Ultime lezioni: Struttura di $\mathbb{Z}$

Multipli e divisori (proprietà della divisibilità).

$a \mid b$ ← si legge in due modi
- a divide b
- b è multiplo di a

La divisibilità ha a che fare con la struttura dei sottogruppi additivi di $\mathbb{Z}$ (← Spoiler: ci piacerà chiamarli ideali).

$$a \mid b \iff b \in (a) \iff (b) \subseteq (a)$$
$$(a) = \{na \mid n \in \mathbb{Z}\}$$
$$(a) = (b) \iff a = \pm b$$

Se $a=0$ ma $b \neq 0$
$b = bxy \Rightarrow xy = 1$
$a = bx$, $b = ay$, $a \neq 0$
$a = axy$
$xy = 1 \Rightarrow x = y = \pm 1$

Se $a=b=0$, lo so già che $a = \pm b$.

Gergo

- Se $xy = 1$, sia x che y si dicono invertibili (In $\mathbb{Z}$ gli unici invertibili sono ± 1)
- Se a si ottiene da b moltiplicandolo per un invertibile allora a e b si dicono "elementi associati"

$a \mid b, b \mid a$
$a = bu \Rightarrow a \in (b)$
u invertibile
$au^{-1} = b \Rightarrow b \in (a)$

- $p \neq 0$ si dice <u>irriducibile</u> se
  - $p = ab \Rightarrow a \circ b$ è invertibile
  - non invertibile ← 1 non è irriducibile perché è invertibile

Tutto non invertibile si dice primo se

- $p \neq 0$ non invertibile [illegible]

$p \mid ab \Rightarrow p \mid a$ oppure $p \mid b$.

Obiettivo di oggi: mostrare che in $\mathbb{Z}$ primalità e irriducibilità sono lo stesso concetto e dimostrare il teorema fondamentale dell'aritmetica ↔ teorema di fattorizzazione unica.

Nella traduzione del concetto di divisibilità (in $\mathbb{Z}$) attraverso i sottogruppi abbiamo visto che

$$MCD(a,b) = d \iff (a) + (b) = (d)$$

- Il MCD esiste sempre (è unico a meno del segno)
- Id. di Bézout: se $MCD(a,b) = d$ allora $d = ha + kb$ per un'opportuna scelta di $h, k \in \mathbb{Z}$.

Primalità e irriducibilità $0 \neq p$ non invertibile

IRRIDUCIBILE	PRIMO
$p = ab \Rightarrow$ a o b è invertibile	$p \mid ab \Rightarrow p \mid a$ oppure $p \mid b$

Prop: p primo $\Rightarrow p$ irriducibile

Dim: $p = ab$ p divide $p = ab$

Poiché p è primo $\Rightarrow p$ divide a oppure p divide b.

Senza perdere di generalità, p divide a

$a = px$ $\quad p = px \cdot b \Rightarrow xb = 1$

$\Rightarrow$ a - p^ ~ 1 1

$p \neq 0$ ⇓ b invertibile

Mi rimane da dimostrare che ogni irriducibile è primo

Lemma tecnico (ma utilissimo) — In $\mathbb{Z}$.

$a \mid bc$, $MCD(a,b)=1$. Allora $a \mid c$.

Dim: Poiché $MCD(a,b)=1$ allora esistono $h,k \in \mathbb{Z}$ tali che $1 = ha + kb$ (h−b)a+(k+a)b = ha − ab + kb + ab

$$c = 1 \cdot c = (ha+kb)c = \underbrace{(hc)\cdot a}_{\text{multiplo di } a} + \underbrace{k\cdot(bc)}_{\text{multiplo di } a}$$

$a \mid bc$!!

$\Rightarrow$ c è multiplo di a, cioè $a \mid c$.

Prop: se p è irriducibile allora è anche primo.

Dim: p è irriducibile

$p \mid ab$.

Se p divide a ho finito

Se invece p non divide a

Voglio mostrare che $p \mid a$ opp $p \mid b$.

$$MCD(p,a) = \begin{cases} 1 \\ p \Rightarrow p \text{ divide } a \end{cases}$$

p IRRIDUCIBILE VUOL DIRE CHE GLI UNICI FATTORI, A MENO DEL SEGNO, SONO 1 e p

$p \mid ab$ $MCD(p,a)=1$ $\Rightarrow$ $p \mid b$.

Teorema fondamentale dell'aritmetica (fattorizzazione unica in $\mathbb{Z}$).

