

Definizioni Algebra

Ian

October 2021

Contents

1	Capitolo 1	4
1.1	Corrispondenza	4
1.2	Relazione	4
1.3	Relazione/Corrispondenza inversa:	4
1.4	Relazione di equivalenza:	4
1.5	Relazione banale (di uguaglianza):	4
1.6	Relazione caotica:	4
1.7	Classe di equivalenza:	4
1.8	Insieme quoziente:	5
1.9	Partizione insiemistica	5
1.10	Funzione/Applicazione:	5
1.11	Iniettiva:	6
1.12	Suriettiva:	6
1.13	Biunivoca (biiettiva):	6
1.14	Funzione caratteristica:	6
1.15	Operazione binaria:	6
1.16	Assiomi di Peano	6
1.17	Principio del buon ordinamento di \mathbb{N} :	7
1.18	Teor: Divisione con resto su \mathbb{N}	7
2	Calcolo combinatorio	7
2.1	Notazione funzionale:	7
2.2	Fattoriale crescente:	7
2.3	Fattoriale decrescente:	7
2.4	Pigeonhole principle (principio dei cassetti):	7
2.5	Permutazione:	7
2.6	Coefficiente binomiale	8
2.7	Formula:	8
2.8	Relazione ricorsiva:	8
2.9	Simmetria:	8
2.10	Relazione d'ordine:	8
2.11	POSET (Partial order set):	8

3	I numeri	9
3.1	Costruzione di \mathbb{Z} (interi)	9
3.2	Definizione di \mathbb{Z} :	9
3.3	Classi su \mathbb{Z} :	9
3.4	Sottoinsiemi di \mathbb{Z} :	9
3.5	Somma su \mathbb{Z} :	9
3.6	Prodotto su \mathbb{Z} :	9
3.7	Proprietà operazioni su \mathbb{Z} :	9
3.8	Gruppo:	10
3.9	Gruppo commutativo (abeliano):	10
3.10	Anello:	10
3.11	Anello unitario:	10
3.12	Divisore dello zero:	11
3.13	Dominio di integrità:	11
3.14	Legge di annullamento del prodotto:	11
3.15	Divisibilità:	11
3.16	Multiplo:	11
3.17	Associati:	11
3.18	Unità:	11
3.19	Irriducibile	11
3.20	Primo:	11
3.20.1	Proposizione: in \mathbb{Z} a è primo $\Rightarrow a$ irriducibile	11
3.20.2	Proposizione: in \mathbb{Z} a irriducibile $\Rightarrow a$ primo	12
3.21	Massimo comune divisore:	12
3.21.1	Teor: Esistenza del MCD tra due numeri	12
3.21.2	Prop: se $c a$ e $c b$ allora c divide ogni combinazione lineare di a e b	13
3.22	Proposizione	13
3.22.1	Lemma $MCD(m, m+1)=1$	13
3.23	Algoritmo di Euclide	13
3.23.1	Lemma1: L'algoritmo termina	13
3.23.2	Lemma2: Se $a = bq + r$ $MCD(a, b) = MCD(b, r)$	13
3.23.3	Corollario: $MCD(a, b) = MCD(r_n, 0) = r_n$	14
3.23.4	Lemma3	14
3.24	Coprimi	14
3.24.1	Osservazione1	14
3.24.2	Osservazione 2	14
3.24.3	Proposizione 1	14
3.24.4	Proposizione 2	14
3.25	Equazione diofantea	14
3.25.1	Teor: Soluzione equazione diofantea	14
3.26	Teorema fondamentale dell'aritmetica	15
3.26.1	Osservazione 1	15
3.26.2	Osservazione 2	15
3.26.3	Dimostrazione esistenza	15
3.27	Dimostrazione unicità	15

3.28	Teor. Euclide - Esistenza infiniti primi	16
4	Congruenze	17
4.1	Congruenza modulo n	17
4.2	Proposizione	17
4.3	Quoziente	17
4.4	Proposizione	17
4.5	Osservazione	18
4.6	Proposizione somma	18
4.7	Dimostrazione prodotto	18
4.8	Campo	18
4.9	Proposizione	19
4.10	Classi resto invertibili	19
4.11	Teorema Uguaglianza sbagliata	19
4.11.1	Grande teorema di Fermat	20
4.11.2	Piccolo teorema di Fermat	20
4.12	Teorema Eulero-Fermat	21
4.13	Corollario	21
5	Semigrupp	22
6	Monoide	22
7	Elenco gruppi	22
8	Gruppo simmetrico	23
8.1	Permutazione	23
8.2	S_n	23
8.3	Proposizione	23
8.4	Proposizione	23
8.5	3^a notazione: Permutazione come prodotto di cicli disgiunti . . .	23
8.6	Orbita	23
8.7	Proposizione	24
8.8	Permutazione ciclica	24
8.9	Teorema prodotto di scambi	24
8.10	Teorema parità	24
8.10.1	Pari, dispari	24
8.11	Gruppo alterno	24
8.12	Segno	24
9	Gruppi finiti	25
9.1	Proprietà 1	25

1 Capitolo 1

Relazione e corrispondenza sono interscambiabili.

1.1 Corrispondenza

Una corrispondenza ρ di X in Y è una terna (ρ, X, Y) dove $\rho \subseteq X \times Y$.

1.2 Relazione

Una Relazione di X in Y , è una corrispondenza ρ di X in Y . Se $(x, y) \in \rho$ si scrive anche $x\rho y$ (notazione infissa), cioè x è in relazione ρ con y .

