alpha$  invertibile  $K^\times = K \setminus \{0\}$ L'unico divisore di zero in  $K$  è  $0_K$ dim • Supponiamo  $\alpha$  divisore di zero:da qui in poi usiamo  $0$  per  $0_K$ 

$\exists b \neq 0$  t.c.  $\alpha b = 0$

però  $b$  è invertibile  $\rightarrow \exists b^{-1} \in K^\times$  t.c.  $b \cdot b^{-1} = 1_K$ quindi posso moltiplicare termine  $\alpha$  termine per  $b^{-1}$ 

$$\underbrace{\alpha b b^{-1}}_1 = \underbrace{0}_0 b^{-1}$$

$$\alpha = 0$$

in  $\mathbb{Z}$ in  $\mathbb{Z}$ , se  $\alpha$  è divisore di  $0$ , allora  $\alpha = 0$  (anche se  $\mathbb{Z}$  non è un campo)dim • sia  $\alpha$  divisore di zero  $\iff \exists b \in \mathbb{Z}^* \text{ t.c. } \alpha b = 0 \quad (-\alpha)(-\alpha) = \alpha b = 0$ Senza perdita di generalità, supponiamo  $\alpha \geq 0$ 

$$\exists b \text{ t.c. } \alpha b = 0 \iff 0 = \alpha b = \underbrace{b + b + b + \dots + b}_{\alpha \text{ volte}} \geq b > 0$$

questo è impossibile se  $\alpha > 0$ .quindi,  $\alpha = 0$  ■def dominiodato  $A$  snello,  $A \neq \{0\}$ , si dice che  $A$  è un dominio se l'unico divisore di zero in  $A$  è  $0_A$ .

- Ogni campo è un dominio, e  $\mathbb{Z}$  è un dominio

es) mostrare che  $\mathbb{Z}/N\mathbb{Z}$  è un dominio  $\iff N$  primo ( $\iff$  campo) (noi non ho capito se basta dimostrare dominio  $\iff N$  primo visto che abbiamo già visto in classe che  $\mathbb{Z}/p\mathbb{Z}$  campo)

- dimostriamo  $\mathbb{Z}/N\mathbb{Z}$  dominio  $\rightarrow N$  primo

Supponiamo  $\mathbb{Z}/N\mathbb{Z}$  dominio. Allora, l'unico divisore di  $0_{k_N}$  è  $0_{k_N}$

Supponiamo per assurdo  $N$  non primo  $\rightarrow \exists a, b, 1 < a < n, 1 < b < n$  t.c.  $N = ab$

quindi,  $[a] \cdot [b] = [ab] = [0]$ .  $k_N$  non è dominio. CONTRAD.

dimostriamo che  $N$  primo  $\rightarrow \mathbb{Z}/N\mathbb{Z}$  dominio

$(\mathbb{Z}/N\mathbb{Z} \text{ dominio} \iff \forall [a], [b] \text{ t.c. } [a] \cdot [b] = [0], \circ [a] = [0] \circ [b] = [0])$

Supponiamo  $\exists [a], [b] \in \mathbb{Z}/N\mathbb{Z}$  t.c.  $[a] \cdot [b] = [0]$

$[a] \cdot [b] = [ab] = [0]$ , significa  $N | ab$  (il resto è 0)

Ma, se  $N | ab$ , poiché  $N$  primo, o  $N | a$  o  $N | b$ . (per def. primo)

Ma, se  $N | a$ ,  $[a] = [0]$  e se  $N | b$ ,  $[b] = [0]$

Quindi, uno dei due divisori è zero

- Se  $\alpha \in A$  non è divisore di zero ( $\forall b \in A \setminus \{0\}, \alpha b \neq 0$ ) e  $\alpha x = 0_A \implies x = 0_A$

Lemma legge di cancellazione (in  $A$  snello)

Se  $\alpha \in A$  non divisore di zero, allora  $\alpha b = \alpha c \implies b = c$

dim:

$$\alpha b = \alpha c \iff \alpha(b-c) = 0 \quad \text{visto che } \alpha \text{ non è divisore di } 0 \implies b-c = 0 \iff b = c$$

$\alpha \neq 0$

OSSERVAZIONE: Questo implica la legge di cancellazione in  $\mathbb{Z}$  (dominio) ( $\alpha \neq 0$  perché  $0$  unico divisore di  $0$  in  $\mathbb{Z}$ )

risoluzione di equazioni in  $A$  (in particolare  $A = \mathbb{Z}$ ,  $A = \mathbb{Z}/n\mathbb{Z}$ )

$$\alpha X = b \quad \alpha, b \in A$$

$X$  indeterminato (può essere un valore o un insieme)  
mentre  $x$  (minuscolo) è un valore

- in  $A = \mathbb{Z}$  una soluzione di  $\alpha X = b$  esiste  $\iff \alpha | b$

infatti, se l'insieme delle soluzioni  $\neq \emptyset$  e se  
 $x$  soluzione, si ha  $\alpha x = b \iff \alpha | b$  (def. | )

Se, invece,  $\alpha | b \implies \exists k \in \mathbb{Z}$  t.c.  $b = \alpha k$  e prendo  $k = x$

esempio:  $2x = 3$  insieme delle soluzioni =  $\{x \in \mathbb{Z} : 2x = 3\} = \emptyset$  vorrebbe dire  $2 | 3$  - impossibile

$$2x = 6 \quad \{x \in \mathbb{Z} : 2x = 6\} = \{3\} \quad \text{osserviamo } 6 = 2 \cdot 3 \quad \text{quindi } 2x = 2 \cdot 3 \implies x = 3$$

- $A = \mathbb{Z}/n\mathbb{Z}$ ,  $n \in \mathbb{N}^*$

$$\alpha X = b$$

- Nel caso in cui  $A$  è un anello qualsiasi e  $\alpha \in A^\times$  di inverso  $\alpha^{-1}$ , posso moltiplicare termine  $\alpha$  termine per  $\alpha^{-1}$

$$\underbrace{\alpha^{-1} \alpha}_1 X = \alpha^{-1} b \quad \text{quindi l'eq. ha l'unica soluzione } X = \alpha^{-1} b$$

(es  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ )

