Matematica Discreta

Luca De Paulis

21 maggio 2020

INDICE

1

INSIEMI NUMERICI

1.1 STRUTTURE ALGEBRICHE FONDAMENTALI

Definizione 1.1.1 (Gruppo)
Si dice **gruppo** una tripla $(G, \cdot, e)$ formata da

- un insieme di elementi G;
- un operazione $\cdot : A \times A \to A$ detta prodotto;
- un elemento $e \in G$

per cui valgono i seguenti assiomi:

(ASSIOMI DI GRUPPO) Per ogni $a, b, c \in G$ vale che

(P1)	$(ab) \in G$	(chiusura rispetto a $\cdot$)
(P2)	$(ab)c = a(bc)$	(associatività di $\cdot$)
(P3)	$a \cdot e = e \cdot a = a$	(e el. neutro di $\cdot$)
(P4)	$\exists a^{-1} \in G. \quad aa^{-1} = e$	(inverso per $\cdot$)

Si dice **gruppo commutativo** un gruppo per cui vale inoltre il seguente assioma:

(P5)	$ab = ba$	(commutatività di $\cdot$)

Definizione 1.1.2 (Anello)
Si dice **anello** una quintupla $(A, +, \cdot, 0, 1)$ formata da

- un insieme di elementi A;
- un operazione $+ : A \times A \to A$ detta somma;
- un operazione $\cdot : A \times A \to A$ detta prodotto;
- un elemento $0 \in A$;
- un elemento $1 \in A$

per cui valgono i seguenti assiomi:

(ASSIOMI DI ANELLO) Per ogni $a, b, c \in A$ vale che

(S1)	$(a+b) \in A$	(chiusura rispetto a $+$)
(S2)	$a+b=b+a$	(commutatività di $+$)
(S3)	$(a+b)+c=a+(b+c)$	(associatività di $+$)
(S4)	$a+0=0+a=a$	(o el. neutro di $+$)
(S5)	$\exists(-a) \in A. \quad a+(-a)=0$	(opposto per $+$)
(P1)	$(ab) \in A$	(chiusura rispetto a $\cdot$)
(P2)	$(ab)c=a(bc)$	(associatività di $\cdot$)
(P3)	$a \cdot 1=1 \cdot a=a$	(1 el. neutro di $\cdot$)
(P4)	$(a+b)c=ac+bc$	(distributività 1)
(P5)	$a(b+c)=ab+ac$	(distributività 2)

Si dice **anello commutativo** un anello per cui vale inoltre il seguente assioma:

(P6)	$ab=ba$	(commutatività di $\cdot$)

Un tipico esempio di anello commutativo è $\mathbb{Z}$: infatti gli anelli generalizzano le operazioni che possiamo fare sui numeri interi e le loro proprietà fondamentali per estenderle ad altri insiemi con la stessa struttura algebrica.

Definizione 1.1.3 (Campo)

Si dice **campo** una quintupla $(F, +, \cdot, 0, 1)$ formata da

- un insieme di elementi F;
- un operazione $+ : F \times F \to F$ detta somma;
- un operazione $\cdot : F \times F \to F$ detta prodotto;
- un elemento $0 \in F$;
- un elemento $1 \in F$

per cui valgono i seguenti assiomi:

(ASSIOMI DI CAMPO) Per ogni $a, b, c \in F$ vale che

(S1)	$(a+b) \in F$	(chiusura rispetto a $+$)
(S2)	$a+b=b+a$	(commutatività di $+$)
(S3)	$(a+b)+c=a+(b+c)$	(associatività di $+$)
(S4)	$a+0=0+a=a$	(o el. neutro di $+$)
(S5)	$\exists(-a) \in F. \quad a+(-a)=0$	(opposto per $+$)
(P1)	$(ab) \in F$	(chiusura rispetto a $\cdot$)
(P2)	$ab=ba$	(commutatività di $\cdot$)
(P3)	$(ab)c=a(bc)$	(associatività di $\cdot$)
(P4)	$a \cdot 1=1 \cdot a=a$	(1 el. neutro di $\cdot$)
(P5)	$(a+b)c=ac+bc$	(distributività)
(P6)	$a \neq 0 \implies \exists a^{-1} \in F. \quad aa^{-1}=1$	(inverso per $\cdot$)

La definizione sopra è equivalente a dire che F è un anello commutativo per cui ogni elemento non nullo ha un inverso moltiplicativo.

Tra gli insiemi numerici classici, gli insiemi $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ sono tutti esempi di campi: infatti le operazioni di addizione e moltiplicazione sono chiuse

rispetto all'insieme, rispettano le proprietà commutativa, associativa e distributiva ed esistono gli inversi per la somma e per il prodotto (per ogni numero diverso da 0). Il concetto di campo serve quindi a generalizzare la struttura algebrica dei numeri razionali/reali/complessi per altri insiemi numerici.

Nei campi vale la seguente proposizione.

Proposizione 1.1.4 (Regola di annullamento del prodotto)
Sia $\mathbb{K}$ *un campo e siano* $a, b \in \mathbb{K}$. *Allora*

$$ab = 0 \implies a = 0 \vee b = 0.$$

Dimostrazione. Sappiamo che $a = 0 \vee b = 0$ è equivalente a $a \neq 0 \implies b = 0$, dunque supponiamo che a sia diverso da 0 e dimostriamo che b è zero.

Dato che $a \neq 0$ allora ammette un inverso. Chiamiamolo a^{-1} e moltiplichiamo entrambi i membri per esso:

$$\begin{aligned} & a^{-1}(ab) = a^{-1} \cdot 0 \\ \iff & (a^{-1}a)b = 0 \\ \iff & b = 0 \end{aligned}$$

che è la tesi. □

1.2 NUMERI COMPLESSI

Definizione 1.2.1 (Unità immaginaria)
Si dice unità immaginaria il numero i tale che

$$i^2 = -1.$$

Definizione 1.2.2 (Numeri complessi)
L'insieme dei numeri complessi $\mathbb{C}$ è l'insieme dei numeri della forma $a + ib$ per qualche $a, b \in \mathbb{R}$, ovvero

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}.$$

Definizione 1.2.3 (Parte reale e immaginaria)
Sia $z \in \mathbb{C}$ tale che $z = a + ib$. Allora si dicono rispettivamente

- parte reale di z il numero $\mathrm{Re}(z) = a$;
- parte immaginaria di z il numero $\mathrm{Im}(z) = b$.

Definizione 1.2.4 (Somma e prodotto sui complessi)
Definiamo le seguenti due operazioni su $\mathbb{C}$:

- $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ tale che $(a + ib) + (c + id) = (a + c) + i(b + d)$;
- $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ tale che $(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc)$.

Osservazione. Le due operazioni vengono naturalmente dalla somma e dal prodotto tra monomi. Infatti

$$\begin{aligned} (a + ib) + (c + id) &= a + c + ib + id = (a + c) + i(b + d); \\ (a + ib) \cdot (c + id) &= ac + iad + ibc + i^2bd \\ &= ac + i(ad + bc) - bd \\ &= (ac - bd) + i(ad + bc). \end{aligned}$$

Notiamo che i numeri complessi della forma $a + i0$ sono numeri reali, dunque $\mathbb{R} \subset \mathbb{C}$. Inoltre possiamo rappresentare i numeri complessi come punti in uno spazio bidimensionale dove la parte reale rappresenta l'ascissa e la parte immaginaria rappresenta l'ordinata: la retta corrispondente all'asse x è il sottoinsieme dei numeri reali.

Definizione 1.2.5 (Coniugato complesso)

Sia $z = a + ib \in \mathbb{C}$. Allora si dice coniugato complesso (o semplicemente coniugato) di z il numero

$$\overline{z} = a - ib.$$

Definizione 1.2.6 (Norma di un numero complesso)

Sia $z = a + ib \in \mathbb{C}$. Allora si dice norma di z il numero reale

$$|z| = \sqrt{a^2 + b^2}.$$

Notiamo che $|z| = 0$ se e solo se $a = b = 0$, ovvero se $z = 0$.

Proposizione 1.2.7

Siano $z, w \in \mathbb{C}$ tali che $z = a + ib$, $w = c + id$. Allora

(i) $\overline{z} + \overline{w} = \overline{z + w}$;

(ii) $\overline{z} \cdot \overline{w} = \overline{zw}$;

(iii) $(\overline{z})^n = \overline{z^n}$.

Dimostrazione. Dimostriamo i tre fatti.

(i) Per definizione di somma

$$\begin{aligned} \overline{z} + \overline{w} &= (a - ib) + (c - id) \\ &= (a + c) - i(b + d) \\ &= \overline{z + w}. \end{aligned}$$

(ii) Per definizione di prodotto

$$\begin{aligned} \overline{z} \cdot \overline{w} &= (a - ib)(c - id) \\ &= (ac - bd) + i(-ad - bc) \\ &= (ac - bd) - i(ad + bc) \\ &= \overline{zw}. \end{aligned}$$

(iii) Dimostriamolo per induzione su n.

CASO BASE. Se $n = 1$ allora banalmente $(\overline{z})^1 = \overline{z} = \overline{z^1}$.

PASSO INDUTTIVO. Supponiamo che la tesi valga per n e dimostriamola per $n + 1$. Allora

$$(\overline{z})^{n+1} = (\overline{z})^n \cdot \overline{z} = \overline{z^n} \cdot \overline{z} = \overline{z^{n+1}}$$

dove l'ultimo passaggio è giustificato dal punto precedente della dimostrazione. □

Proposizione 1.2.8

Sia $z = a + ib \in \mathbb{C}$. Allora valgono i seguenti fatti:

(i) $z + \overline{z} = 2\,\mathrm{Re}(z)$;

(ii) $z\overline{z} = |z|^2$.

Dimostrazione. Dimostriamo i due fatti.

(i) Per definizione di somma $z + \overline{z} = (a + ib) + (a - ib) = 2a = 2\,\mathrm{Re}(z)$.

(ii) Per definizione di prodotto

$$z\overline{z} = (a + ib)(a - ib) = a^2 - iab + iab - i^2b^2 = a^2 + b^2 = |z|^2 . \qquad \square$$

La proposizione precedente ci consente di trovare l'inverso di qualunque numero non nullo in $\mathbb{C}$.

Proposizione 1.2.9 (Inverso tra i complessi)
Sia $z \in \mathbb{C}, z \neq 0$. Allora

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2}.$$

Dimostrazione. Per la proposizione 1.2.8 segue che

$$z\overline{z} = |z|^2 \iff \frac{1}{z} = \frac{\overline{z}}{|z|^2}. \qquad \square$$

Proposizione 1.2.10 (I numeri complessi formano un campo)
L'insieme $\mathbb{C}$ insieme alle operazioni di somma e prodotto con i rispettivi elementi neutri $0, 1 \in \mathbb{C}$ forma un campo.

1.2.1 *Rappresentazione polare dei numeri complessi*

Dato che possiamo considerare i numeri complessi come punti di un piano bidimensionale possiamo rappresentarli in forma polare, cioè considerando il vettore che congiunge l'origine degli assi con il punto (a, b) che rappresenta il numero complesso $a + ib$. La forma polare di un numero complesso è data dalla coppia (r, θ), dove r è il raggio del vettore e θ è l'angolo tra l'asse x e il vettore.

Dunque se $z = a + ib$ è un numero complesso in forma cartesiana, possiamo esprimerlo come $r(\cos\theta + i\sin\theta)$, dove $r = \sqrt{a^2 + b^2} = |z|$ e $\theta = \arctan\frac{a}{b}$.

> **Definizione 1.2.11** (Esponenziale complesso)
> $e^{i\theta} = \cos\theta + i\sin\theta$.

Sfruttando la definizione precedente possiamo scrivere ogni numero complesso nella forma $re^{i\theta}$ che è la forma polare del numero.

Proposizione 1.2.12
Siano $e^{i\alpha}, e^{i\beta} \in \mathbb{C}$. Allora vale

$$e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}.$$

Dimostrazione. Per definizione di esponenziale complesso:

$$\begin{aligned} e^{i\alpha}e^{i\beta} &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) \\ &= \cos(\alpha + \beta) + i\sin(\alpha + \beta) \\ &= e^{i(\alpha+\beta)}. \end{aligned}$$

$\square$

2

DIVISORI E MCD

2.1 DIVISORI DI UN NUMERO

2.1.1 *Definizioni e prime conseguenze*

Definizione 2.1.1 (Divisore)

Siano $a, b \in \mathbb{Z}$; allora si dice che a divide b se $\exists k \in \mathbb{Z}$ tale che $ak = b$, e si scrive $a \mid b$.

Definizione 2.1.2 (Multiplo)

Siano $a, b \in \mathbb{Z}$. Allora si dice che b è multiplo di a se $\exists k \in \mathbb{Z}$ tale che $b = ak$.

Osservazione. La definizione di multiplo è speculare a quella di divisore: se a è divisore di b allora b è multiplo di a.

Proposizione 2.1.3

Siano $a, b, n \in \mathbb{Z}$ tali che $n \mid a$ e $n \mid b$. Allora

$$n \mid a + b \tag{1}$$
$$n \mid a - b \tag{2}$$
$$n \mid ax \qquad \forall x \in \mathbb{Z} \tag{3}$$

Dimostrazione. Per ipotesi, dato che $n \mid a$ e $n \mid b$, allora $\exists h, k \in \mathbb{Z}$ tali che $nh = a$ e $nk = b$. Dunque:

$$\begin{aligned} a + b = nh + nk = n(h + k) &\iff n \mid a + b \\ a - b = nh - nk = n(h - k) &\iff n \mid a - b \\ ax = nhx = n(hx) &\iff n \mid ax \end{aligned}$$

che è la tesi. □

Definizione 2.1.4 (Massimo comun divisore)

Siano $a, b \in \mathbb{Z}$; allora si dice $\text{mcd}(a, b)$ il piu' grande intero positivo tale che $\text{mcd}(a, b) \mid a$ e $\text{mcd}(a, b) \mid b$.

Definizione 2.1.5 (Minimo comune multiplo)

Siano $a, b \in \mathbb{Z}$. Allora si dice minimo comune multiplo di a e b il numero $d = \text{mcm}(a, b)$ tale che d è il piu' piccolo multiplo positivo sia di a che di b.

Definizione 2.1.6 (Coprimo)

Siano $a, b \in \mathbb{Z}$. Se $\text{mcd}(a, b) = 1$ allora a e b si dicono coprimi.

OSSERVAZIONE. Siano $a, b \in \mathbb{Z}$. Allora valgono le seguenti proprietà per $\mathrm{mcd}\,(a, b)$:

$$\begin{aligned} \mathrm{mcd}\,(a, b) &= \mathrm{mcd}\,(\pm a, \pm b) \\ \mathrm{mcd}\,(a, 1) &= \mathrm{mcd}\,(1, a) = 1 \\ \mathrm{mcd}\,(a, 0) &= \mathrm{mcd}\,(0, a) = 0 \\ \nexists\, &\mathrm{mcd}\,(0, 0) \end{aligned}$$

Teorema 2.1.7 (Esistenza e unicità del resto)

Siano $a, b \in \mathbb{Z}$, con $b \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che

$$a = bq + r, \qquad 0 \leq r < |b| \tag{4}$$

Tale r si dice resto della divisione di a per b, e si indica anche con $r = a \bmod b$.

Dimostrazione. Notiamo che i numeri della forma $a - bq$ formano una progressione aritmetica di passo b al variare di $q \in \mathbb{Z}$. Il resto r definito in questo modo è l'unico elemento di questa progressione compreso tra 0 e $b - 1$. □

Proposizione 2.1.8

Siano $a, b, c \in \mathbb{Z}$. Allora

$$\mathrm{mcm}\,(a, b) \mid c \iff a \mid c \wedge b \mid c \tag{5}$$

Dimostrazione. Dimostriamo separatamente i due versi dell'implicazione.

($\Longrightarrow$) Dato che $\mathrm{mcm}\,(a, b)$ è un multiplo di a e di b e per ipotesi c è un multiplo di $\mathrm{mcm}\,(a, b)$, allora per transitività segue che c è un multiplo di a e di b.

($\Longleftarrow$) Supponiamo che c sia un multiplo di a e di b. Allora per il teorema 2.1.7 esistono $q, r \in \mathbb{Z}$ tali che

$$c = \mathrm{mcm}\,(a, b)\, q + r$$

con $0 \leq r < \mathrm{mcm}\,(a, b)$. Dato che a, b dividono sia c (per ipotesi) che $\mathrm{mcm}\,(a, b)$ (per definizione di mcm), allora segue che essi dividono anche r. Ma $0 \leq r < \mathrm{mcm}\,(a, b)$, dunque necessariamente $r = 0$, cioè $c = \mathrm{mcm}\,(a, b)\, q$ e quindi $\mathrm{mcm}\,(a, b) \mid c$. □

2.1.2 *Algoritmo di Euclide e Teorema di Bezout*

Teorema 2.1.9

Siano $a, b \in \mathbb{Z}$. Allora

$$\mathrm{mcd}\,(a, b) = \mathrm{mcd}\,(a, b - a) = \mathrm{mcd}\,(a - b, b)\,. \tag{6}$$

Dimostrazione. Ovviamente $\mathrm{mcd}\,(a, b) = \mathrm{mcd}\,(b, a)$, dunque se vale la prima uguaglianza varrà anche la seconda, in quanto

$$\mathrm{mcd}\,(a, b) = \mathrm{mcd}\,(b, a) = \mathrm{mcd}\,(b, a - b) = \mathrm{mcd}\,(a - b, b)\,.$$

Dunque è sufficiente dimostrare che $\mathrm{mcd}\,(a, b) = \mathrm{mcd}\,(a, b - a)$. Sia $\mathbb{D}_{x,y}$ l'insieme dei divisori comuni a x e y, cioe'

$$\mathbb{D}_{x,y} = \{d \text{ tale che } d \mid x \wedge d \mid y\}$$

Allora per dimostrare la tesi è sufficiente dimostrare che $\mathbb{D}_{a,b} = \mathbb{D}_{a,b-a}$, in quanto se i due insiemi sono uguali necessariamente anche i loro massimi saranno uguali.

Dimostriamo che $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$. Sia $d \in \mathbb{D}_{a,b}$, cioè $d \mid a$ e $d \mid b$. Allora per la proposizione 2.1.3 segue che $d \mid b - a$, cioè $d \in \mathbb{D}_{a,b-a}$, cioè $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$.
Dimostriamo ora che $\mathbb{D}_{a,b-a} \subseteq \mathbb{D}_{a,b}$. Sia $d \in \mathbb{D}_{a,b-a}$, cioè $d \mid a$ e $d \mid b - a$. Allora per la proposizione 2.1.3 segue che $d \mid a + (b - a)$, cioè $d \mid b$, cioè $d \in \mathbb{D}_{a,b}$, cioè $\mathbb{D}_{a,b-a} \subseteq \mathbb{D}_{a,b}$.
Dunque dato che valgono sia $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$ e $\mathbb{D}_{a,b-a} \subseteq \mathbb{D}_{a,b}$, allora vale $\mathbb{D}_{a,b} = \mathbb{D}_{a,b-a}$. In particolare il massimo di questi due insiemi dovrà essere lo stesso, quindi $\operatorname{mcd}(a, b) = \operatorname{mcd}(a, b - a)$, che è la tesi. □

Dunque per calcolare il massimo comun divisore si puo' sfruttare il seguente algoritmo, detto **algoritmo di Euclide**, che si basa sul teorema 2.1.9:

1. Se $a = 1$ oppure $b = 1$ allora $\operatorname{mcd}(a, b) = 1$.
2. Se $a = 0$ e $b \neq 0$ allora $\operatorname{mcd}(a, b) = b$.
3. Se $a \neq 0$ e $b = 0$ allora $\operatorname{mcd}(a, b) = a$.
4. Se $a \neq 0$ e $b \neq 0$, allora
   - se $a \leq b$ segue che $\operatorname{mcd}(a, b) = \operatorname{mcd}(a - b, b)$;
   - se $a > b$ segue che $\operatorname{mcd}(a, b) = \operatorname{mcd}(a, b - a)$

   dove i valori di $\operatorname{mcd}(a - b, b)$ o $\operatorname{mcd}(a, b - a)$ vengono calcolati riapplicando l'algoritmo.

