Numeri interi

sabato 14 ottobre 2023 11:16

$\mathbb{Z}$ = {numeri interi}

$\mathbb{N}$ = {numeri naturali}

principio di induzione (prima forma)

Sia $\mathcal{P}$ un'affermazione sui numeri naturali

supponiamo che:

1: passo base) $\mathcal{P}(0)$ è vera;

2: passo induttivo) per ogni numero naturale n, $n>0$, se $\mathcal{P}(n-1)$ è vera, allora $\mathcal{P}(n)$ è vera

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

principio di induzione (seconda forma)

sia $\mathcal{P}$ un'affermazione sui numeri interi e sia $n_0 \in \mathbb{Z}$

supponiamo che:

1: passo base) $\mathcal{P}(n_0)$ è vera;

2: passo induttivo) per ogni numero intero $n>n_0$, se $\mathcal{P}(n-1)$ è vera, allora $\mathcal{P}(n)$ è vera

Allora $\mathcal{P}(n)$ è vera per ogni $n \geq n_0$

es: dimostrare che $0+1+2+3+\ldots+(n-1)+n=\frac{n(n+1)}{2}$

Usiamo il principio di induzione:

$\mathcal{P}(n)$ = "si ha che $0+1+2+\ldots+n=\frac{n(n+1)}{2}$"

- passo base $\mathcal{P}(0)$ = "$0=\frac{0\cdot 1}{2}$" vera
- passo induttivo vogliamo dimostrare che $0+1+2+\ldots+(n-1)+n=\frac{n(n+1)}{2}$ e supponiamo che $\mathcal{P}(n-1)$ è vera, cioè $0+1+2+\ldots+(n-1)=\frac{(n-1)((n-1)+1)}{2}$

  Aggiungendo n si ottiene $0+1+2+\ldots+(n-1)+n=\frac{(n-1)((n-1)+1)}{2}+n=$

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

  Quindi per il principio di induzione $\mathcal{P}(n)$ è vera $\forall n \in \mathbb{N}$

es: dimostrare che per ogni $q \in \mathbb{R}$, $q \neq 1$, $q^0+q^1+q^2+q^3+\ldots+q^n=\frac{1-q^{n+1}}{1-q}$

- passo base $q^0=\frac{1-q}{1-q}$ vera perchè $1=1$
- passo induttivo vogliamo dimostrare che $q^0+q^1+\ldots+q^n=\frac{1-q^{n+1}}{1-q}$. Sappiamo per induzione che $q^0+q^1+q^2+\ldots+q^{n-1}=\frac{1-q^{(n-1)+1}}{1-q}$

  Aggiungiamo ad entrambi $q^n \longrightarrow q^0+q^1+q^2+\ldots+q^{n-1}+q^n=\frac{1-q^{(n-1)+1}}{1-q}+q^n=$

  $=\frac{1-q^n+q^n(1-q)}{1-q}=\frac{1-q^n+q^n(1-q)}{1-q}=\frac{1-q^n+q^n-q^{n+1}}{1-q}=\frac{1-q^{n+1}}{1-q}$

es: dimostrare che $\forall n \geq 2$ intero si ha $(1-1/2)(1-1/3)(1-1/4)\ldots(1-1/n)=1/n$

- passo base dobbiamo provare che l'uguaglianza è vera per $n=2$, cioè che $(1-1/2)=1/2$ vera
- passo induttivo Sappiamo per induzione che $(1-1/2)(1-1/3)\ldots(1-1/n-1)=\frac{1}{n-1}$

  Moltiplico entrambi i membri per $(1-1/n) \longrightarrow (1-1/2)(1-1/3)\ldots(1-1/n-1)(1-1/n)=$

  $=1/n-1(1-1/n)=1/\cancel{n-1}\left(\frac{\cancel{n-1}}{n}\right)=1/n$

  Quindi grazie al principio di induzione, l'uguaglianza è vera $\forall n \geq 2$

principio di induzione (terza forma)

Sia $n_0 \in \mathbb{Z}$ e sia $\mathcal{P}$ un'affermazione sui numeri interi.

Supponiamo che:

1: passo base) $\mathcal{P}(n_0)$ è vera

2: passo induttivo) per ogni intero $n \geq n_0$, se $\mathcal{P}(m)$ è vera per intero m tale che $n_0 \leq m < n$, allora $\mathcal{P}(n)$ è vera

Allora $\mathcal{P}(n)$ è vera per ogni intero $n \geq n_0$

2: passo induttivo) per ogni intero $n \geq n_0$, se $P(m)$ è vera per intero m tale che $n_0 \leq m < n$, allora $P(n)$ è vera

Allora $P(n)$ è vera per ogni intero $n \geq n_0$

principio del minimo

Sia $A \subseteq \mathbb{N}$ non vuoto, allora $\exists K \in A$ tale che $\forall x \in A$

Si ha $x \geq K \longrightarrow$ l'elemento K viene detto minimo

def: siano $a, b \in \mathbb{Z}$. Si dice che a è un divisore di b (o che divide b) se $\exists K \in \mathbb{Z}$ tale che $b = a \cdot K$.

Si dice anche che b è un multiplo di a.