1.3 Relazione/Corrispondenza inversa:

di ρ di X in Y è la relazione di Y in X denotata con ρ^{-1} data dalla seguente:

$$y\rho^{-1}x \Leftrightarrow x\rho y$$

1.4 Relazione di equivalenza:

una relazione su A (cioè un sottoinsieme ρ di $A \times A$) si dice di equivalenza se verifica le tre seguenti proprietà:

Riflessiva: $\forall a \in A, a\rho a$.

Simmetrica: $\forall a, b \in A, a\rho b \Rightarrow b\rho a$

Transitiva: $\forall a, b, c \in A$ se $(a\rho b \wedge b\rho c) \Rightarrow a\rho c$

1.5 Relazione banale (di uguaglianza):

su A $x, y \in A$ $x\rho y \Leftrightarrow x = y$

1.6 Relazione caotica:

su A $x\rho y \forall x, y \in A$

1.7 Classe di equivalenza:

data la relazione ρ in A , si definisce classe di equivalenza modulo ρ di un elemento $a \in A$ l'insieme di tutti gli elementi che sono equivalenti ad a ; si denota con $[a]_\rho$.

$$[x]_\rho := \{y \in A : y\rho x\}$$

1.8 Insieme quoziente:

data la relazione di equivalenza ρ su A , si definisce insieme quoziente l'insieme delle classi di equivalenza di ρ dato $x \in A$ si denota con A/ρ .

$$A/\rho = \{[x]_\rho : x \in A\}$$

Nota: Relazione di equivalenza e partizioni insiemistiche sono sostanzialmente la stessa cosa.

1.9 Partizione insiemistica

di A è una famiglia di sottoinsiemi di A non vuoti, tali che ad ogni elemento di A corrisponde un solo sottoinsieme.

$$H = \{A_i : i \in I\}$$

con

$$A_i \subseteq A \quad \forall i \in I$$

con

$$i \neq j, \quad i, j \in I \Leftrightarrow A_i \cap A_j = \emptyset$$

che equivale a dire:

$$\cup_{i \in I} A_i = A$$

cioè la famiglia H ricopre A .

1.10 Funzione/Applicazione:

$f : S \rightarrow T$ è un'applicazione di S in T se (f, S, T) è una corrispondenza di S in T , ovvero $f \subseteq S \times T$ che soddisfa la seguente proprietà:

$$\forall x \in S \exists! y \text{ in } T \text{ denotato con } y = f(x)$$

f è una legge univoca (ben definita)

L'elemento $f(x)$ si chiama **immagine dell'elemento**.

L'immagine di f è un sottoinsieme del codominio T definito da:

$$Im(f) := \{y \in T : \exists x \in S, y = f(x)\}$$

Controimmagine di y è il sottoinsieme di S del dominio definito da:

$$f^{-1}(y) := \{x \in S : f(x) = y\} \subseteq S$$

1.11 Iniettiva:

f è iniettiva $\Leftrightarrow \forall x, x' \in S : [f(x) = f(x') \Rightarrow x = x']$.

Definizione alternativa: f è iniettiva $\Leftrightarrow \forall x, x' \in S : [f(x) \neq f(x') \Rightarrow x \neq x']$.

f è iniettiva $\Leftrightarrow \forall y \in T \ |f^{-1}| \leq 1$, ovvero per ogni elemento y in T esiste al più un'immagine.

1.12 Suriettiva:

f è suriettiva se $\Rightarrow \forall y \in T \ \exists x \in S : f(x) = y$

Definizione alternativa: f è suriettiva $\Leftrightarrow f(S) = Im(S) = T$.

f è suriettiva $\Leftrightarrow \forall y \in T \ |f^{-1}(y)| \geq 1$, ovvero per ogni elemento y in T esiste almeno un'immagine.

1.13 Biunivoca (biiettiva):

se f è sia iniettiva che suriettiva.

f è biiettiva $\Leftrightarrow \forall y \in T \ |f^{-1}(y)| = 1$, ovvero per ogni elemento y in T esiste una sola immagine.

1.14 Funzione caratteristica:

è la funzione che vale 1 se $x \in S$, 0 se $x \notin S$.

1.15 Operazione binaria:

su S , è un'applicazione $m : S \times S \rightarrow S$; notazione funzionale $(s, s') \mapsto m(s, s')$; notazione infissa sms' o $s * s$.

1.16 Assiomi di Peano

per la costruzione dei naturali \mathbb{N}

1. I numeri formano una classe
2. Lo "zero" è un numero
3. Se a è un numero allora il successore a' è un numero
4. Se $a \neq b$ sono due numeri allora $a' \neq b'$
5. Lo "zero" non è successore di nessun numero ($\nexists a$ numero tale che $zero = a'$)
6. Assioma di induzione:
Se S è una classe di numeri tale che:
 - $zero \in S$
 - Se $a \in S$ allora $a' \in S$

allora ogni naturale è in S.

I naturali sono la più piccola classe che

- Contiene lo zero
- Chiusa rispetto a contenere i successori

1.17 Principio del buon ordinamento di \mathbb{N} :

Se $S \subseteq \mathbb{N}, S \neq \emptyset$, allora esiste un minimo in S, cioè esiste $m \in S$ tale che se $h \in \mathbb{N}, h < m$ allora $h \notin S$.

1.18 Teor: Divisione con resto su \mathbb{N}

: Siano $a, b \in \mathbb{N}, b \neq 0$; allora esistono $q, r \in \mathbb{N}$ tali che

- $a = bq + r$
- $0 \leq r < b$

$\forall a, b \in \mathbb{Z}, b \neq 0; \exists$ unici $q, r \in \mathbb{Z}$ con $a = bq + r \wedge 0 \leq r < b$

2 Calcolo combinatorio

2.1 Notazione funzionale:

Insieme delle applicazioni da A verso B

$$B^A = \{f : A \rightarrow B\}$$

2.2 Fattoriale crescente:

$$n^{(m)} := n * (n + 1) * \dots * (n + m - 1)$$

2.3 Fattoriale decrescente:

$$n_{(m)} := n * (n - 1) * \dots * (n - m + 1)$$

2.4 Pigeonhole principle (principio dei cassetti):

Se ho n oggetti e m cassetti, se $n > m$ e devo disporre tutti gli oggetti nei cassetti allora esiste un cassetto che contiene almeno due oggetti.