Teorema 2.1.10 (Teorema di Bezout)
Siano $a, b \in \mathbb{Z}$. Allora esistono $x, y \in \mathbb{Z}$ tali che

$$ax + by = \operatorname{mcd}(a, b). \tag{7}$$

2.1.3 *Conseguenze del teorema di Bezout*

Elenchiamo in questa sezione alcune conseguenze del teorema di Bezout sulle proprietà dei divisori e sul loro rapporto con il massimo comun divisore di due numeri.

Proposizione 2.1.11
Siano $a, b, n \in \mathbb{Z}$. Allora

$$n \mid ab \wedge \operatorname{mcd}(a, n) = 1 \implies n \mid b. \tag{8}$$

INTUIZIONE. Se n divide ab, allora tutti i fattori primi che dividono n dovranno essere contenuti in ab. Dato che $\operatorname{mcd}(n, a) = 1$, questi fattori non possono essere contenuti in a, dunque dovranno essere tutti contenuti in b.

Dimostrazione. Per il teorema di Bezout (2.1.10) esistono $x, y \in \mathbb{Z}$ tali che

$$ax + ny = \operatorname{mcd}(a, n) = 1$$

Moltiplicando per b otteniamo

$$abx + nby = b$$

Ma $n \mid abx$ (poiche $n \mid ab$) e $n \mid nby$, dunque $n \mid abx + nby$, cioè $n \mid b$. □

Proposizione 2.1.12
Siano $a, b, t \in \mathbb{Z}$ tali che $t \mid a$, $t \mid b$. Allora $t \leq \operatorname{mcd}(a, b)$.

Dimostrazione. La proposizione deriva direttamente dalla definizione di massimo comun divisore: se t è un divisore comune ad a e b, allora t sarà minore o uguale al massimo dei divisori comuni di a e b, cioè $t \leq \operatorname{mcd}(a, b)$. □

Proposizione 2.1.13

Siano $a, b, t \in \mathbb{Z}$ tali che $t \mid a$, $t \mid b$. Allora $t \mid \mathrm{mcd}(a, b)$.

Dimostrazione. Per la proposizione 2.1.3, se $t \mid a$ e $t \mid b$ allora $t \mid ax + by$ per ogni $x, y \in \mathbb{Z}$.

Per il teorema di Bezout (2.1.10) esistono $\bar{x}, \bar{y} \in \mathbb{Z}$ tali che $a\bar{x} + b\bar{y} = \mathrm{mcd}(a, b)$. Ma quest'espressione è della forma $ax + by$, con $x = \bar{x}$, $y = \bar{y}$, dunque $t \mid a\bar{x} + b\bar{y}$, cioè $t \mid \mathrm{mcd}(a, b)$. □

Proposizione 2.1.14

Siano $a, b, t \in \mathbb{Z}$. Allora

$$t \mid \mathrm{mcd}(a, b) \iff (\forall x, y \in \mathbb{Z}. \quad t \mid ax + by). \tag{9}$$

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Se $t \mid \mathrm{mcd}(a, b)$, allora $t \mid a$ e $t \mid b$, dunque per la proposizione 2.1.3 segue che t dovrà dividere una qualsiasi combinazione lineare di a e b, cioè $t \mid ax + by$ per ogni $x, y \in \mathbb{Z}$.

($\Longleftarrow$) Viceversa supponiamo che $t \mid ax + by$ per ogni $x, y \in \mathbb{Z}$. Siano per il teorema di Bezout (2.1.10) $\bar{x}, \bar{y}$ i numeri tali che $a\bar{x} + b\bar{y} = \mathrm{mcd}(a, b)$. Allora t dovrà dividere anche $a\bar{x} + b\bar{y}$, cioè $t \mid \mathrm{mcd}(a, b)$. □

Proposizione 2.1.15

Siano $a, b, n \in \mathbb{Z}$. Allora

$$\mathrm{mcd}(an, bn) = n \,\mathrm{mcd}(a, b). \tag{10}$$

INTUIZIONE. Se due numeri hanno n come fattore comune, ovviamente il massimo comun divisore dovrà contenere n e quindi dovrà essere un multiplo di n.

Dimostrazione. Osserviamo che se due numeri hanno gli stessi divisori allora sono uguali, a meno del segno. Sia $t \in \mathbb{Z}$ tale che $t \mid an$ e $t \mid nb$. Per la proposizione 2.1.14 allora

$$\begin{aligned} & t \mid \mathrm{mcd}(an, bn) \\ \iff & t \mid nax + nby \qquad \forall x, y \in \mathbb{Z} \\ \iff & t \mid n(ax + by) \qquad \forall x, y \in \mathbb{Z} \end{aligned}$$

dunque scegliendo x, y tali che $ax + by = \mathrm{mcd}(a, b)$ per Bezout (2.1.10)

$$\iff t \mid n \,\mathrm{mcd}(a, b).$$ □

Corollario 2.1.16

Siano $a, b \in \mathbb{Z}$ e sia $d = \mathrm{mcd}(a, b)$. Allora $\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

INTUIZIONE. Se dividiamo due numeri per il loro mcd stiamo eliminando dalla loro fattorizzazione tutti i primi comuni ad entrambi, quindi i due numeri risultanti dall'operazione non potranno avere primi in comune e quindi saranno coprimi.

Dimostrazione. Siano a', b' tali che $a = a'd, b = b'd$. Allora per la proposizione 2.1.15

$$\begin{aligned} \mathrm{mcd}(a, b) &= \mathrm{mcd}(a'd, b'd) \\ &= d \,\mathrm{mcd}(a', b') \\ &= \mathrm{mcd}(a, b) \,\mathrm{mcd}(a', b'). \end{aligned}$$

Dividendo entrambi i membri per $\text{mcd}\,(a,b)$ otteniamo

$$\text{mcd}\,(a',b') = 1$$

che, per definizione di a', b', è equivalente a

$$\text{mcd}\left(\frac{a}{d'},\frac{b}{d}\right) = 1$$

che è la tesi. □

2.2 NUMERI PRIMI

> **Definizione 2.2.1** (Numero primo)
>
> Sia $p \in \mathbb{Z}$. Si dice che p è primo se se gli unici interi che dividono p sono ± 1 e $\pm p$.

Proposizione 2.2.2

Se p è primo e $p \mid ab$, allora $p \mid a$ oppure $p \mid b$.

Dimostrazione. Supponiamo $p \nmid a$. Dato che p è primo, $\text{mcd}\,(a,p) = 1$ oppure p. Tuttavia se $\text{mcd}\,(a,p) = p$ allora $p \mid a$, che va contro l'ipotesi, dunque $\text{mcd}\,(a,p) = 1$. Per la proposizione 2.1.11 allora $p \mid b$, che è la tesi. □

Proposizione 2.2.3

Siano $a, b \in \mathbb{Z}, c \in \mathbb{Z}$ tali che $\text{mcd}\,(a,b) = 1$. Allora

$$a \mid c \wedge b \mid c \iff ab \mid c. \tag{11}$$

Dimostrazione. Per il teorema di Bezout (2.1.10) esistono $x, y \in \mathbb{Z}$ tali che $\text{mcd}\,(a,b) = 1 = ax + by$, da cui segue $n = nax + nby$.

Dato che $a \mid n$, $b \mid n$, allora $ab \mid na$ e $ab \mid nb$ per la proposizione 2.1.3, quindi per la stessa proposizione ab dividerà una loro qualunque combinazione lineare $nak + nbh$, inclusa quella con $k = x, h = y$.

Dunque $ab \mid nax + nby$ che è equivalente a dire che $ab \mid n$, cioè la tesi. □

Proposizione 2.2.4

Siano $a, b, c \in \mathbb{Z}$. Allora

$$\text{mcd}\,(ab,c) = 1 \iff \text{mcd}\,(a,c) = \text{mcd}\,(b,c) = 1. \tag{12}$$

INTUIZIONE. Dimostrazione intuitiva: se a e b sono coprimi con c significa che a non ha nessun fattore in comune con c, e stessa cosa per b. Ma il loro prodotto ab viene diviso dagli stessi primi che dividono a e b separatamente, quindi deve essere anch'esso coprimo con c.

Al contrario, se ab non ha fattori primi in comune con c, allora naturalmente a, b (essendo divisori di ab) non avranno fattori in comune con c.

Corollario 2.2.5

Siano $a_1, a_2, \ldots, a_n \in \mathbb{Z}, c \in \mathbb{Z}$ tali che $a_1, \ldots, a_n$ siano coprimi con c. Allora anche il loro prodotto $\prod_{i=1}^{n} a_i$ è coprimo con c.

INTUIZIONE. Stessa idea della dimostrazione della proposizione 2.2.4 ma estesa a n numeri.

Proposizione 2.2.6

Siano $a_1, a_2, \ldots, a_n \in \mathbb{Z}, c \in \mathbb{Z}$ tali che $a_1, \ldots, a_n$ siano coprimi tra loro e che per ogni $i < n$ vale che $a_i \mid c$. Allora

$$a_1 a_2 \ldots a_n = \left(\prod_{i=1}^{n} a_i\right) \mid c. \tag{13}$$

INTUIZIONE. Quest'ultima proposizione ci dice che se $a_1, \ldots, a_n$ non hanno fattori primi in comune e ognuno di loro divide c, allora anche il loro prodotto dovrà dividere c, perché il loro prodotto è formato esattamente dai fattori primi che dividono c.

Dimostrazione. Dimostriamo la proposizione per induzione su n.

CASO BASE. Sia $n = 0$, cioè $a_1 \ldots a_n = 1$. Allora banalmente $1 \mid c$.

PASSO INDUTTIVO. Supponiamo che la tesi sia vera per $n-1$ e dimostriamola per n. Dunque per ipotesi $\left(\prod_{i=1}^{n-1} a_i\right) \mid c$. Ma per il corollario 2.2.5 a_n è coprimo con $\prod_{i=1}^{n-1} a_i$, dunque per la proposizione 2.2.3 segue che

$$a_n \left(\prod_{i=1}^{n-1} a_i\right) = \left(\prod_{i=1}^{n} a_i\right) \mid c$$

che è la tesi per n.

Dunque la proposizione vale per ogni $n \in N$. □

2.2.1 *Divisori primi*

Proposizione 2.2.7 (Esistenza della scomposizione in primi)

Sia $n \in \mathbb{Z}, n > 1$. Allora n puo' essere espresso come prodotto di potenze di numeri primi.

Dimostrazione. Per induzione forte su n.

CASO BASE. Sia $n = 2$. Dato che 2 è primo, allora è esprimibile come prodotto di numeri primi (in particolare è il prodotto di un solo termine, se stesso).

PASSO INDUTTIVO. Supponiamo che la tesi sia vera per $2, 3, \ldots, n-1$ (induzione forte) e dimostriamola per n. Abbiamo due casi:

- se n è primo, allora è un prodotto di primi e quindi la tesi vale;
- se n non è primo allora dovranno esistere due numeri $1 < a, b < n$ tali che $n = ab$ (infatti se non esistessero n sarebbe primo). Ma per l'ipotesi induttiva forte sappiamo che tutti i numeri compresi tra 2 e $n-1$ inclusi sono scomponibili in fattori primi, dunque anche $n = ab$ dovrà esserlo.

Dunque dal caso base e dal passo induttivo segue che la tesi vale per ogni $n \geq 2$. □

Teorema 2.2.8 (Teorema fondamentale dell'aritmetica)

Sia $n \in \mathbb{Z}$ e siano $p_1, p_2, \ldots, p_k$ i primi che dividono n. Inoltre siano $e_1, e_2, \ldots, e_k$ i massimi esponenti per cui vale che $p_i^{e_i} \mid n$ per ogni $1 \leq i \leq k$. Allora $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

Dimostrazione. Per la proposizione 2.2.7 sappiamo che esistono $p_1, \dots, p_n$. Per la proposizione 2.2.5 segue che

$$p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \mid n$$

in quanto $p_1^{e_1}, p_2^{e_2}, \dots, p_k^{e_k}$ sono coprimi tra loro.

Dunque $n = m \cdot p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ per qualche $m \in \mathbb{Z}$. Supponiamo per assurdo che $m \neq 1$. Allora per la proposizione 2.2.7 m è scomponibile in numeri primi; ma dato che m è un divisore di n segue che i primi che dividono m devono dividere anche n, dunque i primi che dividono m devono essere tra $p_1, \dots, p_k$.

Supponiamo senza perdita di generalità che p_i divida m. Allora dato che $m \cdot p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = n$ deve essere $p_i \cdot p_i^{e_i} = p_i^{e_i+1} \mid n$, che è assurdo in quanto abbiamo supposto che e_i fosse il massimo esponente per cui $p_i^{e_i} \mid n$.

Dunque deve essere $m = 1$, cioè

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

come volevasi dimostrare. □

Proposizione 2.2.9

Siano $a, b, k \in \mathbb{Z}$, $p \in \mathbb{Z}$ primo. Allora

$$p^k \mid \operatorname{mcd}(a,b) \iff p^k \mid a \wedge p^k \mid b \tag{14}$$

$$p^k \mid \operatorname{mcm}(a,b) \iff p^k \mid a \vee p^k \mid b. \tag{15}$$

INTUIZIONE. Il massimo comun divisore di due numeri è un divisore comune ad entrambi, quindi se p^k lo divide deve dividere entrambi i numeri.

Il minimo comune multiplo invece è formato da tutti i fattori primi comuni e non comuni col massimo esponente, quindi se p^k divide il minimo comune multiplo dovrà dividere almeno uno dei due numeri di partenza.

Proposizione 2.2.10

Siano $a, b \in \mathbb{Z}$. Allora se $\operatorname{mcd}(a,b) = 1$ segue che $\operatorname{mcm}(a,b) = |ab|$.

INTUIZIONE. Se i due numeri sono coprimi, allora non hanno fattori primi in comune, dunque il loro minimo comune multiplo sarà formato precisamente da tutti i fattori di entrambi i numeri, cioè dal loro prodotto.

Dimostrazione. Sappiamo per definizione di mcm che $a \mid \operatorname{mcm}(a,b)$ e $b \mid \operatorname{mcm}(a,b)$. Dato che $\operatorname{mcd}(a,b) = 1$ per la proposizione 2.2.3 segue che $ab \mid \operatorname{mcm}(a,b)$, cioè $|ab| \leq \operatorname{mcm}(a,b)$. Ma ab è un multiplo di a e di b, quindi dovrà valere che $|ab| \geq \operatorname{mcm}(a,b)$ in quanto $\operatorname{mcm}(a,b)$ è il minimo multiplo comune ad a e b. Da cio' segue che $\operatorname{mcm}(a,b) = |ab|$, cioè la tesi. □

Proposizione 2.2.11

Siano $a, x, y \in \mathbb{Z}$. Allora

$$\operatorname{mcd}(a,x) = 1 \implies \operatorname{mcd}(a,xy) = \operatorname{mcd}(a,y). \tag{16}$$

INTUIZIONE. Se stiamo calcolando $\operatorname{mcd}(a,b)$ dove $b = xy$ e sappiamo che il fattore x non è comune tra b ed a, allora possiamo escluderlo dal massimo comun divisore.

Dimostrazione. Dato che $\operatorname{mcd}(a,x) = 1$, allora se un primo p divide a sicuramente p non divide x. Per la proposizione 2.2.9 allora vale

$$\begin{aligned} & p^k \mid \operatorname{mcd}(a, xy) \\ \iff & p^k \mid a \wedge p^k \mid xy \end{aligned}$$

ma $p^k \nmid x$ dunque per la 2.1.11

$$\begin{aligned} &\iff p^k \mid a \wedge p^k \mid y \\ &\iff p^k \mid \operatorname{mcd}(a, y)\,. \end{aligned}$$

Dato che $\operatorname{mcd}(a, xy)$ e $\operatorname{mcd}(a, y)$ vengono divisi dagli stessi primi, per il teorema fondamentale devono essere uguali. □

Proposizione 2.2.12

Siano $a, x, y \in \mathbb{Z}$. Allora

$$\operatorname{mcd}(a, \operatorname{mcm}(x, y)) = \operatorname{mcm}(\operatorname{mcd}(a, x), \operatorname{mcd}(a, y))\,. \tag{17}$$

Dimostrazione. Per la proposizione 2.2.9 allora vale

$$\begin{aligned} & p^k \mid \operatorname{mcd}(a, \operatorname{mcm}(x, y)) \\ \iff & p^k \mid a \wedge (p^k \mid x \vee p^k \mid y) \\ \iff & (p^k \mid a \wedge p^k \mid x) \vee (p^k \mid a \wedge p^k \mid y) \\ \iff & p^k \mid \operatorname{mcm}(\operatorname{mcd}(a, x), \operatorname{mcd}(a, y))\,. \end{aligned}$$

Dato che $\operatorname{mcd}(a, \operatorname{mcm}(x, y))$ e $\operatorname{mcm}(\operatorname{mcd}(a, x), \operatorname{mcd}(a, y))$ vengono divisi dagli stessi primi, per il teorema fondamentale devono essere uguali. □

Proposizione 2.2.13

Siano $a, x, y \in \mathbb{Z}$. Allora

$$\operatorname{mcd}(x, y) = 1 \implies \operatorname{mcd}(a, xy) = \operatorname{mcd}(a, x) \operatorname{mcd}(a, y)\,. \tag{18}$$

INTUIZIONE. Se x e y non hanno fattori in comune, i fattori che a ha in comune con il loro prodotto sono o in x o in y, quindi per ottenerli tutti possiamo dividere l'mcd in due e moltiplicare i due risultati.

Dimostrazione. Dato che $\operatorname{mcd}(x, y) = 1$ allora per la proposizione 2.2.10 vale che $\operatorname{mcm}(x, y) = |xy|$. Dunque $\operatorname{mcd}(a, xy) = \operatorname{mcd}(a, |xy|) = \operatorname{mcd}(a, \operatorname{mcm}(x, y)) = \operatorname{mcm}(\operatorname{mcd}(a, x), \operatorname{mcd}(a, y))$ per la proposizione 2.2.12.

Verifichiamo ora che $\operatorname{mcd}(a, x)$ e $\operatorname{mcd}(a, y)$ sono coprimi. Per ipotesi sappiamo che x, y sono coprimi; ma dato che $\operatorname{mcd}(a, x)$ e $\operatorname{mcd}(a, y)$ sono divisori di x e y rispettivamente, allora dovranno essere anche loro coprimi.

Dunque per la proposizione 2.2.10 segue che

$$\operatorname{mcd}(a, xy) = \operatorname{mcm}(\operatorname{mcd}(a, x), \operatorname{mcd}(a, y)) = \operatorname{mcd}(a, x) \operatorname{mcd}(a, y)$$

che è la tesi. □

Proposizione 2.2.14

Siano $a, b, c \in \mathbb{Z}$. Allora

$$a \mid c \wedge b \mid c \iff \frac{ab}{\operatorname{mcd}(a, b)} \mid c. \tag{19}$$

Dimostrazione. Dimostriamo l'implicazione in entrambi i versi.

($\implies$) Supponiamo che $a \mid c$ e $b \mid c$. Sia $d = \operatorname{mcd}(a, b)$. Allora dato che $d \mid a$, $d \mid b$ per transitività $d \mid c$, dunque $\frac{a}{d} \mid \frac{c}{d}$ e $\frac{b}{d} \mid \frac{c}{d}$. Ma dato che per il corollario 2.1.16 sappiamo che $\operatorname{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, dunque per la 2.2.3 segue che il loro prodotto $\frac{ab}{d^2}$ dovrà dividere $\frac{c}{d}$, che è equivalente a dire che $\frac{ab}{d} \mid c$.

