Algebra

Simone Lidonnici

5 maggio 2024

Indice

1

Relazioni di equivalenza

Definizione di relazione

Una relazione ρ da un insieme A ad un insieme B è un sottoinsieme di $A \times B$:

$$\rho \subseteq A \times B$$

In cui:

$$\mathrm{Dom}(\rho) = \{a \in A | \exists b \in B | a\rho b\}$$
$$\mathrm{Im}(\rho) = \{b \in B | \exists a \in A | a\rho b\}$$

Una relazione da A a B è una funzione se:

- $\mathrm{Dom}(\rho) = A$
- $\forall a \in A \ \exists! b \in B | a\rho b$

Data una relazione si può definire la su inversa:

$$\rho^{-1} \subset B \times A = \{(b, a) \in B \times A | a\rho b\}$$

Se ρ è una funzione non è detto che ρ^{-1} lo sia.

Relazione di equivalenza

Una relazione $\rho \subseteq A \times A$ è una relazione di equivalenza se è:

- Riflessiva: $a\rho a \ \forall a \in A$
- Simmetrica: $a\rho b \implies b\rho a$
- Transitiva: $a\rho b \wedge b\rho c \implies a\rho c$

1.1 Classi di equivalenza

Insieme quoziente

Data una relazione di equivalenza ρ e preso un elemento $a \in A$, tutti gli elementi che sono in relazione con a appartengono ad un insieme chiamato **classe di equivalenza** di a:

$$[a] = \{b \in A | b\rho a\} \subseteq A$$

L'insieme di tutte le classi di equivalenza $\{[a]|a \in A\}$ è detto **insieme quoziente** per ρ e la sua cardinalità è il numero di classi di equivalenza esistenti e si indica con $\frac{A}{\rho}$.

Uguaglianza tra classi di equivalenza

Date due classi di equivalenza $[a]$ e $[b]$, queste due classi sono uguali solo se a è in relazione con b.

$$[a] = [b] \iff a\rho b$$

Dimostrazione:
$[a] = [b] \implies b \in [b] \implies b \in [a] \implies b\rho a \iff a\rho b$
Dimostrazione inversa:
$\forall c \in [a] \implies c\rho a \wedge a\rho b \implies c\rho b \implies c \in [b] \implies [a] \subseteq [b]$
$\forall c \in [b] \implies c\rho b \wedge b\rho a \implies c\rho a \implies c \in [a] \implies [b] \subseteq [a]$
$[a] \subseteq [b] \wedge [b] \subseteq [a] \implies [a] = [b]$

1.2 Partizione di un insieme

Definizione di partizione

Dato un insieme A, una **partizione** di A è una collezione di sottoinsiemi di A per cui:

- $A_\alpha \subseteq A$
- $A_\alpha \cap A_\beta \neq \emptyset \iff \alpha = \beta$
- $A_\alpha \cup A_\beta \cup ... \cup A_\omega = A$

Quindi un qualsiasi insieme quoziente creato da una relazione di equivalenza su A è una partizione di A.

1.3 Relazioni di ordine parziale e totale

Relazione di ordine parziale

Una relazione è di ordine parziale se è:

- Riflessiva
- Antisimmetrica: $a\rho b, b\rho a \implies a = b$
- Transitiva
- Alcuni elementi non possono essere messi in relazione tra di loro

Relazione di ordine totale

Una relazione è di ordine totale se è:

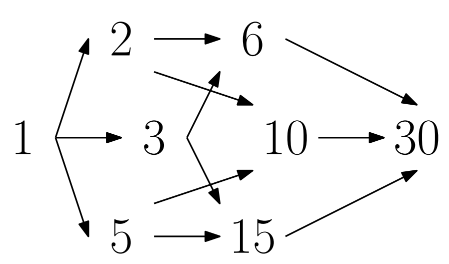
- Riflessiva
- Antisimmetrica: $a\rho b, b\rho a \implies a = b$
- Transitiva
- Tutti gli elementi sono in relazione tra di loro: $\forall a, b \in A \implies a\rho b \vee b\rho a$

1.3.1 Diagramma di Hasse

Preso un insieme (A, ρ) parzialmente ordinato, un elemento a è **coperto** da b e viceversa:

$$a \prec b \iff \nexists x | a\rho x \wedge x\rho b$$

Per rappresentare graficamente queste relazioni si usa il **diagramma di Hasse**.
Esempio:
$A = \{\text{divisori di } 30\} \subseteq \mathbb{N}$
$A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
$a\rho b \implies$ a divide b $\implies a|b$



