Matematica Discreta

Luca De Paulis

23 dicembre 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)	$a + 0 = 0 + a = a$	(0 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 $(\mathbb{K}, +, \cdot, 0, 1)$ formata da

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

per cui valgono i seguenti assiomi:

(ASSIOMI DI CAMPO) Per ogni $a, b, c \in \mathbb{K}$ vale che

(S1)	$(a + b) \in \mathbb{K}$	(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)	$\exists(-a) \in \mathbb{K}. \quad a + (-a) = 0$	(opposto per $+$)
(P1)	$(ab) \in \mathbb{K}$	(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)	$a \neq 0 \implies \exists a^{-1} \in \mathbb{K}. \quad aa^{-1} = 1$	(inverso per $\cdot$)

La definizione sopra è equivalente a dire che $\mathbb{K}$ 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 utile 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

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

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 1.2.1. 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

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

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

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

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 $r(\cos\vartheta + i\sin\vartheta)$, dove $r = \sqrt{a^2 + b^2} = |z|$ e $\vartheta = \arctan\frac{a}{b}$.

Definizione 1.2.11 **Esponenziale complesso.** $e^{i\vartheta} = \cos\vartheta + i\sin\vartheta$.

Sfruttando la definizione precedente possiamo scrivere ogni numero complesso nella forma $re^{i\vartheta}$ 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:

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

□

1.3 SUCCESSIONI PER RICORRENZA

Introduciamo ora il concetto di successine.

Definizione 1.3.1 **Successione.** Si dice successione a valori in un insieme A una funzione $(a_n) : \mathbb{N} \to A$.

Solitamente analizzeremo successioni a valori reali, ovvero $(a_n) : \mathbb{N} \to \mathbb{R}$. Inoltre usiamo equivalentemente le notazioni $(a_n)_k$ o a_k per riferirci alla funzione valutata nel punto $k \in \mathbb{N}$, ovvero al k-esimo elemento della successione.

Osserviamo che possiamo parlare di *somma di successioni* e di *prodotto di una successione per una costante*.

Definizione 1.3.2 **Somma di successioni e prodotto per una costante.** Sia $S_{\mathbb{R}}$ l'insieme delle successioni a valori reali. Allora si può definire una somma tra successioni $+ : S_{\mathbb{R}} \times S_{\mathbb{R}} \to S_{\mathbb{R}}$ tale che

$$(a_n) + (b_n) = (a_n + b_n)$$

e un prodotto per una costante $\cdot : \mathbb{R} \times S_{\mathbb{R}} \to S_{\mathbb{R}}$ tale che

$$k(a_n) = (ka_n).$$

Esempio 1.3.3. Sia $a_n = 3^n$ e $b_n = 2n + 1$. Allora $(c_n) = (a_n) + (b_n)$ è la successione definita dalla legge $c_n = 3^n + 2n + 1$, mentre $(d_n) = 3(b_n)$ è la successione definita da $d_n = 6n + 3$.

Queste operazioni rispettano le solite proprietà (associativa, commutativa, distributiva). In particolare vale quindi la seguente proposizione.

Proposizione 1.3.4 **L'insieme delle successioni è uno spazio vettoriale.** *L'insieme delle successioni a valori reali $S_{\mathbb{R}}$ insieme alle operazioni di somma e prodotto per costanti e alla successione identicamente nulla (0_n) è uno spazio vettoriale su $\mathbb{R}$.*

Definizione 1.3.5 **Ricorrenza lineare omogenea.** Si dice ricorrenza lineare omogenea di ordine k un'equazione della forma

$$a_{n+k} = r_{k-1}a_{n+k-1} + r_{k-2}a_{n+k-2} + \cdots + r_1 a_{n+1} + r_0 a_n. \tag{1}$$

Una soluzione della ricorrenza lineare 1 è una successione (s_n) tale che per ogni $n \in \mathbb{N}$ vale che $s_n, s_{n+1}, \ldots, s_{n+k}$ soddisfano la ricorrenza.

Proposizione 1.3.6 *Sia A l'insieme delle successioni che soddisfano la ricorrenza lineare omogenea*

$$s_{n+k} = r_{k-1}s_{n+k-1} + r_{k-2}s_{n+k-2} + \cdots + r_1 s_{n+1} + r_0 s_n.$$

Allora A è un sottospazio vettoriale di $S_{\mathbb{R}}$.

Dimostrazione. Dobbiamo dimostrare tre fatti:

(i) $(0_n) \in A$;

(ii) se $(a_n), (b_n) \in A$ allora $(c_n) = (a_n) + (b_n) \in A$;

(iii) se $h \in \mathbb{R}$, $(a_n) \in A$ allora $(d_n) = h(a_n) \in A$.

Sia $n \in \mathbb{N}$ qualsiasi.

(i) Verifichiamo che (0_n) sia soluzione. La ricorrenza da verificare è

$$0_{n+k} = r_{k-1}0_{n+k-1} + \cdots + r_1 0_{n+1} + r_0 0_n.$$

Ma dato che (0_n) è la successione identicamente nulla, allora questo equivale a dire $0 = 0r_{k-1} + \cdots + +0r_0 = 0$, che è verificata e quindi $(0_n) \in A$.

(ii) Verifichiamo che (c_n) sia soluzione.

$$\begin{aligned} c_{n+k} &= a_{n+k} + b_{n+k} \\ &= (r_{k-1}a_{n+k-1} + \cdots + r_0 a_n) + (r_{k-1}b_{n+k-1} + \cdots + r_0 b_n) \\ &= r_{k-1}(a_{n+k-1} + b_{n+k-1}) + \cdots + r_0(a_n + b_n) \\ &= r_{k-1}c_{n+k-1} + \cdots + r_0 c_0 \end{aligned}$$

dunque $(c_n) \in A$.

(iii) Verifichiamo che (d_n) sia soluzione.

$$\begin{aligned} d_{n+k} &= ha_{n+k} \\ &= h(r_{k-1}a_{n+k-1} + \cdots + r_0 a_n) \\ &= r_{k-1}(ha_{n+k-1}) + \cdots + r_0(ha_n) \\ &= r_{k-1}d_{n+k-1} + \cdots + r_0 d_0 \end{aligned}$$

dunque $(d_n) \in A$. □

La proposizione precedente ci permette di trovare una soluzione generale ad una ricorrenza lineare omogenea.

Esempio 1.3.7. Siano $a_n = 3^n$ e $b_n = (-1)^n$ due soluzioni di una ricorrenza lineare omogenea. Allora per la proposizione precedente anche $k_1 a_n = k_1 3^n$ e $k_2 b_n = k_2(-1)^n$ saranno soluzioni (per ogni $k_1, k_2 \in \mathbb{R}$), e di conseguenza anche $k_1 a_n + k_2 b_n = k_1 3^n + k_2(-1)^n$.

Cerchiamo di risolvere una ricorrenza lineare omogenea.

Esempio 1.3.8. Sia $a_{n+2} = 2a_{n+1} + 3a_n$ una ricorrenza lineare omogenea di ordine 2. Trovare la soluzione generale. Inoltre trovare una soluzione particolare che soddisfi le condizioni iniziali $a_0 = 0$ e $a_1 = 1$.