Si indica con $a|b$ (a divide b). Se a non è divisore di b si scrive $a \nmid b$.

es: $3|6$, $-3|6$, $3|-6$, $-3|-6$, $0|0$, $3|0$, $1|3$, $0 \nmid 3$, $3 \nmid 1$

in generale $\forall n \in \mathbb{Z} \setminus \{0\}$ si ha $n|0$, $0 \nmid n$, $1|n$

divisione euclidea

Dati $a, b \in \mathbb{Z}$, $a > 0$, esistono e sono unici $q, r \in \mathbb{Z}$ tali che $0 \leq r < a$ e $b = aq + r$

dim: dobbiamo dimostrare che q, r esistono e sono unici

Distinguiamo due casi:

- Supponiamo prima che $b \geq 0$. Utilizziamo il principio di induzione (terza forma) con $P(b) =$ "$\forall a > 0$ $\exists q, r$ con $0 \leq r < a$ tali che $b = aq + r$"
  - passo base dobbiamo provare che $P(0)$ è vera. Si ha $0 = a \cdot 0 + 0$, quindi basta scegliere $q = r = 0$
  - passo induttivo supponiamo che $P(m)$ sia vera per ogni $m \leq b$ e mostriamo che $P(b+1)$ è vera
    - se $b+1 < a$, allora $b+1 = a \cdot 0 + (b+1)$ e quindi $P(b+1)$ è vera
    - se $b+1 \geq a$, considero $b+1-a \geq 0$. Quindi $P(b+1-a)$ è vera, cioè $\exists q', r' \in \mathbb{Z}$ tali che $b+1-a = aq' + r$ e $0 \leq r' < a$. Allora $b+1 = a(q'+1) + r'$, cioè $P(b+1)$ è vera

  Allora per il principio di induzione $P(b)$ è vera $\forall b \in \mathbb{N}$. Quindi l'esistenza è dimostrata $\forall b \geq 0$
- Se $b < 0$, allora $-b > 0$. Quindi per il caso precedente sappiamo che $\exists q', r' \in \mathbb{Z}$ con $0 \leq r' < a$ e $-b = aq' + r'$; quindi $b = a(-q') - r'$. Se $r' = 0$, allora $-r' = 0$ = se $b = a \cdot (-q') - a + a =$ $= a(-q' - 1) + (a - r')$. Notiamo che $0 < a - r < a$, quindi basta scegliere $q = -q' + 1$ e $r = a - r'$ e otteniamo la tesi.

unicità: supponiamo che esistano $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tali che $0 \leq r_1, r_2 < a$

$b = q_1 \cdot a + r_1 = q_2 \cdot a + r_2$

Supponiamo $r_2 \geq r_1 \longrightarrow a(q_1 - q_2) = r_2 - r_1 \geq 0$ $\quad$ $r_2 - r_1 < a$ perchè $r_1 < a$

$0 \leq a(q_1 - q_2) < a \xrightarrow{a>0} 0 \leq q_1 - q_2 < 1 \longrightarrow q_1 - q_2 = 0 \longrightarrow q_1 = q_2 \longrightarrow r_1 = r_2$

$\square$

es:

- $b = 24$ $\quad a = 13$

  $24 = \underbrace{1}_{q} \cdot \underbrace{13}_{a} + \underbrace{11}_{r}$ $\quad 0 \leq r < a$
- $b = -11$ $\quad a = 5$ $\quad 0 \leq r < 5$

  $-11 = -3 \cdot 5 + 4 \longrightarrow$ divisione euclidea

  $-11 = -2 \cdot 5 - 1 \longrightarrow$ non è una divisione euclidea

def: siano $a, b \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$

1) massimo comune divisore

$MCD(a,b)$ di a e b è il più grande divisore positivo comune di a e b, cioè:

$$MCD(a,b) = \max\{n \in \mathbb{N} : n|a, n|b\}$$

se $MCD(a,b) = 1 \longrightarrow a$ e b si dicono coprimi o primi tra loro

2) minimo comune multiplo

$mcm(a,b)$ di a e b è il più piccolo multiplo positivo comune di a e b, cioè:

$$mcm(a,b) = \min\{n \in \mathbb{N} : a|n, b|n\}$$

mcm(a,b) di a e b è il più piccolo multiplo positivo comune di a e b, cioè:

$mcm(a,b)=\min\{n\in\mathbb{N}: a|n, b|n\}$

es:

$MCD(3,6)=3 \quad mcm(3,6)=6$

$MCD(-3,8)=1 \quad mcm(-3,8)=24$

$MCD(12,8)=4 \quad mcm(12,8)=24$

$$mcm(a,b)=\frac{a\cdot b}{MCD(a,b)} \quad \text{se } a,b>0$$

proprietà:

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

$MCD(a,b)=a \leftrightarrow a|b$

$MCD(a,0)=a$

→ ALGORITMO EUCLIDEO

$a,b\in\mathbb{Z} \quad a>0$

Il massimo comune divisore di a e b si determina con le divisioni euclidee:

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

$a=r_1\cdot q_2+r_2, \quad 0\leq r_1,r_2$

$r_1=r_2\cdot q_3+r_3, \quad 0\leq r_3<r_2$

$\vdots$

$r_{n-2}=r_{n-1}\cdot q_n+r_n$

$r_{n-1}=r_n\cdot q_{n+1}+0$

dove $q_i,r_i\in\mathbb{Z}$ tale che $0<r_n<r_{n-1}<\ldots<r_2<r_1$. In tal caso $MCD(a,b)=r_n\neq0$

es: $MCD(235,100)=5=r_3$

$235=2\cdot\underbrace{100}_{\text{lo divido per 100}}+\underbrace{35}_{\text{resto}}$

$100=2\cdot35+30$

$35=1\cdot30+5$

$30=6\cdot5+0$

$r_1=35$
$r_2=30$
$r_3=5$
$r_4=$ nullo (0)

es: $MCD(963,657)=9$

$963=1\cdot657+306$

$657=2\cdot306+45$

$306=6\cdot45+36$

$45=1\cdot36+9$

$36=4\cdot9+0$

$r_1=306$
$r_2=45$
$r_3=36$
$r_4=9$
$r_5=0$

teorema: IDENTITA' DI BEZOUT

siano $a,b\in\mathbb{Z}$, $(a,b)\neq(0,0)$ e sia $d=MCD(a,b)$ allora $\exists x,y\in\mathbb{Z}$ tali che $ax+by=d$

es:

$a=100, \quad b=235$

$d=MCD(a,b)=5$

bezout $\exists x,y\in\mathbb{Z}$ tale che $5=100x+235y$

come trovo x e y? con l'algoritmo euclideo "a ritroso"

$235=2\cdot100+35$

$100=2\cdot35+30$

$35=1\cdot30+5$

$5=35-1\cdot30=35-1(100-2\cdot35)=35-1\cdot100+2\cdot35=3\cdot35-1\cdot100=$
$=3(235-2\cdot100)-1\cdot100=3\cdot235-6\cdot100-1\cdot100=-7\cdot100+3\cdot235=5$

