

Struttura degli interi

* Primi e irriducibili

* Fattorizzazione unica

Def(Primo) Un numero $p \geq 2$

è primo se il fatto
che $p | ab$ implica che
 $p | a$ oppure $p | b$.

Esempio: 6 non è primo perché $6 | 2 \cdot 3 = 6$
ma $6 \nmid 2$ e $6 \nmid 3$

Def(Irriducibile) Un numero $p \in \mathbb{N}$

è irriducibile se il fatto
che $d | p$ implica $\underline{d=1} \circ \underline{p}$



$$p = ad$$

Lemma: Vale la seguente proprietà
 $p \geq 2$ e' primo \Leftrightarrow e' irriducibile.

Dim. ($\text{primo} \Rightarrow \text{irriducibile}$)

Assumiamo p primo

Supponiamo di spezzarlo come
un prodotto $p = ab$

Siccome $p | p = ab$ e p e' primo
necessariamente $p | a$ oppure $p | b$

A meno di riordinare i fattori
possiamo assumere $p | a \Rightarrow a = pq$

$$\begin{aligned} p = ab &\Rightarrow p = p(bq) \\ &= (pq)b && \Rightarrow bq = 1 \\ &&& \Rightarrow b = q = 1 \end{aligned}$$

$$\Rightarrow \begin{cases} a = pq = p \\ b = 1 \end{cases}$$

cioè p e' irriducibile \square

(irriducibile \Rightarrow primo)

Assumiamo che p sia irriducibile

Supponiamo che $p \mid ab$

Vogliamo far vedere che $p \mid a$
oppure $p \mid b$. Due casi: $p \mid a \Rightarrow$ OK
 $p \nmid a$

Supponiamo $p \nmid a$

OssFond: $\text{mcd}(p, a) = 1$

Dim OssFond: $\text{mcd}(p, a) \mid p$

Siccome p è irriducibile

necessariamente $\text{mcd}(p, a) = 1$ oppure p

pero' $\text{mcd}(p, a) \mid a$ e abbiamo

assunto $p \nmid a \Rightarrow$ l'unica

possibilità e' che $\text{mcd}(p, a) = 1$

A

Utilizziamo ora Bezout che
ci dice che $\exists x, y \in \mathbb{Z}$ t.c.

$$1 = \text{mcd}(a, p) = ax + py \quad | \text{Bezout}$$

$$\Rightarrow b = abx + bpY$$

\uparrow
 \uparrow
 multiplo di p (ricordiamo
 $p \nmid ab$)

multiplo di p

$\Rightarrow p \mid b$ come volevamo dim.
 \square

Teorema: Esistono infiniti numeri primi.

Dim. Supponiamo non sia vero
 \Rightarrow possiamo elencare i primi in ordine crescente come

$$p_1 < p_2 < \dots < p_N$$

Consideriamo

n = p_1 \cdots p_N + 1

Oss: $p_j \nmid n \forall j$

(la divisione con resto
da sempre 1)

$\Rightarrow n$ e' esso stesso

un numero primo oppure

lo possiamo scrivere

come prodotto di primi

che non compaiono nella

lista!

Questo e' assurdo

\Rightarrow L'ipotesi iniziale e' falsa

Cioe' $\exists \infty$ primi. $\cancel{\exists}$

Domanda: Perche' ogni numero
naturale si puo' scrivere
come un prodotto di primi?

Teorema Fattorizzazione Unica:

Ogni $n \in \mathbb{N}$ con $n > 1$
si scrive in modo unico
(a meno di riordino dei
fattori) come

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

dove p_j è primo $\forall j$
 $e_j \geq 1 \quad \forall j$.

Dim. Procediamo per induzione

Dobbiamo mostrare due cose:

① Esistenza di una decomposizione

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

② Unicità della decomposizione

Dim ① per induzione.

Caso base $n=2$ OK perché $n=2$
e' primo

Caso induttivo: Supponiamo che

Ipotesi induttiva | ogni naturale $k \leq n$ ammette
una decomposizione come
sopra e mostriamo che
anche $n+1$ la ammette. - tesi
induttiva

Due casi $\rightarrow n+1$ irrid $\Rightarrow n+1$ primo
Lemma

Def.

$n+1$ non e' irrid.

