$\sim$ relazione d'equivalenza su X ($\sim$ tilde)

$[x] = \{ y \in X \mid x \sim y \}$

Si considera l'insieme

$$X/\sim \;:= \{ [x] \mid x \in X \}$$

di tutte le classi d'equivalenza e lo si chiama insieme quoziente di X rispetto a $\sim$

Un elemento qualunque della classe $[x]$ è detto rappresentante di $[x]$. Ad es. x è rappresentante di $[x]$.

<u>Esempio</u> La congruenza mod 2 vista nella lezione precedente da luogo a due sole classi d'equivalenza $[0]$ e $[1]$ pertanto

$$\mathbb{Z}/\equiv_2 = \{ [0], [1] \}.$$

0 è rappresentante di $[0]$, come qualunque numero pari. Ad es. anche 12 è rappresentante di $[0]$, avendosi

$$[0] = [12].$$

Fissiamo un numero naturale $n \in \mathbb{N}$, $n \geq 2$.

Definiamo $a \equiv b \iff a-b$ è divisibile per n, cioè (congruente)

$$\exists\, k \in \mathbb{Z} \text{ t.c. } a-b = nk$$

Scriveremo anche $a \equiv_n b$ o $a \equiv b \pmod{n}$ (modulo n)

Come nel caso $n=2$ si vede che $\equiv_2$ è una relazione d'equivalenza su $\mathbb{Z}$ detta congruenza modulo n.

$[a] = \{a + nk \mid k \in \mathbb{Z}\}$

$[0]$ è costituita dai multipli interi di n.

Facendo la divisione con resto di a per n si ottengono quoziente q e resto r con $0 \leq r < n$ t.c.

$$a = nq + r \implies a \equiv r \pmod{n}$$

$r \in \{0, 1, \dots, n-1\}$

Inoltre se $r_1, r_2 \in \{0, 1, \dots, n-1\}$ e $r_1 \equiv_n r_2 \implies$ $r_1 = r_2$ dato che se fosse ad esempio $r_1 < r_2$ si avrebbe $0 < r_2 - r_1 = nk$ per un certo $k \geq 1$ intero $\implies r_2 - r_1 \geq n$ impossibile.

Poniamo $\mathbb{Z}_n = \mathbb{Z}/n := \mathbb{Z}/\equiv_n$ e si ha quindi:
$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$ ha n elementi.

Somma $[a] + [b] := [a+b]$

Prodotto $[a][b] := [ab]$

Es $\mathbb{Z}_3 = \{[0], [1], [2]\}$

$[1] + [2] = [3] = [0]$ $\qquad [2]^2 = [4] = 1$

Scriviamo anche $1 + 2 = 0$ in $\mathbb{Z}_3$, $2^2 = 1$ in $\mathbb{Z}_3$.

Dato che le operazioni $+$ e $\cdot$ in $\mathbb{Z}_n$ sono definite in termini di rappresentanti occorre mostrare che il risultato non dipende dai rappresentanti scelti, cioè $+$ e $\cdot$ sono **ben definite** su $\mathbb{Z}_n$.

Se $[a]=[a']$ e $[b]=[b']$, cioè $a \equiv_n a'$ e $b \equiv_n b'$ si ha $a' = a + nh$, $b' = b + nk$ per certi $h, k \in \mathbb{Z}$ $\Rightarrow$
$a'+b' = a+b+n(h+k) \equiv_n a+b \Rightarrow [a'+b'] = [a+b]$
e quindi $+$ è ben definita. Vediamo $\cdot$

$$a'b' = (a+nh)(b+nk) = ab + ank + nhb + n^2hk$$
$$= ab + n\underbrace{(ak+bh+nhk)}_{\in\, \mathbb{Z}} \equiv_n ab \Rightarrow [a'b'] = [ab]$$

Pertanto anche $\cdot$ è ben definita.