$5 = 35 - 1 \cdot 30 = 35 - 1(100 - 2 \cdot 35) = 35 - 1 \cdot 100 + 2 \cdot 35 = 3 \cdot 35 - 1 \cdot 100 =$
$= 3(235 - 2 \cdot 100) - 1 \cdot 100 = 3 \cdot 235 - 6 \cdot 100 - 1 \cdot 100 = \underline{-7} \cdot 100 + \underline{3} \cdot 235 = 5$

quindi $x = -7$ e $y = 3$

→ EQUAZIONI DIOFANTEE LINEARI

$a, b, c \in \mathbb{Z}$ soluzioni in $\mathbb{Z}$ $(x, y) \in \mathbb{Z}$

$ax + by = c$

es:

$2x + 3y = 1$

se cerchiamo soluzioni in $\mathbb{R}$

$3y = 1 - 2x$ $y = \frac{1-2x}{3}$

le coppie $(x, \frac{1-2x}{3})$ danno tutte le soluzioni in $\mathbb{R}$ di $2x + 3y = 1$

$(1, \frac{1-2}{3}) = (1, -\frac{1}{3})$

$(0, \frac{1}{3}), (2, \frac{1-4}{3}) = (2, -1)$

le soluzioni in $\mathbb{Z}$ sono più difficili da trovare:

$3x + 6y = 1$ $(x, y) \in \mathbb{Z}^2 \to \mathbb{Z} \times \mathbb{Z}$ entrambi sono in $\mathbb{Z}$

non ha soluzioni in $\mathbb{Z}$ perchè $3x + 6y$ è sempre multiplo di 3

teorema: $a, b, c \in \mathbb{Z}$ allora l'equazione $ax, by = c$ ha soluzioni $x, y \in \mathbb{Z}^2 \longleftrightarrow MCD(a,b) | c$

dim:

- "$\longleftarrow$" sia $d = MCD(a,b)$

  $d | c \to c = \alpha \cdot d$ $\alpha \in \mathbb{Z}$

  bezout: $\exists\, u, v \in \mathbb{Z}$ t.c. $d = au + bv$

  $c = \alpha d = a\underbrace{\alpha u}_{x} + b\underbrace{\alpha v}_{y}$ moltiplicato per α

  scelgo $x = \alpha u$, $y = \alpha v$

  (x, y) è la soluzione

- "$\longrightarrow$" $d = MCD(a,b)$

  tesi $d | c$

  sia $x, y \in \mathbb{Z}$ soluzione di $ax + by = c$

  $d = MCD(a,b) \to d | a \to a = \alpha d$
  $ \to d | b \to b = \beta d$ $\alpha, \beta \in \mathbb{Z}$

  $c = ax + by = \alpha d x + \beta d y = d(\alpha x + \beta y) \to d | c$ □

oss: $ax + by = c$ ha soluzioni $(x, y) \in \mathbb{Z}^2 \longleftrightarrow d = MCD(a,b) | c$

supponiamo ci siano soluzioni

$d | c \to c = \gamma d$
$d | a \to a = \alpha d$ $\alpha, \beta, \gamma \in \mathbb{Z}$
$d | b \to b = \beta d$

1 $\boxed{ax + by = c}$
$\alpha d x + \beta d y = \gamma d$ } dividO per d $\boxed{\alpha x + \beta y = \gamma}$ 2

1 e 2 hanno le stesse soluzioni $\to MCD(\alpha, \beta) = 1$

es:

$42x + 26y = 10$ 1
$21x + 13y = 5$ 2 } $MCD(42, 26) = 2 | 10$

cerchiamo le soluzioni di $21x + 13y = 1$: le troviamo con bezout e algoritmo euclideo

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$1 = 3 - 2 = 3 - (5-3) = 2 \cdot 3 - 5 = 2 \cdot (8-5) - 5 = 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3(13-8) = 5 \cdot 8 - 3 \cdot 13 = 5(21-13) - 3 \cdot 13 =$
$= 5 \cdot 21 - 8 \cdot 13$ $\boxed{1 = 21 \cdot 5 - 13 \cdot 8}$ moltiplico per 5

$5 = 21 \cdot 25 - 13 \cdot 40 = 21 \cdot 25 + 13(-40)$

$x = 25$, $y = -40$ è soluzione di $5 = 21x + 13y$

→ come trovare tutte le soluzioni?

prop: Sia $(x_0, y_0) \in \mathbb{Z}^2$ una soluzione di $ax+by=c$, $a,b,c \in \mathbb{Z}$, $MCD(a,b)=1$
allora tutte le soluzioni di $ax+by=c$ sono:

$$(x,y) = (x_0 + bk, y_0 - ak) \qquad k \in \mathbb{Z}$$

"ricetta" $ax + by = c$ $a,b,c \in \mathbb{Z}$ trovare tutte le soluzioni $(x,y) \in \mathbb{Z}^2$

1) Calcolare $MCD(a,b) = d$, controllare $d|c$
(se $d \nmid c$ non ci sono soluzioni)

2) divido $ax+by=c$ per d, ottengo

$\alpha x + \beta y = \gamma$ con $\alpha, \beta, \gamma \in \mathbb{Z}$ $MCD(\alpha, \beta) = 1$

le soluzioni di $ax+by=c$ e $\alpha x + \beta y = \gamma$ sono le stesse

3) trovo una soluzione $(x_0, y_0) \in \mathbb{Z}^2$ di $\alpha x + \beta y = \gamma$ (ad esempio con bezout)

4) tutte le soluzioni di $\alpha x + \beta y = \gamma$ (e quindi anche quelle di $ax+by=c$) sono

$$\begin{cases} x = x_0 + \beta k \\ y = y_0 - \alpha k \end{cases} \quad k \in \mathbb{Z} \quad \begin{matrix} a = d\alpha \\ b = d\beta \end{matrix}$$

es: $175x + 77y = 329$

1) calcolo $MCD(175, 77) = 7$

$175 = 2 \cdot 77 + 21$
$77 = 3 \cdot 21 + 14$
$21 = 1 \cdot 14 + 7$ → $7 | 329$ ci sono soluzioni
$14 = 2 \cdot 7 + 0$