2

Numeri naturali

2.1 Terna di Peano

Terna di Peano

Una terna di Peano è una terna $(\mathbb{N}, s, 0)$ in cui:

- $\mathbb{N}$ è un insieme(non inteso i numeri reali)
- s è una funzione $s : \mathbb{N} \to \mathbb{N}$ per cui:
  - $s(0) = 1$
  - $s(n)$ è detto successivo di n
- $0 \in \mathbb{N}$

e che rispetta la seguenti caratteristiche:

- s è iniettiva
- $0 \notin Im(s)$
- Se $U \subseteq \mathbb{N} \wedge 0 \in U \wedge (k \in U \implies s(k) \in U) \implies U = \mathbb{N}$

Si dimostra che se $(\mathbb{N}', s', 0')$ è un'altra terna di Peano allora esiste una funzione sia iniettiva che biettiva:

$$\varphi : \mathbb{N} \to \mathbb{N}' | \varphi(0) = 0' \wedge \varphi(s(n)) = s'(\varphi(n))$$

2.2 Principio del buon ordinamento

Principio del buon ordinamento

Sia $(\mathbb{N}, s, 0)$ una terna di Peano con $n, m \in \mathbb{N}$:

$$n \leq m \iff n = m \vee m = s(s(s(...s(n))))$$

Questa è una relazione di ordine totale.
Da questa relazione possiamo definire il principio del buon ordinamento:

$$\forall X \subseteq \mathbb{N}, X \neq \emptyset \; \exists \text{ un minimo}$$

Da questo teorema possiamo definire:

- Somma
- Prodotto

Inoltre l'insieme $\mathbb{N}$ con relazioni di maggiore uguale, somma e prodotto $(\mathbb{N}, \leq, +, \cdot)$ gode di tutte le proprietà base della matematica.

2.2.1 Definizione di somma

La somma è una funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che data una coppia di numeri restituisce la somma:

$$f : (n, m) \to n + m$$

La somma ha delle proprietà:

1. $0 + b = b \ \forall b \in \mathbb{N}$
2. $s(a) + b = s(a + b)$

2.2.2 Definizione di prodotto

Il prodotto è una funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che da una coppia di numeri restituisce il prodotto:

$$f : (n, m) \to n \cdot m$$

Il prodotto a delle proprietà:

1. $0 \cdot b = 0 \ \forall b \in \mathbb{N}$
2. $s(a) \cdot b = a \cdot b + b$

3

Strutture algebriche

Una struttura algebrica è composta da un insieme X e da una o più operazioni binarie, che sono applicazioni:

$$\star : X \times X \to X$$

Esempi:
$(\mathbb{Z}, +)$ è un insieme con un'operazione binaria
$(\mathbb{Z}, \cdot)$ è un insieme con un'operazione binaria

Ci sono diversi tipi di strutture algebriche notevoli:

1. Semigruppo
2. Gruppo
3. Anello
4. Campo

3.1 Semigruppo

Definizione di semigruppo

Un semigruppo è composto da un insieme e da un'operazione $\star$ verificante:

1. $\star$ è associativa: $(s \star s') \star s'' = s \star s' \star s''$
2. esiste un'elemento neutro: $\exists e \in S | e \star s = s \ \forall s$
3. Se $s \star s' = s' \star s$ il semigruppo $(S, \star)$ è commutativo

Un semigruppo generico si scrive $(A, \star)$.

Esempio:
$(\mathbb{N}, +)$ è un semigruppo commutativo avente 0 come elemento neutro

3.2 Gruppo

Definizione di gruppo

Un gruppo è composto da un insieme e da un'operazione $\star$ verificante:

1. $\star$ è associativa: $(s \star s') \star s'' = s \star s' \star s''$
2. esiste un'elemento neutro: $\exists e \in S | e \star s = s \; \forall s$
3. $\forall s \in S \; \exists s' | s \star s' = e = s' \star s$
4. Se $s_1 \star s_2 = s_1 \star s_2 \; \forall s_1, s_2$ il gruppo $(S, \star)$ è commutativo

Un gruppo generico si scrive $(A, \star)$.

