Corso di Laurea in Ingegneria Informatica

Calcolatori — a.a. 2013–2014

Prova in itinere del 7 novembre 2013

Cognome e Nome dello studente: _____

Dato un intero a ed un intero positivo m primi tra loro, si definisce ordine moltiplicativo di a modulo m *il più piccolo intero λ tale per cui $a^\lambda - 1 = 0$ (modulo m). La funzione $\lambda(a, m)$ svolge un ruolo importante nella teoria dei numeri e nella costruzione di sequenze pseudo-casuali. Un algoritmo per il calcolo di $\lambda(2, m)$, con m dispari, è il seguente:*

0. *Poni $\lambda = 0$, $k = 1$.*
1. *Poni $k \leftarrow (2 \times k)$.*
2. *Se $k > m$ allora poni $k \leftarrow (k - m)$.*
3. *Incrementa λ. Se $k = 1$ stop, altrimenti vai al punto 1.*

Progettare (parte operativa e parte di controllo) una macchina sequenziale che calcoli $\lambda(2, m)$ con m dispari minore di 256.

♡ Disegnare la parte operativa della macchina;

♢ Disegnare il diagramma degli stati della parte di controllo;

♮ Disegnare lo schema a blocchi completo delle due parti del sistema e delle loro connessioni, evidenziando i clock ed i segnali di condizione e controllo.

♠ Indicare l'andamento temporale di ingressi, stati e uscite del controllo nel caso $m = 19$;

♣ Realizzare l'hardware della parte di controllo facendo uso di registro di stato e multiplexer.