COGNOME ..... *NOME* ..... *MATRICOLA* .....

Risolvere il massimo numero di 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.* 1 Esercizio = 3 punti. Tempo previsto: 2 ore. Nessuna domanda durante la prima ora e durante gli ultimi 20 minuti.

FIRMA	1	2	3	4	5	6	7	8	9	10	
.....											

1. Si descrivano le complessità delle operazioni elementari tra interi.

2. Descrivere l'algoritmo dei quadrati successivi in un qualsiasi monoide moltiplicativo discutendone la complessità.

3. Dimostrare che il gruppo moltiplicativo di un campo finito è ciclico.

4. Dopo aver descritto la nozione di base forte, si dimostri che tutte le basi modulo un primo sono forti e si fornisca un esempio di un numero composto e di una sua base forte (non banale cioè diversa da -1).

5. Si descriva e si dimostri il Teorema Cinese dei resti discutendo in particolare l'analisi della complessità per determinare le soluzioni di un sistema di congruenze.

6. Si descriva il reticolo dei sottocampi di $\mathbf{F}_{2^6}$ e per ciascun sottocampo proprio, si elenchino i polinomi irriducibili e quelli primitivi.

7. Determinare i polinomi minimi e gli ordini degli elementi di $\mathbf{F}_9$.

8. Fornite un esempio di curva ellittica definita su un campo con 25 elementi per cui $E(\mathbf{F}_{25}$ non è ciclico.

9. Sia $E : y^2 = x^3 5x + 8$ e siano $P = (6, 3), Q = (9, 10) \in E(\mathbf{F}_{101})$. Calcolare $2P$ e $P + Q$.

10. Spiegare il funzionamento di tutti i protocolli crittografici incontrati nel corso.