Appunti di Matematica Discreta

Giuseppe Sollazzo

7 aprile 2002

Indice

Capitolo 1

Nozioni fondamentali sui numeri naturali

1.1 Generalità

Consideriamo l'insieme dei numeri naturali

$$\mathbf{N} = \{0, 1, 2, 3, \ldots\}$$

Questo insieme presenta alcune proprietà fondamentali, dette *Assiomi di Peano*

1. Ogni numero $\in \mathbf{N}$ ha un solo successivo
2. Lo zero è un numero
3. Lo zero non è successivo di alcun numero
4. Ogni numero naturale non nullo è successivo solo di un altro numero naturale
5. Vale il *Principio di induzione*

Principio di induzione 1 *Supponiamo di avere una proposizione* P *sui naturali. Allora:*

a) P(0) è vera

b) P(n) è vera $\Rightarrow$ *P(n+1) è vera*

Per il principio di induzione se a) e b) sono vere, allora P è vera per tutti i numeri naturali.

- Nota - Sarebbe più corretto enunciare il principio di induzione definendo nel caso b) "se P è vera per n, allora P è vera per il successore di n" dato che non si conosce ancora il significato di addizione.
Inoltre, nella sua forma generalizzata, il principio di induzione dice che se supponiamo P(n) vera per n $\geq$ m allora P è vera $\forall$ n $\geq$ m.

1.2 Insiemi generici di naturali

Il discorso appena concluso vale per ogni insieme che sia un sottoinsieme dei naturali. Le operazioni possono essere generalizzate e definite come *applicazioni che da 2 elementi di un generico insieme A restituiscono un elemento dello stesso insieme A.*
$f : A \times A \to A$ cioè $f(a, b) = c$
Dato quindi un insieme possiamo definire quali sono le operazioni possibili su questo insieme. Definiamo, cioè, una *struttura algebrica*:
ad esempio, $(A, *)$ è una struttura algebrica che rappresenta un insieme A su cui è definita la moltiplicazione. L'insieme A si dice *sostegno* della struttura[1].
Una struttura con un'operazione si dice *commutativa* se l'operazione definita gode di tale proprietà:
$(A, *)$ è commutativa se $\forall a, b \in A a * b = b * a$
Per indicare una struttura commutativa basta scrivere $(A, +)$, cioè usiamo il "linguaggio dell'addizione" (notazione additiva in opposizione a quella moltiplicativa[2]).

1.3 Operazioni sui naturali

1.3.1 Addizione

Dati $a, b \in \mathbf{N}$ si scrive $a + b = c$
c si definisce *somma* di a e b.
Possiamo dare una definizione ricorsiva dell'addizione:

$$a + b = \begin{cases} a & \text{se } b = 0 \\ (a + d) + 1 & \text{se } b = d + 1 \end{cases}$$

Quindi la somma di due numeri consiste nel contare, a partire dal primo addendo, tante unità quante sono le unità del secondo addendo

1.3.2 Moltiplicazione

Dati a, b $\in \mathbf{N}$ si scrive $a \cdot b = c$
c si definisce *prodotto* di a e b.

[1] Per rappresentare una struttura algebrica basta indicare il suo sostegno, quando è evidente dal contesto che si sta parlando di una struttura algebrica

[2] Quando si parla in notazione additiva di elemento neutro ci si riferisce allo 0, e si parla di 'opposto', mentre in notazione moltiplicativa l'elemento neutro è l'1 e si parla di 'inverso'

Possiamo dare una definizione ricorsiva della moltiplicazione:

$$a \cdot b = \begin{cases} 0 & \text{se } b = 0 \\ a & \text{se } b = 1 \\ a \cdot d + a & \text{se } b = d + 1 \end{cases}$$

Quindi il prodotto di due numeri consiste nel sommare a se stesso il primo fattore (a), tante volte quante sono le unità del secondo fattore

1.3.3 Proprietà dell'addizione e della moltiplicazione

$\forall a, b, c \in \mathbf{N}$ valgono le seguenti proprietà:

- ELEMENTO NEUTRO
  Esiste ed è unico l'elemento neutro della somma: $a + 0 = a$
  Esiste ed è unico l'elemento neutro del prodotto: $a \cdot 1 = a$

- PROPRIETÀ ASSOCIATIVA
  $(a + b) + c = a + (b + c)$
  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

- PROPRIETÀ COMMUTATIVA
  $a + b = b + a$
  $a \cdot b = b \cdot a$

- LEGGE DI ANNULLAMENTO
  $a + b = 0$ sse $a = b = 0$
  $a \cdot b = 0$ sse $a = 0 \vee b = 0$

- LEGGE DI CANCELLAZIONE
  $a + b = a + c$ sse $b = c$
  $a \cdot b = a \cdot c$ sse $b = c$, con $a \neq 0$

- PROPRIETÀ DISTRIBUTIVA *della somma rispetto al prodotto*
  $(a + b) \cdot c = a \cdot c + b \cdot c$

1.3.4 Elevamento a potenza

$\forall a, b \in \mathbf{N}$si definisce elevamento a potenza: $a^n = \begin{cases} 1 & \text{se } n = 0 \\ a \cdot a^{n-1} & \text{se } n > 0 \end{cases}$

Proprietà dell'elevamento a potenza

1. $a^n \cdot a^m = a^{n+m}$
2. $(a^n)^m = a^{n \cdot m}$
3. $a^m \cdot b^m = (a \cdot b)^m$

1.3.5 Sottrazione

$\forall a \geq b, a - b = c$. c si dice "differenza" di a e b ed indica quel numero tale che $a = b + c$.
La sottrazione così definita *non* è un'operazione, in quanto non si può effettuare su ogni coppia di valori $a, b \in \mathbf{n}$

Proprietà della sottrazione

1. $a - b = 0 \iff a = b$
2. se $b \geq c, (a + b) - c = a + (b - c) \Rightarrow (a + b) - b = a$[3]
3. $a - b = (a + c) - (b + c)$ sse $b \geq c$, altrimenti $a - b = (a - c) - (b - c)$

1.3.6 Divisione

Enunciamo il

Teorema della divisione 2 *Siano* $a, b \in \mathbf{n}$ *e sia* $b \neq 0$. *Esistono e sono unici* $q, r \in \mathbf{N}$ *tali che*
$a = b \cdot q + r, 0 \leq r < b$[4]

Dimostrazione Occorre 1)dimostrare l'esistenza di q, r; 2)dimostrarne l'unicità.

1. Dimostrazione dell'esistenza di q ed r.
   Si presentano i seguenti casi:

   (a) se $a < b$ otteniamo $q = 0, r = a$[5]
   (b) se $a = b$ otteniamo $q = 1, r = 0$
   (c) se $a > b$ sappiamo che $\exists c_1 \in \mathbf{N}, c_1 \neq 0$, tale che $a = b + c_1$. Allora:
   - se $c_1 < b$ allora $q = 1, r = c_1$
   - se $c_1 = b$ allora $q = 2, r = 0$
   - se $c_1 > b$ allora $\exists c_2 \in \mathbf{N}$ tale che $c_1 = b + c_2$ e quindi $a = 2b + c_2$.
     A questo punto, iteriamo il procedimento finchè non giungiamo a una soluzione.
     Il passo generale è:
     se $c_{i-1} > b$ allora $\exists c_i \in \mathbf{N}$ tale che $c_{i-1} = b + c_i, a = i \cdot b + c_i$.
     Quindi:

[3] Non è una vera implicazione; la freccia indica che da quelle premesse possiamo ricavare l'espressione $(a + b) - b = a$
[4] Neanche la divisione è un'operazione in quanto associa coppie di naturali ad altre coppie di naturali, cioè $\mathbf{N} \times \mathbf{N} \to \mathbf{N} \times \mathbf{N}$
[5] ad esempio: $5 : 7 = 0 + 5$

- se $c_i < b$ allora $q = i, r = c_i$
- se $c_i = b$ allora $q = i + 1, r = 0$
- se $c_i = b$ allora si ripete.

Ovviamente riesco a dimostrare l'esistenza se ad un certo punto il procedimento si ferma e trovo il valore di c.[6]

Perchè questo procedimento funziona? Abbiamo costruito un insieme di valori $a, c_1, c_2, \ldots$ in cui si ha sempre $a < c_1 < c_2 < \ldots$. È un insieme di naturali, che sicuramente ammette un minimo c_s tale che $a = b \cdot s + c_s$. c_s non può essere maggiore di b perchè altrimenti potremmo scrivere $c_s = b + c_{s+1}$ mentre per definizione si ha che $c_s > c_{s+1}$, un assurdo logico dato che c_s è il minimo. Perciò

- *se $c_s < b$ allora $q = s, r = c_s$*
- *se $c_s = b$ allora $q = s + 1, r = 0$*

2. Dimostrazione dell'unicità di q ed r.
   Supponiamo per assurdo che q ed r non siano unici. Allora avremmo:
   $a = q \cdot b + r, 0 \leq r < b$
   $a = q_1 \cdot b + r_1, 0 \leq r_1 < b$
   Dobbiamo dimostrare che $q = q_1$ e che $r = r_1$[7]
   Supponiamo $r \geq r_1$. Avremo la seguente uguaglianza: $b \cdot q + r = b \cdot q_1 + r_1$.
   Ad entrambi i membri sottraiamo r_1 ottenendo una nuova uguaglianza:
   $b \cdot q + r - r_1 = b \cdot q_1$
   Essendo $r \geq r_1$ per definizione di maggiore sappiamo che $b \cdot q_1 \geq b \cdot q$[8] dunque $q_1 \geq q$.
   Ad entrambi i membri dell'equazione precedente sottraiamo $b \cdot q$:
   $b \cdot q + (r - r_1) - b \cdot q = b \cdot q_1 - b \cdot q$ cio
   $r - r_1 = b \cdot (q_1 - q)$ per cui se $q_1 = q$ sarebbe $r - r_1 = 0$ cioè $r = r_1$ il che sarebbe assurdo perchè vorrebbe dire $q_1 \geq q$, e quindi $r = b \cdot (q_1 - q) + r_1)$ e quindi sarebbe $r > b$ in contrasto con l'ipotesi avanzata.
   Per cui dati $a, b \neq 0$ si ha che q è il più grande naturale tale che $a \geq q \cdot b, a \leq (q + 1) \cdot b$

