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. Scrivere il proprio nome anche nell'ultima pagina.* Ogni esercizio vale 3 punti.

(1) Sia m un intero dispari. Dopo aver dimostrato che ammette soluzione, si stimi il numero di operazioni bit necessarie a risolvere il seguente sistema

$$\begin{cases} X \equiv 1 \bmod m \\ X \equiv 2 \bmod m+1 \\ X \equiv 3 \bmod m+2. \end{cases}$$

(2) Si descriva un'algoritmo per calcolare $[\sqrt{m}]$, dove $m \in \mathbf{N}$ in tempo polinomiale

(3) Si descrivano i valori di $a \in \mathbf{F}_p$ per cui $x^2 + a \in \mathbf{F}_p[x]$ è irriducibile e si dimostri che non è mai primitivo.

(4) Si dimostri che se m è un intero dispari composto, allora esiste sempre un base $a \in U(\mathbf{Z}/m\mathbf{Z})$ rispetto a cui m non è pseudo primo di Eulero. Quale è l'applicazione di questa proprietà nei test di primalità?

(5) Fattorizzare $f(x) = (x^{12}+3x^4+1)(x^2+x+2)(x^{10}+x^2+1)$ su $\mathbf{F}_2$ e determinare il numero di elementi del campo di spezzamento di f.

(6) Spiegare il funzionamento del crittosistema RSA e simularne un'applicazione con un modulo RSA di esattamente tre cifre.

(7) Dopo aver verificato che si tratta di una curva ellittica, determinare l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_{11}$

$$E : y^2 = x^3 - 1.$$

Quale è l'ordine del punto $(5, 5)$ in $E(\mathbf{F}_{11})$?

(8) Siano m, n interi tali che $m \equiv 3 \bmod 4$, che $m \equiv 2 \bmod n$ e che $n \equiv 1 \bmod 8$. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{(5m+n)^3}{m}\right)$.

(9) Si scriva un programma Pari che implementi il metodo di fattorizzazione di Pollard.

(10) Scrivere un programma in pari che verifichi se un numero n di cui è nota la fattorizzazione in primi ($n = p_1 \cdots p_t$) è o meno un numero di Carmichael.

NOME E COGNOME	1	2	3	4	5	6	7	8	9	10	TOTALE
.....											