Esempio:
$(\mathbb{Z}, +)$ è un gruppo commutativo avente 0 come elemento neutro

3.2.1 Gruppo simmetrico

Definizione di gruppo simmetrico

Dato un insieme X scrivo $S(X)$ l'insieme di tutte le funzioni **biettive** su X:

$$S(X) = \{f : X \to X \text{ biettive}\}$$

Preso $X = [1, n]$, quindi con n elementi, $S(X)$ si scrive S_n ed è un gruppo simmetrico su n elementi.

S_n è composto da permutazioni:

$$S_n = S(\{1, ..., n\}) = \{\sigma : \{1, ..., n\} \to \{1, ..., n\} \text{ biettiva}\}$$

una permutazione σ viene rappresentata come:

$$\sigma : \begin{cases} 1 \to \sigma(1) \\ ... \\ n \to \sigma(n) \end{cases} \implies \begin{pmatrix} 1 & ... & n \\ \sigma(1) & ... & \sigma(n) \end{pmatrix}$$

La cardinalità di S_n: $|S_n| = n!$
Esempio:
$S_3 = \{Id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$
$|S_3| = 3! = 6$

3.3 Unicità dell'elemento neutro e inverso

Unicità dell'elemento neutro

Dato $s \in S$, l'elemento e tale che:

$$s \star e = s = e \star s \forall s$$

è detto elemento **neutro** ed è unico.
Si denota come 1_S.
Dimostrazione:
Sia $\tilde{e}$ un altro elemento neutro allora:
$\tilde{e} \star e = e = e \star \tilde{e}$ perché $\tilde{e}$ è elemento neutro
$e \star \tilde{e} = \tilde{e} = \tilde{e} \star e$ perché e è elemento neutro
Quindi $e = \tilde{e}$

Inverso

Dato $s \in S$, l'elemento s^{-1} tale che:

$$s \star s^{-1} = e = s^{-1} \star s$$

si dice **reciproco** o **inverso** di s ed è unico.

3.4 Anello

Definizione di anello

Un anello è un insieme dotato di due operazioni $\star, \odot$ con le proprietà:

1. $(A, \odot)$ è un gruppo commutativo con O_A elemento neutro
2. $\star$ è associativa
3. Valgono le proprietà distributive: $(a \odot a') \star b = (a \star b) \odot (a' \star b)$
4. Se $\star$ è commutativo allora l'anello è commutativo
5. Se $\exists u \in A | a \star u = a = u \star a$ allora l'anello è unitario

Un anello privo di divisori dello 0 è un **anello di divisione**.
Un anello generico si scrive $(A, \odot, \star)$.

In un anello risulta sempre:

1. $a \cdot 0 = 0$
2. $a \cdot (-b) = -ab = -a \cdot b$
3. $-a(-b) = ab$

4. $a(b - c) = ab - ac$

Dominio di integrità

Un anello commutativo unitario e privo di divisori dello 0 viene anche detto **dominio di integrità** se:

$$a \star b = O_A \implies a = O_A \vee b = O_A$$

$(\mathbb{Z}, +, \cdot, 0, 1)$ è un dominio di integrità.
In un dominio di integrità vale la legge di cancellazione:

$$ca = cb \implies a = b \; \forall c \neq 0$$

Insieme delle unità

In ogni anello unitario si definisce un gruppo chiamato insieme delle unità:

$$u(A) = \{a \in A | \exists a' | aa' = 1 = a'a\}$$

In $\mathbb{Z}$, $u(\mathbb{Z}) = \{\pm 1\}$.
Il prodotto di due elementi di $u(A)$ appartiene ad $u(A)$:

$$a, b \in u(A) \implies a \cdot b \in u(A)$$

Dimostrazione:
Siano a', b' gli inversi moltiplicativi di a, b.
$a'b'$ inverso di $ab \implies (a'b')(ab) = b'(aa')b = b' \cdot 1 \cdot b = bb' = 1$

4
Numeri interi

Partendo dall'insieme dei numeri naturali $\mathbb{N}$ costruiamo un'estensione.
Consideriamo $\mathbb{N} \times \mathbb{N}$ e introduciamo una relazione di equivalenza:

$$(n, m)\rho(n', m') \iff n + m' = n' + m$$

$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\rho =$ classi di equivalenza
Ogni (n, m) fa parte di una tra 2 classe di equivalenza:

$$\begin{cases} (n, m) \in [(a, 0)] & n > m \\ (n, m) \in [(0, a)] & n < m \end{cases} \implies \begin{cases} n + 0 = m + a & a = n - m \\ n + a = m + 0 & a = m - n \end{cases}$$