2) divido per 7

$25x + 11y = 47$

$MCD(25, 11) = 1$

3) troviamo una soluzione $(x_0, y_0) \in \mathbb{Z}^2$ di 2

$\xrightarrow{\text{bezout}} 25 \cdot 4 + 11 \cdot (-9) = 1$

moltiplico per 47

$$25 \cdot \underbrace{(4 \cdot 47)}_{x_0} + 11 \cdot \underbrace{(-9 \cdot 47)}_{y_0} = 47$$

$x_0 = 4 \cdot 47 = 188$
$y_0 = -9 \cdot 47 = -423$ $\qquad 47 = 188 \cdot 25 - 423 \cdot 11$

4) tutte le soluzioni di 1 e 2

$$\begin{cases} x = 188 + 11k \\ y = -423 - 25k \end{cases}$$

→ NUMERI PRIMI

def: un numero intero $a > 1$ si dice numero primo se i suoi soli divisori positivi sono 1 e a.
altrimenti a si dice numero composto
per convenzione 1 e -1 non sono né primi né composti

2, 3, 5, 7, 11, 13, 17, .. sono numeri primi

6 composto $2|6$, $3|6$

$20 = 4 \cdot 5 = 2 \cdot 10 = 2 \cdot 2 \cdot 5$

$2,3,5,7,11,13,17,\dots$ sono numeri primi

6 composto $\quad 2|6\,,\ 3|6$

$20=4\cdot5=2\cdot10=2\cdot2\cdot5$

teorema: sia $a\in\mathbb{Z}\setminus\{-1,0,1\}$ allora a si scrive in modo unico (a meno dell'ordine) come prodotto (finito) di numeri primi

$$\left.\begin{array}{l} a=\pm p_1^{n_1}\cdot\ldots\cdot p_r^{n_r} \\ p_1,\ldots,p_r \to \text{primi} \\ n_1,\ldots,n_r\in\mathbb{Z}_+ \end{array}\right\}\ \text{teorema fondamentale dell'aritmetica}$$

es: $20=2^2\cdot5=2\cdot2\cdot5=5\cdot2^2$

Lemma: $a,b\in\mathbb{Z},\ p$ primo, $p|ab\to p|a$ o $p|b$

dim: supponiamo $p\nmid a$ e mostriamo $p|b$

$p|ab\to ab=kp \quad k\in\mathbb{Z}$

$p\nmid a\to MCD(p,a)=1$

$\xrightarrow{\text{bezout}}\exists x,y\in\mathbb{Z} \quad 1=ax+py$

moltiplico per b $\quad b=abx+pby=kpx+pby=p(kx+by)\longrightarrow p|b\ \square$

dim "esistenza"

possiamo supporre $a>0$ (se a è negativo, consideriamo $-a$)

$\to$ per induzione su $a\geq2$

- passo base $\quad a=2$ primo
- passo induttivo $\quad$ ipotesi: ogni numero $2\leq\alpha\leq a$ si scrive come prodotto di primi

  tesi: $a+1$ si scrive come prodotto di primi

  1) $a+1$ è primo
  2) $a+1$ è composto $\to a+1=b\cdot c$ con $b,c>1\to$

     $2\leq b,c\leq a\xrightarrow{\text{ipotesi}}b=p_1\ldots p_s\quad c=q_1\ldots q_r$

     $p_1,\ldots,p_s,q_1,\ldots,q_r$ primi
     $a+1=p_1,\ldots,p_s,q_1,\ldots,q_r$

unicità

$a=p_1,\ldots,p_s$

$a=q_1,\ldots,q_r \qquad p_i$ e q_i PRIMI $\qquad p_1|q_1\cdot\ldots\cdot q_r\xrightarrow{\text{lemma}}p_1|q_i$ per qualche i

supponiamo $p_1|q_1\longrightarrow p_1=q_1$

$a=p_1\cdot p_2\cdot\ldots\cdot p_s=p_1\cdot q_2\cdot\ldots\cdot q_r\to p_2\cdot\ldots\cdot p_s=q_2\cdot\ldots\cdot q_r\to p_2|q_2\cdot\ldots\cdot q_r$

$\xrightarrow[p_2\text{ primo}]{\text{lemma}}p_2|q_2\xrightarrow{q_2\text{ primo}}p_2=q_2\to\cancel{p_2}\cdot p_3\cdot\ldots\cdot p_s=\cancel{p_2}\cdot q_3\cdot\ldots\cdot q_r$

$\to r=s$ e $p_i=q_i\quad\forall i=1,\ldots,s\ \square$

teorema di euclide: esistono infiniti numeri primi

dim: supponiamo per assurdo che $p_1,\ldots,p_s$ siano tutti e soli i numeri primi

$$N=p_1\cdot\ldots\cdot p_s+1$$

divisione euclidea di N per p_i da resto $1\quad\forall i=1,\ldots,s$

$\to p_i\nmid N\quad\forall 1,\ldots,s\ \lightning\ \square$

es:

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

$(x,y)\mapsto15x+22y$

$f(1,1)=15+22=37$

$f(-1,2)=-15+44=29$

$f(-1,2) = -15+44 = 29$

f INIETTIVA $\leftrightarrow (x_1,y_1),(x_2,y_2)\in\mathbb{Z}^2$ t.c. $f(x_1,y_1)=f(x_2,y_2)\rightarrow(x_1,y_1)=(x_2,y_2)$

$15x_1+22y_1=15x_2+22y_2 \xrightarrow{?} (x_1,y_1)=(x_2,y_2)$

NO $\quad (x_1,y_1)=(0,0) \qquad f(0,0)=0$

$\quad (x_2,y_2)=(22,-15) \qquad f(22,-15)=15\cdot22-15\cdot22=0$

f SURGETTIVA $\leftrightarrow \forall c\in\mathbb{Z} \quad \exists(x,y)\in\mathbb{Z}^2$ t.c. $f(x,y)=c$