($\impliedby$) NON SO FARE QUEST'ALTRA DIMOSTRAZIONE □

Proposizione 2.2.15

Siano $a, b \in \mathbb{Z}$. Allora

$$\operatorname{mcd}(a,b)\operatorname{mcm}(a,b) = |ab|. \tag{20}$$

Dimostrazione. Sia $c \in \mathbb{Z}$ tale che $a \mid c$, $b \mid c$. Allora per la proposizione 2.2.14 segue che $\frac{ab}{\operatorname{mcd}(a,b)} \mid c$. Inoltre per la proposizione 2.1.8 segue che $\operatorname{mcm}(a,b) \mid c$. Dunque i due numeri $\frac{ab}{\operatorname{mcd}(a,b)}$ e $\operatorname{mcm}(a,b)$ hanno gli stessi divisori, dunque devono essere uguali a meno del segno, da cui segue

$$\operatorname{mcd}(a,b)\operatorname{mcm}(a,b) = |ab|.$$

□

2.3 EQUAZIONI DIOFANTEE

Definizione 2.3.1 (Equazione diofantea)

Siano $a, b, c \in \mathbb{Z}$ noti, $x, y \in \mathbb{Z}$ incognite. Allora un'equazione lineare della forma $ax + by = c$ si dice equazione diofantea.

Teorema 2.3.2 (Condizione necessaria e sufficiente per le diofantee)

Siano $a, b, c \in \mathbb{Z}$. Allora l'equazione diofantea $ax + by = c$ ammette soluzioni se e solo se $\operatorname{mcd}(a,b) \mid c$.

Dimostrazione. Dimostriamo prima che se $\operatorname{mcd}(a,b) \mid c$ allora esistono soluzioni di $ax + by = c$ e poi dimostriamo che se $\operatorname{mcd}(a,b) \nmid c$ allora l'equazione $ax + by = c$ non ha soluzioni.

- Supponiamo che $c = k \operatorname{mcd}(a,b)$ per qualche $k \in \mathbb{Z}$. Allora per il teorema di Bezout 2.1.10 esistono $x', y' \in \mathbb{Z}$ tali che $ax' + by' = \operatorname{mcd}(a,b)$. Moltiplicando entrambi i membri per k otteniamo

  $$k \operatorname{mcd}(a,b) = k(ax' + by') = akx' + bky' = a(kx') + b(ky')$$

  dunque $x = kx'$ e $y = ky'$ risolvono l'equazione diofantea.

- Supponiamo ora che c non sia un multiplo di $\operatorname{mcd}(a,b)$ e supponiamo per assurdo che l'equazione abbia soluzione, cioè che esistano $x, y \in \mathbb{Z}$ tali che $ax + by = c$. Sia $d = \operatorname{mcd}(a,b)$.

  Per definizione di $\operatorname{mcd}(a,b)$ e per la proposizione 2.1.3, dato che $d \mid a$ e $d \mid b$ segue che $d \mid ax$, $d \mid by$ e dunque $d \mid ax + by$. Ma $ax + by = c$, quindi $d = \operatorname{mcd}(a,b) \mid c$, che va contro le ipotesi.

  Dunque l'equazione diofantea non ha soluzione, cioè la tesi. □

Teorema 2.3.3 (Soluzioni di una diofantea omogenea con coefficienti coprimi)

Siano $a, b \in \mathbb{Z}$ coprimi. Allora le soluzioni dell'equazione diofantea omogenea $ax + by = 0$ sono tutte e solo della forma $x = -kb, y = ka$ al variare di $k \in \mathbb{Z}$.

Dimostrazione. Dimostriamo innanzitutto che $x = -kb, y = ka$ è una soluzione.

$$\begin{aligned} ax + by &= a(-kb) + b(ka) \\ &= -kab + kab \\ &= 0. \end{aligned}$$

Mostriamo ora che non vi possono essere altre soluzioni.

Dato che $ax + by = 0$, allora $ax = -by$. Dato che $a \mid ax$ allora $a \mid -by$; inoltre per ipotesi $\text{mcd}(a, -b) = \text{mcd}(a, b) = 1$. Dunque per il teorema 2.1.11 segue che $a \mid y$, cioè $y = ak$ per qualche $k \in \mathbb{Z}$. Sostituendo ottengo $x = -b\frac{y}{a} = -bk$, che è la tesi. □

Corollario 2.3.4 (Soluzioni di una diofantea omogenea)

Se a, b non sono coprimi, allora tutte le soluzioni dell'equazione $ax + by = 0$ saranno della forma $x = -kb', y = ka'$ dove $a' = \frac{a}{\text{mcd}(a,b)}$ e $b' = \frac{b'}{\text{mcd}(a,b)}$.

Dimostrazione. Dato che a, b non sono coprimi, allora possiamo dividere entrambi i membri di $ax + by = 0$ per $\text{mcd}(a, b)$ ottenendo l'equazione diofantea equivalente $a'x + b'y = 0$.

Ma per il teorema 2.1.16 $\text{mcd}(a', b') = 1$, dunque per il teorema 2.3.3 le sue soluzioni saranno tutte e solo della forma $x = -kb', y = ka'$.

Ma questa equazione è equivalente all'originale, dunque anche le soluzioni di $ax + by = 0$ saranno tutte e solo della forma $x = -kb', y = ka'$. □

Teorema 2.3.5 (Soluzioni di una diofantea non omogenea)

Siano $a, b \in \mathbb{Z}$ e sia (x, y) una soluzione particolare dell'equazione diofantea $ax + by = c$ (se esiste). Allora le soluzioni di quest'equazione sono tutte e solo della forma $(x + x_0, y + y_0)$ al variare di (x_0, y_0) tra le soluzioni dell'equazione omogenea associata $ax + by = 0$.

Dimostrazione. Dimostriamo innanzitutto che se (x, y) è una soluzione della diofantea non omogenea e (x_0, y_0) è una soluzione dell'omogenea, allora $(x + x_0, y + y_0)$ è ancora soluzione della non omogenea.

$$\begin{aligned} a(x + x_0) + b(y + y_0) &= ax + ax_0 + by + by_0 \\ &= (ax + by) + (ax_0 + by_0) \\ &= c + 0 \\ &= c. \end{aligned}$$

Dimostriamo ora che tutte le soluzioni sono di questa forma. Sia $(\bar{x}, \bar{y})$ una soluzione particolare della diofantea non omogenea e (x, y) un'altra soluzione qualsiasi, e mostriamo che la loro differenza è una soluzione dell'omogenea associata.

$$\begin{aligned} a(x - \bar{x}) + b(y - \bar{y}) &= ax - a\bar{x} + by - b\bar{y} \\ &= (ax + by) - (a\bar{x} + b\bar{y}) \\ &= c - c \\ &= 0 \end{aligned}$$

che è la tesi. □

3 CONGRUENZE

3.1 RELAZIONE DI CONGRUENZA

Definizione 3.1.1 (Congruenza modulo m)

Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora si dice che a è congruo a b modulo m se e solo se $a - b$ è un multiplo di m, e si scrive

$$a \equiv b \pmod{m}.$$

Teorema 3.1.2 (Congruenza come relazione di equivalenza)

Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora la relazione di congruenza modulo m è una relazione di equivalenza, e dunque soddisfa le proprietà:

$$\begin{aligned} &\textit{Riflessiva:} && a \equiv a \ (m) && (21)\\ &\textit{Simmetrica:} && a \equiv b \ (m) \implies b \equiv a \ (m) && (22)\\ &\textit{Transitiva:} && a \equiv b \ (m) \wedge b \equiv c \ (m) \implies a \equiv c \ (m) && (23) \end{aligned}$$

Dimostrazione. Dimostriamo le tre proprietà della congruenza come relazione di equivalenza.

1. $a - a = 0 = 0m$, dunque $a \equiv a \ (m)$.
2. Se $a - b = km$ allora $b - a = -(a - b) = -km = (-k)m$, cioè $b \equiv a \ (m)$.
3. Se $a - b = km$ e $b - c = hm$ allora $a - c = (a - b) + (b - c) = km + hm = (k + h)m$, cioè $a \equiv c \ (m)$. □

Teorema 3.1.3 (Relazione tra congruenza e resto della divisione euclidea)

Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora

$$a \equiv b \ (m) \iff a \bmod m = b \bmod m. \tag{24}$$

cioè a è congruo a b se e solo se a e b hanno lo stesso resto quando divisi per m.

Dimostrazione. Dimostriamo l'implicazione nei due versi.

($\implies$) Supponiamo che $a \equiv b \ (m)$ e dimostriamo che i resti di a e b modulo m siano uguali. Per la proposizione 2.1.7 esistono $q, r \in \mathbb{Z}$ tale che $b = mq + r$ e $0 \leq r < m$. Allora per definizione di congruenza per qualche $k \in \mathbb{Z}$ avremo

$$\begin{aligned} a &= b + mk \\ &= mq + r + mk \\ &= m(q + k) + r \end{aligned}$$

ovvero r è il resto di a modulo m.

($\impliedby$) Siano $r = a \bmod m$, $r' = b \bmod m$ i resti di a e b modulo m, cioè $a = cq + r$ e $b = cq' + r'$ per qualche $q, q' \in \mathbb{Z}$. Supponiamo che $r = a \bmod m = b \bmod m = b$. Allora

$$\begin{aligned} a - b &= cq + r - cq' - r' \\ &= c(q - q') \end{aligned}$$

cioè $a \equiv b \ (m)$. □

Proposizione 3.1.4

Siano $a, b, a', b', m \in \mathbb{Z}$, $m > 0$. Allora valgono le seguenti

$$a \equiv b \ (m) \land a' \equiv b' \ (m) \implies a + a' \equiv b + b' \ (m) \tag{25}$$
$$a \equiv b \ (m) \land a' \equiv b' \ (m) \implies a - a' \equiv b - b' \ (m) \tag{26}$$
$$a \equiv b \ (m) \land a' \equiv b' \ (m) \implies aa' \equiv bb' \ (m) \tag{27}$$

Dimostrazione.

1. Per definizione di congruenza $m \mid a - b$ e $m \mid a' - b'$. Per la proposizione 2.1.3 segue che $m \mid (a - b) + (a' - b')$, cioè $m \mid (a + a') - (b + b')$, che è equivalente a $a + a' \equiv b + b' \ (m)$.
2. Per definizione di congruenza $m \mid a - b$ e $m \mid a' - b'$. Per la proposizione 2.1.3 segue che $m \mid (a - b) - (a' - b')$, cioè $m \mid (a - a') - (b - b')$, che è equivalente a $a - a' \equiv b - b' \ (m)$.
3. Per definizione di congruenza, scriviamo $a - b = km$ e $a' - b' = hm$, che è equivalente a $b = a - km$ e $b' = a' - hm$. Dunque

$$\begin{aligned} bb' &= (a - km)(a' - hm) \\ &= aa' - ahm - a'km + khm \\ &= aa' - (ah + a'k - kh)m \end{aligned}$$

che è equivalente a

$$\begin{aligned} &aa' - bb' = (ah + a'k - kh)m \\ \iff\ &aa' \equiv bb' \ (m)\,. \end{aligned}$$

□

3.2 EQUAZIONI CON CONGRUENZE LINEARI

Proposizione 3.2.1 (Equivalenza diofantea-congruenza)

Siano $a, b, c \in \mathbb{Z}$; sia $ax + by = c$ un'equazione diofantea. Allora tutte le soluzioni della diofantea sono soluzioni delle equazioni $ax \equiv c \ (b)$ e $by \equiv c \ (a)$.

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

1. Siano $x, y \in \mathbb{Z}$ tali che $ax + by = c$. Dato che $ax + by$ è uguale a c segue che $ax + by \equiv c \ (b)$. Ma $b \equiv 0 \ (b)$, dunque x sarà anche soluzione di $ax \equiv c \ (b)$. Analogo ragionamento considerando $ax + by \equiv c \ (a)$.
2. Sia $x \in \mathbb{Z}$ tale che $ax \equiv c \ (b)$. Allora per definizione di congruenza esiste $k \in \mathbb{Z}$ per cui $ax - c = bk$. Sia $y = -k$; l'equazione è quindi equivalente a $ax + by = c$, cioè la coppia (x, y) è una soluzione dell'equazione diofantea. Analogo ragionamento se partiamo da $by \equiv c \ (a)$. □

Tramite questa proposizione possiamo risolvere ogni equazione contenente congruenze risolvendo l'equazione diofantea associata, o viceversa.

Definizione 3.2.2 (Invertibilità e inverso)

Siano $a \in \mathbb{Z}$; allora si dice che a è invertibile modulo m se esiste $x \in \mathbb{Z}$ tale che

$$ax \equiv 1 \ (m)\,.$$

In particolare tra tutti gli x che soddisfano la relazione precedente, il

numero x tale che $0 \leq x < m$ si dice inverso di a modulo m.

Per calcolare gli inversi modulo m basta fare una tabella $m \times m$ in cui le righe e le colonne contengono i numeri tra 0 e $m-1$, e nella casella ij c'è il prodotto tra i numeri i e j modulo m.

Notiamo che non sempre i numeri diversi da 0 ammettono inverso modulo m.

Teorema 3.2.3 (Condizione necessaria e sufficiente per l'invertibilità)

Siano $a, m \in \mathbb{Z}$. Allora a è invertibile modulo m se e solo se $\text{mcd}(a, m) = 1$.

Dimostrazione. Dimostriamo l'implicazione nei due versi.

($\implies$) Supponiamo che a sia invertibile modulo m, cioè che $\exists x \in \mathbb{Z}$ tale che $ax \equiv 1 \ (m)$. Ma sappiamo che $ax + my$ è un multiplo di $\text{mcd}(a, m)$, quindi anche 1 dovrà essere un multiplo di $\text{mcd}(a, m)$, cioè $\text{mcd}(a, m) = 1$.

($\impliedby$) Supponiamo $\text{mcd}(a, m) = 1$. Allora per il teorema di Bezout 2.1.10 $\exists x, y \in \mathbb{Z}$ tali che

$$\begin{aligned} & ax + my = 1 \\ \iff & ax - 1 = m(-y) \\ \iff & ax \equiv 1 \ (m) \end{aligned}$$

dunque x è l'inverso di a modulo m. □

Corollario 3.2.4

Se p è primo e $a \not\equiv 0 \ (p)$, allora a è invertibile modulo p.

Dimostrazione. Se p è primo, allora necessariamente p è coprimo con tutti i numeri che non sono suoi multipli, cioè con tutti gli a tali che $a \equiv 0 \ (p)$. Dunque se $a \equiv 0 \ (p)$ allora $\text{mcd}(a, p) = 1$, cioè per il teorema precedente a è invertibile modulo p. □

Proposizione 3.2.5

Siano $a, b, m \in \mathbb{Z}$; allora se a è invertibile modulo m segue che $\exists x \in \mathbb{Z}$ tale che $ax \equiv b \ (m)$.

Dimostrazione. Dato che a è invertibile modulo m esisterà $x' \in \mathbb{Z}$ tale che $ax' \equiv 1 \ (m)$. Moltiplicando entrambi i membri per b otteniamo $ax'b \equiv b \ (m)$, dunque la $x \equiv x'b \ (b)$ soddisfa $ax \equiv b \ (m)$, cioè la tesi. □

Proposizione 3.2.6 (Condizione necessaria e sufficiente per la risoluzione di congruenze lineari)

Siano $a, b, m, x \in \mathbb{Z}$; allora l'equazione $ax \equiv b \ (m)$ ha soluzione se e solo se $\text{mcd}(a, m) \mid b$.

Dimostrazione. Dimostriamo l'implicazione nei due versi.

($\implies$) Supponiamo che $ax \equiv b \ (m)$ ammetta soluzione. Allora esiste $y \in \mathbb{Z}$ tale che $ax - my = b$. Dato che a e m sono multipli di $\text{mcd}(a, m)$, allora lo sarà anche la combinazione lineare $ax - my$ che è uguale a b, cioè $\text{mcd}(a, m) \mid b$.

($\impliedby$) Supponiamo che $d = \text{mcd}(a, m)$ divida b. Allora $d \mid a$, $d \mid b$, $d \mid m$. Siano $a' = \frac{a}{d}, b' = \frac{b}{d}, m' = \frac{m}{d}$. Allora

$$\begin{aligned} & ax \equiv b \ (m) & \\ \iff & ax - b = mk & \text{per qualche } k \in \mathbb{Z} \\ \iff & a'dx - b'd = m'dk & \text{per qualche } k \in \mathbb{Z} \\ \iff & a'x - b' = m'k & \text{per qualche } k \in \mathbb{Z} \\ \iff & a'x \equiv b' \ (m') \,. & \end{aligned}$$

Ma per il corollario 2.1.16 $\text{mcd}(a', m') = 1$, dunque a' è invertibile modulo m', dunque per la proposizione 3.2.5 segue che $a'x \equiv b' \ (m')$ ha soluzione. Tuttavia $a'x \equiv b' \ (m')$ è equivalente a $ax \equiv b \ (m)$, dunque anche $ax \equiv b \ (m)$ ha soluzione e in particolare ha le stesse soluzioni di $a'x \equiv b' \ (m')$. □

Proposizione 3.2.7

Se vogliamo semplificare una congruenza possiamo sfruttare le seguenti regole:

$$A \equiv B \ (m) \iff A + c \equiv B + c \ (m) \tag{28}$$
$$A \equiv B \ (m) \implies cA \equiv cB \ (m) \tag{29}$$
$$A \equiv B \ (m) \iff (A \bmod m) \equiv (B \bmod m) \ (m) \tag{30}$$
$$Ad \equiv Bd \ (m) \implies A \equiv B \ (m) \quad \text{se } \text{mcd}(d, m) = 1 \tag{31}$$
$$Ad \equiv Bd \ (md) \iff A \equiv B \ (m) \tag{32}$$

Dimostrazione. Dimostriamo le 5 proposizioni.

1. Dato che $c \equiv c \ (m)$, si tratta di un caso particolare della 25. Inoltre l'implicazione inversa si ricava dalla 26, dunque si tratta di un'equivalenza.
2. Dato che $c \equiv c \ (m)$, si tratta di un caso particolare della 27.
3. Dato che $A \equiv (A \bmod m) \ (m)$ e $B \equiv (B \bmod m) \ (m)$, per transitività otteniamo che $A \equiv B \ (m)$ è equivalente a $(A \bmod m) \equiv (B \bmod m) \ (m)$.
4. Se $\text{mcd}(d, m) = 1$ allora esiste l'inverso di d modulo m. Chiamiamo x questo inverso e moltiplichiamo entrambi i membri della congruenza per x, ottenendo
$$\begin{aligned} & Ad \equiv Bd \ (m) \\ \iff & Adx \equiv Bdx \ (m) \\ \iff & A \cdot 1 \equiv B \cdot 1 \ (m) \\ \iff & A \equiv B \ (m). \end{aligned}$$
5. Per definizione di congruenza esiste $y \in \mathbb{Z}$ tale che
$$\begin{aligned} & Ad = Bd + mdy \\ \iff & A = B + my \\ \iff & A \equiv B \ (m). \end{aligned}$$
□

Proposizione 3.2.8

Siano $a, b, m \in \mathbb{Z}$ noti, $x \in \mathbb{Z}$ non noto. Allora per risolvere l'equazione $ax \equiv b \ (m)$ possiamo ricondurci ad uno dei seguenti tre casi:

1. *se $\text{mcd}(a, m) = 1$, allora l'equazione ha soluzione $x \equiv by \ (m)$, dove y è l'inverso di a modulo m;*
2. *se $\text{mcd}(a, m) \neq 1$, $d = \text{mcd}(a, m) \mid b$, allora l'equazione è equivalente all'equazione $a'x \equiv b' \ (m')$, con $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$, che ha soluzione;*
3. *se $\text{mcd}(a, m) \neq 1$, $\text{mcd}(a, m) \nmid b$, allora l'equazione non ha soluzione.*

Dimostrazione. I tre casi sono conseguenza diretta della proposizione 3.2.6. Infatti

1. Per la 3.2.6 l'equazione ha soluzione. Se y è l'inverso di a, moltiplicando entrambi i membri per y otteniamo la soluzione $x \equiv by \ (m)$.

