

Teorema: (algoritmo delle divisioni successive)

✓ coppia di interi $a, b \in \mathbb{Z}$
non nulli, esiste un massimo
comune divisore d
ed esiste $x, y \in \mathbb{Z}$ t.c.

$$d = ax + by$$

dimostrazione:

Assumiamo $a > 0$ $b > 0$, $a > b$

Passo 0) $a_0 := a$, $b_0 := b$

Passo 1) $\exists q_1, r_1$ t.c. $a_0 = q_1 b_0 + r_1$ e
 $0 \leq r_1 < b_0$

Se $r_1 = 0$ TERMINA

Altrimenti
↓

Passo 2) $a_1 := b_0$ $b_1 := r_1$

$\exists q_2, r_2$ t.c. $a_1 = q_2 b_1 + r_2$ e
 $0 \leq r_2 < b_1$

Se $r_2 = 0$ TERMINA

Altrimenti
↓

Passo 3) $a_2 := b_1$ $b_2 := r_2$. . .

Passo i) $a_{i-1} := b_{i-2}$ $b_{i-1} := r_{i-1}$

→ L'algoritmo termina

Se r_n è il primo resto nullo

$$\Rightarrow r_{n-1} = \text{MCD}(a, b)$$

Oss: L'algoritmo produce anche x e y .

Suppongo $r_3 = 0 \Rightarrow a_2 = b_1 \quad b_2 = r_2$

↓

$$a_{i-1} = b_{i-1} q_i + r_i$$

r_2 è tale che $a_1 = b_1 q_2 + r_2$

$$a_1 = b_0 \quad b_1 = r_1$$

r_1 è tale che $a_0 = b_0 q_1 + r_1$
"a" "b"

$$r_1 = a - b q_1$$

$$r_2 = a_1 - b_1 q_2 \quad a_1 = b_0 \quad b_1 = r_1$$

$$r_2 = b - (a - b q_1) \cdot q_2$$

$$r_2 = b - a q_2 + b q_1 q_2$$

$$r_2 = a(-q_2) + b(1 + q_1 q_2)$$

$$r_2 = ax + by$$

— PRIMI IRRIDUCIBILI, TEOREMI DI FATTORIZZAZIONE UNICA —

Def: Un numero $p \in \mathbb{Z}$ $p \neq 0, \pm 1$ si dice **PRIMO** se:

$$p \mid a \cdot b \Rightarrow p \mid a \text{ oppure } p \mid b$$

(cioè se p divide il prodotto di 2 numeri
 \Rightarrow divide almeno uno dei due fattori)

Oss: In un anello $(A, +, \cdot)$ dico che $p \mid a$ se
 $\exists b \in A \mid a \cdot b = p$

0 è il neutro di $+$

1 è il neutro di \cdot , -1 è il suo opposto

10 non è primo perché

$$10 \mid 15 \cdot 4 (=60) \text{ ma } 10 \nmid 15 \text{ e } 10 \nmid 4$$

Def: $z \in \mathbb{Z}$ $z \neq 0, \pm 1$ si dice **IRRIDUCIBILE** se
è divisibile solo per $\pm 1, \pm z$

Oss: In un anello z è divisibile per a se
 $\exists b$ t.c. $z = a \cdot b$ (cioè $a \mid z$)

Oss: Se $z \in \mathbb{N}$ non è divisibile per nessun $n \in \mathbb{N}$
t.c. $1 < n \leq \frac{z}{2} \Rightarrow z$ è IRRIDUCIBILE

(per assurdo)

Se $z = a \cdot b$ $a \neq 1, b \neq 1$ mostriamo che

$$a \leq \frac{z}{2} \text{ oppure } b \leq \frac{z}{2}$$

per assurdo $a > \frac{z}{2}, b > \frac{z}{2}$

Se $z=1 \leadsto$ non faccio niente

$z=2 \leadsto$ è irriducibile

$z=3 \leadsto z$ non è divisibile per 2
 $\leadsto 3$ è irriducibile

\Rightarrow assumo $z \geq 4 \leadsto 4 \leq z \quad \frac{4}{2} \leq \frac{z}{2}$

$$a > \frac{z}{2} \quad 2 \leq \frac{z}{2} < b$$

$$a > \frac{z}{2} \quad b > 2$$

$\Rightarrow a \cdot b > \frac{z}{2} \cdot 2 = z$ ASSURDO (perché $z = a \cdot b$)

Oss: Se $z \in \mathbb{N}$ non è divisibile per nessun n
t.c. $1 < n \leq \sqrt{z} \Rightarrow z$ è irriducibile