Divisibilità

Dati $b, a \in \mathbf{N}, b \neq 0$, diciamo che $b \mid a$ cioè che b è un divisiore di a se esiste $c \in \mathbf{N}$ tale che $a = b \cdot c$[9].
Enunciamo alcune proprietà:

- $\forall a : a \mid a$ in quanto $a = 1 \cdot a$[10]
- $\forall a : 1 \mid a$[11]

[6] Ovviamente, questo prima o poi succede :)
[7] Qui vale la proprietà di tricotomia tra r e r_1 e tra q e q_1
[8] Perchè $b \cdot q = r - r_1$
[9] Notare che b e c sono entrambi divisori di a e che b deve essere diverso da 0 perchè 0 è un "multiplo" di tutti i numeri in quanto risulta $\forall b : 0 = b \cdot 0$
[10] Cioè ogni numero è divisore di se stesso
[11] 1 è divisore di tutti i numeri

- Ogni numero $a \in \mathbf{N}$ ha almeno 2 divisori *impropri* : a e 1[12]
- $b \mid a \wedge b$ divisore proprio di $a \Rightarrow b < a$[13]

1.4 Insiemi ordinati

Una struttura definita come $(A, \leq)$ serve a indicare un insieme ordinato. L'insieme $\mathbf{N}$ è *naturalmente ordinato*. Ciò significa che l'elemento a è più piccolo dell'elemento b se nel contare a viene prima di b e si scrive $a < b$ oppure $a \leq b$. Per generalizzare questo ragionamento scriviamo:
$a \leq b \iff \exists c \in \mathbf{N}$ tale che $b = a + c$
A questo punto enunciamo il

Teorema del minimo 3 *Sia* $\oslash \neq H \subseteq \mathbf{N}$. *Allora H ammette minimo.*
Dimostrazione *Per l'assioma della scelta, possiamo sempre scegliere un elemento a dall'insieme H. Allora:*

- *Se* $0 \in H$, *allora 0 è il minimo.*
- *Se* $0 \notin H$, *prendo 1. Se* $1 \in H$, *allora 1 è il minimo.*
- ...
- *Se* $a - 1 \in H$, *allora a - 1 è il minimo. Altrimenti il minimo è a.*

1.5 Proprietà di N

- PROPRIETÀ RIFLESSIVA
  $\forall a \in \mathbf{N}, a \leq a$[14]
- PROPRIETÀ ANTISIMMETRICA
  $\forall a, b \in \mathbf{N}, a \leq b \wedge b \leq a \iff a = b$[15]
- PROPRIETÀ TRANSITIVA
  $\forall a, b, c \in \mathbf{N}, a \leq b \wedge b \leq c \Rightarrow a \leq c$
- PROPRIETÀ DI TRICOTOMIA
  $\forall a, b \in \mathbf{N}, a \leq b \wedge a \neq b \Rightarrow a < b$[16]
- ORDINAMENTO DELLA SOMMA
  $a \leq b \Rightarrow a + c \leq b + c$
- ORDINAMENTO DEL PRODOTTO
  $a \leq b \Rightarrow a \cdot c \leq b \cdot c$

[12] ne consegue che 1 non ha divisori propri perchè se $1 = b \cdot c, b \neq 1 \wedge c \neq 1 \Rightarrow b > 1 \vee b = 0$ il che contrasta con le ipotesi

[13] Significa che ogni divisore proprio è strettamente minore del numero di cui è divisore. Ad esempio, scriviamo $a = b \cdot c, b \neq 1, c \neq 0, b \neq a$. Possiamo scrivere $b = a + d, d \neq 0$ perchè $b \neq a$. Potendo scrivere $a = (a + d) \cdot c$ otteniamo $a = ac + dc$ che implica $a > a$ (assurdo).

[14] Perchè a = a + b se b = 0

[15] Dato che b=a+c, a=b+d, dunque a=a+(c+d) e ciò implica c+d=0 che è vero sse c=d=0, per cui a=b

[16] per esempio, $5 < 7$ perchè $5 \leq 7 \wedge 5 \neq 7$. Nella proprietà di tricotomia, ovviamente, solo una delle tre ipotesi è verificata: a¡b,a=b,a¿b

1.6 Relazione d'ordine

Se abbiamo un insieme A e una relazione $\mathcal{R}$ tra gli elementi di A, diciamo che A è ordinato secondo la relazione $\mathcal{R}$ se per tale relazione valgono le proprietà:

- riflessiva: $\forall a \in A, a\mathcal{R}a$
- antisimmetrica: $\forall a, b \in A, a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a = b$
- transitiva: $\forall a, b, c \in A, a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c$

Se vale anche la proprietà di tricotomia, allora la relazione si dice totale.[17]
Per indicare che su un insieme vale una relazione d'ordine possiamo scrivere $(A, \mathcal{R})$ oppure$(A, \leq)$

1.6.1 Divisibilità e relazione d'ordine

La divisibilità è una relazione d'ordine parziale, in quanto "a è divisore di b se $a \mid b$"
$(\mathbf{N}, |)$ è un insieme ordinato perchè:

- vale la proprietà riflessiva $\forall a \in \mathbf{N}, a \mid a$
- vale la proprietà antisimmetrica $\forall a, b, c \in \mathbf{N}, a \mid b \wedge b \mid a \iff a = b$
- vale la proprietà transitiva $\forall a, b, c \in \mathbf{N}, a \mid b \wedge b \mid c \Rightarrow a \mid c$[18]
- non vale la proprietà di tricotomia

La divisibilità è compatibile con il prodotto ma non con la somma.

[17] ad esempio, il principio di induzione non è una relazione d'ordine totale dato che valgono solo 3 proprietà

[18] dato che possiamo scrivere $b = a \cdot d$ e $c = b \cdot h$ ottendendo $c = a \cdot d \cdot h = a \cdot (d \cdot h)$ per cui risulta $a \mid c$

Capitolo 2

Numeri primi

p si dice *numero primo* se $p > 1 \wedge p$ non ha divisori propri.

Teorema 4 *Ogni numero o è primo o è prodotto di potenze di numeri primi. Cioè* $a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$ *dove* $p_1, p_2, \ldots, p_n$ *sono numeri primi, e* $r_1, r_2, \ldots, r_n \geq 1$.

Dimostrazione di Euclide Supponiamo di avere un numero qualsiasi: tale numero può avere dei divisori propri o può non averli. Se li ha, ne ha almeno 2. Il più piccolo di tali divisori è un numero primo, perchè se così non fosse tale numero avrebbe a sua volta 2 divisori, più piccoli di quelli che avevamo all'inizio.
Se risulta $p_1 < p_2 < \cdots < p_{n-1} < p_n$ abbiamo la *Fattorizzazione standard di un numero naturale.*

2.1 Massimo Comune Divisore

Dati $a, b \in \mathbf{N}$ il più grande dei divisori comuni di a e b si chiama Massimo Comune Divisore di a e b e si scrive $d = MCD(a, b)$ oppure $d = (a, b)$.
Se $MCD(a, b) = 1$ allora a e b sono *coprìmi o primi fra loro*[1].
- Nota - Se $a \mid b \wedge a \mid c$ allora $a \mid (b+c)$. Se $b > c, a \mid (b-c)$, se $b < c, a \mid (c-b)$[2].

2.1.1 Proprietà del Massimo Comune Divisore

1. Se $a \mid b$ allora $MCD(a, b) = a$[3]

2. Se $a = b \cdot q + t$ allora tutti i divisori comuni della coppia (a,b) sono divisori comuni della coppia (b,r). In particolare $MCD(a, b) = MCD(b, r)$

[1] Su n numeri la definizione di MCD è analoga; ovviamente se 2 di questi n numeri hanno $MCD = 1$ allora il MCD degli n numeri è 1

[2] In quanto possiamo scrivere $b = a \cdot h$ e $c = a \cdot k$ da cui otteniamo $b + c = a \cdot (h + k)$ per cui $a \mid (b + c)$

[3] da cui discende: $MCD(a, a) = a, MCD(a, 0) = a, MCD(a, 1) = 1$

2.1.2 Algoritmo di Euclide o delle divisioni successive

Per trovare il Massimo Comune Divisore di due numeri esiste un procedimento ideato da Euclide che consiste nell'effettuare delle divisioni successive tra varie coppie di numeri.
Dati $a, b \in \mathbf{N}, a \neq b, a > b, 0 \leq r_1 < b$
scriviamo $a = b \cdot q_1 + r_1$.

- Se $r_1 = 0$ allora $MCD(a, b) = b$
- Se $r_1 \neq 0$[4], abbiamo $b = r_1 \cdot q_2 + r_2, 0 \leq r_2 < r_1$.
  - Se $r_2 = 0 \ldots$
- all'*i-esimo* passo avremo $r_i = r_{i+1} \cdot q_{i+2} + r_{i+2}, 0 \leq r_{i+2} < r_{i+1}$.

Quando trovo $r_n = 0$ allora $MCD(a, b) = r_{n-1}$.
In sintesi ad ogni iterazione del procedimento dividiamo il resto precedente per il resto attuale, finchè da tali divisioni non otteniamo un resto nullo.
Dimostrazione. Dobbiamo dimostrare 1) che il procedimento finisce, 2) che troviamo un resto nullo, 3) $r_{n-1} = MCD(a, b)$.
Procediamo così. Prima di tutto abbiamo un insieme $a, b, r_1, \ldots, r_i, \ldots$ che è sicuramente un insieme ordinato, visto l'algoritmo con cui viene costruito. Si ha cioè $a > b > r_1 > \cdots > r_i > \cdots$.

