# I numeri naturali

*(Numeri primi / T. fond. dell'aritmetica / Criteri di divisibilità)*

Ripasso di matematica

Manolo Venturin

~~~ 1 ~~~
~~~

# Obiettivo (corso Analisi Matematica 1)

- Ripasso sui numeri naturali
- Numeri primi
- Teorema fondamentale dell'aritmetica
- Criteri di divisibilità
- Esempi

# Donazione

Se apprezzi le mie slide, considera di fare una donazione per supportare il mio lavoro.

Grazie!

# Gli insiemi numerici

- **Naturali**:

$$\mathbb{N} = \{0,\ 1,\ 2,\ \ldots\ \}$$

# Gli insiemi numerici

- Naturali:

$$\mathbb{N} \;=\; \{0,\; 1,\; 2,\; \dots\, \}$$

- **Interi** o **relativi**:

$$\mathbb{Z} \;=\; \{0,\; \pm 1,\; \pm 2,\; \dots\, \}$$

# Gli insiemi numerici

- Interi o relativi:

$$\mathbb{Z} = \{0,\ \pm 1,\ \pm 2,\ \ldots\}$$

- **Razionali**:

$$\mathbb{Q} = \left\{ r = \frac{p}{q} \colon p \in \mathbb{Z},\ q \in \mathbb{Z},\ q \neq 0 \right\}$$

# Gli insiemi numerici

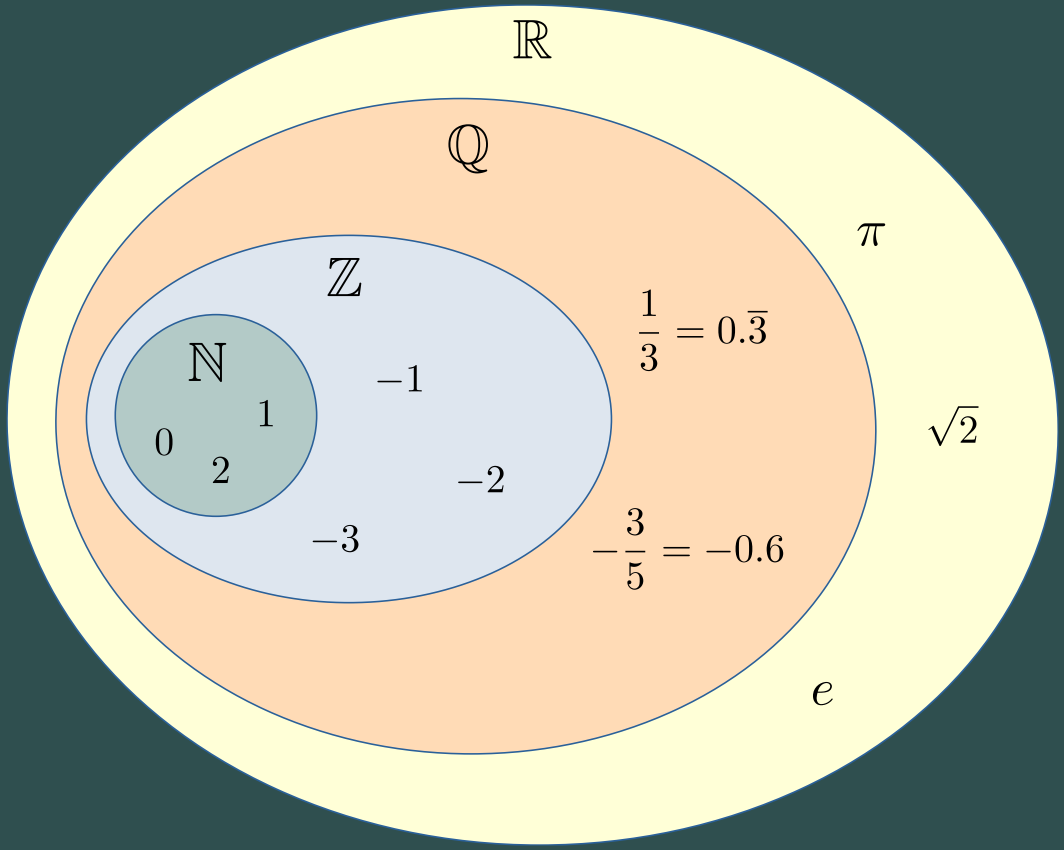
- Razionali:

$$\mathbb{Q} = \left\{ r = \frac{p}{q} \colon p \in \mathbb{Z},\ q \in \mathbb{Z},\ q \neq 0 \right\}$$

- **Reali**:

$$\mathbb{R} = \{\text{razionali e irrazionali}\}$$

# Relazione di inclusione

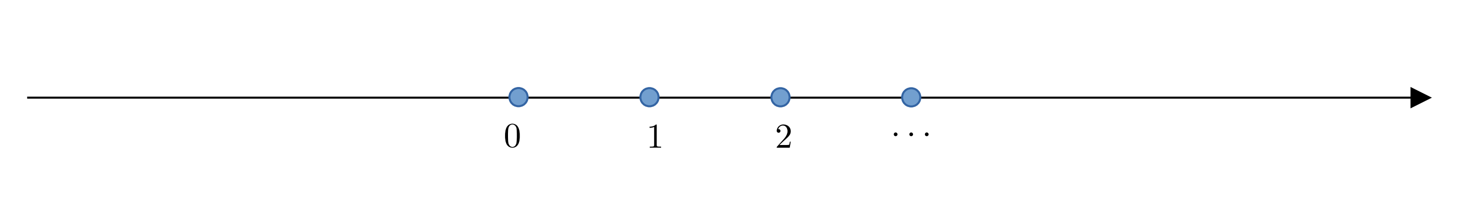



$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

# I numeri naturali

$$\mathbb{N} = \{0,\ 1,\ 2,\ \dots\}$$

- Operazioni ben definite (il risultato sta in $\mathbb{N}$):
  - somma e prodotto
- $\mathbb{N}^+ = \{1,\ 2,\ \dots\} = \{n \in \mathbb{N}\colon\ n > 0\}$
- Ordinamento sulla retta



