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 stimi il numero di operazioni bit necessarie a calcolare l'integrale a di un polinomio di grado n in cui tutti i coefficienti sono minori di e^n.

2. Si risolva il seguente sistema di equazioni di congruenze

$$\begin{cases} x^2 \equiv 4 \bmod 11 \\ x^3 \equiv 2 \bmod 5 \end{cases}.$$

3. Quale è la probabilità che un polinomio irriducibile f di grado 6 su $\mathbf{F}_{11}$ risulti primitivo?

4. Si illustri la nozione di pseudo primo forte e se ne indichi l' applicazione in crittografia.

5. Fattorizzare $f(x) = (x^{14} + 3x^7 + 1)(x^2 + 2)(x^2 + 1)$ su $\mathbf{F}_7$ e dopo aver fissato un campo di spezzamento $\mathbf{F}$ per f, si scrivano tutte le radici di $f(x)$ in $\mathbf{F}$.

6. Spiegare il funzionamento del metodo dello scambio delle chiavi Diffie–Hellman e simularne un applicazione in un campo finito con 19 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 $\mathbf{F}_5$

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

8. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{983932}{72637}\right)$.

9. Scrivere in una sola riga il codice (in PARI) per ottenere:
   a Numero di cifre decimali di x;
   b Il resto della divisione euclidea di a per b;
   c Un più piccolo numero primo con 100 cifre binarie.

10. Scrivere un programma in PARI per ottenere un vettore contenente i numeri minori di 10^{20} che sono pseudoprimi di Eulero, per almeno una base random.

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