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 = 4.5 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. Fornire un esempio di un'equazione di Weierstrass singolare.

   .....

   b. E' vero che in alcuni gruppi ciclici il logaritmo discreto è particolarmente facile da calcolare?

   .....

   c. Fornire due esempi di campi finiti $\mathbf{F}_q$ in cui tutti gli elementi di $\mathbf{F}_q^* \setminus \{1\}$ sono generatori.

   .....

   d. Fornire un esempio di un polinomio primitivo in un campo con 9 elementi.

   .....

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 5 sottocampi.

3. Supponiamo che n, m siano interi, che $m \equiv 5 \bmod 4n$, che $n \equiv 7 \bmod 10$. Calcolare il simbolo di Jacobi $\left(\frac{n}{m}\right)$.

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

5. Spiegare la rilevanza del metodo Baby-Steps-Giant-Steps nella teoria delle curve ellittiche su campi finiti.

6. Sia $E : y^2 = x^3 - x$. Determinare la struttura del gruppo $E(\mathbf{F}_5)$ e calcolare $\#E(\mathbf{F}_{125})$. E' possibile determinare anche la struttura di $E(\mathbf{F}_{125})$?

7. Dimostrare che se E è una curva ellittica definita su un campo finito $\mathbf{F}_q$ con caratteristica dispari da un'equazione $y^2 = x^3 + a_2x^2 + a_4x + a_6$, allora i punti di ordine 2 hanno la forma $(\alpha, 0)$ dove $\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6 = 0$. Si forniscano esempi di curve ellittiche con 0, 1 e 3 punti di ordine 2 e si spieghi percè non è possibilie che ve ne siano 2.

8. Scrivere e dimostrare le formula per l'inverso $-P$ e per il punto $2P$ del punto $P(x, y) \in E(\mathbf{F}_q)$ dove E è una curva ellittica definita da una equazione di Weierstrass generale.