Torniamo alla congruenza modulo n in $\mathbb{Z}$.

Def Sia $n \in \mathbb{N}$, $n \geq 2$, e sia $a \in \mathbb{Z}$. La classe d'equivalenza $[a]_n$ di a rispetto a $\equiv_n$ è detta <u>classe di congruenza</u> di a (mod n).

Pertanto $a \in [a]_n$ e $[a]_n \cap [b]_n \neq \emptyset \iff a \equiv_n b$
$\iff [a]_n = [b]_n$

Si osservi che $b \in [a]_n \iff \exists\, k \in \mathbb{Z}$ t.c.
$b - a = kn \iff b = a + kn,\ k \in \mathbb{Z}$.

Quindi $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$

Per questa ragione si scrive anche

$$[a]_n = a + n\mathbb{Z} \quad (\underline{\text{notazione}})$$

Def L'insieme quoziente di $\mathbb{Z}$ rispetto a $\equiv_n$ si denota con $\mathbb{Z}_n$ (oppure con $\mathbb{Z}/n$), cioè

$$\mathbb{Z}_n \stackrel{\text{def}}{=} \{[a]_n \mid a \in \mathbb{Z}\} \quad (\text{interi modulo } n)$$

Teorema $\mathbb{Z}_n$ ha n elementi: $[0]_n, [1]_n, \dots, [n-1]_n$

Dim $a \in \mathbb{Z}$ divisione con resto di a per n

$\rightsquigarrow \exists!\, q \in \mathbb{Z}$ e $0 \leq r < n$ t.c.
$a = nq + r \implies a \equiv r \pmod{n}$.

Definiamo due operazioni binarie su $\mathbb{Z}_n$

1) addizione

$$[a]_n + [b]_n \overset{def}{=} [a+b]_n$$

operazione che stiamo definendo — addizione di interi

Mostriamo che la definizione ha senso, cioè non dipende dai rappresentanti scelti

Se $a' \equiv_n a$ e $b' \equiv_n b$ si ha $a' = a + kn$ e $b' = b + hn$

per certi $k, h \in \mathbb{Z}$ $\rightsquigarrow$

$$a' + b' = a + kn + b + kn = a + b + (k+h)n \equiv_n a + b$$

$\Longrightarrow$ $+$ è ben definita su $\mathbb{Z}_n$

2) moltiplicazione

$$[a]_n \cdot [b]_n \overset{def}{=} [a \cdot b]_n$$

operazione che stiamo definendo — moltiplicazione di interi

Mostriamo che $\cdot$ è ben definita. Come sopra si ha:

$$a'b' = (a+kn)(b+hn) = ab + (ah + bk + khn)n$$
$$\equiv_n ab \Longrightarrow \cdot \text{ ben definita.}$$

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n, \quad \pi(a) = [a]_n \quad \begin{cases} \pi(a+b) = \pi(a) + \pi(b) \\ \pi(ab) = \pi(a)\pi(b) \end{cases}$$

Le proprietà associative, commutative e distributive per addizione e moltiplicazione di interi implica banalmente che le stesse proprietà valgono per l'addizione e moltiplicazione di classi di congruenza (mod n).

<u>OSS</u> Non ha senso sommare o moltiplicare classi mod n con classi mod m, se $n \neq m$.

<u>OSS</u> $\mathbb{Z}_n$ è un gruppo abeliano rispetto a $+$, infatti $[0]_n$ è l'elemento neutro e

$\forall [a]_n$ si ha $[a]_n + [-a]_n = [0]_n$

cioè $[-a]_n$ è l'opposto di $[a]_n$ in $\mathbb{Z}_n$

(poniamo $-[a]_n \stackrel{def}{=} [-a]_n$). Si osservi che $[n]_n = [kn]_n = [0]_n$ $(\forall k \in \mathbb{Z})$

<u>OSS</u> Se $n = uv$ con $u, v \in \mathbb{N}$, $u, v \geq 2$, cioè se n ammette divisori non banali, si ha $[u]_n \cdot [v]_n = [n]_n = [0]_n$

ma $[u]_n \neq [0]_n$ e $[v]_n \neq [0]_n$

(tali elementi sono detti <u>divisori dello zero</u>)