- Se per esempio  $A = K$  campo

$$\alpha X = b \quad \text{con } \alpha \neq 0 \quad \text{ammette sempre l'unica soluzione } X = \alpha^{-1} b$$

proposizione  $\exists X = b \quad \exists, b \in A = \mathbb{Z}/n\mathbb{Z}$

ammette soluzioni  $\iff \text{MCD}(\alpha, n) = \beta$  con  $\exists = [\alpha], b = [\beta], \alpha, \beta \in \mathbb{Z}$

dim:

• Dimostro ammette soluzioni  $\implies \text{MCD}(\alpha, n) = \beta$

$$[\alpha][x] - [\beta] = [0]$$

quindi  $\exists_n 0$  quindi multiplo  
di  $n$

Sia  $[x]$  soluzione:  $\exists [x] = b$  quindi  $[\alpha][x] = [\beta] \iff \alpha x - \beta \in n\mathbb{Z}$

$$\iff \alpha x - \beta = nk \quad \exists k \in \mathbb{Z} \iff \alpha x - nk = \beta \implies \beta \in \alpha\mathbb{Z} + n\mathbb{Z} = \delta\mathbb{Z} \iff \delta \mid \beta$$

$\beta \in \text{multiplo}$   
 $\text{di } \delta$

• Ora dimostro  $\text{MCD}(\alpha, n) \mid \beta \implies$  ammette soluzioni

Sappiamo  $\delta = \text{MCD}(\alpha, n) \mid \beta \iff \beta = \delta x \implies \beta \in \alpha\mathbb{Z} + n\mathbb{Z}$

$$\iff \exists v, z \text{ t.c. } \beta = v\alpha + vn \iff \beta - v\alpha = vn$$

$\times$  def congr. mod

$$\iff \beta \equiv_n v\alpha \iff [\beta] = [v][\alpha]^{= \delta} \quad b = x\delta$$

esempio:  $[3]X = \emptyset$  in  $A = \mathbb{Z}/6\mathbb{Z}$

$$\alpha = 3, \beta = \emptyset, n = 6 \quad \text{MCD}(\alpha, n) = 3 \mid \emptyset = \beta$$

ci sono soluzioni.  $X = [2]$  è soluzione ( $[3] \cdot [2] = [6] = [0] \text{ in } \mathbb{Z}/6\mathbb{Z}$ )

$X = [4]$  è soluzione ( $[3] \cdot [4] = [12] = [0]$ )

o anche  $[3] \cdot [2] \cdot [2] = [0] \cdot [2] = [0]$ )

$X = [0]$  è soluzione ( $[3] \cdot [0] = [0]$ )

l'insieme delle soluzioni è  $\{[0], [2], [4]\} \subset A$

## Lemma

$a, b, c \in \mathbb{Z}$   $a, b | c$  e  $\text{MCD}(a, b) = 1$  allora  $ab | c$

dim:

$$a, b | c \iff c = ak = bh \quad (\exists h, k \in \mathbb{Z})$$

$$\implies a | bh \quad (\text{o anche } b | ah, \text{ ma sceglieremo } a | bh)$$

• Devo dimostrare  $\text{MCD}(a, b) = 1 \implies a | h^*$   $\implies ab | c$  moltiplicando per  $b$  da entrambi i lati ( $c = bh$ )

•  $\text{MCD}(a, b) = 1 \iff b$  è invertibile modulo  $a$

$$\iff \exists b' \in \mathbb{Z} \text{ t.c. } bb' \equiv 1 + a\mathbb{Z}$$

( $b$  invertibile se  $by \equiv 1$  ovvero  $by - 1 \equiv 0$   
 $\iff by - k \equiv 1 \quad \text{MCD}(a, b) = 1 \iff ax + by = 1$   
 prendo  $x = -k$  e queste cose sono uguali)

$$\begin{aligned} \bullet \text{ Dicendo } a | bh &\implies a | b' | b'b h = (1 + ak)h \iff a | b' = h + ahk \\ &\iff ab' - ahk = h \iff a(b' - hk) = h \quad \text{quindi } a | h \blacksquare \end{aligned}$$

III secolo dal matematico Sun Tsu! ( $\neq$  the art of war Sun Tsu)

## TEOREMA CINESE DEI RESTI

Poniamo  $r_1, \dots, r_s \in \mathbb{N}^*$  e supponiamo  $\text{MCD}(r_i, r_j) = 1 \quad \forall i \neq j$   $\Rightarrow$  due coprimi

Consideriamo inoltre  $c_1, \dots, c_s \in \mathbb{Z}$

Allora il sistema

$$(*) \left\{ \begin{array}{l} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \vdots \\ x \equiv c_s \pmod{r_s} \end{array} \right. \text{ ha un'unica soluzione modulo } R := r_1 \cdot r_2 \cdot \dots \cdot r_s$$

ovvero l'insieme  $E_* = \{x \text{ soluzione in } \mathbb{Z} \text{ di } (*)\}$  è  $x_0 + R\mathbb{Z}$

Come calcolare una soluzione particolare  $x_0$  di  $(*)$ ?

$$\bullet R = r_1 \cdot r_2 \cdot \dots \cdot r_s \quad \bullet \text{ poniamo } R_i = \frac{R}{r_i} = r_1 \cdot r_2 \cdot \dots \overset{\text{"non } c_i \text{ in "}}{r_i} \cdot \dots \cdot r_s = r_1 \cdot r_2 \cdot \dots \cdot r_{i-1} \cdot r_{i+1} \cdot \dots \cdot r_s$$

e notiamo che  $\text{MCD}(R_i, r_i) = 1$  (perché  $r_i, r_j$  ecc primi fra loro e in  $R_i$  "manca" proprio  $r_i$ )

Visto che sono primi fra loro, questa proprietà può essere riformulata dicendo che  $[R_i]$  classe di  $R_i$  in  $\mathbb{Z}/r_i\mathbb{Z}$

è invertibile di inverso  $[s_i] \in \mathbb{Z}/r_i\mathbb{Z}$   $[R_i][s_i] = [1]$

Quindi,  $\underbrace{[R_i]}_{[1]} \underbrace{[s_i]}_{[y_i] \in \mathbb{Z}/r_i\mathbb{Z}} [c_i] = [c_i]$  quindi abbiamo costruito elementi  $[y_1], \dots, [y_s] \in \mathbb{Z}/r_i\mathbb{Z}$  formati dall'inverso di  $R_i$  e  $c_i$

• Ora, dimostriamo che  $x_0 = \sum_{i=1}^s y_i R_i \in \mathbb{Z}$  è soluzione di  $(*)$

\* credo che "basti" il lemma di Gauss? Sospendo e  $\text{MCD}(a, b) = 1$   
 $a | bh$  e  $\text{MCD}(a, b) = 1$  allora  $a | bc \Rightarrow a | c$   
 allora  $a | h$   
 (combinano i vincoli, per Gauss  $a, b \in \mathbb{Z}^*$   
 e non  $\mathbb{Z}$ , ma non credo ci sarebbe  
 perdita di generalità chiedere  
 al prof.)

