Università degli Studi Roma Tre
Corso di Studi in Matematica, a.a. 2016/2017
CR410 – Crittografia1
Esercizi
Foglio 2

1. Sia k un intero positivo: dimostrare che se $2^k + 1$ è primo allora k è una potenza di due.

2. Mostrare se F_n e F_m sono numeri di Fermat con $m \neq n$, allora $(F_n, F_m) = 1$.

3. - Sia n uno pseudoprimo in base a e in base b, con $(a, n) = (b, n) = 1$. Mostrare che n è uno pseudoprimo in base ab e ab^{-1} (inverso $\pmod n$).
   - Sia n uno pseudoprimo di Eulero in base a e in base b, con $(a, n) = (b, n) = 1$. Mostrare che n è uno pseudoprimo di Eulero in base ab e ab^{-1} (inverso $\pmod n$).

4. Sia $n = p_1 \dots p_s$ prodotto di primi distinti. Provare che n è un numero di Carmichael se e solo se $p - 1 | n - 1$ per ogni p divisore primo di n.

5. Sia p un primo dispari, $a, b \in \mathbb{Z}$. Mostrare che
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

6. Caratterizzare i primi dispari p tali che 5 sia un quadrato $\pmod p$.

7. Calcolare i seguenti simboli di Legrendre/Jacobi:
$$\left(\frac{273}{507}\right), \quad \left(\frac{751}{993}\right), \quad \left(\frac{2027}{5103}\right).$$

8. Applicare il test di Solovay-Strassen agli interi $n_1 = 123$ e $n_2 = 73$.

9. Considerando una versione di RSA con $N = 667$ e esponente di cifratura $e = 15$, determinare l'esponente di decifratura d, cifrare il messaggio $x = 20$.