Soluzione Proviamo a risolvere la ricorrenza con una soluzione esponenziale della forma (λ^n) al variare di $n \in \mathbb{N}$. Sostituendo otteniamo

$$\begin{aligned} & \lambda^{n+2} = 2\lambda^{n+1} + 3\lambda^n \\ \iff & \lambda^2 = 2\lambda + 3 \\ \iff & \lambda^2 - 2\lambda - 3 = 0. \end{aligned}$$

Dunque se (λ^n) è una soluzione allora λ deve essere radice di quel polinomio di secondo grado, detto polinomio caratteristico della ricorrenza. Risolvendolo segue che $\lambda_1 = 3$ e $\lambda_2 = -1$ sono soluzioni, dunque le successioni (3^n) e $((-1)^n)$ sono soluzioni della ricorrenza.

La soluzione generale della ricorrenza è dunque una successione della forma $(a_n) = k_1(3^n) + k_2((-1)^n)$ al variare di $k_1, k_2 \in \mathbb{R}$.

Imponiamo ora che $a_0 = 0$ e $a_1 = 1$.

$$\begin{cases} 3^0 k_1 + (-1)^0 k_2 = 0 \\ 3^1 k_1 + (-1)^1 k_2 = 1 \end{cases} \iff \begin{cases} k_1 + k_2 = 0 \\ 3k_1 - k_2 = 1 \end{cases}$$

da cui segue $k_1 = \frac{1}{4}$, $k_2 = -\frac{1}{4}$. La successione che soddisfa le condizioni iniziali è dunque $a_n = \frac{1}{4}(3)^n - \frac{1}{4}(-1)^n$. ⌟

La strategia del sostituire il termine generico a_k della successione con λ^k dà luogo alla seguente definizione.

Definizione 1.3.9 **Polinomio caratteristico di una ricorrenza.** Sia $a_{n+k} = r_{k-1}a_{n+k-1} + \cdots + r_0 a_n$ una ricorrenza lineare omogenea di ordine k. Allora si dice polinomio caratteristico associato alla ricorrenza il polinomio

$$p(\lambda) = \lambda^k - r_{k-1}\lambda^{k-1} - \cdots - r_0.$$

Il polinomio caratteristico si ottiene sostituendo alla ricorrenza lineare la successione (λ^n), esattamente come abbiamo fatto nell'esempio precedente.

Esempio 1.3.10. Consideriamo la successione di Fibonacci $f_{n+2} = f_{n+1} + f_n$ con $f_0 = 0$, $f_1 = 1$. Trovare una successione che risolva la ricorrenza e soddisfi i casi base.

Soluzione Il polinomio caratteristico di questa ricorrenza è

$$p(\lambda) = \lambda^2 - \lambda - 1$$

che ha come radici i numeri $\varphi = \frac{1}{2}(1 + \sqrt{5})$ e $\bar{\varphi} = \frac{1}{2}(1 - \sqrt{5})$.

La soluzione generale della ricorrenza è dunque una successione della forma $(f_n) = k_1(\varphi^n) + k_2(\bar{\varphi}^n)$ al variare di $k_1, k_2 \in \mathbb{R}$.

Imponiamo ora che $f_0 = 0$ e $f_1 = 1$.

$$\begin{cases} \varphi^0 k_1 + \bar{\varphi}^0 k_2 = 0 \\ \varphi^1 k_1 + \bar{\varphi}^1 k_2 = 1 \end{cases} \iff \begin{cases} k_1 + k_2 = 0 \\ \varphi k_1 + \bar{\varphi} k_2 = 1 \end{cases}$$

da cui segue $k_1 = \frac{1}{\sqrt{5}}$, $k_2 = -\frac{1}{\sqrt{5}}$. La successione che soddisfa le condizioni iniziali è dunque

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

⌟

Nel caso che una radice del polinomio caratteristico abbia una molteplicità maggiore di 1 essa darà luogo a più di una soluzione della ricorrenza, come ci dice la seguente proposizione.

Proposizione 1.3.11 *Sia $p(\lambda)$ il polinomio caratteristico di una ricorrenza lineare omogenea e sia λ_0 una radice di molteplicità h con $h \geqslant 2$.*

Allora $(\lambda_0^n), (n\lambda_0^n), \ldots, (n^{h-1}\lambda_0^n)$ sono tutte soluzioni della ricorrenza lineare omogenea.

Osservazione 1.3.1. Ricordiamo che una radice di un polinomio ha molteplicità h se h è il massimo intero per cui $(x-\lambda_0)^h$ compare nella fattorizzazione di $p(\lambda)$.

Ad esempio 1 è una radice di molteplicità 2 per il polinomio $p(x) = x^3 - 2x^2 + x$, in quanto

$$x^3 - 2x^2 + x = x(x^2 - 2x + 1) = x(x-1)^2,$$

dunque $(x-1)$ divide il polinomio $p(x)$ al massimo due volte.

Esempio 1.3.12. Sia $p(\lambda) = (\lambda-3)^3(\lambda+1)^2(\lambda-\sqrt{2})^4$. Allora le seguenti sono tutte soluzioni indipendenti della ricorrenza lineare omogenea associata a $p(\lambda)$:

(i) (3^n);
(ii) $(n3^n)$;
(iii) $(n^2 3^n)$;
(iv) $((-1)^n)$;
(v) $(n(-1)^n)$;
(vi) $(\sqrt{2}^n)$;
(vii) $(n\sqrt{2}^n)$;
(viii) $(n^2\sqrt{2}^n)$;
(ix) $(n^3\sqrt{2}^n)$.

La soluzione generale sarà dunque della forma

$$(a_n) = k_1(3^n) + k_2(n3^n) + k_3(n^2 3^n) + k_4(n(-1)^n) + k_5(n(-1)^n) + \\ + k_6(\sqrt{2}^n) + k_7(n\sqrt{2}^n) + k_8(n^2\sqrt{2}^n) + k_9(n^3\sqrt{2}^n)$$

al variare di $k_1, \ldots, k_9 \in \mathbb{R}$.

2 | DIVISORI E GCD

2.1 DIVISORI DI UN NUMERO

Introduciamo ora formalmente i concetti intuitivi di multiplo e divisore.

Definizione 2.1.1 **Divisore.** Siano $a, b \in \mathbb{Z}$. Si dice che a divide b se esiste $k \in \mathbb{Z}$ tale che $ak = b$. In tal caso 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 esiste $k \in \mathbb{Z}$ tale che $b = ak$.

Osservazione 2.1.1. Ovviamente definizione di multiplo è speculare a quella di divisore: se a è divisore di b allora b è multiplo di a.

La relazione di divisibilità si comporta bene rispetto alla somma e al prodotto.

Proposizione 2.1.3 *Siano $a, b, n \in \mathbb{Z}$ tali che $n \mid a$ e $n \mid b$. Allora valgono le seguenti affermazioni:*

1. $n \mid a + b$
2. $n \mid a - b$
3. *per ogni $x \in \mathbb{Z}$ vale che* $n \mid ax$

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 $\mathrm{mcd}(a, b)$ il più grande intero positivo tale che

$$\mathrm{mcd}(a, b) \mid a \qquad \text{e} \qquad \mathrm{mcd}(a, b) \mid b.$$

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 $d = \mathrm{mcm}(a, b)$ tale che d è il più piccolo multiplo positivo sia di a che di b.