$x_0 = \sum_{i=1}^s y_i R_i \in \mathbb{Z}$  è soluzione di (\*)

infatti, se  $i \neq j$ ,  $r_i | R_j$  perché  $R_j$  è il prodotto di tutti "gli  $r$ " tranne  $r_i$ ,  
quindi l'unico che non lo divide è  $r_i$

Quindi  $x_0 = \sum_{j=1}^s y_j R_j = \sum_{\substack{j=1 \\ j \neq i}}^s y_j R_j + y_i R_i$  isoliamo il termine non divisibile per  $r_i$  (quindi il resto)  
il tutto è quindi  $\equiv_{r_i} y_i R_i$   
(definito come)  
 $\equiv_{r_i} c_i$  quindi abbiamo trovato  $x_0$   
congruente a  $c_i \text{ mod } r_i$

Questo è valido  $\forall i = 1, \dots, s$  dunque  $x_0 = \sum_j y_j R_j$  è una sol. particolare di (\*)

### Sistema omogeneo associato

$$\begin{aligned} *_{(H)}: \quad & \left\{ \begin{array}{l} x \equiv 0 \pmod{r_1} \\ x \equiv 0 \pmod{r_2} \\ \vdots \\ x \equiv 0 \pmod{r_s} \end{array} \right. \\ & x \equiv_r 0, \quad i=1 \dots s \end{aligned}$$

Soluzioni?  $x \equiv_{r_1} 0 \iff r_1 | x$   
 $x \equiv_{r_2} 0 \iff r_2 | x$

ma  $r_1, r_2$  sono primi fra loro, quindi (x lemma)  $r_1 r_2 | x$  (Si può andare avanti fino a  $r_s$ :  
 $x \equiv_{r_3} 0 \iff r_3 | x$ ,  $\text{MCD}(r_1, r_2, r_3) = 1 \Rightarrow r_1 r_2 r_3 | x$  ecc..)

Iterando, ottengo che  $R := r_1 \dots r_s | x$

Quindi, l'insieme delle soluzioni di  $(*)_H$  è  $E_H = R\mathbb{Z}$  (i multipli di  $R$ )

### proposizione

L'insieme delle soluzioni di (\*),  $E_*$  è dato da  $x_0 + R\mathbb{Z}$

dim: •  $E_* \supset x_0 + R\mathbb{Z}$  è chiaro. Infatti, se  $x \in x_0 + R\mathbb{Z}$ , allora  $x = x_0 + Rk \quad \exists k \in \mathbb{Z}$

ma  $Rk \equiv_{r_i} 0 \quad \forall i = 1 \dots s$  ( $r_i | Rk$ , perché  $r_i | R$  -  $R$  è il prodotto di tutti gli  $r_i$ )

• Addizionando con  $x_0$ , che è soluzione particolare, ottengo  $x \equiv_{r_i} c_i + 0 \equiv c_i \text{ mod } r_i$   
 $\Leftrightarrow x \equiv_{r_i} x_0$

• Dimostriamo  $E_* \subset x_0 + R\mathbb{Z}$

$$x \equiv_{r_i} c_i \iff x - c_i \equiv_{r_i} 0$$

(old sistema)

Sia  $x$  soluzione dr (\*). Allora,  $x - x_0 \equiv_{r_i} 0 \quad \forall i = 1 \dots s$

$\Rightarrow x - x_0 \in R\mathbb{Z}$  x Lemma ( $r_i | x - x_0$ , quindi  $r_1 r_2 \dots r_s | x - x_0$ , quindi  $x - x_0$  multiplo di  $R$ )

$\Rightarrow x \in x_0 + R\mathbb{Z} \Rightarrow E_* \subset x_0 + R\mathbb{Z}$

piccola parentesi pratico: quello che ci hanno detto al TUTORAGGIO sul teorema cinese del resto

$$\left\{ \begin{array}{l} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{2} \end{array} \right. \quad \begin{array}{l} \cdot r_1 = 11, \quad r_2 = 5, \quad r_3 = 2 \\ \text{se sono coprimi, ammette un'unica soluzione modulo R} \end{array}$$

$$\bar{x} = R_1 \bar{x}_1 + R_2 \bar{x}_2 + R_3 \bar{x}_3 + Rk \quad k \in \mathbb{Z}$$

con  $R = r_1 \cdot r_2 \cdot r_3$  e  $R_i = \frac{R}{r_i}$  e  $\bar{x}_i$  t.c.  $R_i x \equiv c \pmod{r_i}$

①  $r_1 = 11 \quad r_2 = 5 \quad r_3 = 2$  sono coprimi? sì.

②  $R = r_1 \cdot r_2 \cdot r_3 = 11 \cdot 5 \cdot 2 = 110$  ricordiamo  $c_1 = 1 \quad c_2 = 2 \quad c_3 = 1$

$$R_1 = \frac{11 \cdot 5 \cdot 2}{11} = 10 \quad R_2 = \frac{11 \cdot 5 \cdot 2}{5} = 22 \quad R_3 = \frac{11 \cdot 5 \cdot 2}{2} = 55$$

③  $\bar{x}_i = R_i x \equiv_r c$

•  $\bar{x}_1 = 10x \equiv 1 \pmod{11}$

è un'equazione diofantea di tipo

$10x - 11h = 1$  che posso scrivere  
(per non avere il -)

con  $y = -h \quad 10x + 11y = 1$  (cerco solo  $x$ )

risolvo l'eq.: •  $\text{MCD}(10, 11) = 1$

Bézout  $1 = 10 \cdot \underline{-1} + 11 \cdot 1$

(ho trovato)

$x_0$  particolare

$22 = 4 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

quindi (Bézout)