Inoltre

1) $[a]+[0] = [a+0] = [a]$

2) $[a]+[-a] = [a-a] = [0]$ ($[0]$ elemento neutro per $+$)

Poniamo $-[a] := [-a]$ (opposto di $[a]$)

$\Rightarrow [a]-[a] = [0]$

3) $[a]+[b] = [a+b] = [b+a] = [b]+[a]$ ($+$ commutativa)

4) $[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] =$
$= [(a+b)+c] = [a+b]+[c] = ([a]+[b])+[c]$
($+$ associativa)

5) $[a]\cdot[1] = [a\cdot 1] = [a]$ ($[1]$ elemento neutro per $\cdot$)

6) $[a][b] = [ab] = [ba] = [b][a]$ (· commutativa)

7) $[a]\big([b][c]\big) = [a][bc] = [a(bc)] = [(ab)c] =$
$= [ab][c] = \big([a][b]\big)[c]$ (· associativa)

8) $[a]\big([b]+[c]\big) = [a][b+c] = [a(b+c)] = [ab+ac] =$
$= [ab] + [ac] = [a][b] + [a][c]$
(· distributiva rispetto a +)

<u>OSS</u> La proprietà distributiva collega le due operazioni.

Si ha anche: $[a][0] = [a0] = [0] = [0][a]$

<u>Es</u> 1) In $\mathbb{Z}_3$ $[2]^2 = [2][2] = [4] = [1] \Rightarrow$
$[2]$ ammette inverso moltiplicativo (ed è $[2]$ stesso)

2) In $\mathbb{Z}_5$

$\cdot$	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

Si ha $[1]^2 = [1]$, $[2][3] = [6] = [1]$, $[4]^2 = [16] = [1]$

Pertanto anche in $\mathbb{Z}_5$ tutti gli elementi non nulli hanno inverso moltiplicativo.

Sorprendente perché in $\mathbb{Z}$ solo ± 1 hanno inverso!

3) $\mathbb{Z}_6 \quad [2][3] = [6] = 0 \implies [2]$ e $[3]$ non hanno inverso moltiplicativo. Infatti se per assurdo $[a] \in \mathbb{Z}_6$ fosse inverso di $[2] \implies$

$[2][a] = 1 \implies [2][a][3] = [3] \implies [0] = [3]$

contraddizione.

Si può dimostrare che $[a] \in \mathbb{Z}_n$ ammette inverso $\iff a$ è primo con n, cioè $\iff MCD(a, n) = 1$.

Pertanto se $p \geq 2$ è un numero primo, in $\mathbb{Z}_p$ ogni elemento <u>non nullo</u> ammette inverso e viceversa se in $\mathbb{Z}_p$ ogni elemento non nullo ammette inverso allora p è primo.

Campi

Un campo è un insieme $\mathbb{K}$ con almeno due elementi (o anche infiniti) munito di due operazioni denotate convenzionalmente $+$ e $\cdot$ t.c.

1) $+, \cdot$ commutative $a+b=b+a$ e $ab=ba$
2) $+, \cdot$ associative $a+(b+c)=(a+b)+c$ e $a(bc)=(ab)c$
3) $\cdot$ è distributiva rispetto a $+$
   $a(b+c)=ab+ac$
4) esiste un elemento denotato convenzionalmente $0 \in \mathbb{K}$ t.c. $a+0=0+a=a$ (elemento neutro additivo o zero di $\mathbb{K}$)
5) esiste un elemento denotato $1 \in \mathbb{K}$ t.c. $1 \neq 0$ e $a \cdot 1 = 1 \cdot a = a$ (elemento neutro moltiplicativo)
6) $\forall a \in \mathbb{K}\ \exists -a \in \mathbb{K}$ t.c. $a+(-a)=0$ (opposto di a)
   scriviamo $a-a=0$
7) $\forall a \in \mathbb{K}, a \neq 0, \exists a^{-1} \in \mathbb{K}$ t.c. $a a^{-1} = 1$
   (inverso di a)

<u>Es</u> $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono esempi importanti di campi con infiniti elementi

$\mathbb{Z}_p$ ($p \geq 2$ primo) è un campo finito ($\# \mathbb{Z}_p = p$)
$\mathbb{Z}_p$ è detto <u>campo dei resti (o degli interi)</u> modulo p.

Esistono anche altri campi che noi non tratteremo.