Definizione 2.1.6 **Coprimo.** Siano $a, b \in \mathbb{Z}$. Se $\mathrm{mcd}(a, b) = 1$ allora a e b si dicono coprimi.

Osservazione 2.1.2. Siano $a, b \in \mathbb{Z}$. Allora valgono le seguenti proprietà per $\mathrm{mcd}(a, b)$:

1. $\mathrm{mcd}(a, b) = \mathrm{mcd}(\pm a, \pm b)$
2. $\mathrm{mcd}(a, 1) = \mathrm{mcd}(1, a) = 1$

3. $\mathrm{mcd}(a, 0) = \mathrm{mcd}(0, a) = 0$
4. $\mathrm{mcd}(0, 0)$ non esiste.

Il prossimo teorema ci fornisce la strategia della *divisione euclidea tra interi*.

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*

$$a = bq + r, \qquad 0 \leqslant r < |b| \tag{2}$$

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*

$$\mathrm{mcm}(a, b) \mid c \iff a \mid c \wedge b \mid c \tag{3}$$

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 $0 \leqslant r < \mathrm{mcm}(a, b)$.
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 $0 \leqslant r < \mathrm{mcm}(a, b)$, dunque necessariamente $r = 0$, cioè $c = \mathrm{mcm}(a, b)q$ e quindi $\mathrm{mcm}(a, b) \mid c$. □

2.2 ALGORITMO DI EUCLIDE

Il metodo più efficiente per calcolare il massimo comun divisore tra due numeri è dato dall'algoritmo di Euclide, che si basa sul seguente teorema.

Teorema 2.2.1 *Siano $a, b \in \mathbb{Z}$. Allora*

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b - a) = \mathrm{mcd}(a - b, b). \tag{4}$$

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, cioè

$$\mathbb{D}_{x,y} = \{\, d : d \mid x \wedge d \mid y \,\}.$$

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 $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b - a)$, che è la tesi. □

Dunque per calcolare il massimo comun divisore si può sfruttare il seguente algoritmo, detto **algoritmo di Euclide**, che si basa sul Teorema 2.2.1:

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

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

Possiamo velocizzare il procedimento usando i resti della divisione invece che la sottrazione:

4. Se $a \neq 0$ e $b \neq 0$, allora
   - se $a \leqslant b$ segue che $\mathrm{mcd}(a, b) = \mathrm{mcd}(a \bmod b, b)$;
   - se $a > b$ segue che $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b \bmod a)$

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

I passaggi dell'algoritmo di Euclide ci consentono inoltre di calcolare un'identità molto importante, chiamata **identità di Bézout**.

Teorema 2.2.2

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

$$ax + by = \mathrm{mcd}(a, b). \tag{5}$$

Dimostrazione. Siano $r_0 = a$, $r_1 = b$. Definisco la successione $(()r_n)$ come la sequenza dei resti della divisione dati dall'algoritmo di Euclide per l'gcd:

$$\begin{aligned}
\mathrm{mcd}(a, b) &= \mathrm{mcd}(r_0, r_1) && \text{sia } r_2 = r_0 \bmod r_1 : \\
&= \mathrm{mcd}(r_1, r_2) && \text{sia } r_3 = r_1 \bmod r_2 : \\
&= \dots \\
&= \mathrm{mcd}(r_n, r_{n+1}) && \text{sia } r_{n+2} = r_n \bmod r_{n+1} : \\
&= \dots
\end{aligned}$$

Questo processo ha termine quando un resto r_{m+1} è uguale a 0: in quel caso $\mathrm{mcd}(r_m, r_{m+1}) = \mathrm{mcd}(r_m, 0) = r_m = \mathrm{mcd}(a, b)$.

Dimostriamo che per ogni n possiamo scrivere r_n come $ax_n + by_n$ per qualche $x_n, y_n \in \mathbb{Z}$.

CASO BASE Per r_0 e r_1 è banale:

$$r_0 = 1 \cdot a + 0 \cdot b, \qquad r_1 = 0 \cdot a + 1 \cdot b.$$

PASSO INDUTTIVO Supponiamo di saper scrivere r_n e r_{n-1} come combinazione di a e b e dimostriamo che possiamo farlo anche per r_{n+2}.
Per ipotesi induttiva esistono $x_n, y_n, x_{n+1}, y_{n+1} \in \mathbb{Z}$ tali che

$$r_n = ax_n + by_n, \qquad r_{n+1} = ax_{n+1} + by_{n+1}.$$

Per definizione sappiamo che

$$r_{n+2} = r_n \bmod r_{n+1},$$

ovvero per definizione di resto

$$r_{n+2} = r_n - q_{n+1} r_{n+1}$$

per qualche $q_{n+1} \in \mathbb{Z}$. Sostituendo otteniamo

$$\begin{aligned} r_{n+2} &= r_n - q_{n+1} r_{n+1} \\ &= ax_n + by_n - q_{n+1}(ax_{n+1} + by_{n+1}) \\ &= a(x_n - q_{n+1}x_{n+1}) + b(y_n - q_{n+1}y_{n+1}). \end{aligned}$$

Dunque $x_{n+2} = x_n - q_{n+1}x_{n+1}$ e $y_{n+2} = y_n - q_{n+1}y_{n+1}$, cioè possiamo esprimere r_{n+2} come combinazione lineare di a, b.

Dato che per induzione questo risultato vale per tutti gli $n \in \mathbb{N}$, varrà anche per m, ovvero esistono $x, y \in \mathbb{Z}$ tali che $r_m = ax + by$. Ma $r_m = \mathrm{mcd}(a, b)$, dunque la tesi. □

Esempio 2.2.3. Cerchiamo il massimo comun divisore tra 252 e 198 e i coefficienti del Teorema di Bezout con l'Algoritmo di Euclide.

I passi dell'algoritmo ci dicono di sottrarre dal più grande dei due numeri l'altro ripetutamente: il modo più veloce di far questa cosa è sottrarre un multiplo del numero più piccolo in modo da ottenere il più piccolo resto positivo. Scriviamo esattamente il multiplo usato a destra dei passaggi dell'algoritmo in quanto sarà utile più tardi.

$$\begin{aligned} &\mathrm{mcd}(252, 198) && 54 = 252 - \boxed{1} \cdot 198 \\ =\ &\mathrm{mcd}(54, 198) && 36 = 198 - \boxed{3} \cdot 54 \\ =\ &\mathrm{mcd}(54, 36) && 18 = \ 54 - \boxed{1} \cdot 36 \\ =\ &\mathrm{mcd}(18, 36) && 0 = \ 36 - \boxed{2} \cdot 18 \\ =\ &\mathrm{mcd}(18, 0) \\ =\ &18. \end{aligned}$$

Per il Teorema di Bezout dovranno quindi esistere $x_0, y_0 \in \mathbb{Z}$ tali che

$$252x_0 + 198y_0 = 18.$$

Per trovarli seguiamo la catena di equazioni scritta sopra, ricavando i coefficienti della combinazione lineare per ognuno dei numeri che compare nello svolgimento dell'algoritmo.