1. Tale insieme, per il teorema del minimo, ammette sempre un minimo: quindi ad un certo punto l'algoritmo termina la sua esecuzione.
2. È scontato che il resto sarà 0 perchè in caso contrario l'algoritmo non terminerebbe, in contrasto con quanto abbiamo appena affermato.
3. Essendo $MCD(a, 0) = a$ è ovvio che se $r_n = 0$ avremo $MCD(r_{n-1}, r_n) = r_{n-1}$[5].

Euclide si occupava delle misurazioni dei segmenti. Ecco qual è il significato del suo algoritmo: se $r = 0$ le due grandezze considerate sono *commensurabili*, cioè sono entrambe misurabili dall'unità di misura individuata nel loro Massimo Comune Divisore.
- NOTA -

- Se $MCD(a, b) = d$ allora $a = d \cdot a' \wedge b = d \cdot b'$ dove $(a', b) = 1$[6]
- $(a, b) = 1 \wedge a \mid b \cdot c \Rightarrow a \mid c$

Teorema 5 *Siano $a, b, d \in \mathbf{N}$. Allora sono equivalenti le seguenti affermazioni:*

1. *$d \mid a \wedge d \mid b$, dato un qualunque c divisore comune di a e b risulta che $c \mid d$.*

[4] Essendo in $\mathbf{N}, r_1 > 0$
[5] A questo proposito ricorda la regola dei divisori comuni enunciata precedentemente: $(a, b) = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$
[6] cioè a' e b' sono coprìmi. Infatti se $(a', b') = h$ allora $a = d \cdot h \cdot a'' \Rightarrow a' = h \cdot a''$

2. $d = MCD(a, b)$

Dimostrazione Dobbiamo dimostrare sia che l'affermazione 1) implica l'affermazione 2), sia che l'affermazione 2) implica l'affermazione 1).

- Poniamo $MCD(a, b) = d'$. Dobbiamo dimostrare che $d = d'$.
  Per l'ipotesi 1, sappiamo che $d' \mid d$, per cui $d' \leq d$. Essendo però $d' = MCD(a, b)$ dovrebbe essere necessariamente $d \leq d'$. Perciò per la proprietà antisimmetrica sappiamo che $d = d'$.

- La dimostrazione è immediata in quanto sappiamo che $(a, b) = (b, r) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_{n-1}$

Corollario 6 $\forall a, b, k \in \mathbf{N}$, *se* $(a, k) = 1$[7] *e* $k \mid a \cdot b$ *allora* $k \mid b$.

Dimostrazione Consideriamo i due prodotti $k \cdot b$ e $a \cdot b$. Risulta che $k \mid k \cdot b$ ma per ipotesi sappiamo anche che $k \mid a \cdot b$. Se dimostriamo che $MCD(k \cdot b, a \cdot b) = b$ allora abbiamo dimostrato il teorema.
Poniamo $MCD(k \cdot b, a \cdot b) = d$: dato che b è un divisore comune tra $k \cdot b$ e $a \cdot b$, risulta che $b \mid d$ cioè possiamo scrivere $d = b \cdot h$.
Perchè sia dimostrato il teorema dobbiamo dimostrare che $h = 1$.
Poniamo $k \cdot b = d \cdot m$ e $a \cdot b = d \cdot n$. Se sostituiamo la d con $h \cdot b$ otteniamo le seguenti uguaglianze

$k \cdot b = b \cdot h \cdot m$ che per la legge di cancellazione diventa $k = h \cdot m$

$a \cdot b = b \cdot h \cdot n$ che per la legge di cancellazione diventa $a = h \cdot n$

Essendo $MCD(a, k) = 1$ per ipotesi, necessariamente risulta che $h = 1$ perchè $h \mid (a, k)$

Primo teorema di Euclide 7 *Sia* p *un numero primo. Se* $p \mid a \cdot b$ *allora* $p \mid a \vee p \mid b$.

Dimostrazione Poichè p è primo, se p non dividesse a risulterebbe $(p, a) = 1$. Ma allora, per il teorema precedente, sarebbe $p \mid b$.[8]

Con i teoremi appena enunciati siamo in grado di dimostrare il Teorema Fondamentale dell'Aritmetica, che afferma che ogni numero è rappresentabile come prodotto di numeri primi, affermando inoltre che tale fattorizzazione è unica. Si ricordi, a questo proposito, che il Massimo Comune Divisore di due numeri si può calcolare anche moltiplicando i fattori comuni della fattorizzazione standard dei due numeri.

Secondo teorema di Euclide 8 *Esistono infiniti numeri primi.*

[7] Cioè se a e k sono coprimi

[8] Si deduce in maniera immediata che se p è primo e $p \mid a \cdot b$ dove a e b sono primi, allora $\exists i$ tale che $p = p_i$ cioè p coincide con un numero primo.

Dimostrazione[9] Supponiamo di conoscere i primi n numeri primi:
$p_1, p_2 \dots p_n$.
Dobbiamo dimostrare che ce n'è uno più grande, p, di quelli considerati.
Definiamo la successione dei numeri in modo tale che risulti $p_1 < p_2 < \cdots < p_n$.
Consideriamo il numero $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n$. Tale numero è sicuramente maggiore di p_n.
Consideriamo anche il numero $M = N + 1$. Quindi:

- se M è primo abbiamo dimostrato il teorema perchè $M > p_n$
- se M non è primo, possiamo scrivere $M = p \cdot R$ dove p è il più basso numero primo della fattorizzazione di M.
  Dobbiamo dimostrare che $p > p_n$[10].
  Poniamo $p = p_j$. Allora $p \mid N$ in quanto $p_j \mid N$. Inoltre p_M e quindi $p \mid (M - N) = p \mid 1$; ciò è assurdo perchè per definizione di numero primo, p è necessariamente diverso da 1.

[9] Esistono varie dimostrazioni. Noi useremo quella di Euclide.
[10] Che in questo caso equivale a dimostrare $p \neq p_n$ in quanto $M > p_n$

Capitolo 3

Numeri interi

3.1 Generalità

Consideriamo l'insieme dei numeri interi

$$\mathbf{Z} = \{\cdots, -n, \cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

Z *è il prodotto cartesiano tra l'insieme* **N** *e l'insieme composto dai segni + e -, in cui* $+0 = -0 = 0$

Terminologia

- I numeri con lo stesso segno si dicono **concordi**, quelli di segno diverso si dicono **discordi**.
- Per **valore assoluto** di un numero si intende il numero stesso privato del segno.
- I numeri strettamente maggiori di 0 si chiamano Positivi, e il loro insieme si indica con il simbolo $\mathbf{Z}^+$.[1] Invece i numeri non negativi sono dati da $\mathbf{Z}^+ \cup \{0\}$
- I numeri strettamente minori di 0 si chiamano Negativi, e il loro insieme si indica con il simbolo $\mathbf{Z}^-$. Invece i numeri non positivi sono dati da $\mathbf{Z}^- \cup \{0\}$
- I numeri $+n$ e $-n$ si dicono **opposti**: si tratta di numeri con lo stesso valore assoluto ma con segno diverso.[2]

3.2 Operazioni sui numeri interi

3.2.1 Addizione

$\forall a, b, c \in \mathbf{Z}$ si scrive $a+b = c$. Il numero c è la somma di a, b ottenuta come segue:

[1] Con tale insieme, di solito, i matematici identificano l'insieme dei naturali
[2] Osserva che $-(-a) = a$

1. se a e b sono concordi, c è concorde con essi ed ha per valore assoluto la somma dei loro moduli: $\mid a+b \mid = \mid a \mid + \mid b \mid$
2. se a e b sono discordi e $\mid a \mid \geq \mid b \mid$, c è concorde con a e $\mid c \mid = \mid a \mid - \mid b \mid$
3. se a e b sono discordi e $\mid a \mid < \mid b \mid$, c è concorde con b e $\mid c \mid = \mid b \mid - \mid a \mid$

3.2.2 Sottrazione

$\forall a, b, c \in \mathbf{Z}$ si scrive $a - b = c$. Il numero c è così calcolato: $c = a + (-b)$.[3]

3.2.3 Proprietà dell'addizione

$\forall a, b, c \in \mathbf{Z}$ valgono le seguenti proprietà:

- PROPRIETÀ ASSOCIATIVA: $(a + b) + c = a + (b + c)$
- ESISTENZA DELL'ELEMENTO NEUTRO: $a + 0 = a$
- ESISTENZA DELL'OPPOSTO: $\forall a \in \mathbf{Z} \exists - a \in \mathbf{Z}$ tale che $a + (-a) = 0$
- PROPRIETÀ COMMUTATIVA: $a + b = b + a$
- UNICITÀ DELL'ELEMENTO NEUTRO: L'elemento neutro è unico
- UNICITÀ DELL'OPPOSTO: L'opposto è unico
- OPPOSTO DI UNA SOMMA: L'opposto di una somma è uguale alla somma degli opposti: $-(a + b) = -a - b$
- LEGGE DI CANCELLAZIONE: $a + b = a + c$ sse $b = c$

3.2.4 Gruppi

Sia $(G, \cdot)$ una struttura algebrica. Enunciamo le seguenti proprietà:[4]

1. ASSOCIATIVITÀ: $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. ESISTENZA DELL'ELEMENTO NEUTRO: $\exists e \in G, \forall a \in G : a \cdot e = e \cdot a = a$
3. ESISTENZA DELL'INVERSO: $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$
4. COMMUTATIVITÀ: $\forall a, b \in G : a \cdot b = b \cdot a$.

Se vale la proprietà 1) $(G, \cdot)$ è un **semigruppo**.
Se valgono le proprietà 1) e 2) $(G, \cdot)$ è un **monoide**.
Se valgono le proprietà 1), 2) e 3) $(G, \cdot)$ è un **gruppo**.
Se valgono le proprietà 1), 2), 3) e 4) $(G, \cdot)$ è un **gruppo commutativo o abeliano**.