Oss: $z \in \mathbb{Z}$, z è irriducibile in $\mathbb{Z} \Leftrightarrow |z|$ è
irriducibile in \mathbb{N}

Teorema: $p \in \mathbb{Z}$, $p \neq 0$, $\pm 1 \Rightarrow p$ è primo \Leftrightarrow
 p è irriducibile

dim \Rightarrow) p è primo \Rightarrow è irriducibile

Sia δ un divisore di p ($\delta | p$)

Voglio mostrare che δ è $\pm 1, \pm p$

$$\delta | p \Rightarrow \exists q | p = \delta p$$

$$p | p \Rightarrow p | \delta p \text{ poiché } p \text{ è primo}$$

$$\text{oppure } p | \delta \text{ oppure } p | q$$

se $p \mid \delta$ ma ho $\delta \mid p$ e $p \mid \delta = \pm p = \delta$

se $p \mid q$ e $p = \delta q \Rightarrow q \mid p \Rightarrow q = \pm p$

$\Rightarrow \delta = \pm 1$

dim \Leftarrow) se p è irriducibile \Rightarrow è primo

$p \mid ab$ (voglio mostrare che $p \mid a$ o $p \mid b$)

Suppongo $p \nmid a$ (voglio mostrare $p \mid b$)

Considero $d = \text{MCD}(p, a)$ ($d \mid p, d \mid a$)

$d \mid p$ ma p è irriducibile $\Rightarrow d = \pm 1$

o $d = \pm p$

se $p = \pm d$ ho assurdo perché

\downarrow
 $d \mid a \Rightarrow p \mid a$

$\Rightarrow d = \pm 1$ $1 = \text{MCD}(p, a)$

$\Rightarrow \exists x, y$ t.c. $1 = px + ya$

moltiplico per b $b = xpb + yab$

$p \mid ab$ $\exists k$ t.c. $kp = ab$ \uparrow

$b = xpb + ykp \Rightarrow b = p(xb + yk) \Rightarrow p \mid b$

TEOREMA FONDAMENTALE ARITMETICA

(o fattorizzazione essenzialmente unica)

Ogni $n \in \mathbb{Z} - \{0, 1, -1\}$ può essere scritto come prodotto di $s \geq 1$ numeri primi (= irriducibili) non necessariamente distinti, (oss: ± 1 non sono irriducibili)

Questa scrittura è essenzialmente unica

$n = p_1 \cdot p_2 \cdot \dots \cdot p_s$, $n = q_1 \cdot q_2 \cdot \dots \cdot q_t$ con p_i, q_j primi $\Rightarrow s = t$ a meno di riordinare i fattori $p_i = \pm q_j$

Oss: raccogliendo i fattori con lo stesso valore assoluto ho:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \quad \text{con } p_i \neq p_j \quad i \neq j$$

Def: se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$ chiamo α_i MOLTIPLICITÀ di p_i come fattore di n

Oss: La decomposizione in numeri primi ci permette di trovare tutti i possibili divisori

In particolare se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \Rightarrow$
 n ha $(\alpha_1+1)(\alpha_2+1) \dots (\alpha_r+1)$ divisori positivi

$$\text{es } 24 = 2^3 \cdot 3 \quad \alpha_1 = 3 \quad \alpha_2 = 1$$

$$\Rightarrow \text{ci aspettiamo } (3+1)(1+1) = 8 \text{ divisori}$$

divisori di 24: $(1, 2, 3, 2 \cdot 2, 2 \cdot 3, 2 \cdot 2 \cdot 2, 2 \cdot 2 \cdot 3, 2 \cdot 2 \cdot 2 \cdot 3) = \textcircled{8}$

Teorema: L'insieme dei numeri primi è infinito

dim: Per assurdo $P = \{ \text{insieme dei num. primi} \}$
 $P = \{ p_1, p_2, \dots, p_n \} \quad p_1 < p_2 < p_3 < \dots < p_n$

Max $P = p_n \rightarrow$ è il numero primo più grande

Considero $k = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_{n+1}$

$$k > p_n$$

Mostro che k non si divide per nessun numero primo, ma allora è primo

$$\begin{aligned} [k]_{p_1} &= [p_1 p_2 \dots p_{n+1}]_{p_1} = \\ &\stackrel{\text{in } \mathbb{Z}_{p_1}}{=} \underbrace{[p_1]_{p_1} [p_2]_{p_1} \dots [p_n]_{p_1}}_{=0} + [1]_{p_1} \\ &= 0 \quad = [1]_{p_1} \end{aligned}$$