Innanzitutto ovviamente vale che

$$252 = 252 \cdot \boxed{1} + 198 \cdot \boxed{0}, \quad 198 = 252 \cdot \boxed{0} + 198 \cdot \boxed{1}.$$

La prima uguaglianza nell'algoritmo di Euclide ci dice inoltre che

$$54 = 252 \cdot \boxed{1} + 198 \cdot \boxed{-1}.$$

Per ricavare le decomposizioni successive sfruttiamo le precedenti:

$$\begin{aligned}
36 &= 198 - \boxed{3} \cdot 54 \\
&= (252 \cdot \boxed{0} + 198 \cdot \boxed{1}) - \boxed{3} \cdot (252 \cdot \boxed{1} + 198 \cdot \boxed{-1}) \\
&= 252 \cdot \boxed{0} + 198 \cdot \boxed{1} + 252 \cdot \boxed{-3} + 198 \cdot \boxed{3} \\
&= 252 \cdot \boxed{-3} + 198 \cdot \boxed{4}. \\
18 &= 54 - \boxed{1} \cdot 36 \\
&= (252 \cdot \boxed{1} + 198 \cdot \boxed{-1}) - \boxed{1} \cdot (252 \cdot \boxed{-3} + 198 \cdot \boxed{4}) \\
&= 252 \cdot \boxed{1} + 198 \cdot \boxed{-1} + 252 \cdot \boxed{3} + 198 \cdot \boxed{-4} \\
&= 252 \cdot \boxed{4} + 198 \cdot \boxed{-5}.
\end{aligned}$$

Abbiamo quindi trovato i coefficienti del teorema di Bezout: scegliendo $x_0 = 4$, $y_0 = -5$ riusciamo a scrivere 18 come combinazione lineare a coefficienti interi di 252 e 198.

Osserviamo che ogni volta svolgiamo i calcoli solo sui *coefficienti* di 252 e 198: possiamo abbreviare il procedimento usando una semplice tabella con questa forma:

	252	198
252	1	0
198	0	1
54	1	-1
36	-3	4
18	4	-5

Ogni riga ci dice i coefficienti della combinazione lineare, esattamente come prima. Le prime due righe sono quindi immediate, mentre le successive possono essere trovate semplicemente con questo procedimento:

- cerchiamo l'equazione dell'algoritmo di Euclide che definisce il numero che stiamo considerando (ad esempio la quarta riga ha come numero 36, definito da $36 = 198 - \boxed{3} \cdot 54$);
- ricaviamo il coefficiente della prima colonna prendendo i coefficienti della prima colonna dei numeri che compaiono nell'equazione (in questo caso 198 e 54) e sottraendoli come ci dice l'equazione (otteniamo quindi $0 - \boxed{3} \cdot 1 = -3$, che è il coefficiente della prima colonna della quarta riga);
- ricaviamo il coefficiente della seconda colonna esattamente allo stesso modo.

2.2.1 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 2.2.4 *Siano $a, b, n \in \mathbb{Z}$. Allora*

$$n \mid ab \land \operatorname{mcd}(a, n) = 1 \implies n \mid b. \tag{6}$$

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 (2.2.2) esistono $x, y \in \mathbb{Z}$ tali che

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

Moltiplicando per b otteniamo

$$abx + nby = b$$

Ma $n \mid abx$ (poiché $n \mid ab$) e $n \mid nby$, dunque n divide la loro somma, ovvero

$$n \mid abx + nby = b(ax + ny) = b$$

da cui la tesi. □

Cerchiamo ora di studiare come si relaziona il massimo comune divisore con gli altri divisori di due numeri dati. La prima proposizione ci dice che un divisore comune è sempre minore o uguale del mcd, mentre la seconda ci dice che un divisore comune è sempre *un divisore* del mcd.

Proposizione 2.2.5 *Siano* $a, b, t \in \mathbb{Z}$ *tali che* $t \mid a$, $t \mid b$. *Allora* $t \leqslant \mathrm{mcd}(a, b)$.

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 $t \leqslant \mathrm{mcd}(a, b)$. □

Proposizione 2.2.6 *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 (2.2.2) 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 $t \mid \mathrm{mcd}(a, b)$. □

Possiamo anche dare una condizione necessaria e sufficiente per cui un numero t divide il massimo comun divisore di altri due numeri.

Proposizione 2.2.7 *Siano* $a, b, t \in \mathbb{Z}$. *Allora*

$$t \mid \mathrm{mcd}(a, b) \iff (\forall x, y \in \mathbb{Z}. \quad t \mid ax + by). \tag{7}$$

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 $\bar{x}, \bar{y}$ 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 2.2.8 *Siano* $a, b, n \in \mathbb{Z}$. *Allora*

$$\mathrm{mcd}(an, bn) = n \,\mathrm{mcd}(a, b). \tag{8}$$

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 2.2.7 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 (2.2.2)

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

Corollario 2.2.9 *Siano $a, b \in \mathbb{Z}$ e sia $d = \mathrm{mcd}(a, b)$. Allora $\mathrm{mcd}(a/d, b/d) = 1$.*

Intuizione Se dividiamo due numeri per il loro gcd 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 2.2.8

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

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

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

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

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

che è la tesi. $\square$

2.3 NUMERI PRIMI

Definizione 2.3.1 **Numero primo.** Un numero $p \in \mathbb{Z}$ si dice primo se se gli unici interi che dividono p sono ± 1 e $\pm p$.

Una caratterizzazione equivalente dei numeri primi è quella data dalla seguente proposizione.

Proposizione 2.3.2 *Se p è primo e $p \mid ab$, allora $p \mid a$ oppure $p \mid b$.*

Dimostrazione. Supponiamo che p non divida a. Dato che p è primo, $\mathrm{mcd}(a, p) = 1$ oppure p. Tuttavia se $\mathrm{mcd}(a, p) = p$ allora $p \mid a$, che va contro l'ipotesi, dunque $\mathrm{mcd}(a, p) = 1$. Per la Proposizione 2.2.4 allora $p \mid b$, che è la tesi. $\square$

Proposizione 2.3.3 *Siano $a, b \in \mathbb{Z}, c \in \mathbb{Z}$ tali che $\mathrm{mcd}(a, b) = 1$. Allora*

$$a \mid c \ \wedge \ b \mid c \iff ab \mid c. \tag{9}$$

Dimostrazione. Per il Teorema di Bezout esistono $x, y \in \mathbb{Z}$ tali che $\mathrm{mcd}(a, b) = 1 = ax + by$, 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

$$ab \mid nax + nby = n(ax + by) = n$$

da cui la tesi. □

Proposizione 2.3.4 *Siano $a, b, c \in \mathbb{Z}$. Allora*

$$\mathrm{mcd}(ab)c = 1 \iff \mathrm{mcd}(a, c) = \mathrm{mcd}(b, c) = 1. \tag{10}$$

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 2.3.5 *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 2.3.4 ma estesa a n numeri (per induzione). ⌟

Proposizione 2.3.6 *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*

$$a_1 a_2 \ldots a_n = \left(\prod_{i=1}^{n} a_i\right) \mid c. \tag{11}$$

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 2.3.5 a_n è coprimo con $\prod_{i=1}^{n-1} a_i$, dunque per la Proposizione 2.3.3 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 $n \in \mathrm{N}$. □

2.3.1 Divisori primi

La prossima proposizion serve a dimostrare che ogni numero può essere scomposto in un prodotto di fattori primi, ognuno di essi elevato ad una certa potenza.