[3] Cioè la somma di a con l'opposto di b
[4] Sono le stesse proprietà dell'addizione, però in notazione moltiplicativa

Sia $(G, \cdot)$ un gruppo (o monoide), risulta:

1. L'elemento neutro è unico
2. L'inverso di un elemento è unico
3. L'inverso di un prodotto è uguale al prodotto degli inversi con l'ordine scambiato: $\forall a, b \in \mathbf{G} : (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
4. Vale la legge di cancellazione a destra e a sinistra:
   se $a \cdot b = c \cdot b$ allora $a = c$;
   se $b \cdot a = b \cdot c$ allora $a = c$.

Dimostrazioni delle proprietà appena enunciate[5]

1. **Unicità dell'elemento neutro**: supponiamo che l'elemento neutro non sia unico: $e \neq e'$. Allora:
   $a \cdot e = e \cdot a \forall a$; in particolare per $a = e' : e' \cdot e = e \cdot e' = e'$
   $a \cdot e' = e' \cdot a \forall a$; in particolare per $a = e : e \cdot e' = e' \cdot e = e$
   e quindi:
   $e \cdot e' = e', e \cdot e' = e$ per cui $e = e'$.
2. **Unicità dell'inverso**: supponiamo che l'inverso non sia unico: a^{-1}, b. Allora:
   $a \cdot a^{-1} = a^{-1} \cdot a = e$
   $a \cdot b = b \cdot a = e$;
   scriviamo $b = b \cdot e = b \cdot a \cdot a^{-1} = (b \cdot a) \cdot a^{-1}$ da cui:
   $e = e \cdot a^{-1} \Rightarrow a^{-1} = b$
3. **L'inverso di un prodotto è uguale al prodotto degli inversi con ordine invertito**: cioè $a \cdot b \cdot b^{-1} \cdot a^{-1} = e$[6]
   per la proprietà associativa abbiamo $a \cdot b \cdot (b^{-1} \cdot a^{-1}) = (a \cdot b \cdot b^{-1}) \cdot a^{-1} = [a \cdot (b \cdot b^{-1})] \cdot a^{-1} = (a \cdot e) \cdot a^{-1} = a \cdot a^{-1} = e$
4. **Legge di cancellazione**: abbiamo $a \cdot b = c \cdot b$.
   Moltiplichiamo entrambi i membri per b^{-1} e applichiamo la proprietà associativa: $a \cdot (b \cdot b^{-1}) = c \cdot (b \cdot b^{-1})$
   quindi $a \cdot e = c \cdot e \Rightarrow a = c$

In $\mathbf{Z}$ vale l'ordinamento:
$a \leq b$ sse $\exists c \in \mathbf{Z}$, c non negativo, tale che $b = a + c$. Da questa affermazione consegue che tutti i positivi sono maggiori dei negativi, e che lo zero è maggiore di tutti i negativi e minore di tutti i positivi. L'ordinamento in $\mathbf{Z}$ è totale.

3.2.5 Moltiplicazione

$\forall a, b \in \mathbf{Z}$, definiamo prodotto di a e b il numero c tale che $a \cdot b = c$ determinato come segue:

[5] Queste dimostrazioni valgono anche per le proprietà enunciate in $\mathbf{Z}$
[6] ma anche $b^{-1} \cdot a^{-1} \cdot a \cdot b = e$

a) a,b concordi: c è positivo, $| c | = | a | \cdot | b |$

b) a,b discordi: c è negativo, $| c | = | a | \cdot | b |$

Proprietà della moltiplicazione

$\forall a, b, c \in \mathbf{Z}$ valgono le seguenti proprietà:

- PROPRIETÀ ASSOCIATIVA: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- ESISTENZA DELL'ELEMENTO NEUTRO: $\exists 1 \in \mathbf{Z}$ tale che $a \cdot 1 = a$
- LEGGE DI ANNULLAMENTO DEL PRODOTTO: $a \cdot b = 0 \iff a = 0 \vee b = 0$
- LEGGE DI CANCELLAZIONE: $a \cdot b = a \cdot c, a \neq 0 \Rightarrow b = c$
- PROPRIETÀ COMMUTATIVA: $a \cdot b = b \cdot a$
- PROPRIETÀ DISTRIBUTIVA DELLA SOMMA RISPETTO AL PRODOTTO: $(a + b) \cdot c = a \cdot c + b \cdot c$

3.3 Anelli

$(A, +, \cdot)$ è un anello se:

1. $(A, +)$ è un gruppo commutativo;
2. $(A, \cdot)$ è un semigruppo;[7]
3. vale la proprietà distributiva della somma rispetto al prodotto a sinistra $((a + b) \cdot c = a \cdot c + b \cdot c)$ e a destra $(c \cdot (a + b) = c \cdot a + c \cdot b)$.

3.3.1 Proprietà degli anelli

1. $\forall a \in A : a \cdot 0_A = 0_A \cdot a = 0_A$
2. $\forall a \in A : (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

Dimostrazione delle proprietà

1. $a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$. Essendo un elemento dell'anello, esiste l'opposto $-(a \cdot 0_A)$
   Quindi $a \cdot 0_A + (-a \cdot 0_A) = a \cdot 0_A + a \cdot 0_A + (-a \cdot 0_A)$ cioè
   $a \cdot 0_A - a \cdot 0_A = a \cdot 0_A + a \cdot 0_A - a \cdot 0_A$.
   Per cui $0_A = a \cdot 0_A + (a \cdot 0_A - a \cdot 0_A)$ cioè $0_A = a \cdot 0_A + 0_A$ e quindi $a \cdot 0_A = 0_A$
2. Dobbiamo dimostrare che $a \cdot b + (-a) \cdot b = 0_A$. Applichiamo la proprietà distributiva a destra:
   $a \cdot b + (-a) \cdot b = (a - a) \cdot b$ che significa $0_A \cdot b = 0_A$

[7] Cioè l'operazione definita da $\cdot$ deve essere associativa

3.3.2 Divisori

Prima di tutto definiamo A^* l'anello A ad esclusione dell'elemento nullo, cioè: $A^* = A - 0_A$.
Allora :
$\forall b \in A^*, b \mid a$ se $\exists c \in A$ tale che $a = b \cdot c$.

Per quanto riguarda i divisori dello 0, per gli anelli c'è una definizione particolare:
$\forall b, c \in A^*, b \cdot c = 0$ allora $b \mid 0 \wedge c \mid 0$, con $b \neq 0 \wedge c \neq 0$.

3.3.3 Invertibilità

Definiamo l'anello con unità quell'anello in cui esiste l'elemento neutro per l'operazione definita dal segno $\cdot$ e indichiamo tale elemento con 1_A. La definizione di invertibilità in un anello commutativo è la seguente:
$a \in A$ è invertibile se $\exists a^{-1} \in A$ tale che $a \cdot a^{-1} = 1_A$.

3.3.4 Dominio di integrità, Corpo, Campo

$(A, +, \cdot)$ è un **Dominio di integrità** se non contiene divisori dello 0_A.
$(A, +, \cdot)$ è un **Corpo** se $(A^*, \cdot)$ è un gruppo.
$(A, +, \cdot)$ è un **Campo** se è un corpo commutativo.

$(A, \cdot)$ non può essere un gruppo perchè lo 0 non è invertibile in un anello.
$\mathbf{Z}$ non può essere un corpo o un campo perchè $\mathbf{Z}^*$ non è un gruppo.

3.3.5 M.C.D. in Z

La definizione di più grande dei divisori comuni potrebbe non andare bene perchè il teorema di unicità del MCD non sarebbe più verificato. Per cui potremmo dire che il MCD di due numeri in $\mathbf{Z}$ è quel numero che in modulo è il più grande dei divisori comuni, cioè ammettiamo l'esistenza di due MCD $+d$ e $-d$.

3.4 Equazioni

Si definisce equazione[8] di almeno due incognite un'uguaglianza del tipo $ax+by = 0$ con $a, b \in \mathbf{Z}$.[9].

[8] Le uguaglianze si dividono in identità che sono sempre vere (es. $2 = 1 + 1$) ed equazioni, che sono vere solo per determinati valori (es. $3x = 0$ vera solo per $x = 0$)

[9] Come si vedrà, ci sono equazioni che non hanno soluzioni negli interi. Ad esempio, $2x + 3y = 0$ avrebbe come soluzione $y = -\frac{2}{3}x$ che non appartiene all'insieme $\mathbf{Z}$

Teorema 1 *Scriviamo $a'x + b'y = a$ con $a, b \in \mathbf{Z}$.*
Se $(a', b') = d, a' = d \cdot a e b' = d \cdot b$ allora tutte le soluzioni intere sono date da:

$$\begin{cases} x = b \cdot t \\ y = -a \cdot t \end{cases} \quad \forall t \in \mathbf{Z}$$

Dimostrazione Se $d = (a', b')$ allora $ax + by = 0$ è equivalente a $a'x + b'y = 0$. Allora dobbiamo dimostrare:

1. che ci sono delle soluzioni:
   $ax + by \Rightarrow ax = -by$ cioè $a \mid -by$[10]. Essendo inoltre $(a, b) = 1 : a \mid y$ cioè $\exists t \in \mathbf{Z}$ tale che $y = a \cdot t$.
   Sostituendo nell'equazione precedente si ha $ax = -bat$ con a, b non entrambi uguali a 0. Possiamo quindi applicare la legge di cancellazione, ottenendo $x = -bt$ c.v.d.