# Numeri primi

> Un numero naturale viene detto **primo** se è divisibile solo per $1$ e per se stesso (ha solo due divisori distinti)

Ad esempio i primi 10 primi sono:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$$

Ad esempio, $6$ non è primo perché è divisibile per

$$1,\ 2,\ 3,\ 6$$

# Teorema fondamentale dell'aritmetica

> Ogni numero naturale $n$ maggiore di $1$ può essere scritto in modo unico (a parte l'ordine) come prodotto di fattori primi $p_i$ elevati alla potenza $n_i$, i.e.
>
> $$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_i^{n_i} \cdot \ldots \cdot p_k^{n_k}$$

Ad esempio

$$792 = 2^3 \times 3^2 \times 11$$

# Notazione

- "$\times$" e "$\div$" quando si eseguono dei calcoli in aritmetica
- "$\cdot$" o "$/$" in tutti gli altri casi (es. calcolo letterale)

# Criteri di divisibilità

> **Scopo**: aiutano a fattorizzare un numero in fattori primi

# Criteri di divisibilità

> Scopo: aiutano a fattorizzare un numero in fattori primi

- **Divisibile per 2:** ultima cifra decimale è pari (i.e. 0, 2, 4, 6, 8)

Ad esempio sono divisibili per $2$:

$$4,\ 8,\ 44,\ 26,\ 18,\ 10$$

# Criteri di divisibilità

> Scopo: aiutano a fattorizzare un numero in fattori primi

- **divisibile per 3:** somma di tutte le sue cifre è divisibile per 3 e se la somma è maggiore di 9, si esegue nuovamente tale operazione

Ad esempio sono divisibili per $3$:

$$6,\ 9,\ 12,\ 123,\ 111,\ 66$$

# Criteri di divisibilità

> Scopo: aiutano a fattorizzare un numero in fattori primi

- **divisibile per 5:** ultima cifra è 0 oppure 5

Ad esempio sono divisibili per $5$:

$$25,\ 125,\ 625,\ 10,\ 20,\ 100$$

# Criteri di divisibilità

> Scopo: aiutano a fattorizzare un numero in fattori primi

- **divisibile per 10:** ultima cifra è 0

Ad esempio sono divisibili per $10$:

$$10,\ 100,\ 1000,\ 20,\ 30,\ 150$$

# Esempio: fattorizzazione di $792$

- $792$ è pari e quindi divisibile per $2$, i.e. $792 = 2 \times 396$
- $396$ è divisibile per $3$, i.e. $396 = 3 \times 132$
- $132$ è pari e quindi divisibile per $2$, i.e. $132 = 2 \times 66$
- $66$ è divisibile per $3$, i.e. $66 = 3 \times 22$
- $22$ è pari e quindi divisibile per $2$, i.e. $22 = 2 \times 11$
- $11$ è primo

# Esempio: fattorizzazione di $792$

- $792$ è pari e quindi divisibile per $2$, i.e. $792 = 2 \times 396$
- $396$ è divisibile per $3$, i.e. $396 = 3 \times 132$
- $132$ è pari e quindi divisibile per $2$, i.e. $132 = 2 \times 66$
- $66$ è divisibile per $3$, i.e. $66 = 3 \times 22$
- $22$ è pari e quindi divisibile per $2$, i.e. $22 = 2 \times 11$
- $11$ è primo

$$\begin{aligned} 792 &= 2 \times 3 \times 2 \times 3 \times 2 \times 11 \\ &= (2 \times 2 \times 2) \times (3 \times 3) \times 11 \\ &= 2^3 \times 3^2 \times 11 \end{aligned}$$

# Esercizio

> Calcolare il fattorizzazione in numeri primi di $12$, $280$ e $900$

*Soluzione*

- $12 \;=\; 4 \times 3 \;=\; 2^2 \times 3$
- $280 \;=\; 28 \times 10 \;=\; (7 \times 4) \times (5 \times 2) \;=\; 2^3 \times 5 \times 7$
- $900 \;=\; 9 \times 100 \;=\; 9 \times (25 \times 4) \;=\; 2^2 \times 3^2 \times 5^2$

# Due parole sui numeri primi

- Sono infiniti
- Sono usati nella moderna crittografia dove vengono utilizzate come chiavi dei numeri interi la cui fattorizzazione in numeri primi (molto grandi) non sia calcolabile in tempi ragionevoli
- Ipotesi di Riemann: dimostrare se questa congettura è vera oppure no avrebbe implicazioni nella distribuzione dei numeri primi e quindi facilitare il calcolo della fattorizzazione utilizzata negli algoritmi di crittografia
- Il famoso bug nell'unità FPU del Pentium (anno '94) dove il processore matematico restituiva risultati errati in alcuni calcoli in virgola mobile è stato scoperto dal prof. Thomas Nicely durante le sue ricerche sui numeri primi (gemelli) con la divisione

  $$1/824633702441$$

  dove $824633702441$ è un numero primo


FINE
Manolo Venturin (CC BY-NC-ND)