$1 = 5 - 2 \cdot 2$

$1 = 5 - 2 \cdot (22 - 4 \cdot 5)$

$1 = \underline{-2} \cdot 22 + 9 \cdot 5$

•  $\bar{x}_3 = 55x \equiv 1 \pmod{2}$

55 è dispari, quindi

$\equiv 1 \pmod{2}$

$1x \equiv 1 \pmod{2}$

$[x_3] \equiv [1] \pmod{2}$

• metto l' $x$  particolare  $x = x_0 + \frac{b}{\text{MCD}(a, b)} k$

nella formula

$$x = -1 + \frac{11}{1} k$$

$k$  deve essere  $0 \leq k \leq d-1$  (MCD)

• quindi  $k \in \{0\} \rightarrow x = -1 + 0 = -1$

ma qui cerchiamo  $= 2^*$

quindi moltiplico per 2

$$2 = -4 \cdot 22 + 18 \cdot 5$$

$$x = -4 + \frac{5}{1} k$$

Siamo in  
mod 11

quindi  $[x_1] \equiv [-1] \equiv [10]$

$k \in \{0\} \quad [x_2] \equiv [4] \equiv [1]$

④ metto tutto nella formula finale  $(\bar{x} = R_1 \bar{x}_1 + R_2 \bar{x}_2 + R_3 \bar{x}_3 + Rk)$

$177 - 110$

$$[x] = 10 \cdot 10 + 22 \cdot 1 + 55 \cdot 1 + 110k = 177 + 110k = 67 + 110k$$

### Esercizio 8 (foglio 3)

Esercizio 8. Trovare tutti gli interi  $x \in \mathbb{Z}$  che soddisfino

- (i)  $4x \equiv 7 \pmod{15}$
- (ii)  $6x \equiv 8 \pmod{9}$
- (iii)  $\begin{cases} 1025x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases}$
- (iv)  $4x \equiv 3 \pmod{385}$ .

### METODO PELLARIN CRT

$$\textcircled{1} \quad 4x \equiv 7 \pmod{15}$$

① calcolo l'MCD tra 4 e 15

$$\text{MCD}(4, 15) = 1 \iff [4] \text{ invertibile mod. 15}$$

$$\exists n \in \mathbb{Z} \text{ t.c. } 4 \cdot n \equiv_1 1 \quad (\text{es. } n=4)$$

Io faccio perché voglio che quel  $4x$  diventa un  $(1)x$

② trasformo  $4x$  in  $x \rightarrow$  moltiplico entrambi i lati per 4

$$4 \cdot 4x \equiv_{15} 28$$

$$x \equiv_{15} 13$$

(moltiplo con resto 13)

$$\text{quindi, le sol. sono } \mathcal{E} = 15\mathbb{Z} + 13$$

$$\textcircled{3} \quad \begin{cases} 1025x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases}$$

① notiamo che  $r_1, r_2, r_3$  sono primi tra loro ✓

② semplifichiamo le congruenze

$$\textcircled{4} \pmod{8} \quad 1025 = 1024 + 1 = 2^{10} + 1 = (2^3)^2 \cdot 2 + 1 \equiv 1 \pmod{8}$$

$\equiv_8 0$  perciò  
 $2^3 \equiv_8 0$

$$\cdot 5312065$$

$$\textcircled{5} \quad 8 \mid 40 \quad \text{quindi } 8 \mid 40 \cdot 10\mathbb{Z}$$

$$\text{notiamo che } 5312065 = 4000000 + 1312065$$

$$\text{visto che } 8 \mid 4 \cdot 10^6 \quad 5312065 \equiv_8 1312065$$

$$8 \mid 1200000 \equiv_8 112065 \quad 8 \mid 120000 \equiv_8 -7935$$

$$8 \mid 8000 \equiv_8 65 \equiv_8 1$$

il sistema diventa quindi

$$\begin{cases} x \equiv_8 1 \\ x \equiv_5 2 \\ x \equiv_3 1 \end{cases}$$

$$\textcircled{6} \quad \text{calcoliamo le altre cose: } R = 3 \cdot 5 \cdot 8 = 120$$

$$R_1 = r_2 r_3 = 15$$

$$R_2 = r_1 r_3 = 24$$

$$R_3 = r_1 r_2 = 40$$

$$\textcircled{2} \quad 6x \equiv 8 \pmod{9}$$

notiamo che 6 e 9 non sono coprimi.

$$6x \equiv_9 8 \iff 6x - 8 = 9 \cdot k$$

$$\iff 8 = 6x - 9k \quad \text{ma questo è impossibile}$$

notiamo che questi sono divisibili per 3

mentre 8 non lo è

$$\mathcal{E} = \emptyset$$

$$\textcircled{2} \cdot 36 \equiv_5 1$$

$$\cdot 322 \quad 5 \mid 320 \equiv_5 2$$

$$\textcircled{3} \cdot 4 \equiv_3 1$$

$$\cdot 7 \equiv_3 1$$

④ troviamo gli inversi  $S_i$ :

$$R_1 = 15 \text{ è invertibile modulo } r_1 = 8 \quad 7 \cdot 15 \stackrel{-1}{\equiv} 1 \text{ di inverso } S_1 = 7$$

$$R_2 = 24 \quad 24 \cdot 4 \stackrel{-1}{\equiv} 1 \quad S_2 = 4$$

$$R_3 = 40 \quad 40 \cdot 1 \stackrel{-1}{\equiv} 1 \quad S_3 = 1$$

⑤ calcoliamo  $y_i = S_i c_i$  e li inseriamo nella formula finale

i	$S_i$	$c_i$	$y_i$
1	7	1	7
2	4	2	$8 \stackrel{-1}{\equiv} 3$
3	1	1	1

$$X_0 = \sum_{i=1}^3 y_i R_i = 7 \cdot 15 + 3 \cdot 24 + 1 \cdot 40 = 217 \quad \text{soltuzione particolare}$$

$$\text{Soltuzione generale: } E = 217 + 120Z$$

POLINOMI in una indeterminata  $\Rightarrow$  coeff in un campo

$K$  campo =  $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Un polinomio in  $X$  a coefficienti in  $K$  è definito come

$$P = \sum_{i=0}^n \alpha_i X^i \quad \text{con } \alpha_i \in K \text{ coefficienti, } n \in \mathbb{Z} \text{ (dipende dal polinomio)}$$