$\mathbb{Z} = (\mathbb{Z}^+ = \{[(a, 0)] | a \in \mathbb{N}\backslash\{0\}\}) + (\mathbb{Z}^- = \{[(0, a)] | a \in \mathbb{N}\backslash\{0\}\}) + (0 = [(0, 0)])$

4.1 Definizione di somma e prodotto

Nei numeri interi la definizione di somma e prodotto sono:

$$[(n, m)] + [(n', m')] = [(n + n', m + m')]$$
$$[(n, m)] \cdot [(n', m')] = [(nn' + mm', nm' + mn')]$$

Inoltre:

1. $n + m = [(n + m, 0)] = [(n, 0)] + [(m, 0)]$
2. $n \cdot m = [(nm, 0)] = [(n, 0)] \cdot [(m, 0)]$
3. $[(n, 0)] + [(0, n)] = 0$
4. $[(n, m)] \cdot [(1, 0)] = [(n, m)]$

Teorema sul resto della divisione

Dati $a, b \in \mathbb{Z}$ con $b \neq 0$:

$$\exists!(q, r) \in \mathbb{Z} \times \mathbb{Z} | a = bq + r$$
$$0 \leq r \leq |b|$$

In cui:

- $a =$ dividendo
- $b =$ divisore
- $q =$ quoziente
- $r =$ resto

Dimostrazione:
Supponiamo $b \geq 0$ e $S = \{a - bx \geq 0, x \in \mathbb{Z}\}$
Se $x = -|a| \implies a - bx = a + b|a| \geq 0 \implies b|a| \geq -a \implies S \neq \emptyset$
Applico il principio del buon ordinamento a S e chiamo r il minimo di S
$r = a - bx \implies a = bq + r$
$r \in S \implies r \geq 0$
Per assurdo $r \geq |b| = b \implies r - b \geq 0 \implies a - bq - b \geq 0 \iff a - b(q+1) \geq 0 \implies$
$r - b \in S \implies r - b < r \implies$ impossibile

4.2 Numeri primi

Definizione di numero primo

Un numero $p \geq 2$ è primo se i suoi divisori sono solo $\pm 1, \pm p$:

$$\underbrace{p = xy, x \in u(\mathbb{Z}) \implies y \in u(\mathbb{Z})}_{\text{definizione di elemento irriducibile in } (\mathbb{Z},+,\cdot)}$$

Se p è un numero primo:

$$\underbrace{p|xy \land p \not| x \implies p|y}_{\text{definizione di elemento primo in } (\mathbb{Z},+,\cdot)}$$

Dato un elemento $a \in (A, +, \cdot)$:

$$a \text{ primo} \implies a \text{ irriducibile}$$
$$a \text{ irriducibile} \not\Longrightarrow a \text{ primo}$$

4.3 Massimo comun divisore (MCD)

Divisibilità di un numero

Dati $a, b \in \mathbb{Z}$:

$$a|b \iff \exists c \in \mathbb{Z} | b = ac$$

Ha le seguenti proprietà:

1. a ha sempre come divisori $\pm 1, \pm a$
2. $a|0 \; \forall a \in \mathbb{Z}$
3. $0|a \iff a = 0$
4. $a|1 \iff a = \pm 1$
5. Se $a|b$ e $a|c \implies a|(bx + cy) \; \forall x, y$

Definizione di MCD

Dati $(a, b) \in \mathbb{Z} \times \mathbb{Z}, (a, b) \neq (0, 0)$:

$$\exists! d \geq 1 | \begin{cases} d|a \text{ e } d|b \\ d'|a \text{ e } d'|b \end{cases} \implies d'|d$$

d è l'unico MCD.
Dimostrazione:
$S = \{ax + by > 0 | x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$
$S \neq \emptyset \xRightarrow{\text{buon ordinamento}} \exists d | d \geq x \; \forall x \in S$
$d = ax_0 + by_0$ è il MCD di a e b e $d \geq 1$
$ax + by = dq + r$ con $0 \leq r < d$
$ax + by = (ax_0 + by_0)q + r \implies r = a(x - x_0 q) + b(y - y_0 q)$
Per assurdo $r \in S$ e $r > 0 \implies r < d$ che è il minimo quindi impossibile
Quindi $d|(ax + by) \implies d|a$ e $d|b$

4.3.1 Proprietà

Il minimo comune multiplo ha le seguenti proprietà:

1. $a|b \implies \text{MCD}(a, b) = |a| \; \forall a \neq 0$
2. $\text{MCD}(a, \pm a) = |a|$
3. $\text{MCD}(a, 0) = |a|$
4. $\text{MCD}(\pm 1, b) = 1$
5. $\text{MCD}(ab, ac) = |a| \cdot \text{MCD}(b, c) \; \forall a, b, c \in \mathbb{Z}$
6. $\text{MCD}(a, b) = d \implies \text{MCD}(\frac{a}{d}, \frac{b}{d}) = 1$

Due numeri $a, b \neq (0,0)$ con $\text{MCD}(a,b) = 1$ si dicono **comprimi**.