2.5 Permutazione:

Sia A un insieme. Una biiezione $f : A \rightarrow A$ si chiama anche *permutazione* di A.

2.6 Coefficiente binomiale

Prima interpretazione combinatoria: $\binom{n}{i}$ è il coefficiente di $x^i y^{n-i}$ nello sviluppo $(x+y)^n = \sum_{z_i \in \{x,y\}} z_1 \dots z_n$, ovvero il numero di stringhe binarie (su x, y)

- lunghe n
- con i occorrenze di x
- con n-i occorrenze di y
- $(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i}$

Seconda interpretazione combinatoria: numero di sottoinsiemi di cardinalità i su un insieme $[n]$ di cardinalità n.

2.7 Formula:

$$\binom{n}{i} = \frac{n(n-1) * \dots * (n-i+1)}{i!} = \frac{n!}{i!(n-i)!}$$

2.8 Relazione ricorsiva:

$$\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$$

Dimostrazioni algebrica e combinatoria.

2.9 Simmetria:

$$\binom{n}{i} = \binom{n}{n-i}$$

Il coefficiente binomiale è simmetrico rispetto al centro della riga n-esima $\lfloor \frac{n}{2} \rfloor$ del triangolo rappresentante tutti i coefficienti del coefficiente binomiale.

Dimostrazioni algebrica e combinatoria.

2.10 Relazione d'ordine:

Una relazione ρ su X è una relazione d'ordine (o un ordine, un ordinamento) se valgono per ρ le proprietà:

- (R) $\forall x, x \rho x$
- (AS) $\forall x, y (x \rho y \wedge y \rho x) \Rightarrow x = y$
- (T) $\forall x, y, z (x \rho y \wedge y \rho z) \Rightarrow x \rho z$

2.11 POSET (Partial order set):

Un insieme munito di una relazione d'ordine si dice parzialmente ordinato.

3 I numeri

3.1 Costruzione di \mathbb{Z} (interi)

a partire da \mathbb{N} : prendiamo su $\mathbb{N} \times \mathbb{N}$ la relazione ρ definita sulle coppie $(n, m) \in \mathbb{N} \times \mathbb{N}$ tale che $(n, m)\rho(n', m') \Leftrightarrow n + m' = m + n'$

3.2 Definizione di \mathbb{Z} :

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \rho$$

3.3 Classi su \mathbb{Z} :

$\overline{(0, 0)}$ zero
 $\overline{(m, 0)}, m > 0$ positivi
 $\overline{(0, n)}, n > 0$ negativi

3.4 Sottoinsiemi di \mathbb{Z} :

$$\mathbb{Z} = \mathbb{Z}^{>0} \cup \{0, 0\} \cup \mathbb{Z}^{<0}$$

3.5 Somma su \mathbb{Z} :

$$\overline{(n, m)} + \overline{(n', m')} = \overline{(n + n', m + m')}$$

3.6 Prodotto su \mathbb{Z} :

$$\overline{(n, m)} \cdot \overline{(n', m')} = \overline{(nn' + mm', nm' + mn')}$$

3.7 Proprietà operazioni su \mathbb{Z} :

$\forall a, b, c \in \mathbb{Z}$ (coppie $\overline{(n, m)}$) valgono le seguenti:

1. Associatività: $(a + b) + c = a + (b + c)$
2. Commutatività: $a + b = b + a$
3. Esiste uno *zero* per la somma, cioè un elemento $0 : a + 0 = 0 + a = a$
4. $\forall a \in \mathbb{Z}$ esiste un elemento detto *opposto*, denotato con $-a$, cioè un elemento tale che: $a + (-a) = (-a) + a = 0$.
 $a = \overline{(n, m)}$
 $-a = \overline{(m, n)}$
5. Associatività prodotto: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
6. Commutatività prodotto: $a \cdot b = b \cdot a$

7. Esiste un *elemento neutro* per il prodotto, "1", cioè un numero in \mathbb{Z} tale che:

$$a \cdot 1 = 1 \cdot a = a$$

$$\overline{(n, m)} \cdot \overline{(1, 0)} = \overline{(n, m)}$$

8. Distributività del prodotto sulla somma:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

3.8 Gruppo:

Un insieme S non vuoto, munito di una operazione

$$m : S \times S \rightarrow S$$

$$(a, b) \mapsto m(a, b) = a * b \text{ (notazione infissa)}$$

che verifica i punti 1, 3, 4 si chiama *gruppo* $(S, *)$. L'operazione su S è:

- associativa
- con elemento neutro e , $\forall x, x * e = e * x = x$
- per ogni elemento x esiste un inverso rispetto al prodotto $*$ cioè un elemento y tale che $x * y = y * x = e$, che si denota x^{-1}

3.9 Gruppo commutativo (abeliano):

Se il gruppo $(S, *)$ soddisfa anche la proprietà 2 (quindi associatività, commutatività, elemento neutro, opposto).

3.10 Anello:

Un anello è una terna $(A, +, \cdot)$ con:

- A insieme non vuoto
- $+$ due operazioni binarie, associative
- $(A, +)$ è un gruppo abeliano
- Distributività: $\forall a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c$

Anello commutativo: Se un anello $(A, +, \cdot)$ il prodotto è commutativo, cioè se $\forall a, b \in A, a \cdot b = b \cdot a$.

