Congruenza M/E E equivalenza. $(M, *)$

$(\mathbb{Z}, +, 0)$ $n \in \mathbb{N}$ $a E_n b$ $n \mid b-a$

$a \equiv b \mod n$ $a \equiv_n b$ a è congruo a b modulo n

$$\mathbb{Z}/E_n = \{ [a]_{E_n} : a \in \mathbb{Z} \}$$

$$[a]_{E_n} = \{ a + kn : k \in \mathbb{Z} \} \quad |[a]_{E_n}| = \infty$$

$\mathbb{Z}/n$ $\mathbb{Z}$ su n, $\mathbb{Z}$ modulo n

$(\mathbb{Z}/n, +_n, [0]_{E_n})$ gruppo abeliano

$\bar{a} := [a]_{E_n}$ $+_n : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$

$(\bar{a}, \bar{b}) \mapsto \overline{a+b} =: \bar{a} +_n \bar{b}$

operazione binaria

$\mathbb{Z}/n$ chiuso rispetto a $+_n$

$(\bar{a} +_n \bar{b}) +_n \bar{c} = \bar{a} +_n (\bar{b} +_n \bar{c})$

$\overline{a+b} +_n \bar{c} = \bar{a} +_n \overline{b+c}$ associativa per $+_n$

$\overline{(a+b)+c} = \overline{a+(b+c)}$

$\exists \bar{z} \; \forall \bar{a} : \quad \bar{a} + \bar{z} = \bar{z} + \bar{a} = \bar{a}$

$\overline{a+z} = \overline{z+a} = \bar{a}$ $z = 0$ valido

$\bar{z} = \bar{0}$ $\bar{a} +_n \bar{n} = \bar{a}$

$\forall \bar{a} \; \exists \bar{b}$ $\bar{a} +_n \bar{b} = \bar{b} +_n \bar{a} = \bar{0}$ $\overline{a+b} = \bar{0}$ $b = -a$

$+_n$ comm poiché è comm. + usuale

$(\mathbb{Z}/_n, +_n, \bar{0})$

$n=0 \quad a \equiv_0 b \iff 0 \mid b-a \iff \exists k \in \mathbb{Z} \quad b-a = k\cdot 0 = 0$

$\iff b=a \quad \bar{a} = \{a\} \quad \mathbb{Z} \simeq \mathbb{Z}/_0$ biezione omomorfismo

$a \longleftrightarrow \{a\}$

$a+b \longleftrightarrow \{a\} +_0 \{b\} = \bar{a} +_0 \bar{b}$

$n=1 \quad b-a = k\cdot 1 \quad \bar{0} = \mathbb{Z}$

Notate che $\boxed{E_n = E_{-n}}$ $a E_n b \iff b-a = k\cdot n = (-k)(-n)$

$n \in \mathbb{N}_{>0}$

Teorema: $|\mathbb{Z}/_n| = n$ per $n>0$ $n \in \mathbb{N}$

Inoltre $\mathbb{Z}/_n = \{\bar{0}, \dots, \overline{n-1}\}$

Dim: Dato $a \in \mathbb{Z}$ $\exists r \in \mathbb{Z}$ $0 \le r < n$

$\bar{a} = \bar{r}$ $a = nq + r$ per qualche r $0 \le r \le n-1$

$n \mid a-r \quad a \equiv_n r \quad \mathbb{Z}/_n = \{\bar{0}, \dots, \overline{n-1}\}$

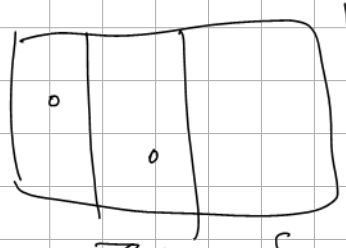
Per ottenere $|\mathbb{Z}/_n| = n$ basta mostrare

$0 \le r \le s \le n-1 \quad \bar{r} = \bar{s} \quad n \mid s-r$ ma

$\bar{r} = \bar{s} \iff r E_n s \iff n \mid s-r$

$n-1 \ge s-r \ge 0$

$\Longrightarrow s-r = 0 \quad s = r$



$n=3 \quad \mathbb{Z}/_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\overline{0} = \{0+3k : k \in \mathbb{Z}\} = 3\mathbb{Z}$

$\overline{1} = \{1+3k : k \in \mathbb{Z}\} = \{\dots -5, -2, 1, 4, 7, 10 \dots\} = 1+3\mathbb{Z}$