Proposizione 2.3.7 **Esistenza della scomposizione in primi.** *Sia $n \in \mathbb{Z}, n > 1$. Allora n può 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 ogni $m < n$ (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 $n \geqslant 2$. □

Teorema 2.3.8 **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 $1 \leqslant i \leqslant k$. Allora $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.*

Dimostrazione. Per la Proposizione 2.3.7 sappiamo che esistono i primi $p_1, \ldots, p_n$. Per la Corollario 2.3.5 segue che

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

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

Dunque $n = m \cdot p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ per qualche $m \in \mathbb{Z}$. Supponiamo per assurdo che $m \neq 1$. Allora per la Proposizione 2.3.7 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 $p_1, \ldots, p_k$.

Sia p_i uno dei primi che divide m. Allora dato che $m \cdot p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} = n$ deve valere che $m \cdot p_i^{e_i}$ divide n, ma siccome $p_i \mid m$ dovrà valere in particolare

$$p_i \cdot p_i^{e_i} = p_i^{e_i+1} \mid n$$

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

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

come volevasi dimostrare. □

Le prossime proposizioni ci danno alcuni legami tra i divisori primi e il massimo comun divisore/minimo comune multiplo.

Proposizione 2.3.9 *Siano* $a, b, k \in \mathbb{Z}$, $p \in \mathbb{Z}$ *primo. Allora*

$$p^k \mid \mathrm{mcd}(a,b) \iff p^k \mid a \wedge p^k \mid b \tag{12}$$

$$p^k \mid \mathrm{mcm}(a,b) \iff p^k \mid a \vee p^k \mid b. \tag{13}$$

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

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 $a \mid \mathrm{mcm}(a,b)$ e $b \mid \mathrm{mcm}(a,b)$. Dato che $\mathrm{mcd}(a,b) = 1$ per la Proposizione 2.3.3 segue che $ab \mid \mathrm{mcm}(a,b)$, cioè $|ab| \leqslant \mathrm{mcm}(a,b)$. Ma ab è un multiplo di a e di b, quindi dovrà valere che $|ab| \geqslant \mathrm{mcm}(a,b)$ in quanto $\mathrm{mcm}(a,b)$ è il minimo multiplo comune ad a e b. Da cio' segue che $\mathrm{mcm}(a,b) = |ab|$, cioè la tesi. □

Proposizione 2.3.11 *Siano* $a, x, y \in \mathbb{Z}$. *Allora*

$$\mathrm{mcd}(a,x) = 1 \implies \mathrm{mcd}(a,xy) = \mathrm{mcd}(a,y). \tag{14}$$

Intuizione Se stiamo calcolando $\mathrm{mcd}(a,b)$ 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 $\mathrm{mcd}(a,x) = 1$, allora se un primo p divide a sicuramente p non divide x. Per la Proposizione 2.3.9 allora vale

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

ma $p^k \nmid x$ dunque per la 2.2.4

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

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

Proposizione 2.3.12 *Siano* $a, x, y \in \mathbb{Z}$. *Allora*

$$\mathrm{mcd}(a, \mathrm{mcm}(x)y) = \mathrm{mcm}(\mathrm{mcd}(a,x))\mathrm{mcd}(a,y). \tag{15}$$

Dimostrazione. Per la Proposizione 2.3.9 allora vale

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

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

Proposizione 2.3.13 *Siano $a, x, y \in \mathbb{Z}$. Allora*

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

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'gcd in due e moltiplicare i due risultati. ⌟

Dimostrazione. Dato che $\mcd(x)y = 1$ allora per la proposizione 2.3.10 vale che $\mcm(x)y = |xy|$. Dunque $\mcd(a, xy) = \mcd(a, |xy|) = \mcd(a, \mcm(x)y) = \mcm(\mcd(a, x))\mcd(a, y)$ per la Proposizione 2.3.12.

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

Dunque per la Proposizione 2.3.10 segue che

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

che è la tesi. □

Proposizione 2.3.14 *Siano $a, b, c \in \mathbb{Z}$. Allora*

$$a \mid c \wedge b \mid c \iff \frac{ab}{\mcd(a, b)} \mid c. \tag{17}$$

Dimostrazione. Dimostriamo l'implicazione in entrambi i versi.

($\implies$) Supponiamo che $a \mid c$ e $b \mid c$. Sia $d = \mcd(a, b)$. 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 2.2.9 sappiamo che $\mcd(\frac{a}{d}, \frac{b}{d}) = 1$, dunque per la 2.3.3 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 2.3.15 *Siano $a, b \in \mathbb{Z}$. Allora*

$$\mcd(a, b)\,\mcm(a, b) = |ab|. \tag{18}$$

Dimostrazione. Sia $c \in \mathbb{Z}$ tale che $a \mid c$, $b \mid c$. Allora per la Proposizione 2.3.14 segue che $\frac{ab}{\mcd(a,b)} \mid c$. Inoltre per la Proposizione 2.1.8 segue che $\mcm(a, b) \mid c$. Dunque i due numeri $\frac{ab}{\mcd(a,b)}$ e $\mcm(a, b)$ hanno gli stessi divisori, dunque devono essere uguali a meno del segno, da cui segue

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

□

2.4 EQUAZIONI DIOFANTEE

In questa sezione studieremo un tipo particolare di equazioni lineari, dette equazioni diofantee.

Definizione 2.4.1 **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.

La prossima proposizione ci dà una semplice condizione necessaria e sufficiente per la risolubilità delle diofantee.

Teorema 2.4.2 **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* $\mathrm{mcd}(a, b) \mid c$.

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

- Supponiamo che $c = k\,\mathrm{mcd}(a, b)$ per qualche $k \in \mathbb{Z}$. Allora per il teorema di Bezout 2.2.2 esistono $x', y' \in \mathbb{Z}$ tali che $ax' + by' = \mathrm{mcd}(a, b)$. Moltiplicando entrambi i membri per k otteniamo

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

  dunque $x = kx'$ e $y = ky'$ risolvono l'equazione diofantea.
- Supponiamo ora che c non sia un multiplo di $\mathrm{mcd}(a, b)$ e supponiamo per assurdo che l'equazione abbia soluzione, cioè che esistano $x, y \in \mathbb{Z}$ tali che $ax + by = c$. Sia $d = \mathrm{mcd}(a, b)$.
  Per definizione di $\mathrm{mcd}(a, b)$ 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 $d = \mathrm{mcd}(a, b) \mid c$, che va contro le ipotesi.
  Dunque l'equazione diofantea non ha soluzione, cioè la tesi. □

Risolvere una diofantea

Avendo dimostrato che una particolare equazione diofantea ha soluzione, per trovare tale soluzione si sfruttano i seguenti teoremi: si trovano prima le soluzioni della diofantea omogenea associata e una soluzione particolare della diofantea non omogenea e le si combinano insieme.

Teorema 2.4.3 **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 $\mathrm{mcd}(a, -b) = \mathrm{mcd}(a, b) = 1$. Dunque per il teorema 2.2.4 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 2.4.4 **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* $a' = \frac{a}{\mathrm{mcd}(a,b)}$ *e* $b' = \frac{b'}{\mathrm{mcd}(a,b)}$.

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

Ma per il teorema 2.2.9 $\mcd(a')b' = 1$, dunque per il teorema 2.4.3 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 2.4.5 **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. □

Esempio 2.4.6. Proviamo a risolvere l'equazione diofantea $1020x + 351y = 21$.