3.11 Anello unitario:

Se esiste un elemento di A , che si denota con 1_A , tale che $a \cdot 1_A = 1_A \cdot a = a$.

3.12 Divisore dello zero:

Un elemento $a \in A$, $a \neq 0_A$ di un anello si dice divisore dello zero se esiste $b \in A, b \neq 0$ con $a \cdot b = 0_A$.

3.13 Dominio di integrità:

se $(A, +, \cdot)$ è privo di divisori dello zero.

3.14 Legge di annullamento del prodotto:

se in un dominio di integrità $a \cdot b = 0_A$ allora $a = 0_A$ oppure $b = 0_A$.

3.15 Divisibilità:

dati $a, b \in \mathbb{Z}$ si dice che a divide b , e si indica $a|b$, se e solo se $\exists c \in \mathbb{Z}$ tale che $b = a \cdot c$. La divisibilità è una relazione sugli interi:

$$a|b \Leftrightarrow \exists c \in \mathbb{Z} : b = a \cdot c$$

3.16 Multiplo:

se $a|b$ diremo che b è un multiplo di a .

3.17 Associati

a, b sono associate se $a|b$ e $b|a$

Oss1: in \mathbb{N}^* sono associati $\Leftrightarrow a = b$.

Oss2: in generale, in $\mathbb{Z} \Leftrightarrow a = b$ oppure $a = -b$.

3.18 Unità:

In \mathbb{Z} sono $+1$ e -1 .

3.19 Irriducibile

Un elemento $a \in \mathbb{Z}$, $a \neq 0$ è irriducibile se $a = b \cdot c \Rightarrow b$ oppure c sono unità.

3.20 Primo:

Un elemento $a \in \mathbb{Z}$ si dice primo se:

$$a|b \cdot c \Rightarrow a|b \text{ oppure } a|c$$

3.20.1 Proposizione: in \mathbb{Z} a è primo $\Rightarrow a$ irriducibile

Sia $a = b \cdot c$: usando l'ipotesi che a è primo allora $a|b$ oppure $a|c$.

Se $a|b \Rightarrow \exists h : b = a \cdot h \Rightarrow a = a \cdot h \cdot c \Rightarrow h \cdot c = 1 \Rightarrow c = \pm 1$

Allora $a = b \cdot (+1)$ oppure $a = b \cdot (-1)$, a è irriducibile.

3.20.2 Proposizione: in \mathbb{Z} a irriducibile \Rightarrow a primo

Ipotesi: a irriducibile

Tesi: a primo Supponiamo che $a|bc \Leftrightarrow \exists h \in \mathbb{Z} : bc = ah$,

voglio mostrare che $a|b$ oppure $a|c$ ovvero che se $a \nmid b$ allora $a|c$.

Ora a irriducibile, i suoi divisori sono $a, -a, 1, -1$. $a \nmid b$ allora anche $-a \nmid b \Rightarrow$ i divisori comuni tra a e b sono $1, -1 \rightarrow MCD(a, b) = 1$.

$$\exists(\text{id. Bézout}) \exists h, k \in \mathbb{Z}$$

$$1 = ah + bk$$

$$c = cah + cbk = a(ck + k) \quad [cb = a]$$

quindi $a|c$.

3.21 Massimo comune divisore:

Dati a, b non entrambi nulli, un elemento $d \in \mathbb{Z}$ si chiama massimo comune divisore tra a e b un numero tale che:

- $d|a \wedge d|b$
- Se $c|a \wedge c|b$, allora $c|d$: d è il massimo tra i divisori comuni.

Chiamiamo massimo comune divisore l'unico positivo che soddisfa le due proprietà.

3.21.1 Teor: Esistenza del MCD tra due numeri

$\forall a, b \in \mathbb{Z}$ non entrambi nulli, esiste un numero $d \in \mathbb{N}^*$ tale che $d = MCD(a, b)$

Il massimo comune divisore si esprime come una combinazione lineare tra a e b , ovvero esistono $s, t \in \mathbb{Z}$ tali che $d = s \cdot a + t \cdot b$ (*identità di Bézout*).

Dimostrazione:

Sia $S = \{xa + yb : x, y \in \mathbb{Z}, xa + yb > 0\}$

1. $S \subseteq \mathbb{N}$
2. $S \neq \emptyset$

a e b sono non entrambi nulli, quindi almeno uno dei due è $\neq 0$. Sia esso a .

Se $a > 0$ allora $1 \cdot a + 0 \cdot b = a > 0$ Se $a < 0$ allora $(-1) \cdot a + 0 \cdot b = a > 0$

Dimostrazione che $d|a$ e $d|b$:

Dividiamo a per d (divisione col resto): $\exists q, r$ con $a = dq + r$, $0 \leq r < d$

Se $r = 0$ allora $d|a$

Se $r \neq 0$ allora $0 < r < d$

$r = a - dq$; dato che $d \in S \Rightarrow d = x_0a + y_0b$ allora

$$r = a - q(x_0a + y_0b) = a - qx_0a - qy_0b = a(1 - qx_0) - (qy_0)b$$

Quindi $r \in S$ perchè è una combinazione lineare > 0 ma $r < d$, però d è il minimo di $S \Rightarrow$ Assurdo.

