COGNOME .... *NOME* .... *MATRICOLA* ....

Risolvere gli esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. *Inserire le risposte negli spazi predisposti.* *NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* Ogni esercizio vale 7.5 punti.

1. Si scriva un unico programma in Pari che dati $m \in \mathbf{N}$ e $a \in \mathbf{Z}/m\mathbf{Z}$ determini se m
   a. è pseudo primo;
   b. è pseudo primo Euleriano;
   c. è pseudo primo forte.

2. Dimostrare che se $m \equiv 3 \bmod 4$ è pseudo primo Euleriano in base a allora è anche pseudo primo forte in base a.

3. Sia q un numero primo tale che $q \equiv 2 \bmod 3$. Dimostrare che, se $4^q \equiv 1 \bmod (2q+1)$, allora $2q+1$ è primo.

4. Sia $m = 65$.
   i. Determinare tutte le soluzioni di $x^2 \equiv -1 \bmod m$;
   ii. Determinare due basi a_1 e a_2 tali che 65 è uno pseudo primo forte in base a_1, in base a_2 ma non in base $a_1 a_2$.
   iii. Cosa possiamo dedurre sull'insieme delle basi forti $S(65)$

5. (Quickies): Scrivere solo la risposta delle seguenti domande:
   i. Si scriva la successione di Miller Rabin modulo 49 delle seguenti basi: $2, 7, 25, 13$.
   ii Determinare dei fattori non banali di 10002200057;
   iii. Determinare dei fattori non banali di 30001600021;

i.

ii.

iii.