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. 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 σ è una funzione moltiplicativa e calcolare una formula per $\sigma(p^\alpha)$*)

2. Mostrare che le moltiplicazioni nell'anello quoziente $\mathbf{Z}/n\mathbf{Z}[x]/(x^d)$ si possono calcolare in $\mathrm{O}(\log^2 n^d)$ operazioni bit mentre le addizioni in $\mathrm{O}(\log n^d)$ operazioni bit.

3. Dato il numero binario $n = (10011100101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

4. Calcolare il massimo comun divisore tra 240 e 180 utilizzando sia l'algoritmo euclideo che quello binario. Calcolare anche l'identità di Bezout.

5. Dimostrare che se $n = p_1 \cdots p_{20}$ è un intero privo di fattori quadratici, e $f(x) \in \mathbf{Z}/n\mathbf{Z}[x]$ ha grado 10, allora la congruenza $f(x) \equiv 0 \bmod n$ è risolvibile se e solo se lo sono le 20 congruenze $\begin{cases} f(x) \equiv 0 \bmod p_1 \\ \vdots \\ f(x) \equiv 0 \bmod p_{20}. \end{cases}$ Dedurre che la prima congruenza $f(x) \equiv 0 \bmod n$ ha al più 10^{20} soluzioni. Sapreste dare un esempio in cui le soluzioni sono esattamente 10^{20}?

6. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. Fare anche un esempio.

7. Mettere in ordine di priorità e spiegare il significato di ciascuna delle seguenti operazioni:

$$x\sim \qquad x \wedge y \qquad x\&y \qquad x{+}{+} \qquad x\backslash y \qquad x = y \qquad x\%y \qquad x|y \qquad x \ll n$$

8. 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 $2^{2^\beta} \equiv -1 \bmod n$ per qualche $\beta < \alpha$.

9. Scrivere un programma in Pari che produca due vettori v e w. In cui v contiene i primi 100 *pseudo-primi composti* in base 2 e il secondo i primi 100 *pseudo primi di Eulero composti* in base 2.

10. Implementare RSA utilizzando il sistema Pari e creando tre funzioni distinte (una per generare le chiavi, una per cifrare e una per decifrare).

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