$n+1 = ab$ con
 $a, b \neq 1$ $a, b > 1$ $\Rightarrow n+1 = ab$
 $\Rightarrow a, b < n+1$ con $a, b \neq 1$
e necessariamente

$$1 < a < n+1 \quad 2 \leq a \leq n$$

$$1 < b < n+1 \quad 2 \leq b \leq n$$

\Rightarrow Sia a che b ammettono
decomposizioni in primi

per l'ipotesi induttiva

$$a = p_1^{e_1} \cdots p_k^{e_k} \quad b = q_1^{f_1} \cdots q_h^{f_h}$$

$$\Rightarrow ab = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_h^{f_h}$$

\Downarrow
 $n+1$ si fattorizza. \checkmark

Dim② Unicità: per induzione sulla lunghezza della fattorizzazione

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

lunghezza \uparrow

$$= e_1 + \cdots + e_k$$
$$= \text{numero di fattori primi che compare}$$

Caso base: $k=1$ Dile

Caso induttivo: Supponiamo di sapere
che ogni naturale che ammette
una decomposizione di lunghezza
 $\leq k$ ha la proprietà che

ip.
induttiva

tesi

questa decomposizione è anche unica, mostriamo
che l'unicità vale anche per
i numeri naturali che ammettono
una decomposizione di
lunghezza $k+1$

Consideriamo

$$n = p_1^{e_1} \cdots p_h^{e_h} \text{ con}$$

$$e_1 + \cdots + e_h = k+1$$

Supponiamo che n ammetta
anche un'altra fattorizzazione
in primi

$$n = q_1^{f_1} \cdots q_r^{f_r}$$

Oss: p_1 è un primo e
 $p_1 | n = q_1^{f_1} \cdots q_r^{f_r} = (q_1 \cdots q_i) \cdots (q_r \cdots q_j)$
 $\Rightarrow p_1$ deve dividere uno
dei fattori q_j

per simmetria diciamo $j=1$
 $p_1 \mid q_1$ (per semplificare
la notazione). Siccome q_1
e' primo e' anche irriducibile
(lemma) $\Rightarrow p_1 = 1 \circ q_1$
 $\Rightarrow p_1 = q_1$ (necessariamente)

ma allora abbiamo

$$p_1(p_1^{e_1-1} \cdots p_h^{e_n}) = q_1(q_1^{f_1-1} \cdots q_r^{f_r})$$

$$\Rightarrow \underbrace{p_1^{e_1-1} \cdots p_h^{e_n}}_{\text{semplificando il fattore comune}} = q_1^{f_1-1} \cdots q_r^{f_r}$$

semplificando
il fattore comune

$$p_1 = q_1$$

questo e' un naturale
con una decomposizione
di lunghezza

$$e_1-1 + \cdots + e_h = k+1-1=k$$



per ipotesi induttiva tale decompos.
 e' anche unica dunque
 i primi q_j corrispondono
 bionivocamente ai primi p_i
 e gli esponenti f_j corrisp.
 bioniv. agli esponenti e_i
 \Rightarrow le due fattorizzazioni

$$n = p_1^{e_1} \cdots p_h^{e_h} = q_1^{f_1} \cdots q_r^{f_r}$$

sono in realtà la stessa fattorizzazione F

$$a^e = a \cdot a \cdot \dots \cdot a \text{ e volte.}$$

Collegiamo ora la fattorizzazione
 al MCD e minimo comune
 multiplo

Lemma: $a, b \in \mathbb{N}$ allora

$$\text{MCD}(a, b) = p_1^{e_1} \cdots p_k^{e_k}$$

dove p_j compare in entrambe le fattorizzazioni uniche di a e b e e_j è l'esponente minimo tra i due esponenti.

Ese:

$$\text{MCD}\left(\underline{2^3 \cdot 5^{15}} \cdot 7 \cdot 13, \underline{2 \cdot 17 \cdot 5^{20}} \cdot 23\right)$$

Il Lemma

$$2^1 \cdot 5^{15}$$

Def. (Minimo comune multiplo)

$a, b \in \mathbb{N}$ mcm(a, b) quel numero
 > 0 t.c.

$$\textcircled{1} \quad a \mid \text{mcm}(a, b) \quad b \mid \text{mcm}(a, b)$$

$$\textcircled{2} \quad \text{se } M \text{ e' t.c. } a \mid M \text{ e } b \mid M \\ \text{allora } \text{mcm}(a, b) \mid M$$

Oss: Il mcm è ben definito

Lemma: $a, b \in \mathbb{N}$ allora

$$\text{mcm}(a, b) = p_1^{e_1} \cdots p_k^{e_k}$$

dove p_j è un primo che compare nella fatt. unica di a oppure b e → se compare in entrambe allora.

e_j è il max dei due esponenti

→ se invece compare solo da una parte allora e_j è il suo esponente in quella fattorizzazione