In questo caso $\mathbb{Z}_n$ <u>non è un campo</u>

Teorema

Siano $a, b \in \mathbb{N}$, $a, b \geq 1$ e sia $d = MCD(a,b)$

Allora $\exists\, t, s \in \mathbb{Z}$ t.c. $d = ta + sb$

Dim

$$a = b q_0 + r_0$$

$$b = r_0 q_1 + r_1$$

$$r_0 = r_1 q_2 + r_2$$

$$\vdots$$

$$r_{k-1} = r_k q_{k+1} + r_{k+1}$$

$$r_k = r_{k+1} q_{k+2}$$

$r_0 = a - b q_0$

$r_1 = b - r_0 q_1, \ \ldots \quad r_{k+1} = ta + sb$

$\ldots$

$k \mid a$ e $k \mid b \iff k \mid b$ e $k \mid r_0$

$k \mid b$ e $k \mid r_0 \iff k \mid r_0$ e $k \mid r_1$

$\vdots$

in ogni passaggio con $r_{i+1} \neq 0$

$$MCD(r_i, r_{i+1}) = MCD(r_{i-1}, r_i) = MCD(a,b)$$

$r_{k+2} = 0 \implies MCD(a,b) = r_{k+1}$.

Esempio $a = 75$, $b = 21$

$$75 = 21 \cdot 3 + 12$$

$$21 = 12 \cdot 1 + 9$$

$$12 = 9 \cdot 1 + 3$$

$$9 = 3 \cdot 3$$

$$MCD(75, 21) = 3$$

$$12 = 75 - 21 \cdot 3$$

$$9 = 21 - 12 = 21 - 75 + 21 \cdot 3 = 21 \cdot 4 - 75$$

$$3 = 12 - 9 = 75 - 21 \cdot 3 - 21 \cdot 4 + 75 =$$

$$= 2 \cdot 75 - 7 \cdot 21$$

$t = 2$, $s = -7$.

Teorema Sia $p \in \mathbb{N}$. Allora $\mathbb{Z}_p$ è un campo se e solo se p è primo.

<u>Dim</u> • L'osservazione precedente mostra che se p è un numero composto (cioè non è primo) allora $\mathbb{Z}_p$ ammette divisori dello zero $\Rightarrow$ $\mathbb{Z}_p$ non è un campo.

• Dimostriamo che se p è primo allora $\mathbb{Z}_p$ è un campo. Resta da far vedere che gli elementi non nulli di $\mathbb{Z}_p$ sono invertibili.

Sia $[a]_p \neq [0]_p \Rightarrow p \nmid a \Rightarrow MCD(p,a)=1$

$\Rightarrow \exists\ t, s \in \mathbb{Z}$ t.c.

$$tp + sa = 1 \Rightarrow sa = 1 - tp \equiv_p 1$$

$$\Rightarrow [s]_p [a]_p = [1]_p$$

cioè $[s]_p = [a]_p^{-1}$.

<u>Esempi</u> $\mathbb{Z}_2 = \{0, 1\}$ $\quad 1+1=0 \quad 1\cdot 1 = 1$

$\mathbb{Z}_3 = \{0, 1, 2\}$ $\quad 2^{-1} = 2 \quad 1+2=0, \quad 2+2=1$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ $\quad 2^{-1} = 3, \quad 3^{-1} = 2, \quad 4^{-1} = 4$

$3+4 = 2, \quad -3 = 2, \quad 4+1 = 0$

<u>OSS</u> $\mathbb{Z}_p$, p primo, è un campo finito con p elementi.

OSS $\mathbb{K}$ campo $\leadsto$ <u>legge di cancellazione</u>

$$a+b = a+c \implies b = c \quad (\text{sommando } -a)$$

$$ab = ac \text{ e } a \neq 0 \implies b = c \quad (\text{moltiplicando } a^{-1})$$