$\alpha_i = 0 \quad \forall i > 0$  (abbastanza grande)

esempio

$$K = \mathbb{R}, \quad 0, \quad \alpha_i = 0 \quad \forall i \quad K = \mathbb{F}_2 \quad [1]x^5 + [0]x^4 + [2]x^3 + [6]x^2 + [1]x + [1] = x^5 + x + [1]$$

### → insieme di polinomi

$A = K[X]$  è l'insieme dei polinomi (ogni  $P \in A$ )

L'insieme di polinomi ha una struttura ad anello (comm. un.)  $(A, -, +, \cdot, 0, 1)$

Definiamo infatti le operazioni di somma e prodotto:

$$\text{con } P = \sum_{i \geq 0} \alpha_i X^i \quad \alpha_i = 0 \quad \forall i > 0 \quad Q = \sum_{i \geq 0} b_i X^i \quad b_i = 0 \quad \forall i > 0$$

- $P + Q := \sum_{i \geq 0} (\alpha_i + b_i) X^i$

prodotto di Cauchy

- $P \cdot Q := \sum_{k \geq 0} c_k X^k \quad \text{con } c_k = \sum_{i+j=k} \alpha_i b_j \quad \begin{array}{l} \text{(qui si nota che } c_k = 0 \quad \forall k > 0 \\ \text{- per numeri abbastanza grandi,} \\ \alpha_i \neq 0 \quad b_j \text{ saranno } 0 \end{array}$

### → grado di un polinomio

$$P \in A[X] \quad P = \sum_{i \geq 0} \alpha_i X^i \quad \alpha_i = 0 \quad \forall i > 0 \quad \text{con } P \neq 0 \quad (\text{ovvero } \{i \in \mathbb{N} \text{ t.c. } \alpha_i \neq 0\} \text{ finito non vuoto})$$

$$\deg(P) = \max \{i \in \mathbb{N}, \alpha_i \neq 0\} \quad \text{grado massimo} \quad \bullet \text{ Si pone } \deg(0) := -\infty$$

Quindi, l'insieme dei gradi è  $\mathbb{N} \cup \{-\infty\}$   $\deg: K[X] \longrightarrow \mathbb{N} \cup \{-\infty\}$

- elementi di grado zero  $\{P \in K[X] : \deg(P) = 0\} = K^\times$  ↗ sono gli invertibili del campo, ovvero (per def campo) tutti gli el del campo sono  $\neq 0$  (quindi sono le "costanti")

Lemmas

$$\textcircled{1} \quad \deg(\alpha) = -\infty \iff \alpha = 0$$

$$\textcircled{2} \quad \deg(\alpha b) = \deg(\alpha) + \deg(b)$$

$$\textcircled{3} \quad \deg(\alpha + b) \leq \max(\deg(\alpha), \deg(b))$$

$$\text{e } \deg(\alpha + b) = \max(\deg(\alpha), \deg(b)) \text{ se } \deg(\alpha) \neq \deg(b)$$

se i gradi sono uguali gli el. di grado maggiore si potrebbero annullare e il grado sarebbe < (es.  $(x^3+x) + (-x^3+2)$ )

$$\text{es. } \alpha = x^2 + x + 1 \quad \deg = 2 \quad b = x + 1 \quad \deg = 1 \quad \alpha + b = x^2 + 2x + 2 \quad \deg = 2$$

# ANALOGIE TRA I POLINOMI E $\mathbb{Z}$

$$\mathbb{Z} \quad A = K[X]$$

anello di polinomi  
Compone

operazioni:

$$\begin{array}{c} \cdot \mathbb{Z} \xrightarrow{1:1} \mathbb{N} \text{ val assoluto} \\ \alpha \longrightarrow \begin{cases} \alpha & \alpha \geq 0 \\ -\alpha & \alpha \leq 0 \end{cases} \end{array}$$

proprietà

- ①  $|\alpha| = 0 \iff \alpha = 0$
- ②  $|\alpha b| = |\alpha| \cdot |b|$
- ③  $|\alpha + b| \leq |\alpha| + |b|$  diseg. triangolare

$$\cdot A \xrightarrow{\deg} \mathbb{N} \sqcup \{-\infty\} \text{ grado polinomio}$$

$$\textcircled{1} \deg(\alpha) = -\infty \iff \alpha = 0$$

$$\textcircled{2} \deg(\alpha b) = \deg(\alpha) + \deg(b)$$

$$\textcircled{3} \deg(\alpha + b) \leq \max(\deg(\alpha), \deg(b))$$

ci sono delle corrispondenze, ma serve qualcosa di più vicino

def c-valore assoluto di un polinomio

Dato un polinomio  $P \in A \setminus \{0\}$

Scegliamo  $c > 1$

$$|P|_c := c^{\deg(P)} \quad (\text{dipende da } c)$$

Allora proprietà

$$\textcircled{1} |\alpha|_c = 0 \iff \alpha = 0$$

$$\textcircled{2} |\alpha b|_c = |\alpha|_c \cdot |b|_c$$

$$\textcircled{3} |\alpha + b|_c \leq \max(|\alpha|_c, |b|_c) \leq |\alpha|_c + |b|_c$$

invece, se  $P = 0$

$$|0|_c := 0 = c^{-\infty}$$

$$\text{Per } \textcircled{2} \quad |\alpha b|_c = c^{\deg(\alpha b)} = c^{\deg(\alpha) + \deg(b)} = |\alpha|_c \cdot |b|_c$$

$$\text{Per } \textcircled{3} \quad |\alpha + b|_c = c^{\deg(\alpha + b)} \leq c^{\max(\deg(\alpha), \deg(b))} \leq c^{\deg(\alpha)} + c^{\deg(b)}$$

## ALGORITMO DELLA DIVISIONE EUCLIDEA SUI POLINOMI

Teorema  $\alpha, b \in A = K[X] \quad (\alpha, b) \neq (0, 0)$

Esiste unica  $(q, r) \in A \times A$  t.c.  $\alpha = qb + r$  dove  $\deg(r) < \deg(b)$  ovvero  $|r|_c < |b|_c$

divisione in colonne

$$\begin{array}{l} \alpha = x^4 + x + 1 \\ b = x^3 - 2 \end{array} \quad \begin{array}{r} x^4 + \\ x^3 - 2 \\ \hline x^4 \quad -2x \end{array} \quad \begin{array}{r} x^3 \quad -2 \\ \hline x \quad \end{array} \quad \begin{array}{r} \textcircled{1} x^4/x^3 \\ \textcircled{2} \text{ moltiplico per } (x^3 - 2) \\ \textcircled{3} \text{ scrivo qui} \\ \textcircled{4} \text{ sottraggo} \\ \textcircled{0} \quad 3x + 1 \end{array}$$

grado <  
quindi fine

$$q = x, \quad r = 3x + 1$$

$\mathbb{Z}$  $A = K[x]$ 

inter:	polinomi	TABELLA ANALOGIE TRA $\mathbb{Z}$ e $K[x]$
divisione euclides	divisione euclides	(il grande ripasso delle proprietà di $\mathbb{Z}$ )
valore assoluto	$  \cdot  _c \circ \deg$	