2. che per qualunque t la coppia è una soluzione:
   dobbiamo dimostrare che $a'(-bt) + b'(at) = 0$. Infatti si ha $a'(-bt) + b'(at) = da(-bt) + db(at) = d(-abt + bat) = d \cdot 0 = 0$

3. che non esistono altre soluzioni oltre quelle date dal sistema precedente:
   dobbiamo quindi dimostrare che se la coppia x_1, y_1 è una soluzione (cioè risulta che $a'x_1 + b'y_1 = 0$ allora esiste un intero t tale che

   $$\begin{cases} x_1 = -b \cdot t \\ y_1 = a \cdot t \end{cases} \quad \forall t \in \mathbf{Z}$$

   Infatti è $a'x_1 + b'y_1 = 0$ ossia $d(ax_1 + by_1 = 0$, cioè ancora $ax_1 + by_1 = 0$ per cui risulta $ax_1 = -by_1$ e quindi $a \mid -by_1$.
   Poichè $(a, b) = 1$ allora per uno dei teoremi del MCD risulterà che $a \mid y_1$ cioè che esiste un intero t tale che $y_1 = at$. Sostituendo nell'equazione precedente otteniamo $a(x_1 + bt) = 0$. Poichè $a \neq 0$ si ha $x_1 + bt = 0$ cioè $x_1 = -bt$.

3.4.1 Teoremi sulle equazioni in Z

Teorema 2 *Siano $a, b, d \in \mathbf{Z}$ non nulli. Sono equivalenti:*

1. *$d = a, b$*
2. *d è il minimo tra gli interi positivi della forma $ax + by$ con $x, y \in \mathbf{Z}$.*
   esempio*: nell'equazione $6x + 10y$ 2 è il minimo intero che possa essere espresso in tale forma perchè l'equazione non sarà mai uguale a 1.*

Corollario (1) 3 *Siano $a, b, d \in \mathbf{Z}$ e sia $d = (a, b)$. Allora l'equazione $ax+by = d$ ha sempre soluzioni intere.*

Corollario (2) 4 *L'equazione $ax + by = 1$ ha soluzioni intere SSE $(a, b) = 1$.*

[10] per un corollario precedentemente dimostrato

Corollario (3) 5 *Se $(a, b) = 1$, l'equazione $ax + by = c$ ha sempre soluzioni intere.*

Corollario (4) 6 *L'equazione $ax+by = c$ ha soluzioni intere SSE $MCD(a, b) \mid c$.*
esempio*: L'equazione $6x + 10y = 3$ non ha soluzioni intere.*

Teorema 7 *Siano $a', b', c' \in \mathbf{Z}$. Se $(a', b') = d, a' = da, b' = db$ e se $d \mid c'$ allora le soluzioni intere dell'equazione $a'x + b'y = c'$ sono tutte e sole le coppie di interi:*

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases} \quad \forall t \in \mathbf{Z}$$

dove x_0, y_0 è una soluzione particolare dell'equazione (cioè $a'x_0 + b'y_0 = c'$)[11].

3.4.2 Metodi di risoluzione delle equazioni in Z

I teoremi appena enunciati ci possono guidare nella ricerca di una soluzione, potendoci ad esempio dire in partenza se un'equazione non ha soluzioni. Per trovare tali soluzioni ci sono due metodi che vanno usati a seconda dei casi (sostanzialmente in base alla grandezza dei coefficienti coinvolti).

Metodo di Eulero

Si basa sull'osservazione che conoscendo una soluzione particolare tutte le soluzioni sono note e dello stesso tipo.
Il metodo di Eulero afferma che data un'equazione, esistono sempre due soluzioni intere x_1, y_1 e x_2, y_2 tali che $0 \leq x_1 \leq |b|$ e $0 \leq y_2 \leq |a|$.
Ora, se dividiamo l'intero x_0 del sistema precedente per b, otteniamo $x_0 = q \cdot b + r, 0 \leq r \leq |b|$. Se poniamo $t = -q$ nello stesso sistema, otteniamo $x = x_0 - qb = r < |b|$[12]. Tale soluzione è ovviamente unica.
Il metodo di Eulero consiste nel risolvere l'equazione rispetto all'incognita che ha il coefficiente minore (in modulo). Supponiamo sia x, otterremmo $x = \frac{c-by}{a}$. Prendiamo $y = 0, 1, \ldots, b - 1$, avremo una sola soluzione in cui il valore di x sarà intero.
Lo svantaggio di questo metodo è che per valori di a e b molto grandi costringe ad eseguire molti calcoli.

Metodo di riduzione (Autori vari)

Meno semplice del metodo di Eulero, si basa sull'osservazione che se uno dei coefficienti, per esempio a, divide c, allora una delle soluzioni è $x = \frac{c}{a}, y = 0$[13]. In particolare, se $MCD(a, b) \mid c$ allora $x = \frac{c}{d}$.
Il metodo consiste nel trovare a partire dall'equazione data un'equazione con uno dei coefficienti che divide il termine noto e quindi attraverso opportune considerazioni ricavare la soluzione dell'equazione data.
Tale metodo è un'applicazione dell'algoritmo euclideo per la ricerca del MCD.

[11] Quindi basta trovare una soluzione particolare per trovarle tutte.
[12] Strettamente minore in quanto il resto della divisione intera è per ovvi motivi strettamente minore del divisore.
[13] ad esempio, una soluzione dell'equazione $3x + 9y = 12$ è $x = 4, y = 0$

Supponiamo $a > 1, b > 1$ (se così non fosse basterebbe porre $-y$ al posto di y). L'algoritmo di Euclide si applica ai coefficienti a,b facendo le seguenti posizioni:

1. Abbiamo $ax + by = c$. Da $a = q_1 b + r_1$ otteniamo (per sostituzione) $b(q_1 x + y) + r_1 x = c$.
   Poniamo $t_1 = q_1 x + y$ otteniamo $bt_1 + r_1 x = c$.
2. Abbiamo $bt_1 + r_1 x = c$. Da $b = q_2 r_1 + r_2$ otteniamo (per sostituzione) $r_1(q_2 t_1 + x) + r_2 t_1 = c$.
   Poniamo $t_2 = q_2 t_1 + x$ otteniamo $r_1 t_2 + r_2 t_1 = c$.
3. Abbiamo $r_1 t_2 + r_2 t_1 = c$. Da $r_1 = q_3 r_2 + r_3$ otteniamo (per sostituzione) $r_2(q_3 t_2 + t_1) + r_3 t_2 = c$.
   Poniamo $t_3 = q_3 t_2 + t_1$ otteniamo $r_2 t_3 + r_3 t_2 = c$.
4. . . . . .
5. Alla fine avremo $r_{n-1} t_n + r_n t_{n-1} = c$ dove $r_n = 0$ e $r_{n-1} = MCD(a, b)$.

Allora, se r_{n-1} non divide c l'equazione non ha soluzione.
Altrimenti una soluzione dell'equazione $r_{n-1} t_n + r_n t_{n-1} = c$ è $t_n = 0, t_{n-1} = \frac{c}{r_n}$. Per sostituzione si ottengono il valore t_{n-2}. Iterando tale procedimento a un certo punto otterremo i valori x_0, y_0 che sono le soluzioni dell'equazione.

Capitolo 4

Congruenze

4.1 Definizione di congruenza

Fissato $n \in \mathbf{Z}$, due interi si dicono **congruenti modulo n** e si scrive $a \equiv_n b$ se $n \mid (a-b)$ cioè se la loro differenza è un multiplo di n. Se ciò non è vero, i due numeri si dicono **incongrui**.

4.2 Proprietà delle congruenze

1. $a \equiv_n b \iff a \equiv_{-n} b$
2. PROPRIETÀ FONDAMENTALE: Sono equivalenti:
   (i) $a \equiv_n b$
   (ii) a e b diviso n danno lo stesso resto

Dimostrazione della proprietà (ii)

1. Dimostrazione che (i) $\Rightarrow$ (ii)
   $n \mid (a-b)$ cioè $a - b = h \cdot n$. Possiamo dividere a e b per n:
   otteniamo $a = q_1 n + r$ e $b = q_2 n + r_1$.
   Dimostrare la proprietà equivale dunque a dimostrare che r e r_2 sono uguali, $0 \leq r < n, 0 \leq r_1 < n$.
   Scriviamo l'equazione $a - b = h \cdot n$ nella forma $a = h \cdot n + b$ e sostituiamo la b: otteniamo $a = h \cdot n + q_2 \cdot n + r_1$ che possiamo anche scrivere come $a = (n + q_2) \cdot n + r_1$.
   Possiamo affermare che $(n+q_2) \cdot n$ e r_1 sono quoziente e resto della divisione di a per n quindi, essendo per definizione unici, abbiamo dimostrato che $r = r_1$.
2. Dimostrazione che (ii) $\Rightarrow$ (i)
   Tale dimostrazione è immediata perchè se dividiamo a e b per n otteniamo lo stesso resto:
   $a - b = (q_1 - q_2) \cdot n$ cioè $n \mid (a-b)$ c.v.d.

Inoltre, valgono le seguenti proprietà:

1. RIFLESSIVA $\forall a \in \mathbf{Z} : a \equiv_n a$
2. SIMMETRICA $\forall a, b \in \mathbf{Z} : a \equiv_n b \iff b \equiv_n a$
3. TRANSITIVA $\forall a, b, c \in \mathbf{Z} : a \equiv_n b \wedge b \equiv_n a \Rightarrow a \equiv_n c$
4. COMPATIBILITÀ CON SOMMA E PRODOTTO
   $\forall a, b, c, d \in \mathbf{Z}, a \equiv_n b \wedge c \equiv_n d : (a + c) \equiv_n (b + d) \wedge (a \cdot c) \equiv_n (b \cdot d)$.

Dimostrazione della proprietà 4

1. Dimostrazione che vale la compatibilità con la somma
   Possiamo scrivere a, b, c, d come risultato di una divisione per n, ottenendo:

   (i) $a = h \cdot n + r$
   (ii) $b = k \cdot n + r$
   (iii) $c = h_1 \cdot n + r_1$
   (iv) $d = k_1 \cdot n + r_1$
   con $0 \leq r < n, 0 \leq r_1 < n$.