Lemma di Euclide

Dati $a, b, c \in \mathbb{Z}$:
$$a|bc \wedge \text{MCD}(a,b) = 1 \implies a|c$$

4.3.2 Calcolare il MCD (Algoritmo euclideo)

Dati $a \geq b > 0$ con $a, b \in \mathbb{N}$ per calcolare il $\text{MCD}(a,b)$ seguiamo:

1. $a = bq_1 + r_1 \implies \text{MCD}(a,b) = \text{MCD}(b, r_1)$
   $0 \leq r_1 < b \rightarrow \begin{cases} r_1 = 0 \implies \text{MCD}(a,b) = b \\ r_1 > 0 \implies \text{ vado al punto 2} \end{cases}$
2. $b = r_1 q_2 + r_2 \implies \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2)$
   $0 \leq r_2 < r_1 \rightarrow \begin{cases} r_2 = 0 \implies \text{MCD}(r_1, r_2) = r_1 \\ r_2 > 0 \implies \text{ vado al punto 3} \end{cases}$
3. $r_1 = r_2 q_3 + r_3 \implies \text{MCD}(r_1, r_2) = \text{MCD}(r_2, r_3)$
   $0 \leq r_3 < r_2 \rightarrow \begin{cases} r_3 = 0 \implies \text{MCD}(r_2, r_3) = r_2 \\ r_3 > 0 \implies \text{ vado al punto 4} \end{cases}$

Così abbiamo una successione strettamente decrescente in cui:

$$b > r_1 > r_2 > ... > r_n > r_{n+1} = 0$$
$$\exists n | r_{n+1} = 0 \implies \text{MCD}(a,b) = \text{MCD}(r_n, 0) = r_n$$

Quindi:
$$\text{MCD}(a,b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) = ... = \text{MCD}(r_n, 0) = r_n$$

Inoltre possiamo trovare:

1. $r_n = r_{n-2} - q_n r_{n-1}$
2. $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$
3. ...
4. $r_2 = b - q_2 r_1$
5. $r_1 = a - q_1 b$

Determino tramite il lemma di Bezout x_0 e y_0:

$$r_n = ax_0 + by_0$$

Esempi:
$a = -123$
$b = -39$
$\text{MCD}(-123, -39) = \text{MCD}(123, 39)$

1. $\underbrace{123}_{a} = \underbrace{39}_{b} \cdot \underbrace{3}_{q_1} + \underbrace{6}_{r_1}$
2. $\underbrace{39}_{b} = \underbrace{6}_{r_1} \cdot \underbrace{6}_{q_2} + \underbrace{3}_{r_2}$
3. $\underbrace{6}_{r_1} = \underbrace{3}_{r_2} \cdot \underbrace{2}_{q_3} + \underbrace{0}_{r_3} \implies \text{MCD}(-139, -39) = r_2 = 3$

Per trovare x_0 e y_0:

1. $\underbrace{3}_{r_2} = \underbrace{39}_{b} - \underbrace{6}_{q_2} \cdot \underbrace{6}_{r_1}$
2. $\underbrace{3}_{r_2} = \underbrace{39}_{b} - \underbrace{6}_{q_2} \cdot (\underbrace{123}_{a} - \underbrace{3}_{q_1} \cdot \underbrace{39}_{b}) = -6 \cdot 123 + 19 \cdot 39 =$
   $6 \cdot -123 + (-19 \cdot -39) \implies x_0 = 6, y_0 = -19$

4.4 Minimo comune multiplo

Definizione di mcm

Dati due numeri $a, b \in \mathbb{Z}$:

$$\text{mcm}(a, b) = h$$

Con:

1. $a|h \wedge b|h$
2. Se $a|h' \wedge b|h' \implies h|h'$

Ha delle proprietà:

1. $\text{mcm}(a, 0) = 0$
2. $\text{mcm}(a, \pm 1) = |a|$
3. $\text{mcm}(a, b) = 0 \implies a = 0 \vee b = 0$

4.5 Teorema fondamentale dell'aritmetica

Teorema fondamentale dell'aritmetica

In $\mathbb{N}$:

$$\forall n \in \mathbb{N}, n \geq 2 \implies n \text{ è prodotto di numeri primi}$$
$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_s^{h_s} \text{ con } s \geq 1, h_i \geq 1$$

In $\mathbb{Z}$:

$$\forall n \in \mathbb{Z}, n \notin [1, -1] \implies n \text{ è prodotto di numeri primi}$$
$$n = (\pm 1) \cdot p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_s^{h_s} \text{ con } s \geq 1, h_i \geq 1$$

Dati due numeri a, b e ammettendo 0 come esponente i due numeri possono sempre essere scritti come prodotto degli stessi numeri primi:

$$a = q_1^{l_1} \cdot \ldots \cdot q_j^{l_j}$$
$$b = q_1^{m_1} \cdot \ldots \cdot q_j^{m_j}$$

Quindi possiamo trovare il $\text{MCD}(a, b)$ e il $\text{mcm}(a, b)$:

$$\text{MCD}(a, b) = q_1^{d_1} \cdot \ldots \cdot q_j^{d_j} \text{ con } d_i = \min(l_i, m_i)$$
$$\text{mcm}(a, b) = q_1^{c_1} \cdot \ldots \cdot q_j^{c_j} \text{ con } c_i = \max(l_i, m_i)$$

4.6 Teoremi su MCD e mcm

MCD per mcm

Dati $a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$:

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

Esistenza dei numeri primi

Esistono infiniti numeri primi.
Dimostrazione per assurdo:
Supponiamo per assurdo che siano finiti: Numeri primi $= \{p_1, p_2, \ldots, p_n\}$
Considero $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$
a fattorizzabile $\implies \exists p_j$ t.c. $p_j | a \implies \exists t | a = tp_j \implies$
$p_j(-(p_1 \cdot \cdots \cdot p_{j-1} \cdot p_{j+1} \cdot \ldots \cdot p_n) + t) = 1 \implies p_j | 1$ impossibile

5

$\mathbb{Z}_n$

Creazione di $\mathbb{Z}_n$

$\mathbb{Z}/_n\mathbb{Z}$ è l'insieme contenenti le classi di equivalenza rispetto alla relazione:

$$a\rho b \iff a - b = kn$$

Scrivendo come $[a]$ la classe che contiene a possiamo scrivere:

$$\mathbb{Z}/_n\mathbb{Z} = \{[0] = [n], [1] = [n+1], ..., [n-1] = [-1]\}$$

$\mathbb{Z}/_n\mathbb{Z} = \mathbb{Z}_n$ e la sua cardinalità è di n elementi.
Un elemento in $\mathbb{Z}_n$ può essere scritto come $[a]_n$
$(\mathbb{Z}_n, +, \cdot)$ è un anello.

5.1 Definizione di somma e prodotto

In $\mathbb{Z}_n$ viene definita la somma:

$$[n] + [m] = [n+m]$$

Dimostrazione:
$\begin{cases} a\rho a' \\ b\rho b' \end{cases} \iff \begin{cases} a - a' = kn \\ b - b' = hn \end{cases} \implies (a+b)\rho(a'+b') \implies (a+b)-(a'+b') = (a-a')+(b-b') = (k+h)n$

In $\mathbb{Z}_n$ viene definita il prodotto:

$$[n] \cdot [m] = [n \cdot m]$$

Dimostrazione:
$(ab)\rho(a'b') \implies ab - a'b' = (a' + kn)(b' + hn) - a'b' = (a'h + b'k + hkn)n$

5.2 Insieme delle unità

In $\mathbb{Z}_n$ il gruppo $u(\mathbb{Z}_n)$:

$$u(\mathbb{Z}_n) = \begin{cases} \mathbb{Z}_n \backslash \{0\} & n \text{ primo} \\ n \cdot \prod_{j=1}^{k}(1 - \frac{1}{p_j}) & n \text{ non primo} \end{cases}$$

In cui p_j è il j-esimo numero primo che compone n.
In $\mathbb{Z}_n$ questo insieme rappresenta anche quello degli invertibili ed è uguale all'insieme dei numeri coprimi con n:

$$u(\mathbb{Z}_n) = \{1 \leq k < n | \,\mathrm{MCD}(k, n) = 1\}$$

5.2.1 Funzione e teorema di Eulero

Funzione di Eulero

La funzione di Eulero φ:

$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$n \to |u(\mathbb{Z}_n)|$$

Rappresenta il numero di elementi coprimi con n, quindi anche la cardinalità dell'insieme delle unità in $\mathbb{Z}_n$.
Dato un numero fattorizzato in numeri primi $n = p_1^{r_1} \cdot ... \cdot p_s^{r_s}$:

$$\varphi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdot ... \cdot (p_s^{r_s} - p_s^{r_s-1})$$

Teorema di Eulero

Dato un $n \geq 2, a \in \mathbb{Z}$ con $\mathrm{MCD}(a, n) = 1$:

$$a^{\varphi(n)} \equiv 1 \quad (n) \iff [a^{\varphi(n)}]_n = [1]_n$$

Esempio:
Calcolare le ultime 2 cifre di 123^{123}
Dobbiamo calcolare $[123^{123}]_{100} = [123]_{100}^{123} = [23]_{100}^{123}$
Applico Eulero:
$\varphi(100) = \varphi(5^2 \cdot 2^2) = (5^2 - 5)(2^2 - 2) = 40$
$23^{40} = 1(100) \implies [23]_{100}^{123} = [23^{40\cdot3+3}]_{100} = [23^3]_{100} = [12167]_{100} = 67$

5.3 Equazioni congruenziali

Le equazioni congruenziali si dividono in 3 casi:

- Caso 1 in $\mathbb{Z}$:

$$ax + by = c$$

  Risolvibile se $\mathrm{MCD}(a, b)|c$:

$$\text{Soluzioni=}\begin{cases} x = x_0 \cdot \frac{c}{\mathrm{MCD}(a,b)} + b't \\ y = y_0 \cdot \frac{c}{\mathrm{MCD}(a,b)} - a't \end{cases} \qquad \forall t \in \mathbb{Z}$$

$$b' = \frac{b}{MCD(a, b)}$$
$$a' = \frac{a}{MCD(a, b)}$$

  (x_0, y_0) si trovano con l'algoritmo euclideo

- Caso 1 in $\mathbb{Z}_n$:

$$ax \equiv b \mod n$$

Risolvibile se $\text{MCD}(n, a)|b$:

$$\text{Soluzioni} = x_0 \cdot \frac{b}{\text{MCD}(n,a)} + \frac{n}{\text{MCD}(n,a)} \cdot t$$
$$\forall t \in [0, \text{MCD}(n,a) - 1]$$

x_0 lo trovo con l'algoritmo euclideo
Il numero di soluzioni è $\text{MCD}(n, a)$

- Caso particolare(trovare l'inverso di un numero a) in $\mathbb{Z}_n$:

$$ax \equiv 1 \mod n$$

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

$$\text{Soluzione} = x_0$$

Esempi:
$15x \equiv 18 \mod 24$

1. $24 = 15 + 9$
2. $15 = 9 + 6$
3. $9 = 6 + 3$
4. $6 = 3 \cdot 2 + 0 \implies \text{MCD}(24, 15) = 3|18$

Trovo x_0:
$3 = 9 - 6 = (24 - 15) - (15 - (24 - 15)) = 15 \cdot -3 + 24 \cdot 2 \implies x_0 = -3$
Soluzioni $= -3 \cdot \frac{18}{3} + \frac{24}{3}k = -18 + 8k = 6 + 8k$

$121x \equiv 22\ (33)$
$\text{MCD}(121, 33) = 11|22$
$121x \equiv 22\ (33) \iff 11x \equiv 2\ (3) \iff 2x \equiv 2\ (3) \implies x_0 = 1$
Soluzioni $= 1 + \frac{33}{11}k = 1 + 3k$

5.3.1 Sistemi di equazioni congruenziali

Un sistema di equazioni congruenziali, scritti:

$$\begin{cases} a_1x \equiv b_1 \quad (n_1) \\ ... \\ a_sx \equiv b_s \quad (n_s) \end{cases}$$

Ammette soluzione se:

$$\text{MCD}(a_i, n_i)|b_i \wedge \text{MCD}(n_i, n_j) = 1$$

Quindi possiamo ricongiungerlo a un sistema di tipo cinese:

$$\begin{cases} x_1 \equiv c_1 \quad (r_1) \\ ... \\ x_s \equiv c_s \quad (r_s) \end{cases} \mid \text{MCD}(r_i, r_j) = 1\ \forall i \neq j$$