$15x+22y=c$ ha soluzione $\leftrightarrow \underbrace{MCD(15,22)}_{=1}\mid c$

si ha sempre soluzioni $\rightarrow f$ suriettiva

→ NUMERI COMPLESSI

- $x-2=0 \qquad x=2 \quad \vee\ \mathbb{N}$
- $x+2=0 \qquad x=-2 \quad \vee\ \mathbb{Z}$
- $2x-3=0 \qquad x=3/2 \quad \vee\ \mathbb{Q}$
- $x^2-2=0 \qquad x=\sqrt{2} \quad \vee\ \mathbb{R}$
- $x^2+2=0$ no soluz in $\mathbb{R}$ $\quad \mathbb{C}$

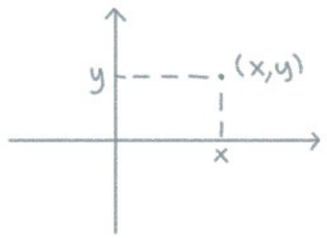
$\mathbb{C}=\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$

denotiamo (x,y) con $x+iy$

$(x+yi)$

$(1,0)=1+0i=1$

$(0,1)=0+1i=i$



somma $\quad (x+iy)+(u+iv)=x+u+i(y+v)$

prodotto $\quad (x+iy)\cdot(u+iv)=(xu-yv)+i(xv+yu)$

$x+iy=z \qquad x,y\in\mathbb{R}$

↪ $x=\mathrm{Re}\,z$ parte reale

$y=\mathrm{Im}\,z$ parte immaginaria

somma:
- commutativa $\qquad z+w=w+z$
- associativa $\qquad z+(w+s)=(z+w)+s \qquad z,w,s\in\mathbb{C}$
- elemento neutro $\qquad (0,0)=0+i0=0 \qquad x+iy+0+i0=x+iy$
- opposto $\qquad x+iy$ è $-x+i(-y) \qquad (x+iy)+(-x+i(-y))=0$

prodotto:
- commutativo $\qquad z\cdot w=w\cdot z$
- associativo $\qquad z(w\cdot s)=(z\cdot w)\cdot s$
- elemento neutro $\qquad 1+0i=1 \qquad (x+iy)(1+0i)=(x\cdot1)-y\cdot0)+i(x\cdot0+y\cdot1)=x+iy$

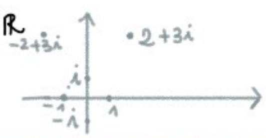
inverso:
$z=x+iy\neq0=0+i0\leftrightarrow(x,y)\neq(0,0)$

$z^{-1}=\frac{1}{z}=\frac{x}{x^2+y^2}+i\,\frac{-y}{x^2+y^2}$

es: $x+iy \quad x,y\in\mathbb{R}$

$2+3i$

$-2+3i$



- I numeri complessi con parte immaginaria zero si identificano con i numeri reali

$x+0i=x \qquad x\in\mathbb{R} \qquad \mathbb{R}\subseteq\mathbb{C} \qquad x\rightarrow x+i0$

- I numeri con parte reale vengono detti immaginari puri

$0+iy=iy \qquad y\in\mathbb{R} \qquad 2i \quad 3i \quad 1i=:i$ unità immaginaria

oss:

• I numeri con parte reale vengono detti immaginari puri

$0+iy=iy \qquad y\in\mathbb{R} \qquad 2i \qquad 3i \qquad 1i=:i$ unità immaginaria

OSS:

$i=(0+i1)$

$i^2=i\cdot i=(0+i1)(0+i1)=(0\cdot 0-1\cdot 1)+i(0\cdot 1+1\cdot 0)=-1+i(0)=-1$

$i^2=-1 \qquad \left.\begin{matrix}x^2=-1\\ x=i\end{matrix}\right\}$ è soluzione

$i^3=i^2\cdot i=-1\cdot i=-i$

$i^4=i^2\cdot i^2=(-1)(-1)=1$

$i^5=i^4\cdot i=1\cdot i=i$

$i^6=-1$

$(x+iy)(u+iv)=xu+xiv+iyu+iy\cdot iv=xu+xiv+iyu+i^2yv=xu+xiv+iyu-yv=$

$=(xu-yv)+i(xv+yu)$

$\mathbb{C}$ numeri complessi $\qquad i^2=-1$

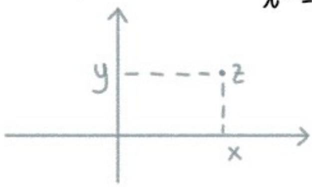
$\cup$

$z=x+iy$

$x,y\in\mathbb{R}$

$x=\mathrm{Re}\, z$

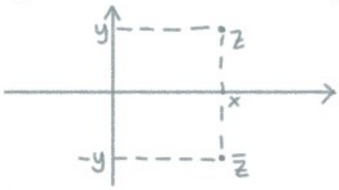
$y=\mathrm{Im}\, z$



• somma $(x+iy)+(u+iv)=(x+u)+i(y+v)$

• prodotto $(x+iy)+(u+iv)=(xu-yv)+i(xv+yu)$

def: $z=x+iy\in\mathbb{C}$ il complesso coniugato di z è $\bar{z}=x-iy$



proprietà: $z,w\in\mathbb{C}$ allora

1) $\overline{zw}=\bar{z}\cdot\bar{w}$

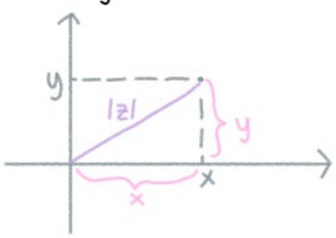
2) $\overline{z+w}=\bar{z}+\bar{w}$

3) $\bar{z}=z \leftrightarrow z\in\mathbb{R}$ (cioè $\mathrm{Im}z=0$)