 $\mathbb{N}^*$   
("positivi")

$A^+ = \{ \text{polinomi monici} \}$   
 in forma  $P = a_0 + a_1 x + \dots + a_n x^n$   
 con  $a_n \neq 0$  (coeff. grado massimo)  
 il prodotto di monici è monico  
 (ma la somma non necessariamente)

 $\mathbb{Z}^\times = \{ \pm 1 \}$ 

inversi sui polinomi:

$$\begin{aligned} A^\times &= K^\times \\ \text{sia } a \in A^\times \exists b \in A^\times \text{ t.c. } ab &= 1 \\ \implies \deg(a) + \deg(b) &= 0 \quad (\deg(ab) = 0 = \deg(a) + \deg(b)) \\ \implies \deg(a) = \deg(b) &\in \mathbb{N} \text{ (o avrei } -\infty) \\ \implies \deg(a) = \deg(b) &= 0 \\ \implies a, b &\in K^\times \text{ ("costanti" diverse da 0)} \end{aligned}$$

divisibilità in  $\mathbb{Z}$ 

$$\begin{aligned} a|b &\iff \exists H \in \mathbb{Z} \text{ t.c. } b = ah \\ a|b &\iff b \in a\mathbb{Z} \\ \exists k \in \mathbb{Z} \text{ t.c. } b &= ak \\ \iff b &\in a\mathbb{Z} \\ \iff b\mathbb{Z} &\subset a\mathbb{Z} \\ &\iff bA \subset aA \end{aligned}$$

proprietà di  $|$  su  $A$ 

$$\begin{aligned} \textcircled{1} \text{ riflessiva} \\ \textcircled{2} \text{ transitiva} \\ a|b, b|c \iff cA \subset bA \subset aA \\ \iff cA \subset aA \iff a|c \\ \textcircled{3} \text{ quasi riflessiva ma non:} \end{aligned}$$

$$\begin{aligned} a, b \in A. \text{ Supponiamo } a|b \wedge b|a \\ \iff \exists u, v \in A \text{ t.c. } b = au, b = bv \\ \text{quindi } a = uv \iff \deg(a) = \deg(u) + \deg(v) + \deg(a) \\ \text{possiamo supporre } a, b \neq 0 \\ \deg(a) = \deg(a) + \deg(u) + \deg(v) \iff 0 = \deg(u) + \deg(v) \\ \iff \deg(u) = \deg(v) = 0 \\ \iff u = \lambda \in K^\times, v = \mu \in K^\times \quad (\text{sempre per la questione } \deg(0) = \text{"costante" } \neq 0) \end{aligned}$$

Quindi  $\exists \lambda \in K^\times = A^\times \text{ t.c. } b = \lambda a$

Lemmas  $A = K[X]$  è un dominio d'integrità

$\mathbb{Z}$  è un dominio d'integrità

dim Sia  $P \in A$  divisore di zero

$$\exists Q \in A \setminus \{\emptyset\} \text{ t.c. } PQ = \emptyset$$

$$\deg(PQ) = \deg(\emptyset) = \deg(P) + \deg(Q) = -\infty$$

impossibile somma due numeri  $\in \mathbb{N} = -\infty$

$$\text{Quindi } \deg(P) = -\infty \iff P = \emptyset$$

$$a \equiv b \pmod{n}$$

$$\iff n | a - b$$

$$a, b \in A, H \in A \setminus \{\emptyset\}$$

$$a \equiv b \pmod{H} \text{ rel d'eq.}$$

$$\text{es. transitività } a \equiv_H b, b \equiv_H c$$

$$\iff H | a - b \wedge H | b - c$$

$$\iff a - b = Hv \quad \exists v \in A, b - c = Hw \quad \exists w \in A$$

$$a - b = b - c = H(v + w)$$

$$\iff H | a - c \iff a \equiv_H c$$

$$A/H \text{ snello}$$

commutativo unitario

$$A/H = \{[a] : a \in A\} = \{a + H_0 : a \in A \text{ t.c. } \deg(a) < \deg(H)\}$$

non alterano il grado di  $a$  rispetto a  $H$

$$a \in A, [a] = a + H_0 \subset A$$

$$\text{Sistema compl. Rapp. mod } H = \{a \in A : \deg(a) < \deg(H)\}$$

de: MCD in  $\mathbb{Z}$

de: MCD in  $A$

Bézout in  $\mathbb{Z}$ :

$$a, b \in A, \text{ poniamo } aA + bA = \{m \in A \text{ t.c. } \exists v, v \in A \text{ con } m = va + vb\}$$

Lemmas Bézout in  $A = K[X]$

$$a, b \in A \text{ t.c. } (a, b) \neq (0, 0)$$

$$\text{allora } aA + bA = \Delta A \quad \exists! \delta \in A^+$$

dimostri che  $\mathcal{E}^+$  contiene un el. di grado minimo unico ( $\delta$ )

(mostrare non vuoto  $(a, b) \neq \emptyset$ , principio Minimo)

$$\mathcal{E} = aA + bA, \quad \mathcal{E}^+ = \{m \in \mathcal{E} \text{ t.c. } m \in A^+\}$$

monico  
(notiamo che infatti è l'insieme "analogo" a  $\mathbb{N}^*$  in  $A$ )

MCD

$$(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$$

prop.  $\exists! d \in \mathbb{N}^*$  t.c.

$$\textcircled{1} \quad d | a \wedge d | b$$

\textcircled{2} se  $d' \in A$  t.c.

$$d' | a \wedge d' | b \Rightarrow d' | d$$

MCD

$$(a, b) \in A^2 \setminus \{(0, 0)\}$$

prop.  $\exists! d \in A^+$  t.c.