2. Per la 3.2.6 l'equazione ha soluzione. Sia $d = \text{mcd}(a, m)$. Allora la congruenza è equivalente a $ax - b = mk$ per qualche $k \in \mathbb{Z}$. Dato che a, b, m sono divisibili per d, dividendo per d otteniamo l'equazione equivalente

$$\begin{aligned} &\frac{a}{d}x - \frac{b}{d} = \frac{m}{d}k \\ \iff &\frac{a}{d}x \equiv \frac{b}{d} \ \left(\frac{m}{d}\right) \end{aligned}$$

Ma per il corollario 2.1.16 $\text{mcd}\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, dunque possiamo trovare la soluzione sfruttando il primo caso.

3. Per la 3.2.6 l'equazione non ha soluzione. □

3.3 SISTEMI DI CONGRUENZE

Teorema 3.3.1 (Teorema Cinese del Resto)

Siano $a_1, a_2, m_1, m_2 \in \mathbb{Z}$ con m_1, m_2 coprimi. Allora esiste un $x \in \mathbb{Z}$ tale che

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \end{cases}$$

e x è unico modulo $(m_1 m_2)$, ovvero se x_0 è un'altra soluzione del sistema segue che

$$x \equiv x_0 \pmod{m_1 m_2}. \tag{33}$$

Possiamo esprimere il teorema cinese in questo modo equivalente.

Teorema 3.3.2 (Teorema Cinese del Resto)

Siano $x_0, m \in \mathbb{Z}$; siano inoltre m_1, m_2 coprimi tali che $m = m_1 m_2$. Allora vale che

$$x \equiv x_0 \ (m) \iff \begin{cases} x \equiv x_0 \ (m_1) \\ x \equiv x_0 \ (m_2) \end{cases} \tag{34}$$

Dato che il Teorema Cinese del Resto ci permette di unire due equazioni con moduli m_1, m_2 coprimi in un'unica congruenza modulo $(m_1 m_2)$, possiamo generalizzare il teorema ad un sistema di n congruenze unendole due a due, come ci dice il prossimo corollario.

Corollario 3.3.3

Siano $a_1, \dots, a_n, m_1, \dots, m_n \in \mathbb{Z}$ con $m_1, \dots, m_n$ coprimi a due a due. Allora esiste un $x \in \mathbb{Z}$ tale che

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \quad \vdots \\ x \equiv a_n \ (m_n) \end{cases}$$

e x è unico modulo $(m_1 \cdots m_n)$, ovvero se x_0 è un'altra soluzione del sistema segue che

$$x \equiv x_0 \pmod{m_1 \cdots m_n}. \tag{35}$$

Vediamo come stabilire se esistono soluzioni di un sistema di congruenze con moduli non coprimi.

Proposizione 3.3.4 (Condizione necessaria e sufficiente per la compatibilità di un sistema di congruenze)

Siano $a_1, a_2, m_1, m_2 \in \mathbb{Z}$. Allora esiste $x \in \mathbb{Z}$ tale che

$$\begin{cases} x \equiv a_1 \ \ (m_1) \\ x \equiv a_2 \ \ (m_2) \end{cases}$$

se e solo se $a_1 \equiv a_2 \pmod{\operatorname{mcd}(m_1, m_2)}$.

Dimostrazione. Consideriamo il sistema di due equazioni. Dalla prima ricaviamo

$$x = a_1 + m_1 y$$

per qualche $y \in \mathbb{Z}$. Allora sostituendo nella seconda otteniamo

$$\begin{aligned} & a_1 + m_1 y \equiv a_2 \ \ (m_2) \\ \iff & m_1 y \equiv a_2 - a_1 \ \ (m_2)\,. \end{aligned}$$

Quest'ultima equazione (per la proposizione 3.2.6) ha soluzione se e solo se

$$\begin{aligned} & \operatorname{mcd}(m_1, m_2) \mid (a_2 - a_1) \\ \iff & (a_2 - a_1) \equiv 0 \ \ (\operatorname{mcd}(m_1, m_2)) \\ \iff & a_1 \equiv a_2 \ \ (\operatorname{mcd}(m_1, m_2))\,. \end{aligned}$$

□

Se abbiamo un sistema con piu' di due equazioni basta risolverle due a due: ogni volta otteniamo una singola equazione, diminuendo di uno il numero di equazioni del sistema senza alterare il numero di soluzioni. Se a un certo punto troviamo una coppia di equazioni non compatibili allora il sistema non ha soluzione, altrimenti la ha ed è unica.

Proposizione 3.3.5

Dato un sistema di congruenze

$$\begin{cases} a_1 x \equiv b_1 \ \ (m_1) \\ a_2 x \equiv b_2 \ \ (m_2) \\ \quad \vdots \\ a_n x \equiv b_n \ \ (m_n) \end{cases}$$

se x_0 è una soluzione particolare, allora tutte le soluzioni del sistema si ottengono sommando a x_0 un multiplo di $\operatorname{mcm}(m_1, m_2, \ldots, m_n)$; o equivalentemente la soluzione del sistema è una singola congruenza della forma

$$x \equiv x_0 \pmod{\operatorname{mcm}(m_1, m_2, \ldots, m_n)} \tag{36}$$

Per quest'ultima proposizione possiamo risolvere un sistema cercando un numero intero x_0 minore del minimo comune multiplo dei moduli che sia soluzione di tutte le equazioni: a quel punto la congruenza che risolve il sistema sarà $x \equiv x_0 \pmod{\operatorname{mcm}(m_1, m_2, \ldots, m_n)}$.

3.4 STRUTTURA ALGEBRICA DEGLI INTERI MODULO M

3.4.1 *Interi modulo m*

Definizione 3.4.1 (Classe di resto)
Siano $a, n \in \mathbb{Z}$; allora si dice classe di resto $[a]_n$ l'insieme

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \ (n)\}. \tag{37}$$

Il numero a si dice rappresentante della classe $[a]_n$.

Due classi di resto si dicono uguali se contengono gli stessi elementi. Il rappresentante di una classe non è unico, anzi per ogni classe ci sono infinite scelte che corrispondono a tutti i numeri appartenenti alla classe. Vale quindi la seguente osservazione:

OSSERVAZIONE. $a \equiv b \ (m) \iff [a]_n = [b]_n$.

Notiamo che per ogni numero n ci sono esattamente n classi di resto modulo n: infatti ce n'é una esattamente per ogni possibile resto della divisione per n, cioè per ogni numero tra 0 e $n-1$ inclusi.

Definizione 3.4.2 (Insieme degli interi modulo n)
Si dice insieme degli interi modulo n l'insieme

$$\mathbb{Z}/(n) = \{[0]_n, [1]_n, \ldots, [n-1]_n\}. \tag{38}$$

Possiamo definire due operazioni in $\mathbb{Z}/(n)$ che sono le operazioni di somma ($+ : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n)$) e prodotto ($\cdot : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n)$) tali che:

$$[a]_n + [b]_n = [a+b]_n \qquad \forall [a]_n, [b]_n \in \mathbb{Z}/(n) \tag{39}$$
$$[a]_n \cdot [b]_n = [ab]_n \qquad \forall [a]_n, [b]_n \in \mathbb{Z}/(n) \tag{40}$$

OSSERVAZIONE. Le operazioni di somma e prodotto sono ben definite: il loro risultato non cambia a seconda dei rappresentanti scelti per le classi di congruenza.

Proposizione 3.4.3 ($\mathbb{Z}/(n)$ **è un anello)**
Per ogni $n \geq 2$ l'insieme $\mathbb{Z}/(n)$ con le operazioni di somma e prodotto tra classi e con gli elementi $[0]_n, [1]_n$ che svolgono il ruolo di 0 e 1 è un anello commutativo.

Dimostrazione. è facile verificare che valgono gli assiomi degli anelli. □

Proposizione 3.4.4 ($\mathbb{Z}/(p)$ **è un anello)**
Per ogni $p \geq 2$, p primo, l'insieme $\mathbb{Z}/(p)$ con le operazioni di somma e prodotto tra classi e con gli elementi $[0]_n, [1]_n$ che svolgono il ruolo di 0 e 1 è un campo.

Dimostrazione. Per la proposizione 3.4.3 sappiamo che $\mathbb{Z}/(p)$ è un anello commutativo. Per la proposizione 3.2.3 un numero è invertibile modulo p se e solo se è coprimo con p; ma tutti i numeri che non sono multipli di p sono coprimi con p, dunque tutte le classi tranne $[0]_p$ sono invertibili, dunque esiste l'inverso per la moltiplicazione per ogni elemento non nullo, cioè $\mathbb{Z}/(p)$ è un campo. □

3.4.2 *Gruppo degli inversi modulo m*

Definizione 3.4.5 (Insieme degli invertibili)

Sia $n \geq 2$. Allora si indica con $(\mathbb{Z}/(n))^\times$ l'insieme delle classi resto invertibili modulo n, ovvero

$$(\mathbb{Z}/(n))^\times = \left\{ [a]_n \mid \exists [a^{-1}]_n \in \mathbb{Z}/(n). \quad [a]_n [a^{-1}]_n = [1]_n \right\}. \tag{41}$$

Proposizione 3.4.6 (Il prodotto di classi invertibili è invertibile)
Sia $n \geq 2$. Allora se $[a], [b] \in (\mathbb{Z}/(n))^\times$ segue che $[ab] \in (\mathbb{Z}/(n))^\times$.

Dimostrazione. Ci basta dimostrare che $[ab]$ è invertibile modulo n. Sia $[x]$ l'inverso, se esiste, allora:

$$\begin{aligned} & [ab][x] = [1] \\ \iff & [a][b][x] = [1] \\ \iff & [a][b][x][a^{-1}][b^{-1}] = [a^{-1}][b^{-1}] \\ \iff & [x] = [a^{-1}][b^{-1}] = [a^{-1}b^{-1}]. \end{aligned}$$

ovvero $[ab]$ è invertibile e $[a^{-1}b^{-1}]$ è il suo inverso. □

Proposizione 3.4.7 ($(\mathbb{Z}/(n))^\times$ è un gruppo)
Per ogni $n \geq 2$ l'insieme $(\mathbb{Z}/(n))^\times$ con l'operazione di prodotto tra classi e con l'elemento $[1]_n$ che svolge il ruolo di 1 è un gruppo commutativo.

Definizione 3.4.8 (Funzione di Eulero)
Sia $n \geq 2$. Allora si dice funzione di Eulero la funzione $\varphi : \mathbb{N} \to \mathbb{N}$ tale che

$$\varphi(n) = \left| (\mathbb{Z}/(n))^\times \right| \tag{42}$$

ovvero $\varphi(n)$ è il numero di elementi invertibili in $\mathbb{Z}/(n)$.

Proposizione 3.4.9
Sia $p \in \mathbb{Z}$, p primo. Allora $\varphi(p) = p - 1$.

Dimostrazione. Tutti le classi resto in $\mathbb{Z}/(p)$ tranne $[0]$ sono coprime con p, dunque ci sono $p - 1$ classi invertibili. □

Proposizione 3.4.10
Siano $n, p \in \mathbb{Z}$, p primo. Allora $\varphi(p^n) = p^n - p^{n-1}$.

Dimostrazione. Il numero di elementi in $\mathbb{Z}/(p^n)$ è p^n.

Da essi dobbiamo escludere tutti i numeri che non sono coprimi con p^n, che sono tutti i numeri che contengono p nella loro fattorizzazione in primi, cioè tutti i multipli di p. In $[0, p^n - 1]$ ci sono esattamente $\frac{p^n}{p} = p^{n-1}$ multipli di p.

Dunque $\varphi(p^n) = p^n - p^{n-1}$. □

Proposizione 3.4.11
Siano $a, b \in \mathbb{Z}$, $\operatorname{mcd}(a, b) = 1$. Allora

$$\varphi(ab) = \varphi(a)\varphi(b). \tag{43}$$

Dimostrazione. Per definizione di φ la tesi è equivalente a

$$\left| (\mathbb{Z}/(ab))^\times \right| = \left| (\mathbb{Z}/(a))^\times \right| \left| (\mathbb{Z}/(b))^\times \right|.$$

Dalla proposizione 4.1.3 del capitolo sulla combinatoria sappiamo che il prodotto tra le cardinalità è la cardinalità del prodotto cartesiano, dunque la tesi è equivalente a

$$\left|(\mathbb{Z}/(ab))^\times\right| = \left|(\mathbb{Z}/(a))^\times \times (\mathbb{Z}/(b))^\times\right|.$$

è sufficiente dunque dimostrare che esiste una corrisponenza biunivoca tra i due insiemi. Scelgo la funzione f tale che

$$f([c]_{ab}) = \langle [c]_a, [c]_b \rangle$$

e dimostro che f è bigettiva.

INIETTIVITÀ. Siano $[h]_{ab}, [k]_{ab} \in (\mathbb{Z}/(ab))^\times$ tali che $f([h]_{ab}) = f([k]_{ab})$, cioè equivalentemente $\langle [h]_a, [h]_b \rangle = \langle [k]_a, [k]_b \rangle$. Dimostriamo che segue che $[h]_{ab} = [k]_{ab}$.

Per definizione di f segue che

$$\begin{cases} h \equiv k \ \ (a) \\ h \equiv k \ \ (b) \end{cases}$$

Dunque per il Teorema Cinese del Resto (3.3.2) (dato che $\text{mcd}\,(a,b) = 1$) segue che deve valere $h \equiv k \ \ (ab)$, ovvero $[k]_{ab} = [h]_{ab}$, ovvero f è iniettiva.

SURGETTIVITÀ. Sia $\langle [r]_a, [s]_b \rangle \in (\mathbb{Z}/(a))^\times \times (\mathbb{Z}/(b))^\times$. Dimostriamo che esiste un $[x]_{ab} \in (\mathbb{Z}/(ab))^\times$ tale che $f([x]_{ab}) = \langle [r]_a, [s]_b \rangle$.

Per il teorema cinese dei resti (3.3.1), esiste ed è unico $[x]_{ab} \in \mathbb{Z}/(ab)$ tale che

$$\begin{cases} x \equiv r \ \ (a) \\ x \equiv s \ \ (b) \end{cases}$$

Dimostriamo ora che $[x]_{ab}$ è invertibile.

Dato che $[r]_a$ e $[s]_b$ sono invertibili segue che x dovrà essere invertibile modulo a e modulo b, dunque $\text{mcd}\,(x,a) = \text{mcd}\,(x,b) = 1$. Per la proposizione 2.2.11, dato che $\text{mcd}\,(x,a) = 1$ allora $\text{mcd}\,(x,ab) = \text{mcd}\,(x,b) = 1$, dunque x è invertibile modulo ab, cioè $[x]_{ab} \in (\mathbb{Z}/(ab))^\times$, ovvero f è surgettiva.

Dunque f è bigettiva e quindi segue la tesi. □

3.5 BINOMIALE E TRIANGOLO DI TARTAGLIA

Definizione 3.5.1 (Coefficiente Binomiale)

Si dice **coefficiente binomiale** $\binom{n}{k}$ il numero intero tale che

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{44}$$

Proposizione 3.5.2

Sia $n \in \mathbb{Z}$, $k \in \mathbb{Z}$ tale che $0 \leq k \leq n$. Allora

$$\binom{n}{k} = \binom{n}{n-k}. \tag{45}$$

Dimostrazione.

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$ □

Proposizione 3.5.3 (Formula ricorsiva per il binomiale)
Sia $n \in \mathbb{Z}$, $k \in \mathbb{Z}$ tale che $0 \leq k \leq n$. Allora

$$\binom{n}{k} = \begin{cases} 1 & \text{se } k = 0 \text{ oppure } k = n \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{altrimenti.} \end{cases} \tag{46}$$

Dimostrazione. Se $k = 0$ allora

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1.$$

Inoltre per la proposizione 3.5.2 segue che

$$\binom{n}{n} = \binom{n}{n-n} = \binom{n}{0} = 1.$$

Se $0 < k < n$ allora

$$\begin{aligned} \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{(k)!(n-1-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!(n-k)} + \frac{(n-1)!}{k(k-1)!(n-1-k)!} \\ &= \frac{(n-1)!k + (n-k)(n-1)!}{k(k-1)!(n-1-k)!(n-k)} \\ &= \frac{(n-1)!k + n(n-1)! - k(n-1)!}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} \\ &= \binom{n}{k} \end{aligned}$$

che è la tesi. □

Teorema 3.5.4 (Teorema del binomiale)
Siano $x, y, n \in \mathbb{Z}$. Allora vale che

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \cdots + \binom{n}{n}x^ny^0 = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k. \tag{47}$$

Definizione 3.5.5 (Triangolo di Tartaglia)
Si dice triangolo di Tartaglia un triangolo che ha le seguenti proprietà:

1. le righe sono numerate a partire da 0;
2. ogni riga ha $n+1$ elementi, che vengono numerati da 0 a n;
3. l'elemento in riga n e posizione k si indica con $T_{n,k}$;
4. $T_{n,0} = T_{n,n} = 1$;
5. per ogni $n \geq 0$, $0 < k \leq n$, $T_{n+1,k} = T_{n,k-1} + T_{n,k}$.

Proposizione 3.5.6
Sia $n \in \mathbb{Z}$. Allora per ogni $k \in \mathbb{Z}$ tale che $0 \leq k \leq n$ segue che

$$T_{n,k} = \binom{n}{k}. \tag{48}$$

Dimostrazione. Per induzione su n.

CASO BASE. Sia $n = 0$, allora dato che $0 \leq k \leq n$ segue che $k = 0$. Dunque

$$T_{0,0} = 1 = \binom{0}{0}.$$

PASSO INDUTTIVO. Supponiamo che la tesi sia vera per n e dimostriamola per $n+1$.

- Se $k = 0$ oppure $k = n+1$ allora per definizione del triangolo di Tartaglia $T_{n+1,0} = T_{n+1,n+1} = 1$ che è esattamente $\binom{n+1}{0} = \binom{n+1}{n+1}$ (per la proposizione 3.5.3),
- Se $0 < k < n+1$ allora per definizione del triangolo di Tartaglia segue che

$$T_{n+1,k} = T_{n,k-1} + T_{n,k} = \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

dove l'ultimo passaggio viene dalla proposizione 3.5.3.

Dunque la tesi è vera per ogni $n \in \mathbb{Z}$. □

Proposizione 3.5.7 (Proprietà del Triangolo di Tartaglia)

Il triangolo di Tartaglia gode delle seguenti proprietà:

1. *la somma degli elementi della riga n è 2^n;*
2. *la somma a segni alterni degli elementi di ogni riga è 0;*
3. *nella riga n, l'elemento al posto k e l'elemento al posto $n-k$ hanno lo stesso valore.*

Dimostrazione. Dimostriamo le tre proposizioni.

1. Dimostriamo che $2^n = \sum_{k=0}^{n} T_{n,k} = \sum_{k=0}^{n} \binom{n}{k}$.

$$2^n = (1+1)^n = \sum_{k}^{0} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k}$$

2. La somma a segni alterni della riga n-esima è

$$\sum_{k=0}^{n} (-1)^k T_{n,k} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{n} (-1)^k 1^{n-k} \binom{n}{k} = (1-1)^k = 0^k = 0.$$

3. Dobbiamo dimostrare che $T_{n,k} = T_{n,n-k}$. Ma dato che $T_{n,k} = \binom{n}{k}$ e $T_{n,n-k} = \binom{n}{n-k}$, allora questo è equivalente a dimostrare che $\binom{n}{k} = \binom{n}{n-k}$, che è vero per la proposizione 3.5.2. □

Proposizione 3.5.8

Se p è primo, allora per ogni k tale che $0 < k < p$ vale che

$$\binom{p}{k} \equiv 0 \ (p). \tag{49}$$

Dimostrazione. Consideriamo un k generico tale che $0 < k < p$. Allora

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \iff p! = \binom{p}{k}(p-k)!k!$$

Ma $p \mid p!$, dunque $p \mid \binom{p}{k}(p-k)!k!$, dunque per la proposizione 2.2.2 segue che

$$p \mid \binom{p}{k} \text{ oppure } p \mid (p-k)! \text{ oppure } p \mid k!.$$

Notiamo che sia k che $p-k$ sono numeri minori di p, dunque $k!$ e $(p-k)!$ sono un prodotto di numeri minori di p. Ma p è primo, dunque è coprimo con tutti i numeri che non siano un multiplo di p (e quindi è coprimo con tutti i numeri compresi tra 0 e p esclusi), dunque per la proposizione 2.2.5 p deve essere coprimo anche con $k!$ e con $(p-k)!$.