4) $z+\bar{z}=2\mathrm{Re}(z)$

5) $z-\bar{z}=2\mathrm{Im}(z)$

def: $z=x+iy\in\mathbb{C}$ il modulo di z è $|z|=\sqrt{x^2+y^2}=\sqrt{(\mathrm{Re}z)^2+(\mathrm{Im}z)^2}\in\mathbb{R}$



[il modulo è la distanza di z dall'origine]

proprietà: $z,w\in\mathbb{C}$ allora

1) $z\cdot\bar{z}=|z|^2$

2) $|zw|=|z||w|$

3) $|z+w|\leqslant|z|+|w|$ disuguaglianza triangolare

4) se $z\neq 0$, allora $\frac{1}{z}=\frac{\bar{z}}{|z|^2}$

dim:

1) $z=x+iy \qquad x,y\in\mathbb{R}$

$z\cdot\bar{z}=(x+iy)(x-iy)=x^2-iyx+iyx-i^2y^2=x^2+y^2=(\sqrt{x^2+y^2})^2=|z|^2$

1) $z = x + iy \qquad x, y \in \mathbb{R}$

$z \cdot \bar{z} = (x+iy)(x-iy) = x^2 - iyx + iyx - i^2 y^2 = x^2 + y^2 = (\sqrt{x^2+y^2})^2 = |z|^2$

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

2) $|zw| = |z||w|$

$\updownarrow \longrightarrow$ vero perchè $|z|, |w|, |zw| \geq 0$

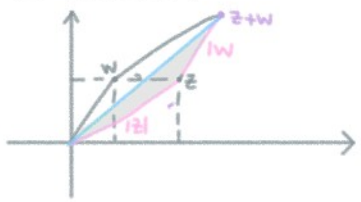
$|zw|^2 = |z|^2 |w|^2$

$z = x + iy \qquad w = u + iv$

$|zw|^2 = |(xu - yv) + i(xv + yu)|^2 = (xu - yv)^2 + (xv + yu)^2 = x^2u^2 + y^2v^2 \cancel{-2xuyv} + x^2v^2 + y^2u^2 \cancel{+2xvyu} =$

$= (x^2 + y^2)(u^2 + v^2) = |z|^2 |w|^2$

3) $|z + w| \leq |z| + |w|$

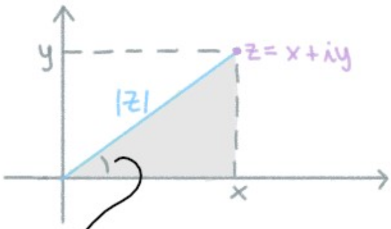


$|z+w|$ = diagonale del parallelogramma

= lato del triangolo $\widehat{0z\ z{+}w} \leq |z| + |w|$

4) $\frac{1}{z} = \left(\frac{x}{x^2+y^2}\right) + i\left(\frac{-y}{x^2+y^2}\right) = \frac{x - iy}{x^2+y^2} = \frac{\bar{z}}{|z|^2} \quad \square$

→ FORMA TRIGONOMETRICA E ESPONENZIALE



$z \neq 0$

$|z| = z^2 + y$

↳ argomento di z $\arg(z)$ è l'angolo compreso tra l'asse x e $|z|$

$\vartheta = \arg z \qquad x = |z| \cos\vartheta$

$\qquad\qquad\qquad y = |z| \sin\vartheta$

$\boxed{\begin{array}{l} \operatorname{Re} z = |z| \cos(\arg(z)) \\ \operatorname{Im} z = |z| \sin(\arg(z)) \end{array}} \qquad z = \operatorname{Re} z + i \operatorname{Im} z$

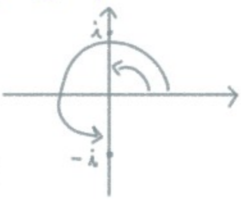
$z = |z| \left(\cos(\arg(z)) + i \sin(\arg(z))\right) \longrightarrow$ forma trigonometrica

$0 \leq \arg z < 2\pi$

$\arg(3) = 0$

$\arg(i) = \frac{\pi}{2}$

$\arg(-i) = \frac{3}{2}\pi \left(= -\frac{\pi}{2}\right)$



$|i| = |0 + i \cdot 1| = \sqrt{\operatorname{Re}(i)^2 + \operatorname{Im}(i)^2} = \sqrt{0^2 + 1^2} = \sqrt{1} = 1$

$\operatorname{Re}(i) = 0 \qquad \operatorname{Im}(i) = 1$

$z = |z| \cdot e^{i\arg(z)}$ forma esponenziale

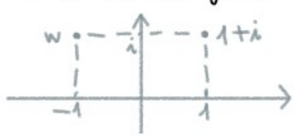
$e^{i\arg(z)} := \left(\cos(\arg(z)) + i \sin(\arg(z))\right)$

es:

$z = 1 + i \longrightarrow$ forma trigonometrica

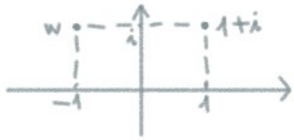
$|z| = \sqrt{1^2 + 1^2} = \sqrt{2}$

$\begin{array}{l} \operatorname{Re} z = |z| \cos(\arg(z)) \\ \operatorname{Im} z = |z| \sin(\arg(z)) \end{array} \longrightarrow \begin{cases} \cos(\arg(z)) = \frac{1}{\sqrt{2}} \\ \sin(\arg(z)) = \frac{1}{\sqrt{2}} \end{cases}$



$\arg(z) = \frac{\pi}{4}$

$z = \sqrt{2}\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right) = \sqrt{2}\, e^{i\frac{\pi}{4}}$



$\arg(z) = \frac{\pi}{4}$

$z = \sqrt{2}\,(\cos\frac{\pi}{4} + i\,\sin\frac{\pi}{4}) = \sqrt{2}\,e^{i\frac{\pi}{4}}$