$$\textcircled{1} \quad d | a \wedge d | b$$

\textcircled{2} se  $d' \in A$  t.c.

$$d' | a \wedge d' | b \Rightarrow d' | d$$

$$\text{inoltre } d = \delta = \text{MCD}(a, b)$$

$$\text{inoltre } d = \delta = \text{MCD}(a, b)$$

$$\text{coprimi } a, b \in \mathbb{Z} \text{ t.c. } \text{MCD}(a, b) = 1$$

$$\text{coprimi } a, b \in A \text{ t.c. } \text{MCD}(a, b) = 1$$

irriducibile  $a \in A \setminus A^\times$

$a$  irriducibile se  $\forall b, c \in A : a = bc$   
allora  $\circ b \in A^\times \circ c \in A^\times$

primo  $a \in A \setminus A^\times, a \neq \emptyset$

primo se  $a | bc \Rightarrow a | b \circ a | c$

irriducibile  $P \in A \setminus A^\times \quad (\deg(P) > 0)$

$P$  è irriducibile se, scrivendo  $P = QR$

allora si ha  $\circ Q \in A^\times \circ R \in A^\times (= K^\times)$

osservazione:

$X - x$  è irriducibile  $\forall x \in K$

$$X - x = U \cdot V$$

$$\deg(X - x) = \deg(U) + \deg(V)$$

$$\Rightarrow \{\deg(U), \deg(V)\} = \{0, 1\} \text{ almeno uno è invertibile (di grado 0)}$$

Lemmas: primo  $\iff$  irriducibile

Lemmas:  $P$  irriducibile  $\iff$   $P$  primo

Teorema Fondamentale Aritmetica

$\forall a \in \mathbb{Z}^*$   $a$  si decomponga  
in modo unico come:

$$d = (\pm 1) \cdot \prod_{\substack{p \\ \text{primo}}} p^{v_p(a)}$$

$v_p(a) \in \mathbb{N}$ ,  $\{p : v_p(a) \neq 0\}$  finito

Teorema della Fattorizzazione Unica

Ogni  $H \in A - \{\emptyset\}$  si decomponga  
in modo unico come prodotto:

$$H = \lambda \cdot \prod_{\substack{P \text{ irr.} \\ P \in A^+}} P^{v_P(H)} \quad v_P(H) \in \mathbb{N} \text{ e} \\ \{P : v_P(H) \neq 0\} \text{ finito}$$

## FATTORIZZAZIONE

in  $K = \mathbb{R}, \mathbb{C}$  la fattorizzazione è "facile" (è facile caratterizzare i polinomi irriducibili), invece in  $K = \mathbb{F}_p, \mathbb{Q}$  la fattorizzazione è difficile

### teorema

• in  $\mathbb{C}[x]$  i monici irriducibili sono tutti i polinomi nella forma  $X - \alpha : \alpha \in \mathbb{C}$  (polinomi di primo grado)

• in  $\mathbb{R}[x]$ , se  $P$  monico irriducibile, allora o: ①  $\deg(P) = 1$  ( $X - \alpha : \alpha \in \mathbb{R}$ )

② se  $\deg(P) = 2$

$$(P = X^2 + \alpha X + b) \text{ allora } \Delta = \alpha^2 - 4b < 0$$

### def VALUTAZIONE

dato  $k \in K$ ,  $F \in K[X] = F_0 + F_1X + \dots + F_nX^n$

la valutazione di  $F$  in  $x$

è  $ev_x(F) = F_0 + F_1x + \dots + F_nx^n$  (è la "sostituzione" di  $X$ )

$$ev: K[X] \longrightarrow K$$

OSSERViamo:

$$\textcircled{1} ev_x(F+G) = ev_x(F) + ev_x(G)$$

$$\textcircled{2} ev_x(F \cdot G) = ev_x(F) \cdot ev_x(G)$$

$$\textcircled{3} \lambda \in k, ev_x(\lambda) = \lambda \text{ (costanti) e non invertibili perché vale per 0}$$

• Si dice che  $ev_x: K[X] \longrightarrow K$  è un MORFISMO DI ANELLI

esempio:  $F = X^2 + 1 \in \mathbb{R}[X]$ ,  $x=1$ ,  $ev_x(F) = 1^2 + 1 = 2$

Lemma Sia  $x \in K$

allora  $ev_x^{-1}(\{0\}) = (X-x)A$   $\hookrightarrow K[X]$   $(x \in K \text{ tali che sostituire danno 0})$   
polinomi che si annullano in  $X$

dim:

• dimostra  $ev_x^{-1}(\{0\}) \subset (X-x)A$   $x-x=0$

Sia  $Q = (X-x)H$ . Allora  $ev_x(Q) = ev_x(X-x) \cdot ev_x(H) = 0$   
 $\implies Q \in ev_x^{-1}(\{0\})$

