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) Si dia una stima (in funzione del parametro t) per il numero di operazioni bit necessarie al calcolo del determinante di una matrice 3×3 a coefficienti interi in cui gli elementi della prima colonna sono in valore assoluto minori di t, quelli della seconda colonna sono in valore assoluto minori di e^t e quelli della terza sono in valore assoluto minori di t^t.

(2) Si descriva un'algoritmo per calcolare in tempo polinomiale $2^m \pmod{m+1}$. Si stimi anche il numero di operazioni bit necessarie.

(3) Si enunci e dimostri la formula per il numero di polinomi irriducibili di grado 8 su $\mathbf{F}_p$. Quale è la probabilità che un polinomio di grado 4 monico su $\mathbf{F}_3$ e che non ammette zeri in $\mathbf{F}_3$ risulti irriducubile su $\mathbf{F}_3$?

(4) Descrivere il test di primalità di Miller Rabin spiegandone gli aspetti probabilistici.

(5) Si descrivano gli ordini degli elementi del campo di spezzamento del polinomio $x^4 + x + 1$ su $\mathbf{F}_2$.

(6) Spiegare il funzionamento del crittosistema Massey–Omura e simularne un'applicazione in un campo con 32 elementi.

(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 $\mathbf{F}_7$

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

determinando l'ordine di ciascun punto.

(8) Sia m un intero tale che $m \equiv 17 \bmod 28$. Si calcoli (se è ben definito) il seguente simbolo di Jacobi: $\left(\frac{5m+7}{m^5}\right)$.

(9) Si scriva un programma Pari che verifichi se un polinomio di grado 3 a coefficienti in $\mathbf{F}_5$ è o meno primitivo.

(10) Scrivere un programma in pari che implementi il metodo di fattorizzazione ρ di Pollard.

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