

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

Calcolatori — a.a. 2021–2022

Compito dell'8 luglio 2022

Cognome e Nome dello studente: _____

Divisibilità (senza divisioni)

Il resto $r = p \% q$ della divisione tra due interi positivi p e q , detto anche residuo di p modulo q , è un intero compreso tra 0 e $q - 1$. Se $r = 0$, allora si dice che p è divisibile per q . Dato un numero $p = (p_1 p_2 p_3 \dots p_{n-1} p_n)_2$ espresso in rappresentazione naturale su n bit, un algoritmo per calcolare il residuo r è il seguente:

```
 $r_0 \leftarrow 0$  [initialize]
for  $t = 1 \dots n$ : [compute]
     $r_t \leftarrow (2r_{t-1} + p_t) \% q$ 
 $r \leftarrow r_n$  [get result]
```

Al passo t -mo, l'algoritmo calcola il residuo $r_t = (p_1 p_2 p_3 \dots p_t)_2 \% q$ utilizzando il residuo del passo precedente. Ne risulta un percorso che, partendo da $r_0 = 0$, raggiunge $r_n = r$ passando eventualmente da altri valori $r_t \in \{0, \dots, q - 1\}$. Ad esempio, per il numero $p = (11101011)_2 = 235$, che è divisibile per $q = 5$, si raggiunge $r = 0$ attraverso la sequenza $r_0 = 0, 1, 3, 2, 4, 4, 3, 2, 0 = r$.

Reti Logiche Progettare, con la tecnica “parte operativa/parte di controllo” e con l’ausilio dell’algoritmo sopra riportato, una macchina per stabilire la divisibilità per $q = 5$ di un intero positivo p espresso su $n = 8$ bit posto in ingresso. In uscita, il bit d segnalerà il risultato ($d = 1$ se p divisibile per q , 0 altrimenti). La parte di controllo realizzerà la fase di calcolo dell’algoritmo come una transizione di stato (da r_{t-1} a r_t), dunque senza fare uso di circuiti aritmetici. Dopo avere disegnato la parte operativa e specificato il controllo attraverso il diagramma degli stati, realizzare il controllo con la tecnica che si ritiene più appropriata. Simulare infine il funzionamento della macchina nel caso $p = (10111101)_2$.

Programmazione Scrivere un programma assembler 8086 che consenta di eseguire l’algoritmo sopra riportato per $q = 7$ e un intero p di $n = 16$ bit posto in memoria. Come per la macchina realizzata al punto precedente, per passare da un residuo al successivo il programma non deve eseguire una divisione; può invece servirsi di una look-up table in memoria. Verificare il funzionamento del programma con $p = 0E54h$.