Da cio' segue che p non puo' dividere $k!$ e $(p-k)!$. L'ultima possibilità è che $p \mid \binom{p}{k}$, che è equivalente a dire che $\binom{p}{k} \equiv 0 \ (p)$. □

Proposizione 3.5.9

Siano $x, y, p \in \mathbb{Z}$, p primo. Allora

$$(x+y)^p \equiv x^p + y^p \ (p)\,. \tag{50}$$

Dimostrazione. Per il teorema del Binomiale (3.5.4) sappiamo che

$$(x+y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y^1 + \cdots + \binom{p}{i}x^{p-i}y^i + \cdots + \binom{p}{p}y^p$$

Ma per la proposizione 3.5.8 tutti i termini intermedi di questa somma sono congrui a 0 modulo p, dunque:

$$\begin{aligned} &\equiv \binom{p}{0}x^p + \binom{p}{p}y^p \ (p) \\ &\equiv x^p + y^p \ (p) \end{aligned}$$

come volevasi dimostrare. □

Corollario 3.5.10

Siano $x_1, x_2, \ldots, x_n, p \in \mathbb{Z}$, p primo. Allora

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \ (p)\,. \tag{51}$$

Dimostrazione. Per induzione su n.

CASO BASE. Sia $n = 1$. Allora $x_1^p \equiv x_1^p \ (p)$ ovviamente.

PASSO INDUTTIVO. Supponiamo che la tesi sia vera per $n-1$ e dimostriamola per n.

$$(x_1 + x_2 + \cdots + x_n)^p \equiv ((x_1 + x_2 + \cdots + x_{n-1}) + x_n)^p \ (p)$$

(per la proposizione 3.5.9)

$$\equiv (x_1 + x_2 + \cdots + x_{n-1})^p + x_n^p \ (p)$$

(per ipotesi induttiva)

$$\equiv x_1^p + x_2^p + \cdots + x_{n-1}^p + x_n^p \ (p)$$

che è la tesi per n.

Dunque dal caso base e dal passo induttivo segue che la tesi vale per ogni n. □

Teorema 3.5.11 (Piccolo Teorema di Fermat)

Se p è primo, allora $x^p \equiv x \ (p)$.

Dimostrazione.

$$x^p \equiv (\overbrace{1 + \cdots + 1}^{x \text{ volte}})^p \ (p)$$

(per il corollario 3.5.10)

$$\equiv \overbrace{1^p + \cdots + 1^p}^{x \text{ volte}} \ (p)$$
$$\equiv \overbrace{1 + \cdots + 1}^{x \text{ volte}} \ (p)$$
$$\equiv x \ (p)$$

che è la tesi. □

Corollario 3.5.12

Se p è primo e $x \not\equiv 0 \ (p)$ allora $x^{p-1} \equiv 1 \ (p)$.

Dimostrazione. Per il piccolo teorema di Fermat (3.5.11) vale che $x^p \equiv x \ (p)$. Dato che $x \not\equiv 0 \ (p)$ allora segue che p e x sono coprimi, dunque x è invertibile modulo p. Moltiplicando entrambi i membri per l'inverso x^{-1} otteniamo

$$x^p x^{-1} \equiv x \cdot x^{-1} \ (p)$$
$$\iff x^{p-1} \equiv 1 \ (p)$$

che è la tesi. □

3.6 CONGRUENZE ESPONENZIALI

Iniziamo con un esempio di congruenza esponenziale.

Esempio 3.6.1. Trovare tutte le soluzioni di $3^x \equiv 5 \ (7)$.

SOLUZIONE. Proviamo per tentativi:

$$x = 0 \implies 3^0 \equiv 1 \not\equiv 5 \ (7)$$
$$x = 1 \implies 3^1 \equiv 3 \not\equiv 5 \ (7)$$
$$x = 2 \implies 3^2 \equiv 9 \equiv 2 \not\equiv 5 \ (7)$$
$$x = 3 \implies 3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \not\equiv 5 \ (7)$$
$$x = 4 \implies 3^4 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \not\equiv 5 \ (7)$$
$$x = 5 \implies 3^5 \equiv 3^2 \cdot 3^3 \equiv 2 \cdot 6 \equiv 12 \equiv 5 \ (7)$$
$$x = 6 \implies 3^6 \equiv 3^3 \cdot 3^3 \equiv 6 \cdot 6 \equiv 36 \equiv 1 \not\equiv 5 \ (7)$$

Dunque $x = 5$ è una soluzione. Non possiamo dire pero' che le soluzioni sono tutti i numeri della forma $x = 5 + 7k$, perché possiamo notiare che i numeri sembrano ripetersi con periodo 6 e non 7 (infatti $3^0 \equiv 3^6 \equiv 1 \ (7)$).

Dimostriamo che se $x = 5$ è soluzione, allora anche $x = 5 + 6k$ lo e'. Infatti

$$3^{5+6k} \equiv 3^5 \cdot 3^{6k} \equiv 3^5 \cdot 1^k \equiv 5 \ (7) \, .$$

Dunque le soluzioni sono tutte le x tali che $x \equiv 5 \ (6)$. Questo vale anche per x negativi, ma dobbiamo definire x^{-1} non come $\frac{1}{x}$ ma come l'inverso di x modulo m.

Definizione 3.6.2 (Ordine moltiplicativo)

Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora si dice ordine di a modulo m il piu' piccolo intero positivo $\text{ord}_m(a)$ tale che

$$a^{\text{ord}_m(a)} \equiv 1 \ (m) \, . \tag{52}$$

OSSERVAZIONE. Notiamo che $\text{ord}_m(a)$ deve essere positivo, e dunque in particolare maggiore di 0. Inoltre la condizione $a \nmid m$, che equivale a $a \not\equiv 0 \ (m)$ serve ad evitare la congruenza banale $0^x \equiv b \ (m)$, che ha soluzione se e solo se $b \equiv 0 \ (m)$.

Proposizione 3.6.3

Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora per ogni $k \in \mathbb{Z}$ vale che

$$a^{k \operatorname{ord}_m(a)} \equiv 1 \pmod{m}. \tag{53}$$

Dimostrazione.

$$a^{k \operatorname{ord}_m(a)} \equiv \left(a^{\operatorname{ord}_m(a)}\right)^k \equiv 1^k \equiv 1 \pmod{m}. \qquad \square$$

Proposizione 3.6.4

Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora

$$a^x \equiv 1 \pmod{m} \iff x \equiv 0 \pmod{\operatorname{ord}_m(a)}. \tag{54}$$

Dimostrazione. Per definizione di congruenza

$$x \equiv 0 \pmod{\operatorname{ord}_m(a)} \iff x \mid \operatorname{ord}_m(a) \iff x = \operatorname{ord}_m(a) \cdot k$$

per qualche $k \in \mathbb{Z}$.

Per l'unicità del resto della divisione euclidea (2.1.7) possiamo scrivere che $x = q \operatorname{ord}_m(a) + r$ per qualche $q, r \in \mathbb{Z}$ con $0 \leq r < \operatorname{ord}_m(a)$. Questo è equivalente a dire

$$\begin{aligned} a^x &= a^{q \operatorname{ord}_m(a) + r} \\ &= a^{q \operatorname{ord}_m(a)} \cdot a^r \end{aligned}$$

che equivale a

$$\begin{aligned} a^x &\equiv a^{q \operatorname{ord}_m(a)} \cdot a^r \pmod{m} \\ &\equiv 1 \cdot a^r \pmod{m} \\ &\equiv a^r \pmod{m} \end{aligned}$$

dove abbiamo sfruttato la proposizione 3.6.3 per dire che $a^{q \operatorname{ord}_m(a)} \equiv 1 \pmod{m}$.

Dunque dato che $a^x \equiv a^r \pmod{m}$ segue che $a^x \equiv 1 \pmod{m}$ se e solo se $a^r \equiv 1 \pmod{m}$. Ma $r < \operatorname{ord}_m(a)$, dunque se r fosse maggiore di 0 avremmo trovato un numero minore di $\operatorname{ord}_m(a)$ per cui $a^r \equiv 1 \pmod{m}$, che è assurdo poiché va contro la minimalità di $\operatorname{ord}_m(a)$.

Segue che $r = 0$, cioè $x = q \operatorname{ord}_m(a)$, cioè equivalentemente $x \equiv 0 \pmod{\operatorname{ord}_m(a)}$, come volevasi dimostrare. $\square$

Proposizione 3.6.5 (Soluzione di una congruenza esponenziale)

Siano $a, b, m \in \mathbb{Z}$, $a \nmid m$. Se $x_0 \in \mathbb{Z}$ è una soluzione di $a^x \equiv b \pmod{m}$ allora le soluzioni sono tutte e solo della forma

$$x \equiv x_0 \pmod{\operatorname{ord}_m(a)}. \tag{55}$$

Dimostrazione. Dimostriamo che se $x = x_0 + k \operatorname{ord}_m(a)$ allora x è soluzione.

$$\begin{aligned} a^{x_0 + k \operatorname{ord}_m(a)} &\equiv a^{x_0} a^{k \operatorname{ord}_m(a)} \pmod{m} \\ &\equiv b \cdot 1 \pmod{m} \\ &\equiv b \pmod{m}. \end{aligned}$$

Dimostriamo ora che se x è soluzione, allora $x \equiv x_0 \pmod{\operatorname{ord}_m(a)}$, cioè equivalentemente $x - x_0 = k \operatorname{ord}_m(a)$.

$$\begin{aligned} a^{x - x_0} &\equiv a^x a^{-x_0} \pmod{m} \\ &\equiv b \cdot b^{-1} \pmod{m} \\ &\equiv 1 \pmod{m}. \end{aligned}$$

Ma per la proposizione 3.6.4 $a^{x - x_0} \equiv 1 \pmod{m}$ se e solo se $x - x_0 \equiv 0 \pmod{\operatorname{ord}_m(a)}$, cioè se e solo se $x \equiv x_0 \pmod{\operatorname{ord}_m(a)}$, che è la tesi. $\square$

Proposizione 3.6.6 (L'ordine è un divisore di $p-1$)

Siano $a, p \in \mathbb{Z}$, $a \nmid p$, p primo. Allora vale che $\operatorname{ord}_p(a) \mid p-1$.

Dimostrazione. Per il corollario al piccolo teorema di Fermat (3.5.12) sappiamo che $a^{p-1} \equiv 1 \ (p)$, cioè $p-1$ è una soluzione dell'equazione $a^x \equiv 1 \ (p)$.

Per la proposizione 3.6.4 segue che $p-1 \equiv 0 \ \big(\operatorname{ord}_p(a)\big)$, cioè $\operatorname{ord}_p(a) \mid p-1$, che è la tesi. □

Dunque se dobbiamo trovare l'ordine di un numero a modulo un primo p ci basta provare tutti i divisori di $p-1$ fino a quando non troviamo il minimo divisore che soddisfa la proprietà.

3.6.1 *Congruenze esponenziali con modulo non primo*

Per risolvere congruenze esponenziali modulo un numero $n \in \mathbb{Z}$ non primo sfruttiamo la funzione φ di Eulero insieme al seguente teorema.

Teorema 3.6.7 (Teorema di Eulero)

Siano $a, n \in \mathbb{Z}$ con a invertibile modulo n. Allora $a^{\varphi(n)} \equiv 1 \ (n)$.

Dimostrazione. Consideriamo l'insieme delle classi resto invertibili modulo n, chiamato $(\mathbb{Z}/(n))^\times$ e sia $k = \varphi(n)$. Dato che $\varphi(n) = |(\mathbb{Z}/(n))^\times|$, questo insieme avrà esattamente k elementi. Indichiamoli con

$$(\mathbb{Z}/(n))^\times = \{[b_1]_n, \dots, [b_k]_n\}.$$

Inoltre dato che a è invertibile modulo n segue che $[a]_n \in (\mathbb{Z}/(n))^\times$.

Moltiplichiamo ora ogni elemento di $(\mathbb{Z}/(n))^\times$ per $[a]_n$, ottenendo l'insieme

$$(a\mathbb{Z}/(n))^\times = \{[a]_n[b_1]_n, \dots, [a]_n[b_k]_n\} = \{[ab_1]_n, \dots, [ab_k]_n\}.$$

Per la proposizione 3.4.6 dato che $[a]_n$ e tutti i $[b_i]_n$ sono invertibili, allora anche i prodotti saranno invertibili. Dunque l'insieme $(a\mathbb{Z}/(n))^\times$ contiene solo numeri invertibili modulo n, quindi deve essere un sottoinsieme di $(\mathbb{Z}/(n))^\times$.

Se dimostriamo che tutti gli elementi di $(a\mathbb{Z}/(n))^\times$ sono distinti, allora $(a\mathbb{Z}/(n))^\times$ è un sottoinsieme di $(\mathbb{Z}/(n))^\times$ con il suo stesso numero di elementi, cioè i due insiemi devono essere uguali.

GLI ELEMENTI DI $(a\mathbb{Z}/(n))^\times$ SONO TUTTI DISTINTI. Supponiamo per assurdo che esistano $[b_i]_n, [b_j]_n \in (\mathbb{Z}/(n))^\times$ con $[b_i]_n \neq [b_j]_n$ tali che

$$[ab_i]_n = [ab_j]_n.$$

Dato che $[a]_n$ è invertibile, allora esisterà $[a^{-1}]_n$ che è l'inverso di $[a]_n$. Moltiplicando entrambi i membri per $[a^{-1}]_n$ otterremo:

$$\begin{aligned} & [a^{-1}]_n[ab_i]_n = [a^{-1}]_n[ab_j]_n \\ \iff & [a^{-1}ab_i]_n = [a^{-1}ab_j]_n \\ \iff & [b_i]_n = [b_j]_n \end{aligned}$$

che è assurdo in quanto abbiamo supposto $[b_i]_n \neq [b_j]_n$. Segue quindi che tutti gli elementi in $(a\mathbb{Z}/(n))^\times$ sono distinti.

Dunque gli insiemi $(\mathbb{Z}/(n))^\times$ e $(a\mathbb{Z}/(n))^\times$ sono uguali, dunque anche il prodotto di tutti i loro elementi dovrà essere uguale.

$$\begin{aligned} & [ab_1]_n[ab_2]_n \cdots [ab_k]_n = [b_1]_n[b_2]_n \cdots [b_k]_n \\ \iff & [ab_1 \cdot ab_2 \cdots ab_k]_n = [b_1b_2 \cdots b_k]_n \end{aligned}$$

Per definizione di uguaglianza tra classi di resto modulo n:

$$\begin{aligned} &\iff ab_1 \cdot ab_2 \cdots ab_k \equiv b_1 b_2 \cdots b_k \ \ (n) \\ &\iff (\overbrace{a \cdot a \cdots a}^{k \text{ volte}}) \cdot (b_1 b_2 \cdots b_k) \equiv (b_1 b_2 \cdots b_k) \ \ (n) \end{aligned}$$

Per invertibilità di $b_1, b_2, \ldots, b_k$:

$$\begin{aligned} &\iff a^k \equiv 1 \ \ (n) \\ &\iff a^{\varphi(n)} \equiv 1 \ \ (n) \end{aligned}$$

che è la tesi. □

Proposizione 3.6.8 (L'ordine è un divisore di $\varphi(n)$)
Siano $a, n \in \mathbb{Z}$, a invertibile modulo m. Allora vale che

$$\operatorname{ord}_n(a) \mid \varphi(n).$$

Dimostrazione. Per il teorema di Eulero (3.6.7) sappiamo che $a^{\varphi(n)} \equiv 1 \ \ (n)$, ovvero $\varphi(n)$ è una soluzione dell'equazione $a^x \equiv 1 \ \ (n)$.

Dunque per la proposizione 3.6.4 segue che $\varphi(n) \equiv 0 \ \ (\operatorname{ord}_n(a))$, ovvero $\operatorname{ord}_n(a) \mid \varphi(n)$. □

4 CALCOLO COMBINATORIO

4.1 INSIEMI E STRINGHE

Definizione 4.1.1 (Cardinalità di un insieme)

Sia A un insieme di elementi. Allora si dice cardinalità di A il numero di elementi contenuti in A, e si indica con $|A|$.

Ad esempio se $A = \{4, 1, 5, 7, 9\}$ allora $|A| = 5$.

Definizione 4.1.2 (Prodotto cartesiano)

Siano A, B due insiemi. Allora si dice prodotto cartesiano di A e di B l'insieme $A \times B$ tale che

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Il prodotto cartesiano di due insiemi è quindi l'insieme delle coppie ordinate (a, b) dove il primo elemento appartiene al primo insieme e il secondo appartiene al secondo insieme.

Notiamo che le coppie con gli stessi elementi ma diverso ordine sono diverse: prendiamo $A = \{4, 5, 6\}$, $B = \{3, 4, 5\}$; allora

$$A \times B = \{(4,3), (4,4), (4,5), (5,3), (5,4), (5,5), (6,3), (6,4), (6,5)\}.$$

Quindi $(4, 5) \neq (5, 4)$ ad esempio.

Possiamo definire anche un prodotto cartesiano di tre o piu' insiemi nello stesso modo: gli elementi del prodotto cartesiano di n insiemi si dicono n-uple oppure stringhe.

Proposizione 4.1.3 (Cardinalità del prodotto cartesiano)

Siano $A_1, \ldots, A_n$ insiemi. Allora

$$|A_1 \cdots A_n| = |A_1| \cdots |A_n|. \tag{56}$$

Dimostrazione. Possiamo scegliere il primo elemento tra uno qualunque degli elementi del primo insieme: abbiamo dunque $|A_1|$ possibilità; per ognuna di queste abbiamo $|A_2|$ possibilità di scegliere il secondo elemento, dunque abbiamo $|A_1| \cdot |A_2|$ possibilità per i primi due; e cosi' via. □

4.2 CONTEGGI PARTICOLARI

Disposizioni con ripetizione

Supponiamo di avere un insieme A di cardinalità $|A| = n$ e voler costruire una stringa di k elementi che appartengono ad n, potendoli anche ripetere.

Queste stringhe sono tutte e sole le stringhe formate scegliendo uno degli elementi di A come primo carattere, uno degli elementi di A come secondo, eccetera... Dunque sono tutte e solo le stringhe che appartengono a $\overbrace{A \times \cdots \times A}^{k \text{ volte}} = A^k$ che ha cardinalità $\left|A^k\right| = |A|^k = n^k$.

Questo numero si dice **numero delle disposizioni con ripetizioni di n elementi in k posizioni**, e si indica con $D'_{n,k} = n^k$.

Disposizioni senza ripetizione

Supponiamo di avere un insieme A di cardinalità $|A| = n$ e voler costruire una stringa di k elementi che appartengono ad n, senza poterli ripetere.

Seguendo il ragionamento di prima abbiamo n possibilità per il primo elemento, $n-1$ per il secondo, in quanto dobbiamo escludere il primo per evitare di ripeterlo, $n-2$ per il terzo, eccetera, fino ad arrivare a $n-(k-1) = n-k+1$ per il k-esimo. Dunque il numero totale di possibilità è

$$n(n-1)\cdots(n-k+1) = \frac{n(n-1)\cdots(n-k+1)(n-k)\cdots 2\cdot 1}{(n-k)\cdots 2\cdot 1} = \frac{n!}{(n-k)!}$$

Questo numero si dice **numero delle disposizioni senza ripetizioni di n elementi in k posizioni**, e si indica con $D_{n,k} = \frac{n!}{(n-k)!}$.