Dimostrazione se $d'|a$ e $d'|b$ allora $d'|d$:

Poichè $d'|a$ e $d'|b$ si ha che

$$\exists h : a = d' \cdot h, \exists k : b = d' \cdot k$$

Ora

$$\begin{aligned} d &= x_0 a + y_0 b \\ &= x_0 (d' h) + y_0 (d' k) = \\ &= d' (x_0 h + y_0 k) \Rightarrow d' | d \end{aligned}$$

3.21.2 Prop: se $c|a$ e $c|b$ allora c divide ogni combinazione lineare di a e b

$$\begin{aligned} a &= ch \\ b &= ck \\ \Rightarrow xa + yb &= xch + yck \\ &= c(xh + yk) \Rightarrow \in \mathbb{Z} \\ &\Rightarrow c|xa + yb \end{aligned}$$

3.22 Proposizione

$$1 = at + bs \Rightarrow MCD(a, b) = 1$$

3.22.1 Lemma $MCD(m, m+1)=1$

Sia $m \in \mathbb{N}$, $m \geq 1$ allora $MCD(m, m+1) = 1$.

Dimostrazione:

$$m + 1 - m = 1 \Rightarrow 1(m + 1) + (-1)m = 1$$

Potendo scrivere 1 come combinazione lineare di m e $m+1$, m e $m+1$ sono primi tra loro.

3.23 Algoritmo di Euclide

3.23.1 Lemma1: L'algoritmo termina

La successione dei resti è un numero $0 \leq \dots < r_2 < r_1 < b$.

3.23.2 Lemma2: Se $a = bq + r$ $MCD(a, b) = MCD(b, r)$

TODO: scrivere dimostrazione

3.23.3 Corollario: $MCD(a, b) = MCD(r_n, 0) = r_n 1$

Per il lemma 2 $MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2) = \dots = MCD(r_{n-1}, r_n) = MCD(r_n, 0)$

3.23.4 Lemma3

Se $x \in \mathbb{N}^*$ allora $MCD(x, 0) = x$

3.24 Coprimi

a, b non entrambi nulli, a e b si dicono coprimi (o *primi fra loro*) se $MCD(a, b) = 1$.

3.24.1 Osservazione1

Se a e b sono primi fra loro, allora

$$\exists x, y \in \mathbb{Z} : 1 = xa + yb$$

3.24.2 Osservazione 2

Se

$$d = MCD(a, b) \Rightarrow \exists x, y : d = ax + by$$

3.24.3 Proposizione 1

Se $\exists x_0, y_0$ con $1 = ax + by$ allora a, b sono primi tra loro.

3.24.4 Proposizione 2

Se a e b sono coprimi e dividono un terzo numero c , allora $ab|c$.

3.25 Equazione diofantea

Equazione con una o più incognite sugli interi di cui si cercano le soluzioni intere.

3.25.1 Teor: Soluzione equazione diofantea

L'equazione diofante lineare in x e y $ax + by = c$ $a, b, c \in \mathbb{Z}$ possiede soluzioni intere $(x, y) \in \mathbb{Z}^2 \Leftrightarrow d = MCD(a, b) | c$

(Dim \Rightarrow) La condizione $MCD(a, b) | c$ è necessaria.

Ipotesi: esiste una soluzione di $x^2 + y^2 = z^2$

Tesi: $d | \text{termine noto}, d = MCD(a, b) : d | a \text{ e } d | b \Rightarrow d | \text{ogni combinazione lineare di } a, b$.

Se x_0, y_0 sono una soluzione, allora $ax_0 + by_0 = c \Rightarrow d | c = ax_0 + by_0$

(Dim \Leftarrow) La condizione è sufficiente.

Ipotesi $MCD(a, b) = ah + bk$, per opportuni $h, k \in \mathbb{Z}$

3.26 Teorema fondamentale dell'aritmetica

$\forall n > 1, n \in \mathbb{N}, \exists p_1, \dots, p_j \in \mathbb{N}$ (irriducibili) $\exists h_1, \dots, h_j \geq 1$ tali che:

- $n = p_1^{h_1} \dots p_j^{h_j}$ p_1, \dots, p_j distinti
- la fattorizzazione di $n = p_1^{h_1} \dots p_j^{h_j}$ p_1, \dots, p_j è unica a meno di riordinare i fattori

3.26.1 Osservazione 1

j può essere 1, cioè potrebbe esserci un solo irriducibile nella fattorizzazione di n , anche h possono essere 1. Se n è irriducibile $\Rightarrow n = n$ è la fattorizzazione in irriducibili di n .

3.26.2 Osservazione 2

1 non è considerato irriducibile perché si perderebbe l'unicità della scrittura in irriducibili.

3.26.3 Dimostrazione esistenza

Con principio di induzione in forma forte.

Base: $n=2$, 2 è irriducibile.

Per **oss1** $2 = 2^1$ è la fattorizzazione in primi in irriducibili di 2

Ipotesi induttiva: ogni $2 \leq a < n$ ($2 \leq a \leq n-1$) è fattorizzabile in irriducibili: $\exists \alpha_1 \dots \alpha_t \alpha_i \leq 1$ e q_1, \dots, q_t irriducibili con $a = q_1^{\alpha_1} \dots q_t^{\alpha_t}$

Passo induttivo: provare che n sia prodotto di irriducibili

Primo caso: n irriducibile \rightarrow fatto, per *oss.1*

Secondo caso: n riducibile: $\exists b, c \in \mathbb{Z}, 1 \neq b, c \neq n$ (divisori propri) con $n = bc \Rightarrow 2 \leq b, c < n$.

Allora per b e c vale l'ipotesi induttiva e quindi

$$b = q_1^{\alpha_1} \dots q_t^{\alpha_t} \quad c = x_1^{\beta_1} \dots x_s^{\beta_s}$$

$$n = bc = q_1^{\alpha_1} \dots q_t^{\alpha_t} x_1^{\beta_1} \dots x_s^{\beta_s}$$

3.27 Dimostrazione unicità

Per induzione su m , con m è la lunghezza minima di una fattorizzazione per n .
 m : minimo numero di irriducibili di una fattorizzazione di n

Base: $m = 1 \Rightarrow n = n$ è primo.

