gennaio 2016 (28) 22 dicembre 2016

$[r]_n$ classe di resto r modulo n $\quad 0 \le r \le n-1$

↓

insieme degli interi relativi che divisi per n danno resto r

Teorema fondamentale dell'aritmetica

$$a = q \cdot n + r$$

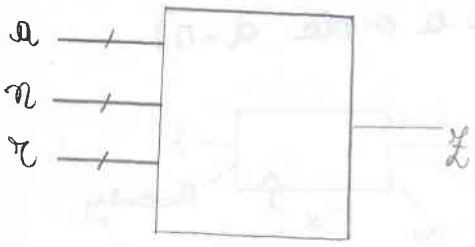
(a: dividendo, n: divisore, q: quoziente, r: resto)

$[3]_4 = \{\dots, -13, -9, -5, -1, 3, 7, 11, 15, \dots\}$

$q = \dots, -4, -3, -2, -1, 0, 1, 2, 3, \dots$

la distanza tra due elementi consecutivi di questo insieme è 4

• Progettare la macchina sequenziale che, dati in ingresso $a \ge 0$, $n > 0$, $0 \le r \le n-1$, $r \in R_n = \{0, \dots, n-1\}$, dà in uscita



$$z \text{ (1 bit)} = \begin{cases} 0 & \text{se } a \notin [r]_n \\ 1 & \text{altrimenti} \end{cases}$$

→ se $a=-9$ $n=4$ $r=3$ esce 1

→ se $a=13$ $n=4$ $r=3$ esce 0

La macchina deve essere implementata usando la ALU

Idea: sottraggo ripetutamente n da a, fin quando non si ha $a < n$; a questo punto, se $a \equiv r \pmod n$ è $z=1$, altrimenti $z=0$

t	α	$\alpha - 4$	
0	13 (=a)	$9 \notin R_4$	→ devo controllare $a > r$
1	9	5	
2	5	$1 \in R_4$	

α variabile di appoggio $\quad a \in [3]_4 \Leftrightarrow \alpha \in R_4 \ \& \ \alpha = 3$

dal momento che $1 \neq 3$ deduciamo che $13 \notin [3]_4$

t	α	$\alpha - 4$	
0	19		
1	15	15	$15 \ge n = 4$
2	11	11	
3	7	7	
		$3 = r$, $3 \in R_4$	$\Rightarrow 19 \in [3]_4$

Ipotesi: stiamo considerando $a \geq 0$. Se fosse $a < 0$ dovrei sommare ripetutamente n per ferrarmi al primo resto positivo (coppia $0 \leq r < n$).

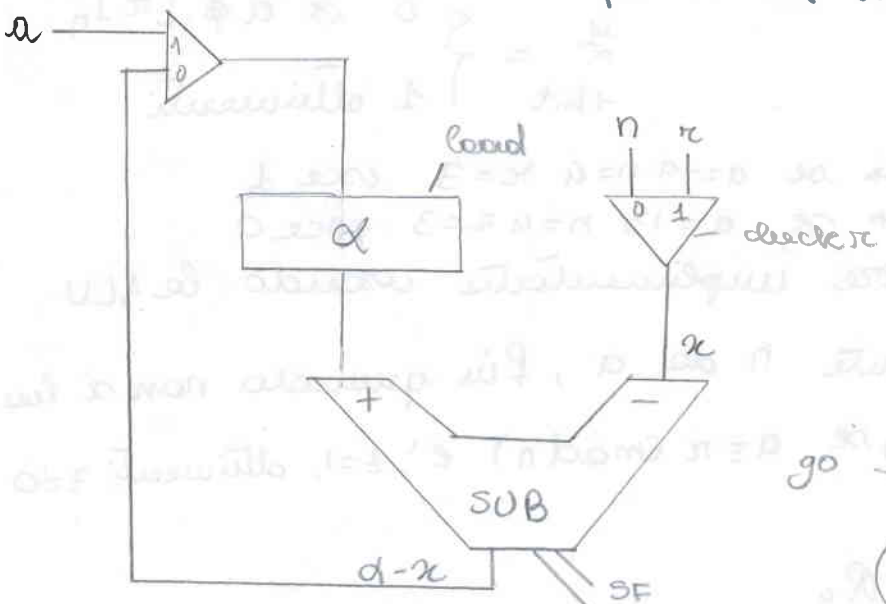
[inizializzazione] 0. $\alpha \leftarrow a$

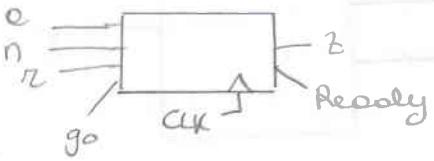
[check della condizione di terminazione] 1. if $(\alpha - n) < 0$
goto 3

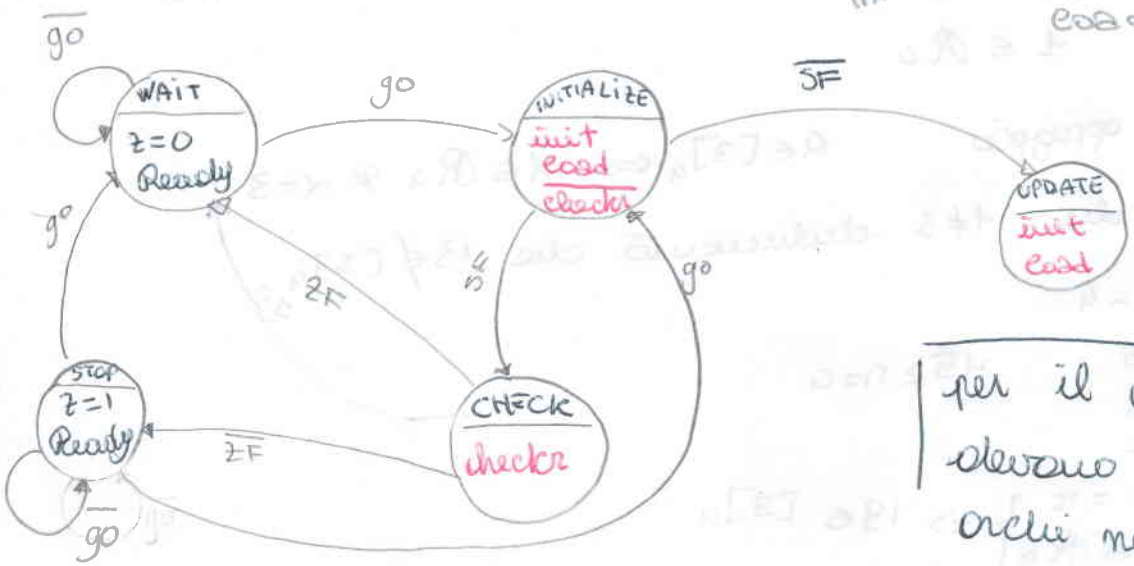
[aggiornamento] 2. $\alpha \leftarrow \alpha - n$
goto 1

[decisione e terminazione] 3. if $\alpha - r = 0$
$z = 1$
else
$z = 0$; stop

"regole della gara": - 1 registro per α . SF (per 1)
- 1 ALU in configurazione SUB flag
- 1 MUX per selezionare input della porta - ZF (per 0)
- 1 MUX per load (o da a o da $a-n$)







per il caso $a < 0$ devono essere apportati archi nell'automa