Permutazioni senza ripetizione

Consideriamo una stringa di n elementi distinti e cerchiamo di contare i modi in cui possiamo ordinarli per ottenere stringhe diverse. Notiamo che questo è equivalente a chiederci in quanti modi possiamo creare una stringa di n elementi a partire da un insieme di n elementi, cioè a quante sono le disposizioni senza ripetizione di n elementi in n posizioni:

$$D_{n,n} = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

Questo numero si dice **numero delle permutazioni senza ripetizioni di n elementi**, e si indica con $P_n = n!$.

Anagrammi

Consideriamo una stringa di n elementi, non necessariamente distinti, e cerchiamo di contare i modi in cui possiamo scambiarli di posto ottenendo stringhe diverse.

Dato che alcuni elementi si ripetono, scambiandoli di posto otterremmo una stringa uguale all'originale, dunque il numero degli anagrammi di una parola di n lettere non necessariamente distinte è minore al numero delle permutazioni senza ripetizione.

Per capire come ottenere il numero di anagrammi, consideriamo un esempio. Prendiamo la parola ASSASSINI e rendiamo le lettere distinte tra loro aggiungendo dei pedici, ottenendo $A_1S_1S_2A_2S_3S_4I_1NI_2$. A questo punto il numero di anagrammi di questa parola è esattamente il numero di permutazioni senza ripetizioni, dunque 9! stringhe.

Se torniamo alla parola originale pero' alcune possibilità sono contate piu' volte, in quanto si ottengono scambiando due lettere uguali (ad esempio $A_1S_1S_2A_2S_3S_4I_1NI_2$ e $A_1S_3S_2A_2S_1S_4I_1NI_2$ si ottengono l'una dall'altra scambiando una S, dunque contano come la stessa stringa).

Possiamo scambiare le 4 S tra loro in 4! modi, le A in 2! modi e le I in 2! modi; il risultato sarà quindi ottenuto dividendo il numero totale delle permutazioni per ciascuno dei modi di permutare le lettere uguali (che sono il numero di possibilità che contiamo piu' volte), ottenendo in questo caso

$$\frac{9!}{4!2!2!}.$$

Combinazioni senza ripetizioni

Consideriamo un insieme di n elementi distinti e cerchiamo di contare i modi di estrarre da questo insieme un sottoinsieme di k elementi; dato che siamo

interessati ai sottoinsiemi l'ordine degli elementi non è rilevante, dunque il numero che cerchiamo deve essere minore di $D_{n,k}$.

Chiamiamo il numero di sottoinsiemi distinti **numero delle combinazioni senza ripetizioni** e indichiamolo con $C_{n,k}$. Possiamo notare che ogni sottoinsieme ottenuto corrisponde ad una stringa di lunghezza k che puo' essere permutata in P_k modi per ottenere tutte le disposizioni possibili. Dunque

$$\begin{aligned} C_{n,k}P_k &= D_{n,k} \\ \iff C_{n,k} &= \frac{D_{n,k}}{P_k} \\ &= \frac{n!}{k!(n-k)!} \\ &= \binom{n}{k}. \end{aligned}$$

4.2.1 *Esempi*

Esempio 4.2.1. Contare i sottoinsiemi di $\{1,2,3,4,5\}$ di cardinalità 3.

SOLUZIONE. Dato che stiamo cercando sottoinsiemi l'ordine non conta, dunque dobbiamo usare le combinazioni, ottenendo che la soluzione è

$$C_{5,3} = \binom{5}{3} = \frac{5!}{3!2!} = \frac{5*4}{2} = 10.$$

Esempio 4.2.2. Quante sono le stringhe binarie di lunghezza n? Quante sono le stringhe binarie di lunghezza 10 con 3 cifre '1' e 7 cifre '0'?

SOLUZIONE. Ogni posizione di una stringa binaria puo' essere riempita con 2 valori ('0' oppure '1') e ci sono n posizioni, dunque il numero di stringhe possibili è il numero di disposizioni con ripetizione di 2 elementi in n posizioni, cioè 2^n.

Per risolvere il secondo punto possiamo scegliere due strade equivalenti.

(i) Prendiamo una qualunque stringa che rispetta le condizioni, come 1110000000; allora il numero di stringhe con 3 uni e 7 zeri è il numero di anagrammi di questa stringa, che è

$$\frac{10!}{3!7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2} = 120.$$

(ii) Notiamo che il problema è equivalente al seguente problema: ho 10 posizioni possibili e devo sceglierne 3 in cui mettere le cifre '1'; infatti a quel punto le altre 7 sono automaticamente riempite con zeri. Dunque dato che dobbiamo scegliere un sottoinsieme (non ordinato) di posizioni tra 10 posizioni, il risultato sarà

$$\binom{10}{3} = \frac{10!}{3!7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2} = 120.$$

Scegliere le 7 posizioni per gli zeri è ovviamente equivalente.

Definizione 4.2.3

Sia A un insieme. Allora si dice insieme delle parti di A l'insieme $\mathcal{P}(A)$ tale che

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

Ad esempio se $A = \{1,2,3\}$ allora

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

Proposizione 4.2.4

Sia A un insieme tale che $|A| = n$. Allora $|\mathcal{P}(A)| = 2^n$.

Dimostrazione. Passiamo ad una rappresentazione alternativa dei sottoinsiemi di A: fissiamo un ordine per l'insieme iniziale, poi associamo ad ogni sottoinsieme una stringa binaria che ha in posizione i il numero 1 se e solo se l'elemento in posizione i nell'insieme iniziale è contenuto nel sottoinsieme.

Ad esempio, se $A = \{1, 2, 3, 4\}$ e il sottoinsieme è $\{3, 4\}$ allora la stringa binaria ad esso associato è 0011, in quanto gli elementi in prima e seconda posizione dell'insieme A (1 e 2) non sono nel sottoinsieme, mentre gli elementi in terza e quarta sono nel sottoinsieme.

Questa associazione è biunivoca, poiché a ogni sottoinsieme corrisponde una e una sola stringa e ad ogni stringa corrispone uno e un solo sottoinsieme, dunque il numero di stringhe è uguale al numero di sottoinsiemi.

Dato che ci sono 2^n stringhe binarie di lunghezza n, allora ci saranno 2^n sottoinsiemi, dunque la cardinalità dell'insieme delle parti $|\mathcal{P}(A)|$ sarà 2^n. □

Esempio 4.2.5. Consideriamo l'insieme dei numeri da 1 a 100. In quanti modi posso formare un sottoinsieme di cardinalità 3 in modo che la somma dei numeri sia pari?

SOLUZIONE. Posso farlo in due modi diversi:

(i) Scelgo tre numeri pari. Allora il problema diventa equivalente a scegliere tre numeri tra i numeri pari da 1 a 100, che sono 50; abbiamo quindi
$$\binom{50}{3} = \frac{50!}{3!47!} = \frac{50 * 49 * 48}{3 \cdot 2}$$
modi per scegliere tre numeri pari.

(ii) Scelgo due numeri dispari e un pari. I due numeri dispari vanno scelti in $\binom{50}{2}$ modi, in quanto non conta l'ordine; il pari puo' essere scelto tra uno qualsiasi dei 50 numeri pari, dunque abbiamo
$$50\binom{50}{2} = 50\frac{50!}{2!48!} = 50\frac{50 * 49}{2}$$
modi.

In totale i modi per formare un sottoinsieme che rispetti le condizioni del testo sono
$$\binom{50}{3} + 50\binom{50}{2} = 50\frac{50 * 49 * 48}{3 \cdot 2}\frac{50 * 49}{2}.$$

Esempio 4.2.6. Quante sono le triple ordinate (x, y, z) di numeri naturali tali che $x + y + z = 4$?

SOLUZIONE. Possiamo rappresentare una soluzione nel seguente modo:
$$\overbrace{1 \dots 1}^{x \text{ volte}} \mid \overbrace{1 \dots 1}^{y \text{ volte}} \mid \overbrace{1 \dots 1}^{z \text{ volte}}$$
dove le linee verticali fanno da separatori tra i gruppi di uni che vanno contate nelle x, nelle y e nelle z.

Dato che la somma deve fare 4 devono esserci 4 uni e due separatori, cioè in totale 6 oggetti; allora il numero di soluzioni puo' essere ottenuto trovando il numero di permutazioni di questi oggetti, che è
$$\frac{6!}{2!4!} = \frac{6 \cdot 5}{2} = 15.$$

Alternativamente dopo aver rappresentato la soluzione come stringa di uni e separatori, potevamo equivalentemente scegliere 2 posizioni su 6 per mettere i separatori, e cio' si puo' fare in

$$\binom{6}{2} = \frac{6!}{2!4!} = 15$$

modi. A quel punto tutte le altre posizioni vengono occupate da uni, dunque la soluzione al problema non cambia.

Esempio 4.2.7. Abbiamo 4 colori: giallo, rosso, verde e blu.

(i) Quanti colori posso formare usando 5 gocce di questi colori?

(ii) Quanti colori posso formare usando 5 gocce di questi colori avendo a disposizione solo 3 gocce di ogni colore?

SOLUZIONE. Indichiamo con g il numero di gocce di colore giallo che usiamo, r la gocce di rosso, v le gocce di verde e con b le gocce di blu.

(i) Il problema è equivalente a chiederci quante quadruple (g, r, v, b) di naturali soddisfano l'equazione $g + r + v + b = 5$. Rappresentiamo come nell'esercizio precedente una soluzione come uni e separatori:

$$\overbrace{1\dots1}^{g \text{ volte}} \mid \overbrace{1\dots1}^{r \text{ volte}} \mid \overbrace{1\dots1}^{v \text{ volte}} \mid \overbrace{1\dots1}^{b \text{ volte}}.$$

Dunque abbiamo 8 oggetti in totale, di cui 5 sono uni e 3 sono separatori. Segue quindi che il numero totale di modi per permutare questi oggetti è

$$\binom{8}{3} = \frac{8!}{5!3!} = \frac{8 \cdot 7 \cdot 6}{6} = 56.$$

(ii) Dal conto del punto (i) sappiamo che senza restrizioni abbiamo 56 possibilità. Da queste dobbiamo togliere tutte le possibilità in cui usiamo 4 o 5 gocce di un colore.

Ho esattamente 4 possibilità di usare 5 gocce dello stesso colore:

$$(5,0,0,0); \quad (0,5,0,0); \quad (0,0,5,0); \quad (0,0,0,5).$$

Contiamo ora in quanti modi posso avere quattro gocce dello stesso colore. Innanzitutto scelgo il colore di cui uso 4 gocce, e posso farlo in 4 modi; dopo scelgo il colore che uso per l'ultima goccia, ed ho 3 possibilità; in tutto ho quindi $12 = 4 \cdot 3$ possibilità. (Notiamo che in questo caso non sto scegliendo due colori tra 4 senza considerare l'ordine, in quanto il primo colore è quello di cui uso 4 gocce, dunque l'ordine conta.)

In totale avro' quindi $56 - 4 - 12 = 40$ possibilità.

Esempio 4.2.8. Consideriamo una tabella 3×3. In quanti modi possiamo colorare ogni casella di bianco o di nero in modo che:

(i) ogni riga è colorata in modo diverso;

(ii) esiste una e una sola riga bianca;

(iii) esiste almeno una riga monocromatica.

SOLUZIONE. Innanzitutto consideriamo una singola riga: dato che è formata da 3 caselle che possono essere colorate in 2 modi, in totale la riga potrà essere colorata in 2^3 modi distinti.

(i) Coloro la prima riga: dato che non ho ulteriori restrizioni lo posso fare in $2^3 = 8$ modi. Ora ho solo 7 modi per colorare la seconda riga, in quanto non posso ripetere la stessa colorazione della prima; e infine ho 6 modi per colorare l'ultima, in quanto non posso ripetere la prima o la seconda. In totale ho quindi $8 \cdot 7 \cdot 6$ modi di colorare la tabella.

(ii) Ho 3 possibilità per scegliere la riga bianca. Ora ho 7 modi per colorare la prima riga non bianca e sempre 7 modi per colorare la seconda riga non bianca (devo escludere la colorazione formata da 3 quadratini bianchi). In totale ho dunque $3 \cdot 7 \cdot 7$ modi di colorare la tabella.

(iii) Potrei pensare di ragionare in questo modo: scelgo una riga monocromatica tra 3; posso colorarla in due modi (tutta bianca o tutta nera); ora posso colorare le due righe rimanenti in 8 modi ciascuna. In realtà questo ragionamento non funziona, perché conterei piu' volte combinazioni in cui ci sono piu' righe monocromatiche.

Abbiamo quindi due modi alternativi a disposizione.

1. Conto separatamente i casi in cui ci sono una, due o tre righe monocromatiche.

   Supponiamo che ci sia una singola riga monocromatica. Dunque dobbiamo scegliere quale riga è (3 possibilità) e se la riga è bianca o nera (2 possibilità); infine le altre due righe non possono essere monocromatiche dunque avremo $8 - 2 = 6$ possibilità per ciascuna di esse. Dunque in questo caso ci sono $3 \cdot 2 \cdot 6^2 = 6^3$ possibilità.

   Supponiamo che ci siano due righe monocromatiche. Allora possiamo sceglierle tra le tre in $\binom{3}{2} = 3$ modi, e possiamo scegliere il loro colore in $2 \cdot 2 = 4$ modi. L'ultima riga deve essere non monocromatica, dunque possiamo sceglierla in 6 modi diversi, ottenendo in totale $3 \cdot 4 \cdot 6 = 72$ possibilità.

   Supponiamo infine che tutte le righe siano monocromatiche. Per ognuna di esse abbiamo due possibilità, dunque abbiamo in totale $2^3 = 8$ scelte possibili.

   Facendo la somma delle varie possibilità otteniamo che ci sono $6^3 + 72 + 8 = 296$ tabelle con almeno una riga monocromatica.

2. Passo al complementare: conto i casi in cui non c'è nessuna riga monocromatica e lo sottraggo dal totale. Se nessuna riga è monocromatica significa che abbiamo $8 - 2 = 6$ possibilità per riga; il numero totale di possibilità senza restrizioni è 2^9 dunque la soluzione al terzo punto è $2^9 - 6^3 = 296$.

Definizione 4.2.9

Indicheremo d'ora in poi con $[n]$ o con $\mathbb{N}_n$ il sottoinsieme dei numeri naturali compresi tra 1 e n inclusi, ovvero

$$\mathbb{N}_n = [n] = \{1; 2; \ldots; n\}. \tag{57}$$

Esempio 4.2.10. Contare i sottoinsiemi di $\mathbb{N}_{100}$ che contengono almeno 3 pari.

Dimostrazione. Scelgo i numeri pari e i dispari da includere nel sottoinsieme indipendentemente.

1. Posso inserire nel sottoinsieme un numero qualunque di dispari, dunque posso scegliere un sottoinsieme qualsiasi dei numeri dispari in $\mathbb{N}_{100}$: dato che in $\mathbb{N}_{100}$ ci sono 50 dispari, il numero di sottoinsiemi di numeri dispari è 2^50.

2. Per contare i possibili sottoinsiemi con i pari passo al complementare e sottraggo dal totale ($2^5 0$ per le stesse motivazioni) il numero di sottoinsiemi con nessun pari (ovvero $\binom{50}{0}$), il numero di sottoinsiemi con un solo pari (ovvero $\binom{50}{1}$) e il numero di sottoinsiemi con due numeri pari (ovvero $\binom{50}{2}$).

□

Esempio 4.2.11. Quante sono le triple (n, m, k) con $n, m, k \in \mathbb{N}_{100}$ tali che $nmk = 100$?

SOLUZIONE. Dato che $100 = 2^2 5^2$ segue che n, m, k devono avere come soli fattori primi 2 e 5, ovvero

$$n = 2^{a_1} 5^{b_1}, \quad m = 2^{a_2} 5^{b_2}, \quad k = 2^{a_3} 5^{b_3}.$$

Dunque $nmk = 2^{a_1+a_2+a_3} 5^{b_1+b_2+b_3} = 2^2 5^2$, ovvero

$$a_1 + a_2 + a_3 = 2, \quad b_1 + b_2 + b_3 = 2.$$

Per trovare in quanti modi posso scegliere a_1, a_2, a_3 considero un insieme di 2 '1' e 2 separatori e lo permuto, ottenendo $\frac{4!}{2!2!} = 6$ modi. Equivalentemente, i modi di scegliere b_1, b_2, b_3 sono 6.

In totale ho quindi $6 \cdot 6 = 36$ modi.

4.2.2 *Teorema del binomiale*

Forniamo ora una dimostrazione del teorema del Binomiale (3.5.4) usando il calcolo combinatorio.

Dimostrazione del Teorema del Binomiale (3.5.4). Per definizione

$$(x+y)^n = \overbrace{(x+y)\cdots(x+y)}^{n \text{ volte}}.$$

Dunque il risultato dell'elevamento a potenza sarà la somma di tutti i monomi formati da una sequenza di x e y di lunghezza n, in quanto ogni addendo sarà dato dalla scelta di x o di y in ogni fattore di $(x+y)\cdots(x+y)$.

Ad esempio

$$\begin{aligned}(x+y)^3 &= (x+y)(x+y)(x+y)\\ &= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy\\ &= xxx + (xxy + xyx + yxx) + (xyy + yxy + yyx) + yyy\\ &= x^3 + 3x^2y + 3xy^2 + y^3.\end{aligned}$$

Ognuno di questi monomi puo' essere semplificato alla forma $x^k y^h$, ma dato che il numero di x e y deve essere n segue che $k + h = n$, cioè $h = n - k$, cioè ogni monomio puo' essere scritto nella forma $x^k y^{n-k}$. Dato che ogni monomio ha al minimo o fattori uguali a x e al massimo n fattori uguali a x, sommando i monomi uguali insieme otterremo:

$$\begin{aligned}(x+y)^n &= c_0 x^0 y^n + c_1 x^1 y^{n-1} + \cdots + c_{n-1} x_{n-1} y_1 + c_n x^n y^0\\ &= \sum_{k=0}^{n} c_k x^k y^{n-k}\end{aligned}$$

dove i coefficienti c_k rappresentano il numero di monomi uguali sommati insieme.

Troviamo quindi un'espressione per c_k per un k generico. Dato che c_k rappresenta il numero di termini nell'espressione originale che possono

essere semplificati a $x^k y^{n-k}$, allora c_k indica il numero di termini con k fattori uguali a x (edi conseguenza i restanti $n-k$ uguali a y).

Il numero di questi termini è uguale al numero di modi in cui possiamo posizionare k 'x' in una stringa di n elementi, che è il numero di modi in cui possiamo scegliere k posizioni da un insieme di n elementi. Inoltre una volta scelte le posizioni per le x le y andranno in tutte le restanti $n-k$ posizioni, dunque

$$c_k = \binom{n}{k}.$$

Sostituendolo nell'espressione per $(x+y)^n$ otteniamo

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

che è la tesi. □

4.2.3 *Poker*

Cerchiamo di calcolare il numero di modi in cui possiamo fare punteggi nel Poker tradizionale.

Innanzitutto descriviamo il gioco: abbiamo un mazzo di 52 carte divise in 4 semi, con valori 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K. Si pescano 5 carte e viene assegnato un punteggio alla mano se è in una delle seguenti combinazioni:

Scala reale massima. una scala formata da 10, J, Q, K, 1 dello stesso seme (es. 10-J-Q-K-1 di cuori);

Scala reale. una scala formata da cinque carte consecutive dello stesso seme (es. 8-9-10-J-Q di fiori);

Colore. cinque carte dello stesso seme (es. 1-3-5-6-J di fiori);

Scala. una scala formata da cinque carte consecutive, non tutte dello stesso seme;

Poker. quattro carte dal valore uguale e una diversa (es. 3-3-3-3-5);

Full. una coppia di carte dal valore uguale e un tris di carte dal valore uguale (es. 2-2-4-4-4);

Tris. tre carte dal valore uguale e due diverse (es. 3-3-3-1-2);

Doppia coppia. due coppie di carte dal valore uguale e una diversa (es. J-J-5-5-8);

Coppia. una coppia di carte dal valore uguale e tre diverse (es. K-K-1-9-10).