Se per assurdo $n = q_1 \dots q_s$, $s \geq 2$ allora $n|q_1$ o $n|q_2 \dots q_s$.

Prendiamo $n|q_1$, anche q_1 è primo $\Rightarrow n = q_1$; semplificando da entrambe le parti $\Rightarrow 1 = q_2 \dots q_s$ che porterebbe ad un assurdo perché $1 = 1$.

Quindi $n = q_1$ ed è l'unica fattorizzazione.

Ipotesi induttiva: se il minimo numero di primi in una fattorizzazione di n è $m - 1$, allora la fattorizzazione è unica a meno dell'ordine.

Passo induttivo: m è il minimo di una fattorizzazione di n .

3.28 Teor. Euclide - Esistenza infiniti primi

L'insieme $P = \{p \in \mathbb{N} : p \text{ è primo}\}$ è infinito.

Dimostrazione: Supponiamo che P sia finito, cioè $P = \{p_1, \dots, p_n\}$.

Sia $m = p_1 \dots p_n$ il prodotto di tutti i primi.

Considero $m + 1$: per il teorema fondamentale dell'aritmetica $m + 1 = p_1^{k_1} \dots p_n^{k_n}$, $k_1, \dots, k_n \geq 0$ almeno uno degli esponenti $\neq 0$.

Per il lemma su MCD di un numero ed il suo successivo m e $m+1$ sono coprimi.

Sia j tale che $k_j > 0$, cioè $p_j^{k_j} | m + 1$; vale anche $p_j | m$ allora $p_j | MCD(m, m+1) = 1$ che è un assurdo.

4 Congruenze

4.1 Congruenza modulo n

La congruenza modulo n (n fissato) è una relazione di equivalenza definita su \mathbb{Z} .

$$x \equiv y \pmod{n} \Leftrightarrow x - y \text{ multiplo di } n \Leftrightarrow n | x - y$$

4.2 Proposizione

La congruenza \pmod{n} è una relazione di equivalenza.

Dimostrazione:

(R)

$$\forall x \in \mathbb{Z} : x \equiv x \pmod{n} \Leftrightarrow n | (x - x)$$

Vera perché $0 = 0 \cdot n$.

(S)

$$\forall x, y \in \mathbb{Z} : x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$$

So che $n | x - y \Leftrightarrow x - y = nh$ per qualche $h \in \mathbb{Z}$.

Moltiplicando per -1: $y - x = -nh = n(-h)$ quindi $n | y - x \Rightarrow y \equiv x \pmod{n}$

(T)

$$x \equiv y \pmod{n} \wedge y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$$

$$(x - y) = nh_1 \wedge (y - z) = nh_2$$

$$(x - z) = (x - y) - (y - z) = nh_1 - nh_2 = n(h_1 - h_2) \text{ quindi } n | x - z \Rightarrow x \equiv z \pmod{n}$$

4.3 Quoziente

Il quoziente della congruenza \pmod{n} si denota come $\mathbb{Z}_{/\equiv \pmod{n}} = \{[x]_n : x \in \mathbb{Z}\}$.

Il quoziente \mathbb{Z}_n si chiama anche **interi modulo n**.

4.4 Proposizione

Dati $x, y \in \mathbb{Z}$ si ha: $x \equiv y \pmod{n} \Leftrightarrow$ il resto delle divisioni di x e di y per n è lo stesso.

Dimostrazione \Rightarrow (se $x \equiv_n y$ hanno lo stesso resto $x - y = nh$ (per qualche h)

$$x = nh + y$$

Dividendo y per n : $\exists! q, r \in \mathbb{Z} : y = nq + r, 0 \leq r < n$.

Scambiando in x : $x = nh + nq + r = n(h + q) + r$, x ed y hanno quindi lo stesso resto.

4.5 Osservazione

Sia $x = nq + r$, $0 \leq r < n$ la divisione con resto di x per n .
Allora

$$[x]_n = [r]_n \Leftrightarrow x \equiv r \pmod{n} \Leftrightarrow x - r = nq$$

Quindi

$$n \mid x - r$$

4.6 Proposizione somma

La somma classi resto in \mathbb{Z}_n , definita da: $\overline{x} + \overline{y} := \overline{x + y}$, è ben posta, ovvero non dipende dalla scelta dei rappresentanti.

Dimostrazione Siano $x' \in \overline{x}$, cioè $\overline{x'} = \overline{x}$ e $y' \in \overline{y}$ cioè $\overline{y'} = \overline{y}$, allora

$$x' \equiv x \pmod{n} \Leftrightarrow x' = x + kn$$

$$y' \equiv y \pmod{n} \Leftrightarrow y' = y + hn$$

Da verificare: $\overline{x' + y'} = \overline{x + y} \Leftrightarrow x' + y' = x + y + tn$

Quindi:

$$\begin{aligned} x' + y' &= x + kn + y + hn \\ &= x + y + kn + hn \\ &= x + y + (k + h)n \quad [(k + h) = t] \end{aligned}$$

4.7 Dimostrazione prodotto

$$\begin{aligned} x' \cdot y' &= (x + kn)(y + hn) \\ &= xy + xhn + kny + khn^2 \\ &= xy + n(xh + ky + khn), \quad [(xh + ky + khn) = t] \end{aligned}$$

4.8 Campo

Un campo è una terna $(K, +, \cdot)$ con K insieme non vuoto e 2 operazioni.