La prima cosa da fare è verificare se l'equazione ha soluzione tramite il Teorema 2.4.2: dobbiamo quindi verificare che $\mcd(1020, 351)$ divida 21.

Per calcolare il massimo comun divisore dei coefficienti sfruttiamo l'algoritmo di Euclide e annotiamo accanto ai vari passi le sottrazioni effettuate per svolgere i passaggi: questo servirà più avanti per calcolare i coefficienti dell'identità di Bezout.

$$\begin{aligned} &\mcd(1020, 351) && 318 = 1020 - \boxed{2} \cdot 351 \\ = \ &\mcd(318, 351) && 33 = 351 - \boxed{1} \cdot 318 \\ = \ &\mcd(318, 33) && 21 = 318 - \boxed{9} \cdot 33 \\ = \ &\mcd(21, 33) && 12 = 33 - \boxed{1} \cdot 21 \\ = \ &\mcd(21, 12) && 9 = 21 - \boxed{1} \cdot 12 \\ = \ &\mcd(9, 12) && 3 = 12 - \boxed{1} \cdot 3 \\ = \ &\mcd(9, 3) && 0 = 9 - \boxed{3} \cdot 3 \\ = \ &\mcd(3, 0) \\ = \ &3. \end{aligned}$$

Siccome 3 divide 21 l'equazione ha soluzione.

Troviamo innanzitutto la soluzione della diofantea omogenea associata

$$1020x + 351y = 0.$$

Dato che i coefficienti non sono coprimi (abbiamo visto che il loro massimo comun divisore è 3) possiamo ricondurci all'equazione equivalente

$$\frac{1020}{3}x + \frac{351}{3}y = 0 \iff 340x + 117y = 0.$$

I coefficienti di quest'ultima equazione sono coprimi, dunque per il Teorema 2.4.3 le sue soluzioni sono tutte e sole della forma

$$x = -117k, \quad y = 340k$$

al variare di $k \in \mathbb{Z}$.

Dobbiamo trovare ora una soluzione particolare della diofantea non omogenea. Per far ciò sfruttiamo l'identità di Bezout, ovvero troviamo $x_0, y_0 \in \mathbb{Z}$ tali che

$$1020x_0 + 351y_0 = 3.$$

A quel punto moltiplicando tutto per $21/3 = 7$ otteniamo

$$1020 \cdot (7x_0) + 351 \cdot (7y_0) = 21,$$

da cui la soluzione particolare cercata è $\bar{x} = 7x_0$, $\bar{y} = 7y_0$.

Per trovare x_0 e y_0 usiamo i coefficienti trovati durante l'esecuzione dell'algoritmo di Euclide costruendo una tabella con due colonne e tante righe quanti sono i numeri trovati durante l'algoritmo: ogni riga contiene i coefficienti per cui devo moltiplicare 1020 e 351 per ottenere il numero che identifica la riga.

	1020	351
1020	1	0
351	0	1
318	1	−2
33	−1	3
21	10	−29
12	−11	32
9	21	−61
3	−32	93

Le prime due righe della tabella si ottengono facilmente: infatti è ovvio che

$$1020 = \boxed{1} \cdot 1020 + \boxed{0} \cdot 351, \quad 351 = \boxed{0} \cdot 1020 + \boxed{1} \cdot 351.$$

Per ottenere le righe seguenti usiamo le uguaglianze calcolate durante l'algoritmo di Euclide: ad esempio siccome $318 = 1020 - 2 \cdot 351$ per calcolare i coefficiente sulla prima colonna prendiamo il coefficiente della prima colonna della riga di 1020 (cioè 1) e gli sottraiamo 2 volte il coefficiente della prima colonna della riga di 351; stesso procedimento per la seconda colonna e per le righe successive.

I coefficienti dell'ultima riga ci dicono che

$$3 = 1020 \cdot (-32) + 351 \cdot 93,$$

come è facilmente verificabile con una calcolatrice. Questi due coefficienti sono quindi x_0 e y_0 dell'identità di Bezout, da cui per calcolare la soluzione particolare è sufficiente moltiplicarli per 7, ovvero

$$\bar{x} = -32 \cdot 7 = -224, \quad \bar{y} = 93 \cdot 7 = 651.$$

Concludendo, per il Teorema 2.4.5 le soluzioni di questa equazione diofantea non omogenea sono tutte e sole della forma

$$(x, y) = (-224 - 117k, 651 + 340k).$$

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:*

$$\begin{aligned} &\textit{Riflessiva:} && a \equiv a \pmod{m} && (19)\\ &\textit{Simmetrica:} && a \equiv b \pmod{m} \implies b \equiv a \pmod{m} && (20)\\ &\textit{Transitiva:} && a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m} && (21) \end{aligned}$$

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

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

Teorema 3.1.3 **Relazione tra congruenza e resto della divisione euclidea.** *Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora*

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m. \tag{22}$$

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 $a \equiv b \pmod{m}$ 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 $0 \leqslant r < m$. 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.

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

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

cioè $a \equiv b \pmod{m}$. □

Proposizione 3.1.4 *Siano* $a, b, c, d, m \in \mathbb{Z}$, $m > 0$. *Allora valgono le seguenti*

$$a \equiv b \ (m) \land c \equiv d \ (m) \implies a + c \equiv b + d \ (m) \tag{23}$$
$$a \equiv b \ (m) \land c \equiv d \ (m) \implies a - c \equiv b - d \ (m) \tag{24}$$
$$a \equiv b \ (m) \land c \equiv d \ (m) \implies ac \equiv bd \ (m) \tag{25}$$

Dimostrazione.

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

$$\begin{aligned} bd &= (a - km)(c - hm) \\ &= ac - ahm - ckm + khm \\ &= ac - (ah + ck - kh)m \end{aligned}$$

che è equivalente a

$$\begin{aligned} &ac - bd = (ah + ck - kh)m \\ \iff\ &ac \equiv bd \ (m). \end{aligned}$$

□

3.2 EQUAZIONI CON CONGRUENZE LINEARI

Vogliamo ora risolvere congruenze lineari, ovvero della forma $ax \equiv b \ (m)$, dove $a, c, m \in \mathbb{Z}$ e $m > 0$. La prima proposizione interessante è che ogni congruenza può essere trasformata in una diofantea equivalente e viceversa.

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. Tuttavia per ottenere un risultato più velocemente è necessario sviluppare degli strumenti che ci permettano di risolvere direttamente le congruenze lineari.

Figura 1: Tabella dei prodotti mod 5

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Figura 2: Tabella dei prodotti mod 6

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Definizione 3.2.2 **Invertibilità e inverso.** Siano $a \in \mathbb{Z}$; allora si dice che a è invertibile modulo m se esiste un numero $k \in \mathbb{Z}$ tale che

$$ak \equiv 1 \pmod{m}.$$

In particolare tra tutti gli interi che soddisfano la relazione precedente, il numero k_0 tale che $0 \leqslant k_0 < m$ 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.

Come possiamo notare dalle tabelle in Figura 2, non sempre i numeri diversi da 0 ammettono inverso modulo m: se il modulo è 6 gli unici numeri che ammettono inverso sono 1 e 5.

Vediamo ora il criterio generale per stabilire se un numero è invertibile.