Calcoliamo il numero di mani possibili. Dato che dobbiamo scegliere 5 carte da 52 e non abbiamo altre restrizioni, il numero di mani possibili è

$$\binom{52}{5}.$$

Ora calcoliamo il numero di possibilità per ogni combinazione che dà punteggio.

Scala reale massima. Ho una scala reale massima per seme, dunque in tutto devo avere 4 scale reali massime.

Scala reale. Ho 10 scale reali per seme: infatti ne posso costruire una che parte da 1, una che parte da 2,..., una che parte da 10. Dato che ho 4 semi, il numero totale di scale reali è $4 \cdot 10 = 40$.

Colore. Scegliamo un seme (4 possibilità). Allora il numero di colori che possiamo fare in un dato seme equivale al numero di modi in cui possiamo scegliere 5 carte di quel seme, che è $\binom{13}{5}$. Dunque in totale il numero di colori che non siano scale reali è $4\binom{13}{5} - 40$.

Scala. Ci sono 10 sequenze di valori possibili che formano una scala: infatti ne posso costruire una che parte da 1, una che parte da 2,..., una che parte da 10. Dato che posso scegliere liberamente il seme di ogni carta della scala, il numero totale di scale è $4^5 \cdot 10$. Sottraendo ad esse il numero di scale reali otteniamo il numero di scale non reali, che sono $4^5 \cdot 10 - 40$.

Poker. Scelgo innanzitutto la carta che si deve ripetere 4 volte, e dato che ho 13 valori diversi avro' 13 possibilità di sceglierla. Dopo devo scegliere l'ultima carta, che puo' essere una qualunque tra le $52 - 4 = 48$ rimanenti. Dunque in totale ho $13 \cdot 48$ modi per fare poker.

Full. Scelgo il valore della carta che formerà il tris, e posso sceglierlo in 13 modi; poi scelgo il valore della carta che formerà la coppia, che posso scegliere in $13 - 1 = 12$ modi.

Ora devo scegliere i valori dei semi: per quanto riguarda il tris devo scegliere 3 semi su 4 (l'ordine non conta), e posso farlo in $\binom{4}{3} = 4$ modi; per quanto riguarda la coppia devo scegliere 2 semi su 4 e posso farlo in $\binom{4}{2} = 6$ modi.

In totale ho dunque $4 \cdot 6 \cdot 12 \cdot 13$ modi di fare full.

Tris. Scelgo il valore della carta del tris in 13 modi e i semi in $\binom{4}{3} = 4$ modi. Non posso tuttavia scegliere le altre due carte liberamente, in quanto altrimenti potremmo ricadere nel poker o nel full.

Dunque scelgo il valore delle due carte rimanenti tra 12 valori (tutti tranne quello del tris), poi scelgo un seme tra 4 per la prima e un seme tra 4 per la seconda. In totale ho quindi $13 \cdot 4 \cdot \binom{12}{2} \cdot 4^2 = 4^3 \cdot 13\binom{12}{2}$ modi di fare tris.

Doppia coppia. Scelgo il valore delle due coppie tra 13 valori possibili in $\binom{13}{2}$ modi; ora scelgo i semi delle due coppie, e posso farlo in $\binom{4}{2}$ per la prima e $\binom{4}{2}$ per la seconda.

Scelgo la quinta carta in modo che abbia un valore diverso dalle due coppie per non contare anche i full: dunque posso sceglierla in $13 - 2 = 11$ modi per 4 semi diversi. In totale ho quindi $4 \cdot 11\binom{13}{2}\binom{4}{2}^2$ modi di ottenere una doppia coppia.

Coppia. Scelgo il valore della coppia tra 13 valori possibili e i semi in $\binom{4}{2}$ modi. Scelgo le tre carte rimanenti diverse tra di loro e diverse dal valore della coppia per evitare doppie coppie, full e poker: dunque ho $\binom{12}{3}$ modi di sceglierle e, dato che ognuna di esse puo' avere un seme qualunque, ho 4 possibilità per ciascuna. In totale ho quindi $4^3 \cdot 13\binom{4}{2}\binom{12}{3}$ modi di fare coppia.

4.3 PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Il principio di inclusione-esclusione mette in relazione la cardinalità dell'unione di due o piu' insiemi con la cardinalità delle intersezioni e degli insiemi presi singolarmente. Per due insiemi vale che

$$|A \cup B| = |A| + |B| - |A \cap B| . \tag{58}$$

Per tre insiemi vale che

$$\begin{aligned}|A \cup B \cup C| = |A| + |B| + |C| + \\ - |A \cap B| - |A \cap C| - |B \cap C| + \\ + |A \cap B \cap C| .\end{aligned}$$

Dunque per n insiemi si sommano le cardinalità degli insiemi, poi si sottraggono le cardinalità delle intersezioni due a due, poi si sommano le cardinalità delle intersezioni tre a tre, eccetera.

Esempio 4.3.1. Contare i numeri di $\mathbb{N}_{100}$ che non sono divisibili né per 3 né per 5.

SOLUZIONE. Sia A l'insieme dei numeri divisibili per 3 e B l'insieme dei numeri divisibili per 5, dunque A^C sono i numeri non divisibili per 3 e B^C sono i numeri non divisibili per 5.

Noi vogliamo calcolare $\left|A^C \cap B^C\right|$, cioè la cardinalità dell'insieme dei numeri che non sono né divisibili per 3 né per 5. Per De Morgan:

$$\left|A^C \cap B^C\right| = |\mathbb{N}_{100}| - |A \cup B| = 100 - |A \cup B| .$$

Per il principio di inclusione-esclusione:

$$|A \cup B| = |A| + |B| - |A \cap B| .$$

Dunque

- un numero su 3 è divisibile per 3, dunque $|A| = \frac{100}{3} = 33$;
- un numero su 5 è divisibile per 5, dunque $|A| = \frac{100}{5} = 20$;
- i numeri divisibili sia per 3 che per 5 sono tutti i numeri divisibili per 15, dunque $|A \cap B| = \frac{100}{15} = 6$;

ovvero

$$\left|A^C \cap B^C\right| = 100 - (33 + 20 - 6) = 100 - 47 = 53.$$

4.4 CONTARE FUNZIONI

Esempio 4.4.1. Quante sono le funzioni $f : \mathbb{N}_n \to \mathbb{N}_m$?

SOLUZIONE. La funzione f mappa ogni elemento di $\mathbb{N}_n$ in un elemento di $\mathbb{N}_m$. Dunque per $f(1)$ possiamo scegliere $|\mathbb{N}_m| = m$ possibili output, per $f(2)$ possiamo sceglierne altri $|\mathbb{N}_m| = m$, eccetera.

In totale dunque abbiamo $\underbrace{m \cdots m}_{n \text{ volte}} = m^n$ possibili funzioni.

Esempio 4.4.2. Quante sono le funzioni $f : \mathbb{N}_{20} \to \mathbb{N}_{20}$ che in output hanno almeno un valore maggiore o uguale a 11?

SOLUZIONE. Basta sottrarre al numero totale di funzioni da $\mathbb{N}_{20}$ a $\mathbb{N}_{20}$ (che è 20^{20}) il numero di funzioni che non hanno un valore in output maggiore o uguale a 11, ovvero il numero di funzioni $f : \mathbb{N}_{20} \to \mathbb{N}_{10}$ (che è 10^{20}).

Dunque avro' $20^{20} - 10^{20}$ funzioni.

Esempio 4.4.3. Quante sono le funzioni $f : \mathbb{N}_{20} \to \mathbb{N}_{20}$ che in output hanno esattamente un valore maggiore o uguale a 11?

SOLUZIONE. Sia k il valore maggiore o uguale a 11 assunto dalla funzione: posso scegliere k in 10 modi. Il numero di funzioni $f : \mathbb{N}_{20} \to \mathbb{N}_{10} \cup \{k\}$ è 11^{20}, in quanto $|\mathbb{N}_{10} \cup \{k\}| = 10 + 1 = 11$. Da queste devo togliere tutte le funzioni che non hanno k come valore in output, che sono tutte e solo le funzioni $f : \mathbb{N}_{20} \to \mathbb{N}_{10}$, che sono 10^{20}.

In totale ho quindi $10(11^{20} - 10^{20})$ funzioni.

Esempio 4.4.4. Quante sono le funzioni $f : \mathbb{N}_{10} \to \mathbb{N}_{20}$ strettamente crescenti?

SOLUZIONE. Se la funzione è strettamente crescente i valori in output devono essere tutti diversi tra loro.

Scelgo quindi 10 valori in $\mathbb{N}_{20}$. Scelti questi valori, c'è un solo modo per cui la funzione sia crescente, cioè ordinarli in ordine crescente. Dunque ad ogni sottoinsieme di 10 valori tra 20 corrisponde una funzione, dunque ho in tutto $\binom{20}{10}$ funzioni che soddisfano la proprietà.

Esempio 4.4.5. Quante sono le funzioni $f : \mathbb{N}_n \to \mathbb{N}_k$ iniettive?

SOLUZIONE. Dato che la funzione è iniettiva, i valori in output devono essere tutti diversi tra loro. Ovviamente se $k > n$ non puo' esserci una funzione iniettiva da $\mathbb{N}_n$ a $\mathbb{N}_k$, dunque il numero di funzioni iniettive è 0 in questo caso.

Supponiamo $k \leq n$. Dunque scelgo il valore di $f(1)$ in n modi, il valore di $f(2)$ in $n-1$ modi, eccetera. In totale il numero di funzioni iniettive che rispettano queste proprietà è

$$n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!} = D_{n,k}.$$

Esempio 4.4.6. Quante sono le funzioni $f : \mathbb{N}_4 \to \mathbb{N}_3$ surgettive?

SOLUZIONE. Definiamo il seguente insieme:

$$\begin{aligned} F_i &:= \text{ insieme delle funzioni } f : \mathbb{N}_4 \to \mathbb{N}_3 \text{ tali che } i \in \operatorname{Im} f \\ &= \{f \mid f : \mathbb{N}_4 \to \mathbb{N}_3, i \in \operatorname{Im} f\} \end{aligned}$$

e dunque il suo complementare

$$\begin{aligned} F_i^C &:= \text{ insieme delle funzioni } f : \mathbb{N}_4 \to \mathbb{N}_3 \text{ tali che } i \notin \operatorname{Im} f \\ &= \{f \mid f : \mathbb{N}_4 \to \mathbb{N}_3, i \notin \operatorname{Im} f\}. \end{aligned}$$

L'insieme delle funzioni $f : \mathbb{N}_4 \to \mathbb{N}_3$ surgettive è l'insieme delle funzioni tali che $1, 2, 3, \in \operatorname{Im} f$, cioè è dato da $F_1 \cap F_2 \cap F_2$. Per De Morgan:

$$|F_1 \cap F_2 \cap F_2| = |U| - \left|(F_1 \cap F_2 \cap F_2)^C\right| = |U| - \left|F_1^C \cup F_2^C \cup F_3^C\right|,$$

dove U è l'insieme di tutte le funzioni $f : \mathbb{N}_4 \to \mathbb{N}_3$, dunque ha cardinalità $|U| = 3^4$.

Per il principio di inclusione-esclusione:

$$\begin{aligned} \left|F_1^C \cup F_2^C \cup F_3^C\right| = &\left|F_1^C\right| + \left|F_2^C\right| + \left|F_3^C\right| + \\ &- \left|F_1^C \cap F_2^C\right| - \left|F_1^C \cap F_3^C\right| - \left|F_2^C \cap F_3^C\right| + \\ &- \left|F_1^C \cap F_2^C \cap F_3^C\right|. \end{aligned}$$

Calcoliamo le cardinalità degli insiemi che abbiamo:

- F_1^C è l'insieme di tutte le funzioni che non hanno 1 nell'immagine, cioè contiene tutte e solo le funzioni da $\mathbb{N}_4$ a $\{2, 3\}$, dunque la sua cardinalità è 2^4; stesso ragionamento per F_2^C e F_3^C;
- $F_1^C \cap F_2^C$ è l'insieme di tutte le funzioni che non hanno 1 e 2 nell'immagine, cioè contiene tutte e solo le funzioni da $\mathbb{N}_4$ a $\{3\}$, dunque la sua cardinalità è $1^4 = 1$; stesso ragionamento per $F_1^C \cap F_3^C$ e $F_2^C \cap F_3^C$;
- $F_1^C \cap F_2^C \cap F_3^C$ è l'insieme di tutte le funzioni che non hanno 1, 2, e 3 nell'immagine, cioè contiene tutte e solo le funzioni $\mathbb{N}_4$ all'insieme vuoto $\varnothing$, dunque ha cardinalità 0 (non ci sono funzioni che hanno come codominio l'insieme vuoto).

In totale abbiamo quindi

$$|F_1 \cap F_2 \cap F_2| = 3^4 - (3 \cdot 2^4 - 3 + 0) = 3^4 - 3(2^4 - 1)$$

funzioni surgettive da $\mathbb{N}_4$ a $\mathbb{N}_3$.

5 POLINOMI

5.1 DEFINIZIONI BASE

Definizione 5.1.1 (Polinomio)

Sia A un anello. Allora si dice polinomio a coefficienti in A un'espressione del tipo

$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n \tag{59}$$

dove $a_0, \ldots, a_n \in A$.

L'insieme di tutti i polinomi a coefficienti in A si indica con $A[x]$.

Nel seguito indicheremo con A un anello generico (come $\mathbb{Z}$, $\mathbb{Z}/(n)$ con n non primo) e con $\mathbb{K}$ un campo generico (come $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/(p)$ con p primo). Notiamo inoltre che, dato che un campo è anche un anello, tutte le definizioni e le proposizioni che valgono per gli anelli valgono anche per i campi (ma non viceversa).

Definizione 5.1.2 (Funzione associata ad un polinomio)

Sia $p(x) \in A[x]$. Allora la funzione associata al polinomio p e' la funzione $p : A \to A$ tale che per ogni $x \in A$ vale che

$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n.$$

Definizione 5.1.3 (Grado di un polinomio)

Sia $p(x) \in A[x]$ (ovvero, sia $p(x)$ un polinomio a coefficienti nell'anello A). Si dice grado di p il massimo n tale che $a_n \neq 0$, e si indica con $\deg p$.

Definizione 5.1.4 (Radice di un polinomio)

Sia $p(x) \in A[x]$. Allora si dice che $r \in A$ è radice (o zero) di p se

$$p(r) = 0. \tag{60}$$

Proposizione 5.1.5 (Radici di un polinomio di grado 0)

Sia $p(x) \in A[x]$ tale che $\deg p = 0$. Allora p non ha radici oppure ne ha infinite.

Dimostrazione. Dato che $\deg p = 0$, allora sarà $p(x) = a_0$ per qualche $a_0 \in A$.

Abbiamo due casi:

- se $a_0 = 0$, allora $p(x) = 0$ per ogni $x \in A$, dunque ogni elemento di A è radice del polinomio;
- se $a_0 \neq 0$ allora $p(x) \neq 0$ per ogni $x \in A$, dunque nessun elemento di A è radice del polinomio. □

Proposizione 5.1.6 (Radici di un polinomio di primo grado)

Sia $p(x) \in \mathbb{K}[x]$ tale che $\deg p = 1$. Allora esiste almeno una radice di p.

Dimostrazione. Dato che $\deg p = 1$, allora sarà $p(x) = a_0 + a_1 x$ per qualche $a_0, a_1 \in \mathbb{K}$.

Sia r una radice di p, allora deve valere che

$$\begin{aligned} & p(r) = 0 \\ \iff & a_0 + a_1 r = 0 \\ \iff & a_1 r = -a_0 \\ \iff & r = -a_0 a_1^{-1} \end{aligned}$$

ovvero esiste $r \in \mathbb{K}$ e vale $-a_0 a_1^{-1}$. □

Osservazione. I polinomi di grado 1 potrebbero non avere radici in un anello A. Ad esempio sia $p(x) \in \mathbb{Z}/(8)$, $p(x) = -3 + 4x$. Allora

$$\begin{aligned} & 4x - 3 \equiv 0 \ (8) \\ \iff & 4x \equiv 3 \ (8) \end{aligned}$$

che non ha soluzioni in quanto $\text{mcd}\,(4, 8) \nmid 3$.

Osservazione. I polinomi di secondo grado possono avere radici o possono non averne.

- $p(x) \in \mathbb{Q}[x]$, $p(x) = x^2 - 4$ ha come radici $x = \pm 2$;
- $p(x) \in \mathbb{Q}[x]$, $p(x) = x^2 - 2$ non ha radici;
- $p(x) \in \mathbb{R}[x]$, $p(x) = x^2 - 2$ ha come radici $x = \pm\sqrt{2}$;
- $p(x) \in \mathbb{R}[x]$, $p(x) = x^2 + 1$ non ha radici;
- $p(x) \in \mathbb{C}[x]$, $p(x) = x^2 + 1$ ha come radici $x = \pm i$.

Definizione 5.1.7 (Polinomio monico)

Sia $p(x) \in A[x]$ un polinomio. Allora p si dice monico se il coefficiente del termine di grado massimo è 1, ovvero se

$$p(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

per qualche $a_0, \ldots, a_{n-1} \in A$.

Proposizione 5.1.8 (Il grado del prodotto è la somma dei gradi)

Siano $p(x), q(x) \in A[x]$. Allora $\deg(p \cdot q) = \deg p + \deg q$.

5.2 DIVISIONE E FATTORIZZAZIONI

Teorema 5.2.1 (Esistenza e unicità della divisione polinomiale nei campi)

Siano $p(x), q(x) \in \mathbb{K}[x]$. Allora esistono e sono unici $q(x), r(x) \in \mathbb{K}[x]$ tali che

$$p(x) = g(x)q(x) + r(x), \quad \textit{con } \deg r < \deg g. \tag{61}$$

Proposizione 5.2.2 (Esistenza e unicità della divisione polinomiale negli anelli)

Siano $p(x), g(x) \in A[x]$ con g monico. Allora esistono e sono unici $q(x), r(x) \in A[x]$ tali che

$$p(x) = g(x)q(x) + r(x), \quad \textit{con } \deg r < \deg g. \tag{62}$$

Definizione 5.2.3 (Divisibilità tra polinomi)

Siano $p(x), g(x) \in A[x]$. Allora si dice che $g(x) \mid p(x)$ se e solo se esiste $q(x) \in A[x]$ tale che

$$p(x) = g(x)q(x).$$

Per questa definizione di divisione euclidea possiamo definire un massimo comun divisore e un minimo comune multiplo tra polinomi.

Definizione 5.2.4 (Massimo comun divisore tra polinomi)

Siano $p(x), g(x) \in K[x]$. Allora si dice massimo comun divisore di $p(x), g(x)$ il polinomio $h(x)$ di grado massimo tale che

$$h(x) \mid p(x) \wedge h(x) \mid g(x)$$

e si indica con $\operatorname{mcd}(f(x), g(x))$.

Definizione 5.2.5 (Minimo comune multiplo tra polinomi)

Siano $p(x), g(x) \in K[x]$. Allora si dice minimo comune multiplo di $p(x), g(x)$ il polinomio $h(x)$ di grado minimo tale che

$$p(x) \mid h(x) \wedge g(x) \mid h(x)$$

ovvero tale che $h(x)$ è multiplo sia di $p(x)$ che di $g(x)$ e si indica con $\operatorname{mcm}(f(x), g(x))$.

Molti teoremi sul massimo comun divisore e massimo comune multiplo continuano a valere negli insiemi dei polinomi, come ad esempio il seguente.