   Allora riscriviamo le uguaglianze della proprietà usando questi risultati:
   $a + c = (h + h_1)n + r + r_1$
   $b + d = (k + k_1)n + r + r_1$
   cioè dalla definizione di divisore e di congruenza abbiamo:
   $(a+c) \equiv_n (r+r_1)$ e $(b+d) \equiv_n (r+r_1)$ in quanto $a+c-(r+r_1)$ è multiplo di n.
   Applicando la proprietà transitiva alle due uguaglianze ottenute, otteniamo $(a + c) \equiv_n (b + d)$.

2. Dimostrazione che vale la compatibilità con la somma
   Anche qui seguiamo un procedimento analogo: scriviamo $a \cdot c = A \cdot n + r \cdot r_1$ e $b \cdot d = B \cdot n + r \cdot r_1$.
   Otteniamo così le seguenti congruenze:
   $(a \cdot c) \equiv_n (r \cdot r_1)$ e $(b \cdot d) \equiv_n (r \cdot r_1)$ da cui otteniamo per la proprietà transitiva:
   $(a \cdot c) \equiv_n (r \cdot r_1)$

4.3 Equivalenze

L'equivalenza è denotata dal seguente simbolo: $\equiv$. Dati un insieme A e una relazione $\mathcal{R}$, la relazione si dice **relazione di equivalenza** se valgono le proprietà:

1. RIFLESSIVA: $\forall a \in A : a\mathcal{R}a$
2. SIMMETRICA: $\forall a, b \in A : a\mathcal{R}b \iff b\mathcal{R}a$
3. TRANSITIVA: $\forall a, b, c \in A : a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c$

Si definisce **Classe di Equivalenza** ($[a]$ l'insieme così costituito:
$\{x \in A \mid x\mathcal{R}a\}, \forall a$. Si tratta cioè di ogni sottoinsieme di A formato da elementi equivalenti. L'elemento indicato tra parentesi si dice che è un **rappresentante** della classe.

Si definisce **Insieme quoziente modulo** $\simeq$ l'insieme di tutte le classi di equivalenza di A. Ovvero, l'insieme, appartenente a una partizione di A, che ha per elementi le classi di equivalenza di A.[1]

4.4 Classi di Congruenza Modulo n

Le classe di congruenza modulo n sono gli insiemi di interi costituiti da numeri congruenti modulo n.
Ognuna di queste classi è indicata dal simbolo $[a]_{/\equiv}$ oppure $[a]_{/\equiv n}$ oppure $[a]_{/n}$ oppure semplicemente $[a]$.
L'insieme di tali classi è detto **Insieme Quoziente** e si indica con $\mathbf{Z}_n$.

Se $n = 0, a \equiv_n b$ sse la loro differenza 0, cioè se i due numeri sono uguali. Quindi una congruenza modulo 0, in realtà un'uguaglianza.
Se $n = 1$ si ha una sola classe di congruenza che è costituita da tutto $\mathbf{Z}$ perchè 1 è divisore di tutti gli interi.
Supponiamo quindi $n \geq 2$. Poichè l'insieme quoziente $\mathbf{Z}_n$ è una partizione di $\mathbf{Z}$ allora:

a) Ogni classe di congruenza è non vuota

b) Due classi diverse non hanno elementi in comune

c) Ogni intero sta in una sola classe di congruenza

Per la proprietà fondamentale delle congruenze, una classe contiene solo elementi che divisi per n danno lo stesso resto (più il resto stesso). Di solito è quindi proprio il resto che viene scelto come rappresentante, come conseguenza del fatto che due resti diversi sono sempre incongrui. Quindi le classi di congruenza modulo n, sono tante quanti sono i resti: esattamente n. Tali classi si chiamano **classi di resti** o **classi di residui modulo n**.
Per esempio: $\mathbf{Z}_n = \{[0], [1], \ldots, [r], \ldots, [n-1]\}$; così si indica il fatto che i resti della divisione di un intero per n sono tutti e soli gli interi r tali che $0 \leq r < n$.

Se A è un insieme di numeri, $a \in A$ allora:

- con $a + 1$ si intende l'insieme di numeri ottenuto sommando a, a tutti gli elementi di A
- con $a * 1$ si intende l'insieme di numeri ottenuto moltiplicando a, a tutti gli elementi di A
- $\cdots$

Quindi per $\mathbf{Z}_n$:

$0 = \{m \in \mathbf{Z} \mid m = pn \forall p \in \mathbf{Z}\} = n\mathbf{Z}$

[1] Una partizione di A è una classe di sottoinsiemi di A tale che: 1)Ogni insieme non è vuoto, 2)Insiemi diversi sono disgiunti, 3)L'unione di tali insiemi è A.

$1 = \{m \in \mathbf{Z} \mid m = pn + 1 \forall p \in \mathbf{Z}\} = 1 + n\mathbf{Z}$

- $\cdots$

n-1 $= \{m \in \mathbf{Z} \mid m = pn + n - 1 \forall p \in \mathbf{Z}\} = n - 1 + n\mathbf{Z}$

4.5 Altre proprietà delle congruenze

4.5.1 Proprietà che coinvolgono il modulo

1. $a \equiv_n b \iff ac \equiv_{nc} bc$
2. $ac \equiv_n bc \wedge MCD(c, n) = d \Rightarrow a \equiv_{\frac{n}{d}} b$
3. $a \equiv_{mn} b \Rightarrow a \equiv_m b \wedge a \equiv_n b$
4. Per l'implicazione inversa della 3) occorre una condizione aggiuntiva, cioè: $a \equiv_m \wedge a \equiv_n b \wedge MCD(m, n) = 1 \Rightarrow a \equiv_{mn} b$

4.5.2 Proprietà di una congruenza di modulo fissato

1. $ac \equiv_n bc \wedge MCD(c, n) = d \Rightarrow a \equiv_{\frac{n}{d}} b$
2. $a \equiv_n b \Rightarrow a^m \equiv_n b^m$
3. $a \equiv_n b, c \equiv_n d \Rightarrow ax + cy \equiv_n bx + dy \forall x, y \in \mathbf{Z}$
4. $a \equiv_n b \Rightarrow f(a) \equiv_n f(b) \forall f$ polinomio a coefficienti interi

Dalla 4) discendono numerose proprietà quali le regole di divisibilità per 3 e per 11. Ad esempio, sappiamo che un numero è divisibile per 11 se la differenza tra la somma delle cifre pari e la somma delle cifre dispari è 0, 11 o un suo multiplo. Allora questa verifica si effettua partendo dal presupposto che un numero naturale scritto in base 10 è una somma di potenze di 10 con un loro coefficiente: esempio $436 = 6 \cdot 10^0 + 3 \cdot 10^1 + 4 \cdot 10^2$.
Allora un numero a può essere così descritto: $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$.
Sappiamo che $10 \equiv_{11} -1$ possiamo scrivere:
$a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0 \equiv_{11} a_n \cdot (-1)^n + \cdots + a_1 \cdot (-1) + a_0$
Il secondo termine della congruenza indica che le cifre pari sono positive e quelle dispari negative: la loro differenza, dunque, dev'essere 0 o multiplo di 11.

4.6 Somma e prodotto in $\mathbf{Z}_n$

Possiamo definire due operazioni all'interno dell'insieme quoziente $\mathbf{Z}_n$:

1. La somma, definita come funzione $+ : \mathbf{Z}_n \times \mathbf{Z}_n \to \mathbf{Z}_n$ si indica come $[a] + [b] = [c] = [a + b]$ ed è la classe che ha come rappresentate la somma dei rappresentanti delle due classi-addendi.
2. Il prodotto, definito come funzione $\cdot : \mathbf{Z}_n \times \mathbf{Z}_n \to \mathbf{Z}_n$ si indica come $[a] \cdot [b] = [c] = [a \cdot b]$.

Ovviamente in entrambi i casi il rappresentante può essere sostituito dal resto che rappresenta la classe in cui si sta operando.[2].

[2] Ad esempio, in $\mathbf{Z}_{13}[5] \cdot [9] = [45] = [6]$

Potrebbe sorgere un dubbio: se sostituiamo i rappresentanti con altri rappresentanti, la definizione resta valida? Se così non fosse la definizione di somma e prodotto non avrebbe senso perchè non sarebbe più possibile individuare le classi somma e prodotto. Dobbiamo quindi verificare che le definizioni sono **ben poste**, dimostrando che cambiando rappresentanti non cambia risultato.
Chiamiamo a' un rappresentante della stessa classe di a, tale che $a \equiv_n a'$ e b' un rappresentante della stessa classe di b, tale che $b \equiv_n b'$.
Occorre verificare che $a + b \equiv_n a' + b'$ e che $a \cdot b \equiv_n a' \cdot b'$. Questo, però, è già dimostrato perchè la congruenza è compatibile con la somma e col prodotto.[3]

4.7 L'anello $\mathbf{Z}_n$

La struttura $(\mathbf{Z}_n, +, \cdot)$ è un **anello commutativo con unità**. In questa struttura non valgono sempre:

- la legge di annullamento del prodotto; per esempio, in $\mathbf{Z}_{12}[3] \cdot [4] = [12] = [0]$ pur essendo $3, 4 \neq 0$. Ne concludiamo, inoltre, che esistono divisori dello 0.

- la legge di cancellazione del prodotto; per esempio in $\mathbf{Z}_{12}[3] \cdot [6] = [18] = [6]$ che può anche essere scritto $[3] \cdot [6] = [1] \cdot [6]$. Se valesse la legge di cancellazione, allora risulterebbe $[3] = [1]$ ma sappiamo che ciò non è vero.

