**Università degli Studi Roma Tre**
**Corso di Studi in Matematica**
**CR410 Crittografia a chiave pubblica**
**Esercizi**
**Foglio 2**

1. Sia $k$ un intero positivo: dimostrare che se $2^k + 1$ è primo allora $k$ è una potenza di due, e che se $2^k - 1$ è primo, allora $k$ è primo. Cosa possiamo dire di $a^k + 1$ e $a^k - 1$, con $a > 2$ intero?

2. Dimostrare che se $n$ è prodotto di due primi distinti, la conoscenza di $\varphi(n)$ equivale alla conoscenza dei due fattori primi di $n$.

3. Motrare che per i numeri di Fermat $F_n = 2^{2^n} + 1$ vale

$$F_n - 2 = \prod_{i=0}^{n-1} F_i.$$

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

4. Fattorizzare senza usare la calcolatrice il numero 16383.
   (Sugg: chiaramente è un multiplo di 3, ma osservate che $2^{14} = 16384$.)

5. - 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 $\pmod n$).

6. 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 $n$.

7. Sia $p$ un primo dispari, $a, b \in \mathbb{Z}$. Mostrare che

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

8. Caratterizzare i primi dispari $p$ tali che -3 sia un quadrato $\pmod p$.

9. Calcolare i seguenti simboli di Legendre/Jacobi:

$$\left(\frac{273}{507}\right), \quad \left(\frac{751}{993}\right), \quad \left(\frac{2027}{5103}\right).$$

10. Sia $n$ un intero positivo dispari di lunghezza $k$, e $1 \leq a < n$. Stimare la complessità computazionale del calcolo del simbolo di Jacobi $(\frac{a}{n})$.

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

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