Proposizione 5.2.6

Siano $p(x), g(x) \in \mathbb{K}[x]$. *Allora* $\operatorname{mcd}(p(x), g(x)) = \operatorname{mcd}(p(x) - g(x)h(x), g(x))$, *con* $h(x) \in \mathbb{K}[x]$.

Proposizione 5.2.7

Sia $p(x) \in A[x]$ *e sia* $a \in A$. *Sia* $r(x) \in A[x]$ *il resto della divisione di* $p(x)$ *per* $(x - a)$. *Allora* $r(x) = r_0$ *per qualche* $r_0 \in A$ *e* $p(a) = r_0$.

Dimostrazione. Per il teorema sulla divisione tra polinomi (5.2.3), dato che $x - a$ è un polinomio monico, sappiamo che esistono $q(x), r(x) \in A[x]$ tali che

$$p(x) = (x - a)q(x) + r(x).$$

Dato che $\deg(x - a) = 1$ e $\deg r < \deg a$ segue che $\deg r = 0$, cioè per ogni $x \in A$ vale che $r(x) = r_0$ per qualche $r_0 \in A$.

Ora valutiamo il polinomio in a, ottenendo

$$\begin{aligned} p(a) &= (a - a)q(a) + r(a) \\ &= 0q(a) + r_0 \\ &= r_0 \end{aligned}$$

che è la tesi. □

Teorema 5.2.8 (Teorema di Ruffini)

Sia $p(x) \in A[x]$ *e sia* $a \in A$. *Allora*

$$(x - a) \mid p(x) \iff p(a) = 0$$

ovvero $x - a$ *divide* $p(x)$ *se e solo se* a *è una radice di* p.

Dimostrazione. Per il teorema sulla divisione tra polinomi (5.2.3), dato che $x - a$ è un polinomio monico, sappiamo che esistono $q(x), r(x) \in A[x]$ tali che

$$p(x) = (x - a)q(x) + r(x).$$

Dato che $\deg(x - a) = 1$ e $\deg r < \deg a$ segue che $\deg r = 0$, cioè per ogni $x \in A$ vale che $r(x) = r_0$ per qualche $r_0 \in A$.

Per la proposizione 5.2.7 segue che $p(a) = r_0$, dunque a è radice se e solo se $r_0 = 0$, cioè se e solo se il polinomio $p(x)$ è divisibile per $(x - a)$. □

Definizione 5.2.9 (Polinomio irriducibile)

Sia $p(x) \in A[x]$. Allora p si dice irriducibile se non esistono $a(x), b(x) \in A[x]$ tali che valgano le seguenti tre condizioni:

- $\deg a < \deg p$;
- $\deg b < \deg p$;
- $p(x) = a(x)b(x)$.

OSSERVAZIONE. Tutti i polinomi p tali che $\deg p \leq 1$ sono irriducibili.

Definizione 5.2.10 (Fattorizzazione di un polinomio)

Sia $p \in A[x]$. Fattorizzare p significa trovare $a_1(x), \dots, a_n(x) \in A[x]$ tali che:

- $a_1(x), \dots, a_n(x)$ sono tutti irriducibili;
- $p(x) = a_1(x) \cdots a_n(x)$.

Proposizione 5.2.11

Sia $p(x) \in \mathbb{K}[x]$. Allora la fattorizzazione di p è unica (a meno di fattori costanti).

OSSERVAZIONE. La fattorizzazione di p non è unica negli anelli!

Proposizione 5.2.12

Sia $p(x) \in \mathbb{K}[x]$ e siano $g(x), h(x) \in \mathbb{K}[x]$ tali che $p(x) = g(x)h(x)$. Allora $r \in \mathbb{K}$ è una radice di p se e solo se è radice di g o è radice di h.

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Supponiamo che $p(r) = 0$. Allora $p(r) = g(r)h(r) = 0$, dunque per la regola di annullamento del prodotto (1.1.4) segue che $g(r) = 0 \vee h(r) = 0$.

($\Longleftarrow$) Supponiamo senza perdita di generalità che $g(r) = 0$. Allora $p(r) = g(r)h(r) = 0h(r) = 0$. □

Corollario 5.2.13

Sia $p(x) \in \mathbb{K}[x]$ e sia $p_1(x), \dots, p_n(x) \in \mathbb{K}[x]$ una fattorizzazione di p. Allora $r \in \mathbb{K}$ è una radice di p se e solo se è radice di uno tra $p_1, \dots, p_n$.

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Infatti $p(r) = p_1(r) \cdots p_n(r) = 0$, dunque per la regola di annullamento del prodotto (1.1.4) segue che

$$p_1(r) = 0 \vee p_2(r) = 0 \vee \cdots \vee p_n(r) = 0$$

ovvero la tesi.

($\Longleftarrow$) Supponiamo senza perdita di generalità che $p_1(r) = 0$. Allora $p(r) = p_1(r)p_2(r)\cdots p_n(r) = 0p_2(r)\cdots p_n(r) = 0$. □

OSSERVAZIONE. La proposizione 5.2.12 vale soltanto nei campi, mentre negli anelli vale solo una delle due implicazioni (in particolare quella che dice che se r è radice di un fattore, allora è radice anche del polinomio) in quanto non vale la regola di annullamento del prodotto. La conseguenza di questo fatto è che in un anello A un polinomio ha piu' radici di quante ne abbiano i suoi fattori, cioè la fattorizzazione di un polinomio non è unica.

Proposizione 5.2.14 (Un polinomio di grado n ha al massimo n radici in un campo)

Sia $p(x) \in \mathbb{K}[x]$ tale che $n = \deg p$. Allora p ha al massimo n radici.

Dimostrazione. Dimostriamolo per induzione su n.

CASO BASE. Se $n = 1$ allora $p(x) = a_0 + a_1x$, dunque l'unica radice è $-a_0a_1^{-1}$.

PASSO INDUTTIVO. Supponiamo che la tesi valga per n e dimostriamola per $n+1$. Consideriamo due casi:

- Se p non ha radici allora p ha meno radici di $n+1$, che è la tesi.
- Se p ha una radice r allora p è divisibile per $x - r$, ovvero esiste $q(x) \in \mathbb{K}[x]$ tale che $p(x) = (x - r)q(x)$. Per la proposizione 5.1.8 segue che $\deg q = n$, dunque per ipotesi induttiva il numero di radici di q è minore o uguale a n. Aggiungendo la radice r segue infine che p ha al massimo $n+1$ radici.

Dunque per induzione la tesi vale per ogni $n \geq 1$. □

5.3 FATTORIZZAZIONE IN INSIEMI SPECIFICI

5.3.1 *Fattorizzazione in $\mathbb{C}$*

Teorema 5.3.1 (Teorema Fondamentale dell'Algebra)

Sia $p(x) \in \mathbb{C}[x]$ tale che $\deg p \geq 1$. Allora esiste almeno una radice di p in $\mathbb{C}$, ovvero esiste almeno un $\lambda \in \mathbb{C}$ tale che $p(\lambda) = 0$.

Corollario 5.3.2 (Ogni polinomio ha n radici complesse)

Sia $p(x) \in \mathbb{C}$ e sia $n = \deg p \geq 1$. Allora p ha esattamente n radici complesse, ovvero p è fattorizzabile in esattamente n fattori lineari (non necessariamente distinti).

Dimostrazione. Dimostriamo per induzione su n.

CASO BASE Sia $n = 1$. Allora $p(x) = a_0 + a_1x$ che ammette la radice $-a_0a_1^{-1}$. Inoltre $p(x)$ è fattorizzabile in fattori lineari in quanto esso stesso è lineare.

PASSO INDUTTIVO Supponiamo che la tesi valga per n e dimostriamo che vale anche per $n+1$.

Sia $p(x)$ di grado $n+1$. Allora per il Teorema Fondamentale dell'Algebra (5.3.1) p ammette almeno una radice $\lambda \in \mathbb{C}$.

Per il teorema di Ruffini (5.2.8) segue che $(x - \lambda)$ è un divisore di $p(x)$, ovvero esiste $q(x) \in \mathbb{C}[x]$ tale che

$$p(x) = (x - \lambda)q(x).$$

Il grado di q dovrà essere $\deg p - 1 = n + 1 - 1 = n$, dunque per ipotesi induttiva q ha n radici ed è fattorizzabile in n fattori lineari.

Di conseguenza p ha $n+1$ radici ed è fattorizzabile in $n+1$ fattori lineari.

Per induzione allora la tesi vale per ogni $n \geq 1$. □

Proposizione 5.3.3 (Un polinomio reale ha radici complesse coniugate)
Sia $p(x) \in \mathbb{R}[x]$ un polinomio a coefficienti reali. Allora $\lambda \in \mathbb{C}$ è una radice di p se e solo se $\overline{\lambda}$ è una radice di p.

Dimostrazione. Sia $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ con $a_0, \ldots, a_n \in \mathbb{R}$. Supponiamo che $p(\lambda) = 0$. Allora

$$\begin{aligned} p(\overline{\lambda}) &= a_0 + a_1\overline{\lambda} + \cdots + a_n\overline{\lambda^n} && (\text{se } a \in \mathbb{R} \text{ allora } \overline{a} = a) \\ &= \overline{a_0} + \overline{a_1} \cdot \overline{\lambda} + \cdots + \overline{a_n} \cdot \overline{\lambda^n} && (\text{per la 1.2.7}) \\ &= \overline{a_0} + \overline{a_1\lambda} + \cdots + \overline{a_n\lambda^n} && (\text{per la 1.2.7}) \\ &= \overline{a_0 + a_1\lambda + \cdots + a_n\lambda^n} \\ &= \overline{p(\lambda)}. \end{aligned}$$

Dunque $p(\lambda) = 0 \iff \overline{p(\lambda)} = \overline{0} \iff p(\overline{\lambda}) = 0$, come volevasi dimostrare. □

5.3.2 *Fattorizzazione in* $\mathbb{R}$

Lemma 5.3.4
Sia $\lambda \in \mathbb{C}$. Allora il polinomio

$$p(x) = (x - \lambda)(x - \overline{\lambda})$$

è un polinomio a coefficienti reali.

Dimostrazione.

$$\begin{aligned} p(x) &= (x - \lambda)(x - \overline{\lambda}) \\ &= x^2 - (\lambda + \overline{\lambda})x + \lambda\overline{\lambda} && (\text{per 1.2.8}) \\ &= x^2 - 2(\operatorname{Re}(\lambda))x + |\lambda|^2 . \end{aligned}$$

Dato che $2\operatorname{Re}(\lambda), |\lambda|^2 \in \mathbb{R}$ segue la tesi. □

Proposizione 5.3.5
Sia $p(x) \in \mathbb{R}[x]$. Allora p è fattorizzabile su $\mathbb{R}$ come prodotto di fattori di grado minore o uguale a 2.

Dimostrazione. Dimostriamolo per induzione forte su $n = \deg p$.

CASO BASE Sia $n = 1$ oppure $n = 2$. Allora p è banalmente già fattorizzato in fattori di grado 1 o 2.

PASSO INDUTTIVO Sia $n > 2$ e supponiamo che la tesi sia vera per ogni n' tale che $1 \leq n' < n$.

Per il teorema fondamentale dell'algebra (5.3.1) allora esiste sicuramente $\lambda \in \mathbb{C}$ tale che $p(\lambda) = 0$. Distinguiamo due casi.

- Se $\lambda \in \mathbb{R}$ allora per il teorema di Ruffini (5.2.8) segue che $(x-\lambda) \mid p(x)$, ovvero esiste $g(x) \in \mathbb{R}[x]$ tale che

  $$p(x) = (x-\lambda)g(x).$$

  Dato che $\deg g = \deg p - 1 = n-1$ segue che per ipotesi induttiva g è fattorizzabile come prodotto di fattori di grado 1 o 2, dunque anche f lo è.
- Se $\lambda \notin \mathbb{R}$ allora per la proposizione 5.3.3 anche $\overline{\lambda}$ è radice di p. Per il teorema di Ruffini (5.2.8) segue che

  $$(x-\lambda) \mid p(x), \quad (x-\overline{\lambda}) \mid p(x)$$

  dunque

  $$(x-\lambda)(x-\overline{\lambda}) \mid p(x).$$

  Per il lemma 5.3.4 il polinomio $h(x) = (x-\lambda)(x-\overline{\lambda})$ è un polinomio a coefficienti reali, dunque dato che $h(x) \mid p(x)$ esiste $g(x) \in \mathbb{R}[x]$ tale che

  $$p(x) = h(x)g(x) = (x-\lambda)(x-\overline{\lambda}) \cdot g(x).$$

  Dato che $\deg g = \deg p - 2 = n-2$ segue che per ipotesi induttiva g è fattorizzabile come prodotto di fattori di grado 1 o 2, dunque anche p lo è.

Per induzione ogni polinomio in $\mathbb{R}[x]$ è esprimibile come prodotto di fattori di grado minore o uguale a 2. □

Un modo equivalente di esprimere la proposizione sopra è dire che ogni polinomio a coefficienti reali di grado maggiore di due è riducibile in $\mathbb{R}$.

5.3.3 *Fattorizzazione in $\mathbb{Z}$ o in $\mathbb{Q}$*

Proposizione 5.3.6 (Radici razionali di un polinomio a coefficienti interi)
Sia $p(x) \in \mathbb{Z}[x]$ un polinomio a coefficienti interi tale che

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Sia $\frac{c}{d} \in \mathbb{Q}$ ridotta ai minimi termini (ovvero $\operatorname{mcd}(c,d) = 1$).
Allora se $\frac{c}{d}$ è una radice di p segue che $c \mid a_0$ e $d \mid a_n$.

Dimostrazione. Per definizione di radice di un polinomio

$$p\left(\frac{c}{d}\right) = a_0 + a_1\frac{c}{d} + \cdots + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + a_n\left(\frac{c}{d}\right)^n = 0.$$

Moltiplicando entrambi i membri per d^n otteniamo

$$\iff a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n = 0.$$

Se vale l'uguaglianza, allora i due membri saranno anche congrui modulo d:

$$a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n \equiv 0 \ \ (d).$$

Tutti i termini tranne l'ultimo contengono una potenza di d, dunque:

$$\iff a_n c^n \equiv 0 \ \ (d)$$

Dato che $\operatorname{mcd}(c,d) = 1$, allora c^n è invertibile modulo d)

$$\iff a_n \equiv 0 \ \ (d)$$
$$\iff d \mid a_n.$$

Consideriamo ora la congruenza modulo c:

$$a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n \equiv 0 \ (c)\,.$$

Per lo stesso ragionamento segue che:

$$\begin{aligned} &\iff a_0 d^n \equiv 0 \ (c) \\ &\iff a_0 \equiv 0 \ (c) \\ &\iff c \mid a_0. \end{aligned}$$

□

Teorema 5.3.7 (Lemma di Gauss)

Sia $p(x) \in \mathbb{Z}[x]$ un polinomio a coefficienti interi. Allora se p è riducibile in $\mathbb{Q}[x]$ segue che p è riducibile in $\mathbb{Z}[x]$.

Per il Lemma di Gauss dunque se vogliamo cercare la fattorizzazione di un polinomio in $\mathbb{Q}[x]$ ci basta cercare una fattorizzazione in $\mathbb{Z}[x]$ (cioè tra i polinomi a coefficienti interi). Viceversa, se non esiste una fattorizzazione in $\mathbb{Z}[x]$ allora il polinomio è irriducibile anche in $\mathbb{Q}[x]$.

Proposizione 5.3.8 (Criterio di Eisenstein)

Sia $f(x) \in \mathbb{Z}[x]$ tale che $f(x) = a_0 + \cdots + a_n x^n$. Allora se esiste un primo $p \in \mathbb{Z}$ tale che

- $a_0 \equiv a_1 \equiv \cdots \equiv a_{n-1} \ (p)$;
- $p \nmid a_n$;
- $p^2 \nmid a_0$

allora f è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Sia $f_p(x) \in \mathbb{Z}/(p)[x]$ il polinomio ottenuto considerando $f(x)$ nel campo $\mathbb{Z}/(p)$. Per le prime due ipotesi segue che

$$\begin{aligned} f_p(x) &= [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \cdots + [a_0]_p \\ &= [a_n]_p x^n \end{aligned}$$

con $[a_n]_p \neq 0$ per la seconda ipotesi.

Supponiamo per assurdo che $f(x)$ si fattorizzi in $\mathbb{Z}[x]$, ovvero che esistano $g(x), h(x) \in \mathbb{Z}[x]$ tali che

$$f(x) = g(x)h(x).$$

Notiamo che $a_0 = f(0) = g(0)h(0)$.

Consideriamo ore le rispettive proiezioni $g_p(x), h_p(x) \in \mathbb{Z}/(p)[x]$. Dato che $g(x) \mid f(x)$, $h(x) \mid f(x)$ segue che $g_p(x) \mid f_p(x)$ e $h_p(x) \mid f_p(x)$. Ma $f_p(x)$ è un monomio, quindi anche $g_p(x)$ e $h_p(x)$ devono essere monomi:

$$g_p(x) = kx^r, h_p(x) = hx^{n-r}$$

con $k, r \in \mathbb{Z}/(p)$, k, r entrambi diversi da 0.

Notiamo che $g_p(0) = h_p(0) = 0$, che in $\mathbb{Z}/(p)$ significa che $g(0) \equiv h(0) \equiv 0 \ (p)$, cioè $p \mid g(0)$, $p \mid h(0)$. Ma questo significa che $p^2 \mid g(0)h(0)$, ovvero $p^2 \mid a_0$, che è assurdo poiché abbiamo assunto che $p^2 \nmid a_0$.

Dunque segue che $f(x)$ non è fattorizzabile in $\mathbb{Z}[x]$, che è la tesi. □

Proposizione 5.3.9 (Criterio della sostituzione)

Sia $p(x) \in \mathbb{Z}[x]$ e sia $n \in \mathbb{Z}$. Allora $p(x)$ è riducibile in $\mathbb{Z}[x]$ se e solo se $p(x+n)$ è riducibile in $\mathbb{Z}[x]$.

5.3.4 *Polinomi ciclotomici*

Definizione 5.3.10 (Polinomio ciclotomico)
Sia $p \in \mathbb{Z}$ primo. Si dice polinomio ciclotomico il polinomio

$$f(x) = 1 + x + \cdots + x^{p-1}.$$

Proposizione 5.3.11
Sia $p \in \mathbb{Z}$ primo e sia $f(x) \in \mathbb{Z}[x]$ il polinomio ciclotomico di grado $p-1$. $f(x)$ non è fattorizzabile in $\mathbb{Z}[x]$.

Dimostrazione. Notiamo che $f(x)$ rappresenta una serie geometrica, dunque

$$f(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Per il criterio di sostituzione (5.3.9) vale che $f(x)$ è riducibile in $\mathbb{Z}[x]$ se e solo se $f(x+1)$ lo è. Dunque

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x+1-1} && \text{(per il teorema del Binomiale (3.5.4))} \\ &= \frac{1}{x}\left(x^p + \binom{p}{1}x^{n-1} + \cdots + \binom{p}{p-1}x + 1 - 1\right) \\ &= \frac{1}{x}\left(x^p + \binom{p}{1}x^{n-1} + \cdots + \binom{p}{p-1}x\right) \\ &= x^{p-1} + \binom{p}{1}x^{n-2} + \cdots + \binom{p}{p-1}. \end{aligned}$$

Applichiamo il criterio di Eisenstein col primo p:

- per la proposizione 3.5.8 segue che tutti i coefficienti tranne il coefficiente direttore sono congrui a 0 modulo p;
- dato che il coefficiente direttore è 1, segue che $p \nmid 1$;
- il termine noto è $\binom{p}{p-1} = p$, dunque $p^2 \nmid p$.

Per il criterio di Eisenstein (5.3.8) dunque il polinomio $f(x+1)$ non è fattorizzabile in $\mathbb{Z}[x]$, dunque per il criterio di sostituzione neanche $f(x)$ lo è. □