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* $\mathrm{mcd}(a, m) = 1$.

Dimostrazione. Dimostriamo l'implicazione nei due versi.

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

($\impliedby$) Supponiamo $\mathrm{mcd}(a, m) = 1$. Allora per il teorema di Bezout 2.2.2 $\exists x, y \in \mathbb{Z}$ tali che

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

dunque x è l'inverso di a modulo m. □

Corollario 3.2.4 *Se* p *è primo e* $a \not\equiv 0 \pmod{p}$, *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

$a \equiv 0 \pmod{p}$. Dunque se $a \equiv 0 \pmod{p}$ allora $\mathrm{mcd}(a,) = 1$, 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 esiste $x \in \mathbb{Z}$ tale che $ax \equiv b \pmod{m}$.*

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

Possiamo ora mostrare il criterio generale per la risoluzione delle congruenze lineari.

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 $ax \equiv b \pmod{m}$ ha soluzione se e solo se $\mathrm{mcd}(a, m) \mid b$.*

Dimostrazione. Dimostriamo l'implicazione nei due versi.

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

($\Longleftarrow$) Supponiamo che $d = \mathrm{mcd}(a, m)$ 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

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

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

Proposizione 3.2.7 *Se vogliamo semplificare una congruenza possiamo sfruttare le seguenti regole:*

$$A \equiv B \pmod{m} \iff A + c \equiv B + c \pmod{m} \tag{26}$$

$$A \equiv B \pmod{m} \implies cA \equiv cB \pmod{m} \tag{27}$$

$$A \equiv B \pmod{m} \iff (A \bmod m) \equiv (B \bmod m) \pmod{m} \tag{28}$$

$$Ad \equiv Bd \pmod{m} \implies A \equiv B \pmod{m} \quad \textit{se } \mathrm{mcd}(d)m = 1 \tag{29}$$

$$Ad \equiv Bd \pmod{md} \iff A \equiv B \pmod{m} \tag{30}$$

Dimostrazione. Dimostriamo le 5 proposizioni.

1. Dato che $c \equiv c \pmod{m}$, si tratta di un caso particolare della 23. Inoltre l'implicazione inversa si ricava dalla 24, dunque si tratta di un'equivalenza.
2. Dato che $c \equiv c \pmod{m}$, si tratta di un caso particolare della 25.
3. Dato che $A \equiv (A \bmod m) \pmod{m}$ e $B \equiv (B \bmod m) \pmod{m}$, per transitività otteniamo che $A \equiv B \pmod{m}$ è equivalente a $(A \bmod m) \equiv (B \bmod m) \pmod{m}$.

4. Se $\mathrm{mcd}(d)m = 1$ allora esiste l'inverso di d modulo m. Chiamiamo x questo inverso e moltiplichiamo entrambi i membri della congruenza per x, ottenendo

$$\begin{aligned} & Ad \equiv Bd \pmod{m} \\ \iff & Adx \equiv Bdx \pmod{m} \\ \iff & A \cdot 1 \equiv B \cdot 1 \pmod{m} \\ \iff & A \equiv B \pmod{m}. \end{aligned}$$

5. Per definizione di congruenza esiste $y \in \mathbb{Z}$ tale che

$$\begin{aligned} & Ad = Bd + mdy \\ \iff & A = B + my \\ \iff & A \equiv B \pmod{m}. \end{aligned}$$

□

Proposizione 3.2.8 *Siano $a, b, m \in \mathbb{Z}$ noti, $x \in \mathbb{Z}$ non noto. Allora per risolvere l'equazione $ax \equiv b \pmod{m}$ possiamo ricondurci ad uno dei seguenti tre casi:*

1. *se $\mathrm{mcd}(a, m) = 1$, allora l'equazione ha soluzione $x \equiv by \pmod{m}$, dove y è l'inverso di a modulo m;*
2. *se $\mathrm{mcd}(a, m) \neq 1$, $d = \mathrm{mcd}(a, m) \mid b$, allora l'equazione è equivalente all'equazione $a'x \equiv b' \pmod{m'}$, con $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$, che ha soluzione;*
3. *se $\mathrm{mcd}(a, m) \neq 1$, $\mathrm{mcd}(a, m) \nmid b$, 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 $x \equiv by \pmod{m}$.
2. Per la 3.2.6 l'equazione ha soluzione. Sia $d = \mathrm{mcd}(a, m)$. 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 **??** $\mathrm{mcd}(\frac{a}{d})\frac{m}{d} = 1$, 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*

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

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

$$x \equiv x_0 \pmod{m_1 m_2}. \tag{31}$$

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*

$$x \equiv x_0 \pmod{m} \iff \begin{cases} x \equiv x_0 \pmod{m_1} \\ x \equiv x_0 \pmod{m_2} \end{cases} \tag{32}$$

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*

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

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

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

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*

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

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

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

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

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

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

□

Se abbiamo un sistema con più 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*

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

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

$$x \equiv x_0 \pmod{\operatorname{mcm}(m_1, m_2, \ldots, m_n)} \tag{34}$$

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

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

$$[a]_n = \{ x \in \mathbb{Z} : x \equiv a \pmod{n} \}. \tag{35}$$

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

Quando il modulo è chiaro dal contesto si scrive anche $[a]$ oppure $\overline{a}$.

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 3.4.1. $a \equiv b \pmod{m} \iff [a]_n = [b]_n$.

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

$$\mathbb{Z}/(n) = \{ [0]_n, [1]_n, \ldots, [n-1]_n \}. \tag{36}$$

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:

$$[a]_n + [b]_n = [a+b]_n \qquad \forall [a]_n, [b]_n \in \mathbb{Z}/(n) \tag{37}$$

$$[a]_n \cdot [b]_n = [ab]_n \qquad \forall [a]_n, [b]_n \in \mathbb{Z}/(n) \tag{38}$$

Osservazione 3.4.2. 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 $n \geqslant 2$ 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 $p \geqslant 2$, 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. □

Gruppo degli inversi modulo m

Gli elementi invertibili modulo n formano un sottoinsieme molto importante degli interi modulo n.

Definizione 3.4.5 **Insieme degli invertibili.** Sia $n \geqslant 2$. Allora si indica con $(\mathbb{Z}/(n))^\times$ l'insieme delle classi resto invertibili modulo n, ovvero

$$(\mathbb{Z}/(n))^\times = \left\{ [a]_n \,:\, \exists [a^{-1}]_n \in \mathbb{Z}/(n). \quad [a]_n \left[a^{-1}\right]_n = [1]_n \right\}. \tag{39}$$

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

Dimostrazione. Ci basta dimostrare che $\overline{ab}$ è invertibile modulo n. Sia $[x]$ l'inverso, se esiste. Allora:

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

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

Proposizione 3.4.7 **$(\mathbb{Z}/(n))^\times$ è un gruppo.** *Per ogni $n \geqslant 2$ 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 $n \geqslant 2$. Allora si dice funzione di Eulero la funzione $\phi : \mathbb{N} \to \mathbb{N}$ tale che

$$\phi(n) = \left| (\mathbb{Z}/(n))^\times \right| \tag{40}$$

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

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

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 $\phi(p^n) = p^n - p^{n-1}$.*

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 $\{0, \dots, p^n - 1\}$ ci sono esattamente $\frac{p^n}{p} = p^{n-1}$ multipli di p (ve ne è uno ogni p elementi).
Dunque $\phi(p^n) = p^n - p^{n-1}$. □

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

$$\phi(ab) = \phi(a)\phi(b). \tag{41}$$

Dimostrazione. Per definizione di ϕ la tesi è equivalente a

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

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

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

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 $[h]_{ab}, [k]_{ab} \in \left(\mathbb{Z}/(ab)\right)^\times$ 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 $\mathrm{mcd}(a, b) = 1$) 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 $\mathrm{mcd}(x)a = \mathrm{mcd}(x)b = 1$. Per la proposizione **??**, dato che $\mathrm{mcd}(x)a = 1$ allora $\mathrm{mcd}(x)ab = \mathrm{mcd}(x)b = 1$, 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

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{42}$$

Proposizione 3.5.2 *Sia* $n \in \mathbb{Z}$, $k \in \mathbb{Z}$ *tale che* $0 \leqslant k \leqslant n$. *Allora*

$$\binom{n}{k} = \binom{n}{n-k}. \tag{43}$$

Dimostrazione.