• dimostra  $ev_x^{-1}(\{0\}) \subset (X-x)A$

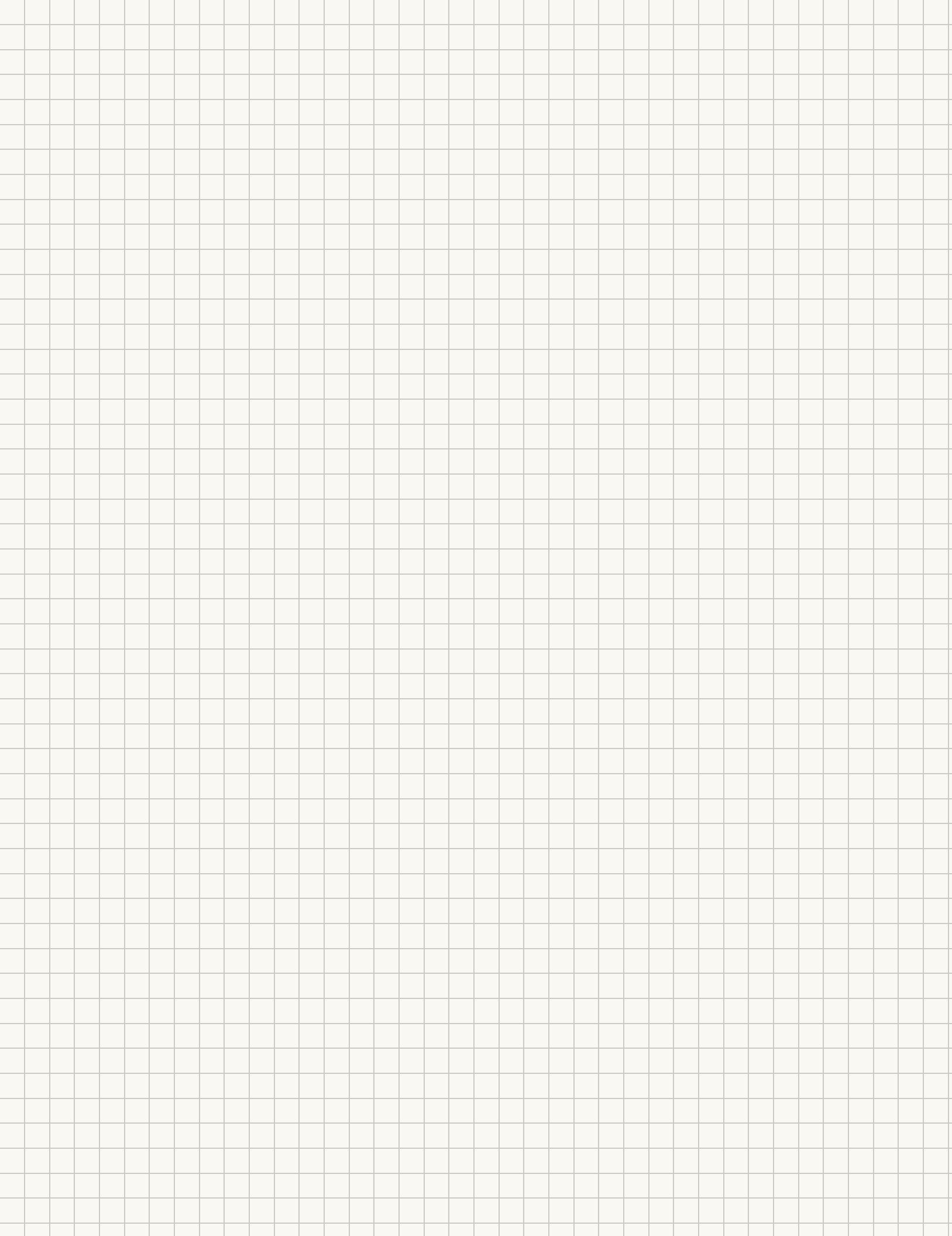
Sia  $P \in A$  t.c.  $ev_x(P) = 0$ .

per l'algoritmo di divisione euclidea per  $X-x$   $\exists ! (q, r) \in A \times A$  t.c.  $P = q(X-x) + r$   $\deg(r) < \deg(X-x)$  deve essere  $\deg(r) < \deg(b)$

$$ev_x(P) = ev_x(q(X-x) + r) = ev_x(q) \underbrace{ev_x(X-x)}_{0 \text{ per ipotesi}} + ev_x(r)$$

$$\implies ev_x(r) = 0 \iff r \in K$$

$$(0 = 0 + ev_x(r))$$



## FATTORIZZAZIONE

$K = \mathbb{R}, \mathbb{C}$  fattorizzazione "fisica" e facile caratterizzazione  
i polinomi irriducibili

DA COPIARE

IN BELLA

Teorema

In  $\mathbb{C}[x]$  i monici irriducibili sono tutti i pol.  $x - \alpha : \alpha \in \mathbb{C}$  (primo grado)

in  $\mathbb{R}[x]$  se  $P$  monico irriducibile allora: ①  $\deg(P) = 1$  ( $x - \alpha : \alpha \in \mathbb{R}$ )

$$\textcircled{2} \deg(P) = 2$$

$$P = x^2 + ax + b \quad \Delta = a^2 - 4b < 0$$

$K = \mathbb{F}_p, \mathbb{Q}$  fattorizzazioni difficili

valutazione  $\rightarrow F_0 + F_1 x + \dots + F_n x^n$

$x \in K, F \in K[X]$

la valutazione di  $F$  in  $x$

$$\text{è } ev_x(F) = F_0 + F_1 x + \dots + F_n x^n$$

$$ev : K[x] \longrightarrow K$$

OSSERViamo

$$\textcircled{1} ev_x(F+G) = ev_x(F) + ev_x(G)$$

$$\textcircled{2} ev_x(F \cdot G) = ev_x(F) \cdot ev_x(G)$$

$$\textcircled{3} \lambda \in K, ev_x(\lambda) = \lambda \quad (\text{costanti - non inv per lez sulle 0})$$

si dice che  $ev_x : K[x] \rightarrow K$  è un MORFISMO DI ANELLI

$$\text{es. } F = x^2 + 1 \in \mathbb{R}[x]$$

$$x=1$$

$$ev_x(F) = x^2 + 1 = 2$$

Lemma Sia  $x \in K$   $(K[x])$

$$\text{allora } ev_x^{-1}(\{0\}) = (x-x)A$$

polinomi che si annullano in  $X$

$x \in K$  tale che  
sostituiti danno 0

dim(?)

$$\text{Sia } Q = (x-x)H \text{ allora } ev_x(Q) = ev_x(x-x) ev_x(H) = 0$$

$$x-x = 0$$

$$\Rightarrow Q \in ev_x^{-1}(\{0\})$$

$$(c) \text{ Sia } P \in A \text{ t.c. } ev_{(x)}(P) = 0$$

Algo div. escluder per  $x-x$

$$\exists ! (q, r) \in A \times A \text{ t.c. } P = q(x-x) + r$$

$$\text{e } \deg(r) \in \{-\infty, 0\}$$

$$r = 0 \quad \wedge \quad r \text{ const} \neq 0$$

$$\deg(b) = 1$$

$$\underbrace{ev_x(p)}_{\text{ipotesi}} = ev_x(q(x-x) + r) \xrightarrow{\quad} ev_x(q) \underbrace{ev_x(x-x)}_{\emptyset} + ev_x(r)$$

$$\Rightarrow ev_x(r) = \emptyset$$

$$\Leftrightarrow r \in K \quad \} \text{ per } ③$$

$$\text{quando } r = ev_x(r) = \emptyset$$

$$\text{quando } P \in (x-x) A \quad \blacksquare$$

$P$  ha una radice in  $x \Leftrightarrow x-x \mid P$

$$ev_x(P) = \emptyset$$