$\overline{2} = \{2+3k : k \in \mathbb{Z}\} = \{\dots -4, -1, 2, 5, 8 \dots\} = 2+3\mathbb{Z}$

$\overline{0} \cup \overline{1} \cup \overline{2} = \mathbb{Z}$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}=\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

1ª $\overline{0}$ compare in ogni riga/colonna

0ª $\overline{0}$ el. neutro

ossia $\forall \bar{a} \ \exists -\bar{a} = \overline{-a}$

$\overline{1} + \overline{2} = \overline{3} = \overline{0} \quad -\overline{1} = \overline{2} \quad 2 = 3 - 1$

2ª Ogni elemento compare una ed una sola volta in ogni e in ogni colonna

Equazioni (semplici) in $\mathbb{Z}/n$

$\forall n \ \mathbb{Z}, \mathbb{Q}, \mathbb{R} \quad a + x = b$ a, b INPUT x incognita

$x = b - a \qquad -a + (a + x) = -a + b$

$(-a + a) + x = -a + b$

$0 + x = -a + b$

$x = -a + b$

$x = b - a$

$a + x \equiv_n b \qquad x \equiv_n b - a$

$n = 4 \quad a = 107, b = -25 \quad x \equiv_4 -25 - 107 \equiv_4 -132 \equiv_4 0$

$\overline{x} = \overline{0} \quad x \in 4\mathbb{Z} \quad \overline{b} = \overline{3} \quad 4 \mid -25 - 3 \quad a \equiv_4 3$

$x \equiv_4 3 - 3 = 0$

Quadrato Latino ⟷ Esperimenti

$\mathbb{Z}/n = \{\bar{0}, \ldots, \overline{n-1}\}$ $0 \le r \le n-1$ RAPPRESENTANTI CANONICI

resti

$\left\{\frac{-n+1}{2}, \ldots, 0, \ldots, \frac{n-1}{2}\right\}$ n dispari

RIDOTTI

$\left\{\frac{-n+2}{2}, 0, \ldots, \frac{n}{2}\right\}$ n pari

$n=4$ $\{-\bar{1}, \bar{0}, \bar{1}, \bar{2}\}$

$n=7$ $\{-3, -2, -1, 0, 1, 2, 3\}$

$(\mathbb{Z}/n, \cdot, \bar{1})$ $\bar{a}\cdot\bar{b} = \overline{ab}$ monoide

$\cdot : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$ · associativa $\bar{a}\cdot\bar{u} = \bar{u}\cdot\bar{a} = \bar{a}$ $\exists \bar{u}\ \forall \bar{a}$

Ex $\bar{a}\bar{u} = \bar{u}a = \bar{a}$ $u = 1$

$n=3$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}=\bar{1}$

1. $\bar{0}$ uccide tutto
2. Simmetrico = commut $\bar{1}\ \bar{2}$ $\bar{2}\ \bar{1}$
3. $\bar{1}$ in ogni riga/colonna
4. Ogni classe compare ogni riga/colonna (quadrato latino $\bar{1}, \bar{1}$)

$n=4$

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

1 3
3 1

1, 3 hanno inverso

$n=5$

	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

Notate che ogni $a \not\equiv_5 0$ $\exists b$:

$ab \equiv_5 1$ $1^{-1} \equiv_5 1$ $2^{-1} \equiv 3$ $3^{-1} \equiv 2$ $4^{-1} \equiv_5 4$

$(-1)^{-1} \equiv_5 -1$

$n=6$ Quali elementi sono invertibili $ax \equiv_n 1$ ammette soluzioni?

$\exists$ in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ $ax + b = 0$ $ax = -b$ se $\exists \bar{a}^{-1}$

$a^{-1}(ax) = a^{-1} \cdot (-b)$ $\quad 1 \cdot x = (-b) \cdot a^{-1}$ $\quad x = -(b a^{-1})$

in $\mathbb{Z}$ $\quad 2x + 3 = 0$ $\quad \nexists 2^{-1}$ No

$2x + 4 = 0$ $\quad$ Si $\quad 2(x+2) = 0$ $\quad x+2 = 0$

$x = -2$

in $\mathbb{Z}/n$ $\quad ax \equiv_n -b$ $\quad n, a$ legati

Criteri divisibilità $\quad 2|a$, $3|a$, $5|a$, $9|a$, $11|a$

$7|a$