Esempio: $\text{mcm}\left(\frac{2^3}{\underline{5}} \cdot \frac{15}{\underline{7} \cdot \underline{13}}, \frac{1}{2} \cdot \frac{17}{5} \cdot \frac{20}{23}\right)$
Il Lemma

$$2^3 \cdot 5^1 \cdot 7^1 \cdot 13^1 \cdot 17^1 \cdot 23^1$$

Lemma: $a, b \in \mathbb{N}$

$$\text{MCD}(a,b) \cdot \text{mcm}(a,b) = \underbrace{ab}_{P_1^{\min\{e_1, f_1\}} P_1^{\max\{e_1, f_1\}} P_1^{e_1 + f_1}}$$

Dim. Per i lemmi precedenti
i fattori primi a sx e dx
sono gli stessi. Controlliamo
gli esponenti:

$$a = P_1^{e_1} \cdot (\dots)$$
$$b = P_1^{f_1} \cdot (\dots)$$

primi diversi da P_1

Allora la potenza massima di P_1
che compare a dx è $e_1 + f_1$

$$ab = P_1^{e_1 + f_1} (\dots)$$

no P_1

P_1 compare in $\text{MCD}(a,b)$

$\min\{e_1, f_1\}$ volte (primo lemma sopra)

e compare in $\text{mcm}(a,b)$
 $\max\{e_1, f_1\}$ volte ^{secondo}
(lemma sopra)

$\Rightarrow p_1$ compare in $\text{MCD} \cdot \text{mcm}$
esattamente $\min\{e_1, f_1\} + \max\{e_1, f_1\}$
 $= e_1 + f_1$
 $=$ stesso esponente
di p_1 in ab ☒
 \Rightarrow le fatt. di $sx =$ fatt. di dx .

Oss:

$$\text{mcm}(a,b) = \frac{a \cdot b}{\text{MCD}(a,b)}$$

Esercizio:

i fattori x, y
possono essere
 > 0 o < 0 !

Trovare le soluzioni interne di

$$x^2 - y^2 = 17$$

Esercizio = stessa cosa con $1 \cdot 25$
 $25 \cdot 1$
 $\underline{17 \rightarrow 25 = 5 \cdot 5}$

Oss: $x^2 - y^2 = (x+y)(x-y)$

$$\Rightarrow 17 = (x+y)(x-y)$$

$(-1)(-25)$
 $(-25)(-1)$
 $(-5)(-5)$
cioè
 $x^2 - y^2 = 25$

17 è primo = irriducibile

\Rightarrow ammette solo fattorizzazioni

banali = "fattorizzazione
in cui uno dei
fattori è ±1"

\Rightarrow 4 casi

$\textcircled{1} \quad \left\{ \begin{array}{l} x+y=1 \\ x-y=17 \end{array} \right.$	$\textcircled{2} \quad \left\{ \begin{array}{l} x+y=17 \\ x-y=1 \end{array} \right.$
--------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------

$\textcircled{3} \quad \left\{ \begin{array}{l} x+y=-1 \\ x-y=-17 \end{array} \right.$	$\textcircled{4} \quad \left\{ \begin{array}{l} x+y=-17 \\ x-y=-1 \end{array} \right.$
----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

$$\begin{array}{l} \text{I } \left\{ \begin{array}{l} x+y = A \\ x-y = B \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \stackrel{\text{I+II}}{2x = A+B} \\ \stackrel{\text{I-II}}{2y = A-B} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x = \frac{A+B}{2} \\ y = \frac{A-B}{2} \end{array} \right. \end{array}$$

$$\textcircled{1} \quad \left\{ \begin{array}{l} x = \frac{1+17}{2} = 9 \\ y = \frac{1-17}{2} = -8 \end{array} \right. \quad \textcircled{2} \quad \left\{ \begin{array}{l} x = \frac{1+17}{2} = 9 \\ y = \frac{17-1}{2} = 8 \end{array} \right.$$

$$\textcircled{3} \quad \left\{ \begin{array}{l} x = \frac{-1-17}{2} = -9 \\ y = \frac{-1+17}{2} = 8 \end{array} \right. \quad \textcircled{4} \quad \left\{ \begin{array}{l} x = \frac{-17-1}{2} = -9 \\ y = \frac{-17+1}{2} = -8 \end{array} \right.$$

$$(x, y) = (9, 8), (-9, 8), (-9, -8), (9, -8)$$

↑ Oss: se (x, y) è sol. allora
anche $(\pm x, \pm y)$ è sol.
 scegliendo
segni in modo indip.