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

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

$$\binom{n}{k} = \begin{cases} 1 & \text{se } k = 0 \text{ oppure } k = n \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{altrimenti.} \end{cases} \tag{44}$$

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. $\square$

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

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \cdots + \binom{n}{n}x^ny^0 = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k. \tag{45}$$

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 $n \geqslant 0$, $0 < k \leqslant n$, $T_{n+1,k} = T_{n,k-1} + T_{n,k}$.

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

$$T_{n,k} = \binom{n}{k}. \tag{46}$$

Dimostrazione. Per induzione su n.

CASO BASE. Sia $n = 0$, allora dato che $0 \leqslant k \leqslant n$ 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*

$$\binom{p}{k} \equiv 0 \pmod{p}. \tag{47}$$

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 2.3.2 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 2.3.5 p deve essere coprimo anche con $k!$ e con $(p-k)!$.

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

Proposizione 3.5.9 *Siano $x, y, p \in \mathbb{Z}$, p primo. Allora*

$$(x+y)^p \equiv x^p + y^p \pmod{p}. \tag{48}$$

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:

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

come volevasi dimostrare. □

Corollario 3.5.10 *Siano $x_1, x_2, \ldots, x_n, p \in \mathbb{Z}$, p primo. Allora*

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod{p}. \tag{49}$$

Dimostrazione. Per induzione su n.

CASO BASE. Sia $n = 1$. Allora $x_1^p \equiv x_1^p \pmod{p}$ ovviamente.

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

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

(per la proposizione 3.5.9)

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

(per ipotesi induttiva)

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

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 $x^p \equiv x \pmod{p}$.*

Dimostrazione.

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

(per il corollario 3.5.10)

$$\begin{aligned} &\equiv \overbrace{1^p + \cdots + 1^p}^{x \text{ volte}} \pmod{p} \\ &\equiv \overbrace{1 + \cdots + 1}^{x \text{ volte}} \pmod{p} \\ &\equiv x \pmod{p} \end{aligned}$$

che è la tesi. □

Corollario 3.5.12 *Se p è primo e $x \not\equiv 0 \pmod{p}$ allora $x^{p-1} \equiv 1 \pmod{p}$.*

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

$$\begin{aligned} x^p x^{-1} &\equiv x \cdot x^{-1} \pmod{p} \\ \iff x^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

che è la tesi. □

3.6 CONGRUENZE ESPONENZIALI

Iniziamo con un esempio di congruenza esponenziale.

Esempio 3.6.1. Trovare tutte le soluzioni di $3^x \equiv 5 \pmod{7}$.
Proviamo per tentativi:

$$\begin{aligned} x = 0 &\implies 3^0 \equiv 1 \not\equiv 5 \pmod{7} \\ x = 1 &\implies 3^1 \equiv 3 \not\equiv 5 \pmod{7} \\ x = 2 &\implies 3^2 \equiv 9 \equiv 2 \not\equiv 5 \pmod{7} \\ x = 3 &\implies 3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \not\equiv 5 \pmod{7} \\ x = 4 &\implies 3^4 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \not\equiv 5 \pmod{7} \\ x = 5 &\implies 3^5 \equiv 3^2 \cdot 3^3 \equiv 2 \cdot 6 \equiv 12 \equiv 5 \pmod{7} \\ x = 6 &\implies 3^6 \equiv 3^3 \cdot 3^3 \equiv 6 \cdot 6 \equiv 36 \equiv 1 \not\equiv 5 \pmod{7} \end{aligned}$$

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 $3^0 \equiv 3^6 \equiv 1 \pmod{7}$).

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

$$3^{5+6k} \equiv 3^5 \cdot 3^{6k} \equiv 3^5 \cdot 1^k \equiv 5 \pmod 7.$$

Dunque le soluzioni sono tutte le x tali che $x \equiv 5 \pmod 6$. 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 più piccolo intero positivo $\operatorname{ord}(a, m)$ tale che

$$a^{\operatorname{ord}(a,m)} \equiv 1 \pmod m. \tag{50}$$

Osservazione 3.6.1. Notiamo che $\operatorname{ord}(a, m)$ deve essere positivo, e dunque in particolare maggiore di 0. Inoltre la condizione $a \nmid m$, che equivale a $a \not\equiv 0 \pmod m$ serve ad evitare la congruenza banale $0^x \equiv b \pmod m$, che ha soluzione se e solo se $b \equiv 0 \pmod m$.

Proposizione 3.6.3 *Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora per ogni $k \in \mathbb{Z}$ vale che*

$$a^{k \operatorname{ord}(a,m)} \equiv 1 \pmod m. \tag{51}$$

Dimostrazione.

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

Proposizione 3.6.4 *Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora*

$$a^x \equiv 1 \pmod m \iff x \equiv 0 \pmod{\operatorname{ord}(a, m)}. \tag{52}$$

Dimostrazione. Per definizione di congruenza

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

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

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

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

che equivale a

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

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

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

Segue che $r = 0$, cioè $x = q \operatorname{ord}(a, m)$, cioè equivalentemente $x \equiv 0 \pmod{\operatorname{ord}(a, m)}$, 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*

$$x \equiv x_0 \pmod{\operatorname{ord}(a, m)}. \tag{53}$$

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

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

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

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

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

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* $\mathrm{ord}(a, []) \mid p - 1$.

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

Per la proposizione 3.6.4 segue che $p - 1 \equiv 0 \pmod{\mathrm{ord}(a, [])}$, cioè $\mathrm{ord}(a, []) \mid p - 1$, 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* $a^{\phi(n)} \equiv 1 \pmod{n}$.

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

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

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

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

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 $[b_i]_n, [b_j]_n \in \left(\mathbb{Z}/(n)\right)^\times$ 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 $\left(\mathbb{Z}/(n)\right)^\times$ 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:

$$\begin{aligned} & \iff ab_1 \cdot ab_2 \cdots ab_k \equiv b_1b_2 \cdots b_k \pmod{n} \\ & \iff (\overbrace{a \cdot a \cdots a}^{k \text{ volte}}) \cdot (b_1b_2 \cdots b_k) \equiv (b_1b_2 \cdots b_k) \pmod{n} \end{aligned}$$

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

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

che è la tesi. □

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

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

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

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