- $(K, +, \cdot)$ anello commutativo unitario
- Detto 0_k l'elemento neutro della somma e denotato con $K^* = K \setminus \{0_k\}$, deve valere che $\forall x \in K^* : x \cdot x^{-1} = 1_k$

Quindi campo \Leftrightarrow anello commutativo unitario con in più $K \setminus \{0_k\} = (K^*, \cdot)$ gruppo.

4.9 Proposizione

$a \in \mathbb{Z}, \bar{a}$ invertibile in $\mathbb{Z}_n \Leftrightarrow MCD(a, n) = 1$

Dim \Rightarrow

Ipotesi: $\bar{a} \in \mathbb{Z}$ invertibile

Tesi: $(a, n) = 1$

Esiste $b \in \mathbb{Z} : \bar{a} \cdot \bar{b} = 1$

$$\Leftrightarrow ab \equiv 1 \pmod{n}$$

$$\Leftrightarrow n \mid 1 - ab$$

$$\Leftrightarrow 1 - ab = nk$$

$$\Leftrightarrow 1 = ab + nk$$

$$\Rightarrow MCD(a, n) = 1$$

Dim \Leftarrow

Ipotesi: $MCD(a, n) = 1$

Tesi: \bar{a} è invertibile

Se $MCD(a, n) = 1$ allora esistono $h, k \in \mathbb{Z} :$

$$1 = ah + nk \in \mathbb{Z}$$

$$\bar{1} = \overline{ah + nk}$$

$$\bar{1} = \bar{a}\bar{h} + \bar{n}\bar{k} \in \mathbb{Z}$$

$$\bar{n}\bar{k} = \bar{0}\bar{k}$$

$$\bar{1} = \bar{a}\bar{h} \Rightarrow \bar{h} = (\bar{a})^{-1}$$

4.10 Classi resto invertibili

$$\cup(\mathbb{Z}_n) := \{a \in \mathbb{Z}_n : \bar{a} \text{ invertibile}\} \subseteq \mathbb{Z}_n$$

$$\cup(\mathbb{Z}_n) = \{\bar{a} : MCD(a, n) = 1\}$$

4.11 Teorema Uguaglianza sbagliata

Se p è primo allora $\forall x, y \in \mathbb{Z}$ vale:

$$(x + y)^p \equiv x^p + y^p \pmod{p}$$

$$(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p \pmod{p}$$

Dimostrazione: $(x + y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i}$

$$\binom{p}{0} = 1 = \binom{p}{p}$$

$$\binom{p}{0} x^0 y^p = 1 y^p$$

$$\binom{p}{p} x^p y^0 = 1 x^p$$

Considerare con $0 < i < p$ il coefficiente binomiale è:

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i(i-1)\dots 2 \cdot 1} \in \mathbb{N}$$

$$p \left(\frac{(p-1)\dots(p-i+1)}{i!} \right) \Rightarrow p \mid \binom{p}{i} \forall i = 2, \dots, p-1$$

$$\Rightarrow \binom{p}{i} \equiv 0 \pmod{p}$$

4.11.1 Grande teorema di Fermat

$x^n + y^n = z^n, n \geq 3$ non ha soluzioni intere.

4.11.2 Piccolo teorema di Fermat

$\forall a \in \mathbb{Z}, \forall p \text{ primo}$ si ha che: $a^p \equiv a \pmod{p}$ in \mathbb{Z}_p , p primo vale $\bar{a}^p = \bar{a}$.

Dimostrazione per $a \in \mathbb{N}$

Per induzione su a

Base:

$$a = 0$$

$$0^p \equiv 0 \pmod{p}$$

$$0^p = 0 \in \mathbb{Z} \Rightarrow 0^p \equiv 0 \pmod{p}$$

Ipotesi induttiva: supponiamo vera per a l'affermazione $a^p \equiv a \pmod{p}$

Passo induttivo: verifichiamo per $(a + 1)$.

$$(a + 1)^p \equiv a^p + 1^p \equiv a + 1$$

$a^p \rightarrow a$ e $1^p \rightarrow 1$ per ipotesi induttiva.

Se $a < 0$ è ancora vero?

Se $a < 0$ allora $-a > 0$, cioè $(-a)^p \equiv -a \pmod{p}$. Ora:

$$0 = a - a$$

$$0^p = (a - a)^p$$

$$0^p \equiv (a - a)^p \equiv a^p + (-a)^p$$

$$\equiv a^p - a \equiv 0 \pmod{p} \Leftrightarrow a^p \equiv a \pmod{p}$$

4.12 Teorema Eulero-Fermat

Se $(a, p) = 1$ cioè se $\bar{a} \neq \bar{0}$ in \mathbb{Z}_p allora

$$a^{p-1} \equiv 1 \pmod{p}$$

Dimostrazione: se $(a, p) = 1$ allora esiste l'inverso moltiplicativo di \bar{a} in \mathbb{Z}_p .

So che

$$a^p \equiv a \pmod{p}$$

$$(\bar{a}^p) \equiv \bar{a} \pmod{p}$$

$$\Rightarrow \text{moltiplicando per l'inverso} \Rightarrow \bar{a}^{p-1} = \bar{1} \text{ in } \mathbb{Z}_p$$

$$\Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$$

4.13 Corollario

Se $(a, p) = 1$ e se p primo allora \bar{a}^{p-2} è l'inverso moltiplicativo di \bar{a} in \mathbb{Z}_p

Dimostrazione: l'inverso di \bar{a} è \bar{x} con $\bar{a} \cdot \bar{x} = \bar{2}$, ma

$$\bar{a} \cdot \bar{a}^{p-2} = \bar{a}^{p-1} = \bar{1}$$

per il *teorema di Eulero-Fermat*.

5 Semigrupp

Sia X un insieme non vuoto.