Se $n \in \mathbb{Z}$ è diverso da 0 allora si può fattorizzare nella forma

ESISTENZA DELLA FATTORIZZAZIONE

$$n = u \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k$$

dove u è invertibile e $p_1, \dots, p_k$ sono primi

Inoltre, se

$$u \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k = v \cdot q_1 \cdot q_2 \cdot \dots \cdot q_\ell$$ dove

u e v sono invertibili e $p_1, \dots, p_k, q_1, \dots, q_\ell$ sono primi

allora

- $k = \ell$ UNICITÀ DELLA FATTORIZZAZIONE
- a meno di riordinare $q_1, \dots, q_\ell$

si ha che p_i è associato a q_i per ogni i

(In $\mathbb{Z}$ $p_i = \pm q_i$)

Dim: esistenza

Se u è invertibile, allora $u = u$ $k=0$

Altrimenti per induzione su $|n| \neq 0, 1$.

n è irriducibile $\quad n = \underset{\text{inv}}{1} \cdot \underset{\text{primo}}{n}$ $\quad k=1$

n non è irriducibile

$\Downarrow$

$n = a \cdot b$ con a e b entrambi non invertibili

$|a| \neq 1 \quad |b| \neq 1$

$\Rightarrow |a| < |n|, \quad |b| < |n|. \Rightarrow$ posso usare l'ipotesi

'induttiva per a e b

$a = u \cdot p_1 p_2 \cdots p_r$

$b = u' \cdot p_{r+1} p_{r+2} \cdots p_k$

$n = ab = (uu')\, p_1 p_2 \cdots p_k$

ESISTENZA ✓

UNICITÀ Premessa: se p e q sono primi e p divide q allora p e q sono associati ($p = \pm q$)

Dim: p divide q $\quad q = p \cdot x$ MA q è irriducibile $\Rightarrow$ uno tra p e x è invertibile $\Rightarrow$ l'invertibile è x.

Se u, v invertibili

$$u\, p_1 p_2 \cdots p_k = v\, q_1 q_2 \cdots q_\ell \qquad p_i, q_j \text{ primi.}$$

allora $k = \ell$ e, a meno di riordinare i primi nel 2° membro, p_i è associato a q_i.

Per induzione su k

k=0 $\quad u = v\, q_1 \cdots q_\ell \Rightarrow \ell = 0$.

In effetti, se $\ell > 0$, il secondo membro ha valore assoluto > 1. (poiché se p è primo $|p| > 1$)

Passo induttivo **k>0**

$$u\, p_1 p_2 \cdots p_k = v\, q_1 q_2 \cdots q_\ell \qquad (*)$$

p_1 divide il 1° membro e quindi anche il 2° membro per primalità divide uno dei fattori a 2° membro.

A meno di riordinare i primi a 2° membro, p_1 divide $q_1 \Rightarrow p_1$ e q_1 sono associati

Es: se x divide un invertibile allora è invertibile

$q_1 = p_1 \cdot w$, w invertibile. Sostituisco in (*)

$u \cancel{p_1} p_2 \cdot \dots \cdot p_k = (vw) \cancel{p_1} q_2 \cdot \dots \cdot q_\ell$ A primo membro ho $k-1$ fattori primi

Utilizzando l'ipotesi induttiva $k-1 = \ell-1 \Longrightarrow k = \ell$

Inoltre, a meno di riordinare $q_2, \dots, q_\ell$ ho che p_i e q_i sono associati per $i = 2, 3, \dots, k$

Enunciato alternativo (più semplice)

$n > 0$ i primi sono tutti positivi.

Prop: Ogni $n \neq 1$ si scrive come prodotti di primi, unici a meno dell'ordine.

$\sqrt{2}$ è irrazionale. Non esiste alcun numero razionale il cui quadrato sia 2.

$m, n \in \mathbb{N}$.

$\left(\frac{m}{n}\right)^2 = 2 \Longrightarrow m^2 = 2n^2$

$\#_0$

se fattorizzo in primi entrambi i membri, a 1° membro ogni primo compare un # pari di volte, mentre a 2° membro il primo 2 compare un # dispari di volte.

Assurdo!

$\sqrt{N}$ è razionale esattamente quando è intera ($\in \mathbb{N}$)

(cioè quando N è un quadrato perfetto).

$\sqrt{N} = \frac{m}{n}$ $m, n > 0$. $N > 0$

$\times 0$

$m^2 = N \cdot n^2$ Fattorizzo in primi entrambi i membri.

In m^2 e n^2 ogni primo compare un numero pari di volte. Pertanto anche in N ogni primo compare un # pari di volte $\Longrightarrow N$ è un quadrato perfetto

Es: $\sqrt[n]{m}$ è razionale $\Longleftrightarrow$ m è una n.esima potenza perfetta
$\uparrow$ $\Updownarrow$
$\mathbb{N}$. è intero

Esistono infiniti numeri primi.

Dim: supponiamo che vi sia solo una quantità finita di primi $p_1, p_2, \dots, p_k$.
tutti primi, tutti distinti
non ce ne sono altri

$N = p_1 p_2 \dots p_k + 1 > 1$

N non è multiplo di $p_1, \dots, p_k$. N non è neanche invertibile

Assurdo. poiché per N non vale il teo fond. dell'aritmetica.