$w = -1 + i$

$|w| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}$

$\operatorname{Re} w = \cos(\arg(w))$

$\operatorname{Im} w = \sin(\arg(w))$ $\qquad \arg(w) = \frac{3}{4}\pi$

$w = \sqrt{2}\,(\cos(\frac{3}{4}\pi) + i\,\sin(\frac{3}{4}\pi)) = \sqrt{2}\,e^{i\frac{3}{4}\pi}$

teorema: $z, w \in \mathbb{C} \quad z, w \neq 0$

$|zw| = |z| \cdot |w| \quad \arg(z \cdot w) = \arg(z) + \arg(w)$

$z \cdot w = |z||w|\,(\cos(\arg(z)) + \arg(w) + i\,(\sin(\arg(z) + \arg(w)))$

$z \cdot w = |z||w|\,e^{i(\arg(z) + \arg(w))}$

es: $z = 1 + i \qquad w = -1 + i$

$z \cdot w = ?$

$|z \cdot w| = |z||w| = \sqrt{2} \cdot \sqrt{2} = 2$

$\arg(z \cdot w) = \arg(z) + \arg(w) = \frac{\pi}{4} + \frac{3}{4}\pi = \pi$

$z \cdot w = 2\,(\cos(\pi) + i\,\sin(\pi)) = 2\,(-1 + 0i) = -2$

$z \cdot w = \sqrt{2}\,e^{i\frac{\pi}{4}} \cdot \sqrt{2}\,e^{i\frac{3}{4}\pi} = \sqrt{2}\sqrt{2}\,e^{i(\frac{\pi}{4} + \frac{3}{4}\pi)} = 2e^{i\pi}$

cor:
$$\left.\begin{array}{l} z \in \mathbb{C},\ z \neq 0,\ n \in \mathbb{N}_+ \\ |z^n| = |z|^n \quad \arg(z^n) = n \arg(z) \\ z^n = (|z|e^{i\arg(z)})^n = |z|^n e^{ni\arg(z)} \end{array}\right\} \text{de moivre}$$

es: $z = 1 + i = \sqrt{2}\,e^{i\frac{\pi}{4}}$ $\qquad z^{140} = (\sqrt{2})^{140}\,e^{i\,140\frac{\pi}{4}} = 2^{70}e^{i35\pi} = 2^{70}e^{i\pi} = -2^{70}$

$\arg(z^{140}) = 35\pi = 34\pi + \pi = 17(2\pi) + \pi = \pi$

→ RADICI N-ESIME COMPLESSE

$x^2 = -1 \begin{cases} x = i \\ x = -i \end{cases}$ $\qquad x^2 = $ negativo

$\qquad x^n = $ negativo n pari

def: $n \in \mathbb{N}, n \geq 1, \alpha \in \mathbb{R}, \alpha \neq 0$ la radice n-esima reale di α è:

1) se n è dispari, l'unico $x \in \mathbb{R}$ t.c. $x^n = \alpha$
2) se n è pari, $\alpha > 0$, l'unico $x \in \mathbb{R}$, $x > 0$ t.c. $x^n = \alpha$
3) se n è pari $\alpha < 0$, non esiste

se esiste denotiamo la radice n-esima di α con $\sqrt[n]{\alpha}$

es: $\sqrt[3]{8} = 2 \qquad \sqrt[3]{-8} = -2$

$\sqrt[4]{16} = 2 \qquad 2^4 = 16 \qquad (-2)^4 = 16$

se n pari $(\sqrt[n]{\alpha})^n = (-\sqrt[n]{\alpha})^n = \alpha$

$\sqrt[4]{-16}$ non esiste

teorema: $z \in \mathbb{C}, z \neq 0, n \in \mathbb{N}_+$

le soluzioni in $\mathbb{C}$ dell'equazione $x^n = z$ sono n numeri complessi $z_0, z_1, \dots, z_{n-1}$ distinti

dati da $z = \sqrt[n]{|z|}\left(\cos\left(\frac{\arg(z) + 2k\pi}{n}\right) + i\,\sin\left(\frac{\arg(z) + 2k\pi}{n}\right)\right)$

$k = 0, 1, \dots, n-1$

$z_0, z_1, \dots, z_{n-1}$ sono le radici n-esime complesse di z se $z = 0$, $x^n = 0$ ha solo soluzione $x = 0$

es:

$z_0, z_1, \dots, z_{n-1}$ sono le radici n-esime complesse di z se $z=0$, $x^n=0$ ha solo soluzione $x=0$

es: le radici cubiche di $z=-8$ $(n=3)$

$|z| = |-8| = \sqrt{(-8)^2+0^2} = \sqrt{8^2} = 8$

$\arg(-8) = \pi \longrightarrow$

$$\begin{cases} -8 = |z| \cos(\arg(z)) \\ 0 = |z| \sin(\arg(z)) \end{cases}$$

$-8 = 8\cos(\dots)$ $\quad \begin{cases} \cos(\arg(z)) = -1 \\ \sin(\arg(z)) = 0 \end{cases}$

$0 = 8\sin(\dots)$

3 radici z_0, z_1, z_2 $\quad \sqrt[3]{|z|} = \sqrt[3]{8} = 2$

- $z_0 = 2\left(\cos\left(\frac{\pi}{3}\right) + i \sin\left(\frac{\pi}{3}\right)\right)$
- $z_1 = 2\left(\cos\left(\frac{\pi+2\pi}{3}\right) + i \sin\left(\frac{\pi+2\pi}{3}\right)\right) = 2(\cos\pi + i\sin\pi)$
- $z_2 = 2\left(\cos\left(\frac{\pi+4\pi}{3}\right) + i \sin\left(\frac{\pi+4\pi}{3}\right)\right) = 2\left(\cos\left(\frac{5}{3}\pi\right) + i \sin\left(\frac{5}{3}\pi\right)\right)$

$z \in \mathbb{C}, z \neq 0 \qquad n \in \mathbb{N}_+$

z ha n radici complesse n-esime: $z_0, z_1, \dots, z_{n-1}$

$$z_k = \sqrt[n]{|z|}\left(\cos\left(\frac{\arg(z)+2k\pi}{n}\right) + i \sin\left(\frac{\arg(z)+2k\pi}{n}\right)\right)$$