$*$:

$$X * X \rightarrow Z$$

$$(a.b) \mapsto a * b$$

una operazione binaria associativa: $\forall a, b, c \in X : a + (b + c) = (a + b) + c$

Un insieme X , munito di una operazione associativa si chiama **semigrupp**.

6 Monoide

Se $(X, +)$ è un semigrupp e inoltre esiste un elemento 1_X tale che $a + 1_X = 1_X * a = a$ (1_X elemento neutro dell'operazione $*$), allora $(X, +)$ si chiama **monoid**.

7 Elenco gruppi

(A^*, \cdot) è un monoid non commutativo.

$(\mathbb{N}, +)$ (commutativo) monoid (0 el. neutro) ma non è un gruppo.

$(\mathbb{Z}, +)$ gruppo commutativo (0 el. neutro).

$(\mathbb{Q}, +)$ gruppo commutativo (0 el. neutro); $\frac{p}{a} \rightarrow \text{opposto} - \frac{p}{q}$.

(\mathbb{N}^*, \cdot) monoid, non è un gruppo.

(\mathbb{Z}^*, \cdot) monoid, non è un gruppo.

(\mathbb{Q}, \cdot) non è un gruppo, 0 non ha inverso.

(\mathbb{Q}^*, \cdot) gruppo.

$(\mathbb{R}, +)$ gruppo.

(\mathbb{R}^*, \cdot) monoid, gruppo.

$(\mathbb{Z}_n, +)$ gruppo finito commutativo; el. neutro $\bar{0}$.

(\mathbb{Z}_n, \cdot) monoid, semigrupp (non è un gruppo $\bar{0}$ non è invertibile).

$(\cup(\mathbb{Z}_n), \cdot)$ gruppo, el. neutro $\bar{1} = \{\bar{a} : (a, n) = 1\}$ (el. invertibili).

8 Gruppo simmetrico

8.1 Permutazione

$f : [n] \rightarrow [n]$ si chiama permutazione di n elementi se f è biiettiva.

8.2 S_n

$$\begin{aligned} S_n &:= \{\sigma : [n] \rightarrow [n] : \sigma \text{ è biiettiva}\} \\ &= \{\sigma : \sigma \text{ è una biiezione}\} \end{aligned}$$

8.3 Proposizione

$$|S_n| = n!$$

8.4 Proposizione

(S_n, \cdot) l'insieme delle permutazioni di n elementi con il prodotto di composizione funzionale è un gruppo di cardinalità $n!$ non commutativo.

Dimostrazione

- S_n non vuoto, $n \geq 1$
- Esiste un elemento neutro rispetto al prodotto \cdot , la permutazione identica:
 $\sigma \circ id = id \circ \sigma = \sigma$.
- Prodotto associativo $\forall \sigma, \tau, \rho \in S_n$ $(\sigma \circ \tau) \circ \rho(i) = \sigma \circ (\tau \circ \rho)(i) = \sigma(\tau(\rho(i)))$
- $\forall \sigma \in S_n$ esiste un elemento σ^{-1} tale che $\sigma \circ \sigma^{-1} = id$.

8.5 3^a notazione: Permutazione come prodotto di cicli disgiunti

S_n : Definire una relazione di equivalenza su $[n]$ associata a $\sigma \in S_n$.

$$x, y \in [n]$$

$$x \equiv_{\sigma} y \Leftrightarrow \exists i : y = \sigma^i(x)$$

Si osservi che $\sigma \in S_n$, allora la potenza i -esima di σ , con $i \in \mathbb{N}$ è la permutazione $\sigma^i = \sigma \circ \dots \circ \sigma$ per i volte.

8.6 Orbita

L'orbita di $x \in [n]$ è la classe di equivalenza di x nella relazione \equiv_{σ} .

$$O_{\sigma}(x) = \{y \in [n] \mid \exists i \text{ con } y = \sigma^i(x)\}$$

8.7 Proposizione

Se τ_1 e τ_2 hanno cicli disgiunti $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$

8.8 Permutazione ciclica

Chiamo ciclica una permutazione di S_n in cui nella rappresentazione in cicli disgiunti ha al più un solo ciclo di lunghezza > 1

8.9 Teorema prodotto di scambi

Ogni permutazione si può scrivere come prodotto di scambi

Dimostrazione 1: Se la permutazione ha un solo ciclo $\sigma = (a_1, a_2, \dots, a_k) =$ un k -ciclo $= (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_3)(a_1, a_2) = (a_1, a_2, a_3, \dots, a_k)$

Dimostrazione 2: Se ho un σ qualunque, allora

$$\sigma = C_1 \cdot C_2 \cdot \dots \cdot C_k$$

dove C_i è un ciclo (nella decomposizione in cicli disgiunti)

$$C_1 = (a_1, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2)$$

$$C_2 = (b_1, \dots, b_j) = (b_1, b_j)(b_1, b_{j-1}) \dots (b_1, b_2)$$

...

$$\sigma = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2) (b_1, b_j)(b_1, b_{j-1}) \dots (b_1, b_2)$$

8.10 Teorema parità

Il numero di scambi usati in diverse fattorizzazioni di una permutazione ha sempre la stessa parità.

8.10.1 Pari, dispari

Una permutazione è pari se il numero di scambi (in una sua fattorizzazione in scambi) è pari, dispari altrimenti.

8.11 Gruppo alterno

Le permutazioni pari si chiamano *gruppo alterno*.

8.12 Segno

Data σ in S_n , il segno di σ è $\varepsilon(\sigma) = (-1)^{\text{parità di } (\sigma)}$

9 Gruppi finiti

9.1 Proprietà 1

Dato G, \cdot gruppo e $x, y \in G$ allora $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ (l'inverso del prodotto è il prodotto degli inversi in ordine inverso)