$\Rightarrow k$ non si divide per p_1

k è primo e $k >$ del più grande dei numeri primi \rightarrow assurdo

Teorema: $(\mathbb{Z}_n, +, \cdot)$ è campo $\Leftrightarrow n$ è primo

dim: \Leftarrow)

Se n è primo $\Rightarrow (\mathbb{Z}_n, +, \cdot)$ è campo

$(\mathbb{Z}_n, +, \cdot)$ è anello, per dire che è campo basta mostrare che:

$$\forall [b]_n \in \mathbb{Z}_n \quad [b]_n \neq [0]_n$$

$$\exists [c]_n \text{ t.c. } [b]_n [c]_n = [1]_n$$

$$n \text{ è primo} \Rightarrow \forall 1 \leq a < n$$

$$\text{MCD}(a, n) = 1$$

In particolare considero $[b]_n$

$$1 \leq b < n \quad \text{MCD}(b, n) = 1$$

$$\Rightarrow x, y \in \mathbb{Z} \text{ t.c. } 1 = bx + ny$$

$$\Rightarrow [1]_n = [bx + ny]_n$$

$$[1]_n = [b]_n [x]_n + \underbrace{[n]_n [y]_n}_{=0}$$

$$\Rightarrow [x]_n \text{ è } \text{INVERSO} \text{ di } [b]_n$$

$$\text{pongo } [c]_n = [x]_n$$

dim: \Rightarrow) $(\mathbb{Z}_n, +, \cdot)$ è campo $\Rightarrow n$ è primo

Per assurdo se $n = ab$ $\underbrace{a \neq n, b \neq n}$

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

$$[a] \neq 0 \quad [b] \neq 0$$

$$\downarrow \\ = [n]_n = [0]_n$$

$\Rightarrow [a]_n, [b]_n$ sono divisori dello zero,

assurdo!

Qss: In un campo non ci sono divisori dello zero

Mostro che in un campo non ci sono divisori dello zero

Sia K un campo ($x \neq 0$)

Suppongo che $xy = 0$ (mostro che allora $y = 0$ è zero ho mostrato che x non è divisore di zero)

$$y = 1 \cdot y = \underbrace{x^{-1}x}_{//} \cdot y = x^{-1}(xy) = x^{-1} \cdot 0 = \underline{\underline{0}}$$

x è campo $\exists x^{-1}$ t.c. $x^{-1}x = 1$

Def: Un polinomio $a(x) \in \mathbb{R}[x]$ con $\deg a(x) \geq 1$ si dice **RIDUCIBILE** se:

$$\begin{aligned} \exists p(x), q(x) \text{ con } 1 \leq \deg p(x) < \deg a(x) \\ 1 \leq \deg q(x) < \deg a(x) \\ \text{t.c. } a(x) = p(x) \cdot q(x) \end{aligned}$$

Altrimenti diciamo che $a(x)$ è irriducibile

Les •) I polinomi di grado 1 sono irriducibili

•) $x^2 + 1$ è irriducibile in $\mathbb{R}[x]$

↳ uso Ruffini (?)

Ricordo che $(x - \xi) \mid q(x) \Leftrightarrow q(\xi) = 0$

•) Un polinomio reale di grado > 2

è sempre riducibile, ma può non avere radici (la radice di un polinomio $p(x)$ è ξ t.c. $p(\xi) = 0$)

$(x^2+1)(x^2+2)$ non ha radici, ma è
riducibile

Teorema: (Fattorizzazione essenzialmente unica)

Ogni polinomio $a(x) \in \mathbb{R}[x]$ di
grado $n \geq 1$, può essere scritto come
prodotto di $s \geq 1$ polinomi irriducibili
(non necessariamente distinti)

cioè:

$$a(x) = p_1(x) p_2(x) \dots p_s(x)$$

p_i irriducibile
 $\deg p_i \geq 1$

Questa fattorizzazione è
essenzialmente unica se:

$$a(x) = q_1(x) q_2(x) \dots q_r(x)$$

q_i irriducibile
 $\deg q_i \geq 1$

$\Rightarrow s = r$ e a meno di riordinarli q_i

si ha $p_i(x) = k q_i(x) \quad k \in \mathbb{R}$

$$\begin{aligned} (3x+1)(x+2) &= 3x^2+7x+2 = (x+\frac{1}{3})(3x+6) = \\ &= 3(x+\frac{1}{3})(x+2) \end{aligned}$$

Def: Un polinomio è detto **MONICO** se $\deg a(x) = n$
 $a(x) = a_n x^n + \dots$ e $a_n = 1$