Università degli studi di Roma Tre
Corso di Laurea in Matematica, a.a. 1999/2000
Matematica Applicata 2
Terzo Test

1. In $U(\mathbf{Z}/33\mathbf{Z})$ si determini una base (non banale) rispetto a cui 33 è pseudo primo di Eulero.
   (*Sugg. si cerchi tra le radici quadrate di 1 modulo 33*)

2. Si calcoli il seguente simbolo di Jacobi senza fattorizzare:
$$\left(\frac{1234}{8765}\right)$$

3. Supponiamo di voler controllare se un numero di 70 cifre (decimali) è primo. Quante iterazioni del test di Solovay-Strassen è necessario compiere per avere una probabilità di insuccesso minore di 10^{-4}.

4. Determinare una base rispetto a cui 65 non è pseudo primo di Eulero.

5. In meno dieci righe si spieghi cosa è RSA e a cosa serve.

6. (facoltativo) Si dimostri che se $n \equiv 3 \bmod 4$ allora n è uno pseudo primo di Eulero se e solo se è uno pseudo primo forte.