$k = 0, \dots, n-1$

oss: le radici n-esime hanno lo stesso modulo $\sqrt[n]{|z|}$ si dispongono su una circonferenza di raggio $\sqrt[n]{|z|}$

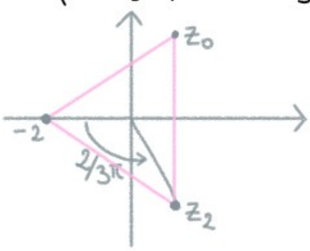
La differenza tra gli argomenti di due radici z_k e z_{k-1} è sempre $\boxed{\frac{2\pi}{n}}$

$\rightarrow z_0, \dots, z_{n-1}$ sono i vertici di un poligono regolare di n lati

es: $z = -8 \rightarrow z_0 = (\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) = 2\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 1 + \sqrt{3}i$

$z_1 = 2(\cos\pi + i\sin\pi) = -2$

$z_2 = 2\left(\cos\left(\frac{5}{3}\pi\right) + i\sin\left(\frac{5}{3}\pi\right)\right) = 2\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 1 - \sqrt{3}i$



$|z_k| = 2$

triangolo equilatero inscritto in una circonferenza di raggio

es: $z = 1 \quad n=4$ radici quadrate di 1 (radici dell'unità) $\quad (z_k)^4 = 1$

$|1| = 1 \quad \arg(1) = 0 \qquad k = 0,1,2,3$

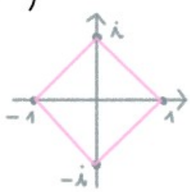
$z_k = \sqrt[4]{1}\left(\cos\left(\frac{0+2k\pi}{4}\right) + i\sin\left(\frac{0+2k\pi}{4}\right)\right)$

$z_0 = \cos 0 + i \sin 0 = 1$

$z_1 = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i$

$z_2 = \cos\pi + i\sin\pi = -1$

$z_3 = \cos\left(\frac{3}{2}\pi\right) + i\sin\left(\frac{3}{2}\pi\right) = -i$



quadrato inscritto in una circonferenza di raggio 1

sappiamo trovare le soluzioni di equazioni del tipo

$x^n - \alpha = 0 \quad \forall \alpha \in \mathbb{C} \quad \forall n \in \mathbb{N}$

$x^2 - \alpha = 0$

$x^2 + ax + b = 0$

prop: ogni equazione $ax^2+bx+c=0$ con $a,b,c \in \mathbb{C}$ ha soluzioni in $\mathbb{C}$

dim:

prop: ogni equazione $ax^2+bx+c=0$ con $a,b,c \in \mathbb{C}$ ha soluzioni in $\mathbb{C}$

dim: $ax^2+bx+c=0$ supponiamo $a \neq 0$

moltiplichiamo per $4a \neq 0$

$4a^2x^2+4abx+4ac=0$

aggiungo e tolgo b^2

$4a^2x^2+4abx+4ac+b^2-b^2=0$

$\underbrace{4a^2x^2+4abx+b^2}_{(2ax+b)^2} = b^2-4ac =: \Delta$

$\boxed{\mathcal{X}^2=\Delta}$

$\exists\ \delta_1, \delta_2 \in \mathbb{C}$ soluzioni di $\mathcal{X}^2=\Delta$

cioè $\delta_1^2=\delta_2^2=\Delta$

$\boxed{\begin{array}{ll} \text{se } \Delta=0 & \delta_1=\delta_2=0 \\ \text{se } \Delta\neq 0 & \delta_1\neq\delta_2 \end{array}}$

$(2ax+b)^2=(\delta_1)^2=(\delta_2)^2$

$2ax+b=\begin{cases}\delta_1\\ \delta_2\end{cases}$

$2ax+b=\delta_1 \to x=\dfrac{-b+\delta_1}{2a}$

$2ax+b=\delta_2 \to x=\dfrac{-b+\delta_2}{2a}$

$\square$

es: $x^2+4x+5=0$ $\quad \Delta=b^2-4ac=4^2-4\cdot 5=16-20=-4$

$\delta_1,\delta_2\in\mathbb{C}$ t.c. $\delta_1^2=\delta_2^2=-4$

$\delta_1=2i \qquad \delta_2=-2i$

$|-4|=4$, $\arg(-4)=\pi$

$z_k=\sqrt[2]{|-4|}\left(\cos\left(\frac{\pi+2k\pi}{2}\right)+i\sin\left(\frac{\pi+2k\pi}{2}\right)\right) \qquad k=0,1$

$\delta_1=2\left(\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}\right)=2(0+i)=2i$

$\delta_2=2\left(\cos\left(\frac{3}{2}\pi\right)+i\sin\left(\frac{3}{2}\pi\right)\right)=2(0-i)=-2i$

$x_1=\dfrac{-b+\delta_1}{2}=\dfrac{-4+2i}{2}=-2+i$

$x_2=\dfrac{-b+\delta_2}{2}=\dfrac{-4-2i}{2}=-2-i$

→ TEOREMA FONDAMENTALE DELL'ALGEBRA

Sia $p(x)=a_nx^2+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$

$n\in\mathbb{N}_+$, $a_0,\ldots,a_n\in\mathbb{C}$, $a_n\neq 0$

Allora $p(x)=0$ ha n soluzioni (contate con molteplicità), cioè $p(x)=a_n(x-w_1)^{m_1},\ldots,(x-w_r)^r$

$m_1,\ldots,m_r\in\mathbb{N}$, $w_1,\ldots,w_r\in\mathbb{C}$ soluzioni o radici

m_j è detto molteplicità di w_j

$m_1+\ldots+m_r=n$

es: $x^2+4x+5=0$

$w_1=-2+i \qquad w_2=-2-i$

$x^2+4x-5=(x-w_1)(x-w_2)=(x-(-2+i))(x-(-2-i))$

$m_1=1$ molt di w_1

$m_2=1$ molt di w_2

es: $x^2-2x+1=(x-1)^2$

$\Delta=0 \qquad w_1=1 \qquad m_1=2$