In cui:
$r_i = \frac{n_i}{\text{MCD}(a_i,n_i)}$
$c_i = \dfrac{b_i}{\text{MCD}(a_i, n_i)} \cdot \underbrace{(\dfrac{a_i}{\text{MCD}(a_i, n_i)})^{-1}}_{\text{inverso di (...)(} \mod r_i)}$
Questo sistema ha una sola soluzione in $(\mod r_1 \cdot r_2 \cdot ... \cdot r_s)$
Per risolverla scriviamo:
$R = r_1 \cdot r_2 \cdot ... \cdot r_s$ con $R_k = \frac{R}{r_k}$
Risolviamo $R_k x = c_k(r_k)$ e troviamo x_k
La soluzione dell'intero sistema:

$$\tilde{x} = R_1 x_1 + ... + R_s x_s$$

Esempio:
$\begin{cases} 8x \equiv 3(5) \\ 8x \equiv 3(7) \\ 8x \equiv 3(11) \end{cases}$
Le singole equazioni sono risolvibili perché:
$\text{MCD}(8, 5) = 1|3$
$\text{MCD}(8, 7) = 1|3$
$\text{MCD}(8, 11) = 1|3$
Il sistema è risolvibile perché:
$\text{MCD}(5, 7) = 1$
$\text{MCD}(7, 11) = 1$
$\text{MCD}(11, 5) = 1$
Il sistema si riconduce a:
$\begin{cases} x \equiv 3 \cdot 2(5) \\ x \equiv 3 \cdot 1(7) \\ x \equiv 3 \cdot 7(11) \end{cases} \xRightarrow{\text{faccio diventare tutti } c_i < n_i} \begin{cases} x \equiv 1(5) \\ x \equiv 3(7) \\ x \equiv 10(11) \end{cases}$
Calcoliamo R_k:
$R = 5 \cdot 7 \cdot 11$
$R_1 = 7 \cdot 11$
$R_2 = 5 \cdot 11$
$R_3 = 5 \cdot 7$
La soluzione quindi è:
$\tilde{x} = R_1 x_1 + R_2 x_2 + R_3 x_3$
$77x_1 \equiv 1(5) \implies 2x_1 \equiv 1(5) \implies x_1 = 3$
$55x_2 \equiv 3(7) \implies 6x_2 \equiv 3(7) \implies -1x_2 \equiv 3(7) \implies x_2 = 4$
$35x_3 \equiv 10(11) \implies 2x_3 \equiv 10(11) \implies x_3 = 5$
$\tilde{x} = 77 \cdot 3 + 55 \cdot 4 + 35 \cdot 5 = 626$

5.3.2 Trasformare equazioni singole in sistemi

Data un'equazione congruenziale:

$$ax \equiv b \quad (n)$$

se n non è primo possiamo fattorizzarlo come:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$$

e possiamo scrivere l'equazione come un sistema:

$$\begin{cases} ax \equiv b \quad (p_1^{r_1}) \\ ax \equiv b \quad (p_2^{r_2}) \\ \dots \\ ax \equiv b \quad (p_n^{r_n}) \end{cases}$$

in cui:

$$\tilde{x}(\text{soluzione del sistema}) = x(\text{soluzione dell'equazione})$$

Esempio:

$6x \equiv 7 \quad (24) \implies \begin{cases} 6x \equiv 7 \quad (8) \\ 6x \equiv 7 \quad (3) \end{cases}$

5.4 Piccolo teorema di Fermat

Piccolo teorema di Fermat

Dati p numero primo e $a \in \mathbb{Z}$:

$$a^p \equiv a \quad (p)$$

Dimostrazione per induzione:

1. Caso base:
   $a = 0 \implies 0^p \equiv 0 \ \ (p)$
2. Passo induttivo:
   Suppongo vero che $a^p \equiv a \ \ (p)$
3. Dimostrazione induttiva:
   $(a+1)^p \equiv (a^p + 1) \ \ (p) = (a+1) \ \ (p)$

Se $\text{MCD}(a, p) = 1$:

$$a^{p-1} \equiv 1 \ \ (p)$$

Se n è primo allora:

$$u(\mathbb{Z}_n) = \mathbb{Z}_{(n-1)} \iff \mathbb{Z}_n \backslash \{0\} = \{1, a, a^2, ..., a^{n-2}\}$$

6
Campo