Un altra proprietà che possiamo enunciare riguarda l'invertibilità: La classe $[a]$ è invertibile se $\exists [b]$ tale che $[a] \cdot [b] = [b] \cdot [a] = 1$. Inoltre se $[b]$ esiste, allora è unica.
Dimostrazione dell'unicità: Supponiamo che la classe abbia due inverse: $[b]$ e $[b']$. Risulterebbe $[a] \cdot [b'] = [b'] \cdot [a] = 1$ e analogamente $[a] \cdot [b] = [b] \cdot [a] = 1$. Prendiamo la prima di tali uguaglianze.
Abbiamo quindi che $[b'] = [1] \cdot [b']$ cioè $[b'] = [ab][b']$. Applichiamo la proprietà associativa e riscriviamo l'uguaglianza come $[b'] = [ab'][b]$ e dunque, essendo per ipotesi $[ab'] = 1$ risulta ovvio che $[b] = [b']$. Dunque la classe inversa è unica, c.v.d.

In un anello $\mathbf{Z}_n$ ci sono sempre e solo 2 elementi invertibili: $[1]$ e $[n-1]$ che hanno come inversi loro stesse.
Ad esempio, in $\mathbf{Z}_{12}$: $[11] \cdot [11] = [1]$.

4.8 Congruenze di primo grado a un'incognita

Si tratta di risolvere congruenze nella forma $ax \equiv_n b$ che equivale alla scrittura $[a] \cdot [x] = [b]$.

[3] Un esempio del prof. Tinaglia può rendere più facile comprendere il concetto di congruenza: Se diciamo che fra 10 giorni è sabato, in realtà noi stiamo eseguendo una somma nella congruenza modulo 7, essendo 7 i giorni della settimana.

Un intero è una soluzione della congruenza se sostituito a x la rende vera. Se x_1 è una soluzione della congruenza, allora sono soluzioni tutti gli elementi della classe $[x_1]$.[4]
Due soluzioni x_1, x_2 si dicono coincidenti se $x_1 \equiv_n x_2$. In caso contrario si dicono distinte.
Ovviamente, risolvere una congruenza significa trovare la classe o le classi di resti che la rendono vera, o riconoscere che è impossibile trovare tali classi.

Teorema 1 *La congruenza $ax \equiv_n b$ ha soluzioni se e solo se $MCD(a,b) \mid b$. Sia $d = MCD(a,n)$ con $a = da', b = db', n = dn'$.*
Allora la congruenza ha un numero d di soluzioni date da:
$x = x_0 + n'h$ con $h = 0, 1, \ldots, d-1$ dove x_0 è una soluzione particolare della congruenza.

Dimostrazione Prima di tutto dimostriamo che esiste una soluzione se e solo se $MCD(a,n) \mid b$.
Riprendiamo la definizione di congruenza di primo grado: $ax \equiv_n b$ significa che $n \mid (ax - b)$. Quindi $\exists y$ tale che $ax - b = ny, ax - ny = b$. Sappiamo che un'equazione del genere ha soluzioni se e solo se $MCD(a,n)|b$. Quindi il teorema dimostrato in quanto se $b = db'$ le soluzioni sono tutte e solo quelle date dalle soluzioni dell'equazione $a'x - n'y = b$.
Inoltre sappiamo che se x_0, y_0 è una soluzione particolare di questa equazione, le sue soluzioni sono tutte e solo quelle date da:

$$\begin{cases} x = x_0 + n'h \\ y = y_0 + a'h \end{cases}$$

Ovviamente quello che ci interessa per la soluzione della congruenza è la x, cioè quei valori dati dalla prima delle due equazioni del sistema.

Le soluzioni sono quindi:
$x_1 = x_0 + n'h + nt$
$x_2 = x_0 + n'h_1 + nt$
. Quando queste sono coincidenti (cioè sono congruenti modulo n)?
$x_1 \equiv_n x_2$ se e solo se $(x_0 + n'h + nt) \equiv_n (x_0 + n'h_1 + nt$. Da questa congruenza possiamo, per le proprietà enunciate all'inizio, cancellare gli addendi uguali e i multipli di n, perciò otteniamo:
$x_1 \equiv_n x_2 \iff n'h \equiv_n n'h_1$ che per le proprietà riguardanti le congruenze e il Massimo Comune Divisore d, può anche essere scritta $n'h \equiv_{n'd} n'h_1$ cioè $h \equiv_d h_1$

Corollario 2 *Dato che $ax \equiv_n 1$ ha soluzioni se e solo se $(a,n) = 1$ allora una classe in $\mathbf{Z}_n$ è invertibile se e solo se $(a,n) = 1$.*

Corollario 3 *In $\mathbf{Z}_n$ ogni classe $[a] \neq [0]$ è invertibile se e solo se n è primo.*

Corollario 4 *In $\mathbf{Z}_n$ l'anello $(Z_n, +, \cdot)$ è un campo se e solo se n è primo.*

[4] Cioè sono soluzioni della congruenza tutti gli $x_1 + kn$ (kn = multipli di n) tali che $ax_1 \equiv_n b$

4.9 La funzione di Eulero

È molto importante conoscere gli elementi invertibili di $\mathbf{Z}_n$ o almeno il loro numero. Esiste una funzione che ci permette di conoscere questo numero: la **funzione di Eulero**, che associa ad ogni naturale n il numero di naturali m, primi con n, tali che $m \leq n$. Tale numero si indica con $\varphi(n)$.

Come determinare tale numero?
Se $n \neq 1, \varphi(n)$ è il numero di naturali m primi con n e minori di n e si dimostra che:

1. se p è primo, $\varphi(p) = p - 1$ e $\varphi(p^n) = p^n - p^{n-1} = p^n \cdot (1 - \frac{1}{p})$;
2. se $(a, b) = 1$ allora $\varphi(ab) = \varphi(a)\varphi(b)$.

Formula generale Definita con $n = (p_1)^{h_1}(p_2)^{h_2} \cdots (p_m)^{h_m}$ la fattorizzazione standard di un numero naturale, possiamo applicare la seguente formula:
$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m})$
Per esempio, $n = 600 : \varphi(600) = 600(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})$

Teorema di Eulero-Fermat 5 *Se* $(a, n) = 1$ *allora* $a^{\varphi(n)} \equiv_n 1$.
Quindi, dato $[a], [a]^{-1} \equiv a^{\varphi(n)-1}$

Teorema di Fermat (corollario) 6 *Se n è primo e n non divide a allora* $a^{n-1} \equiv_n 1$ [5]

Teorema di Wilson 7 *Sono equivalenti le seguenti:*

1. *n è primo*
2. $(n-1)! \equiv_n -1$.

Per esempio, 5 è primo perchè $24 \equiv_5 -1$ *o meglio* $24 + 1 \equiv_5 0$.[6]

[5] In realtà questo teorema è meglio definito come corollario in quanto è solo un'applicazione del teorema principale di Eulero-Fermat.

[6] Questo teorema non è di grande utilità pratica, in quanto per capire se un numero è primo, occorre calcolare il fattoriale di un numero di un ordine di grandezza simile; ad esempio, se volessimo scoprire se 1000 è primo, dovremmo calcolare 999!: questo non semplificherebbe per niente la scoperta della primalità di 1000.

Capitolo 5

Numeri razionali

5.1 Generalità

Passiamo a considerare ora l'insieme dei numeri razionali, che si indicano con il simbolo **Q** e sono ottenuti dal seguente prodotto cartesiano: $\mathbf{Z} \times \{\mathbf{Z} - \{0\}\}$ che consiste cioè delle coppie ordinate (a,b) con $b \neq 0$ solitamente scritte sotto la forma grafica $\frac{a}{b}$.
Solitamente, si suole chiamare a **numeratore** e b **denominatore** della **frazione** $\frac{a}{b}$.

Due coppie $\frac{a}{b}, \frac{c}{d}$ sono equivalenti se e solo se $\frac{a}{b} = \frac{c}{d}$ cioè se $ad = bc$.
Se $(m, n) = 1$ la frazione $\frac{m}{n}$ si dice **ridotta ai minimi termini**.
Infatti, il numero razionale $\frac{m}{n}$ è definibile come la totalità delle frazioni equivalenti ad esso (ottenibile moltiplicando m ed n per uno stesso intero).

Per cui: **Q** è l'insieme di tutte le frazioni ridotte ai minimi termini.
Z è l'insieme $\subset$ **Q** delle frazioni $\frac{m}{n}$ tali che m è multiplo di n.

5.2 Somma e prodotto in Q

1. Si definisce somma dei due numeri razionali $\frac{a}{b} + \frac{c}{d}$ il numero razionale dato da $\frac{ad+bc}{bd}$.

2. Si definisce prodotto dei due numeri razionali $\frac{a}{b} \cdot \frac{c}{d}$ il numero razionale dato da $\frac{ac}{bd}$.

Anche in questo caso occorre verificare che la definizione è ben posta, cioè che sostituendo a, b, ced con altri elementi l'uguaglianza è sempre valida.
Verifichiamo dunque che se $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ allora $\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd'+b'c'}{b'd'}$.
Ciò equivale a verificare che se $ab' = a'b$ e $cd' = c'd$ allora
per la somma $b'd' \cdot (ad + bc) = bd \cdot (a'd' + b'c')$
e per il prodotto $acb'd' = a'c'bd$.
Infatti, poichè avevamo posto $ab' = a'b$ e $cd' = c'd$, abbiamo $b'd'(ad + cb) = b'd'ad + b'd'cb = (ab')dd' + (cd')bb' = a'bdd' + c'dbb' = bd(a'd' + c'b')eb'd'ac = (ab')(cd') = a'bc'd$. Quindi le definizioni date sono ben poste.

5.3 Il campo Q

$(\mathbf{Q}, +, \cdot)$ è un campo, in cui modulo e ordinamento sono definiti come in $\mathbf{Z}$:
$\forall a, b : a \leq b$ se $\exists c \geq 0$ tale che $b = a + c$. L'ordinamento è totale, compatibile con somma e prodotto.

Capitolo 6

Altri insiemi numerici

Ci sono altri due insiemi numerici di cui diamo delle definizioni sommarie.

