

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

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

1	2	3	4	5	6	7	8	9	TOT.

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

a. E' vero che se  $E$  è una curva ellittica definita su  $\mathbf{F}_{3^n}$ , allora non ha mai un equazione della forma  $y^2 = x^3 + ax + b$ ?

.....

b. E' vero che se tutti i fattori primi di  $n - 1$  sono più piccoli di  $\log n$ , allora è possibile determinare un fattore non banale di  $n$  in modo rapido? come?

.....

c. E' vero che se  $p > 3$ , il polinomio  $X^2 + 1 \in \mathbf{F}_p$  non è mai primitivo ma qualche volta è irriducibile?

.....

d. E' vero che esistono modi per moltiplicare interi con complessità inferiore a quella quadratica?

.....

2 Se  $n \in \mathbf{N}$ , sia  $\sigma(n)$  la somma dei divisori di  $n$ . Supponiamo che sia nota la fattorizzazione (unica) di  $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ . Calcolare il numero di operazioni bit necessarie per calcolare  $\sigma(n)$ . (*Suggerimento: Usare il fatto che  $\sigma$  è una funzione moltiplicativa e calcolare una formula per  $\sigma(p^\alpha)$ ).*

3. Siano  $m, n$  interi tali che  $m \equiv 3 \pmod{4}$ , che  $m \equiv 2 \pmod{n}$  e che  $n \equiv 1 \pmod{8}$ . Si calcoli il seguente simbolo di Jacobi:  
$$\left( \frac{(5m+n)^3}{m} \right).$$

4. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. Considerare la curva ellittica  $E: y^2 = x^3 - x$ . Illustrare l'algoritmo appena descritto calcolando  $[5](1,0)$  dove  $(1,0) \in E(\mathbf{F}_{13})$ .

5. Si dia la definizione di pseudo primo forte in base 2 e si mostri che se  $n = 2^\alpha + 1$  è pseudo primo forte in base 2, allora  $2^{2^\beta} \equiv -1 \pmod{n}$  per qualche  $\beta < \alpha$ .
6. Fissare una radice primitiva di  $\mathbf{F}_{33}$  ed utilizzarla per simulare un scambio chiavi alla Diffie–Hellmann.
7. Dopo aver definito la nozione di polinomio primitivo su un campo finito, si calcoli la probabilità che un polinomio irriducibile  $f$  di grado 8 su  $\mathbf{F}_7$  risulti primitivo?.

8. Fattorizzare  $f(x) = (x^{12} + 3x^4 + 1)(x^2 + x + 2)(x^{10} + x^2 + 1)$  su  $\mathbf{F}_2$  e determinare il numero di elementi del campo di spezzamento di  $f$ .

9. Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la risposta) l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su  $\mathbf{F}_7$

$$y^2 = x^3 - x + 5.$$