Cognome ..... *Nome* ..... *Matricola* .....

Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* 1 Eesrcizio = 4 punti. Tempo previsto: 2 ore. Nessuna domanda durante le prima ora e durante gli ultimi 20 minuti.

1	2	3	4	5	6	7	8	TOT.

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:

   a. Esistono campi finiti con 48 elementi?

   .....

   b. E' vero che non esistono identità di Bezout con coefficienti a segno discorde?

   .....

   c. Fornire un esempio di campi finiti diversi con 16 elementi.

   .....

   d. Scrivere tutti i polinomi primitivi in $\mathbf{F}_2[x]$ di grado minore uguale a 4.

   .....

2. Enunciare e dimostrare il Teorema di struttura dei sottocampi di $\mathbf{F}_{p^n}$. Lo si utilizzi per costruire un esempio di campo finito con esattamente 6 sottocampi.

3. Determinare tutti le radici primitive di $\mathbf{F}_5[\tau], \tau^2 = 2$.

4. Spiegare il funzionamento di alcuni sistemi crittografici che basano la propria sicurezza sul problema del logaritmo discreto.

5. Spiegare in dettaglio if funzionamento dell'Algoritmo Pohlig–Hellman.

6. Si applichi l'algoritmo delle approssimazioni successive per calcolare la parte intera del numero binario $\sqrt{101011101}$

7. Si determini il grado del campo di spezzamento su $\mathbf{F}_3$ del sequente polinomio $(x^{3^{11}} + 6x - x^9 + 30)(x^6 + 1)(x^9 + 15x - 1)$

8. Calcolare il massimo comun divisore $\gcd(273, 130)$ utilizzando sia l'algoritmo binario che quello esteso di Euclide. Utilizzare l'algoritmo di Euclide anche per calcolare un identità di Bezout.