6.1 L'insieme R

I numeri reali, indicati dal simbolo $\mathbf{R}$, sono costituiti dai reali razionali (identificabili con $\mathbf{Q}$) che hanno una rappresentazione decimale finita o periodica e dai reali irrazionali, che invece hanno una rappresentazione decimale non finita e aperiodica.
La struttura $(\mathbf{Q}, +, \cdot)$ è un campo. Per i reali razionali vale lo stesso ordinamento dell'insieme $\mathbf{Q}$, per cui tale ordinamento è totale.

6.2 L'insieme C

I numeri complessi si indicano con il simbolo $\mathbf{C}$. La struttura $(\mathbf{C}, +, \cdot)$ è un campo.

Capitolo 7

Alcune strutture fondamentali

7.1 Generalità

Possiamo definire alcune strutture fondamentali. Ad esempio, definiamo queste due operazioni:
$* : A \times B \longrightarrow A$
$\cdot : A \times B \longrightarrow A$
Si considera strutturato il codominio: $(A, *), (A, \cdot)$.
Si dice che A è una struttura su B o che A è una B-struttura.

Consideriamo un campo $\mathbf{K}$ dove $\mathbf{K}$ è uno degli insiemi $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_m$. Noi studieremo gli **spazi vettoriali** V, che sono dei gruppi abeliani che sono anche K-strutture.

7.1.1 Proprietà

Valgono le seguenti proprietà:

1. $\forall v \in V : 1 \cdot v = v$
2. $\forall a, b \in \mathbf{K}, \forall v \in V : a(bv) = (ab)v$
3. $\forall a \in \mathbf{K}, \forall v_1, v_2 \in V : a(v_1 + v_2) = av_1 + av_2$
4. $\forall a, b \in \mathbf{K}, \forall v \in V : (a + b)v = av + bv$

7.2 Il gruppo $(\mathbf{K}^n, +)$

$\mathbf{K}^n$, per $n \geq 1$ intero, è l'insieme delle **n-ple** ordinate di elementi di $\mathbf{K}$ e quindi un suo elemento X è della forma $(x_1, x_2, \ldots, x_i, \ldots, x_n)$ dove x_1 si chiama **prima componente**, x_i è la componente i-esima, x_n la componente n-esima.

7.2.1 Somma di n-ple

La somma di n-ple viene così definita:
$+ : \mathbf{K}^n \times \mathbf{K}^n \longrightarrow \mathbf{K}^n$.
Quindi, date due n-ple $X = (x_1, x_2, \ldots, x_i, \ldots, x_n)$ e $Y = (y_1, y_2, \ldots, y_i, \ldots, y_n)$, la n-pla somma è la seguente:
$X + Y = (x_1 + y_1, x_2 + y_2, \ldots, x_i + y_i, \ldots, x_n + y_n)$

Vogliamo ora dimostrare che la struttura $(\mathbf{K}^n, +$ è un gruppo abeliano. Verifichiamo dunque se valgono le proprietà di un gruppo abeliano:

(i) $(X + Y) + Z = X + (Y + Z)$: la dimostrazione è immediata perchè la somma si effettua componente per componente ottenendo $(x_i + y_i) + z_y = x_i + (y_i + z_i)$, dove le componenti appartengono a $\mathbf{K}$, dove vale la proprietà associativa.

(ii) $X + Y = Y + X$: per lo stesso motivo, anche questa proprietà è verificata

(iii) $\exists 0 = (0, 0, \ldots, 0, \ldots, 0)$, elemento neutro tale che $X + 0 = X$: stesso discorso

(iv) esistenza dell'opposto: si tratta delle componenti cambiate di segno in quanto: $X + (-X) = 0$ (dimostrabile con lo stesso criterio)

7.2.2 Prodotto per scalari

Il prodotto per scalari è un'operazione così definita:
$\cdot : \mathbf{K} \times \mathbf{K}^n \longrightarrow \mathbf{K}^n$. Il prodotto si ottiene moltiplicando per un intero, tutte le componenti della n-pla:
$aX = (ax_1, \ldots, ax_i, \ldots, ax_n)$. Anche in questo caso valgono le proprietà della moltiplicazione, e si nota che se $n = 1$, il prodotto in $\mathbf{K}^n$ equivale al prodotto in $\mathbf{K}$.

Capitolo 8

Matrici

8.1 Generalità

Dato il campo $\mathbf{K}$ si definisce **matrice** del tipo $m \times n$ una tabella della forma:

$$\mathbf{A} = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mj} & \cdots & a_{mn} \end{pmatrix}$$

dove le righe sono n-ple e le colonne sono m-ple. Ogni elemento è dunque contrassegnato dal simbolo a_{ij} dove i indica la riga e j la colonna su cui giace l'elemento.

Quando $m = n$ la matrice si dice quadrata, in caso contrario è rettangolare e allora n si chiama ordine della matrice.
Di solito una matrice $A \in \mathbf{K}^{m,n}$ si indica con $A = (a_{ij})_{i=1,\ldots,m}^{j=1,\ldots,n}$ o semplicemente con (a_{ij}).

8.2 Somma di matrici

La somma di matrici è un'operazione così definita:
$+ : \mathbf{K}^{m,n} \times \mathbf{K}^{m,n} \longrightarrow \mathbf{K}^{m,n}$.
Date $A = (a_{ij}), B = (b_{ij})$ si scrive $A + B = C$, dove $C = (c_{ij})$ è la matrice somma ottenuta dalla somma di elementi omonimi delle due matrici addendi: $c_{ij} = a_{ij} + b_{ij}$.

Anche $\mathbf{K}^{m,n}$ è un gruppo commutativo, in quanto le sue proprietà vanno a cadere in $\mathbf{K}$.

8.3 Prodotto di un numero per una matrice

Il prodotto di un numero per una matrice è un'operazione che si esegue moltiplicando ogni elemento della matrice per l'intero. In simboli:
$a \cdot A = C$ dove $C = (c_{ij})$ e $c_{ij} = a \cdot (a_{ij})$.

8.4 Prodotto righe per colonne di matrici

Date le due matrici $A \in \mathbf{K}^{m,n}, B \in \mathbf{K}^{n,p}$ in cui cioè il numero di colonne di A è uguale al numero di righe di B.
Sapendo che $A = (a_{rs}), B = (b_{hk})$, scriviamo $A \cdot B = C$ dove gli elementi della matrice C sono così individuati:
$c_{ij} = \sum_{q=1}^{n} a_{iq} \cdot b_{qj}$.
$C \in \mathbf{K}^{m,p}$ cioè la matrice risultante dal prodotto ha lo stesso numero di righe di A e lo stesso numero di colonne di B.

Praticamente si esegue la somma tra il prodotto di ogni elemento di una riga di A con ogni elemento di una colonna di B. Un esempio pratico:

$$\begin{pmatrix} 2 & 3 & 1 \\ 4 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 & 4 & 3 \\ 2 & 1 & 3 & 1 \\ 3 & 3 & 2 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 2\cdot 3+3\cdot 2+1\cdot 3 & 2\cdot 1+3\cdot 1+1\cdot 3 & 2\cdot 4+3\cdot 3+1\cdot 2 & 2\cdot 3+3\cdot 1+1\cdot 1 \\ 4\cdot 3+3\cdot 2+2\cdot 3 & 4\cdot 1+3\cdot 1+2\cdot 3 & 4\cdot 4+3\cdot 3+2\cdot 2 & 4\cdot 3+3\cdot 1+2\cdot 1 \end{pmatrix}$$

8.4.1 Proprietà del prodotto tra matrici

(i) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$

(ii) $(a \cdot A) \cdot B = A \cdot (a \cdot B) = a \cdot (A \cdot B)$

(iii-i) $(A + B) \cdot C = AC + BC$

(iii-ii) $C \cdot (A + B) = CA + CB$

8.5 Matrice trasposta

Si definisce trasposta quella matrice ottenuta scambiando le righe con le colonne.
In simboli:
data la matrice $A \in \mathbf{K}^{m,n}$, la sua trasposta è la matrice $A^t \in \mathbf{K}^{n,m}$ tale che $a^t_{ij} = a_{ji}$.

Nota che $(A^t)^t = A$ e che $(AB)^t = B^t A^t$ cioè la trasposta di un prodotto è il prodotto delle trasposte con l'ordine scambiato.

8.6 Matrici quadrate

Per matrice quadrata si intende una matrice in cui il numero di righe è uguale al numero di colonne, cioè $A \in \mathbf{K}, m = n$. In questo caso il numero m viene denominato ordine della matrice.

Si dice **diagonale principale** la n-pla formata dagli elementi a_{ij} in cui $i = j$. Si dice **diagonale secondaria** la n-pla formata dagli elementi a_{ij} in cui $i + j = n + 1$.
I due elementi a_{ij} e a_{ji} si dicono **coniugati**.

Vediamo ora alcuni particolari tipi di matrici che meritano una nomenclatura che li differenzi:

- **Matrice identica**

  È la matrice in cui sono nulli tutti gli elementi ad esclusione di quelli della diagonale principale:

  $$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

  Per cui: $I = (\delta_{ij})$ dove vale la seguente proprietà:

  $$(\delta_{ij}) = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

- **Matrice triangolare alta**
  Si tratta di una matrice in cui sono nulli tutti gli elementi sotto la diagonale principale.

- **Matrice triangolare bassa**
  Si tratta di una matrice in cui sono nulli tutti gli elementi sopra la diagonale principale.

- **Matrice diagonale**
  Si tratta di una matrice in cui sono nulli tutti gli elementi che non stanno sulla diagonale principale (ovvero è una matrice contemporaneamente triangolare alta e bassa).

Da ciò che abbiamo detto è evidente che il prodotto in $\mathbf{K}^{n,n}$ è sempre possibile e che quindi $(\mathbf{K}^{n,n}, \cdot)$ è un monoide il cui elemento neutro è la matrice identità di ordine n, mentre $(\mathbf{K}^{n,n}, +, \cdot)$ è un anello non commutativo.