

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.

1. Se $n \in \mathbf{N}$, sia $\varphi(n)$ la funzione di Eulero. Supponiamo che sia nota la fattorizzazione (unica) di $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Stimare il numero di operazioni bit necessarie per calcolare $\varphi(n)$.

2. Stimare in termini di k il numero di operazioni bit necessarie per calcolare $\left[\sqrt{2^{k^k} \bmod 3^k} \right]$.

3. Dato il numero binario $n = (111001011101)_2$, calcolare $\lceil \sqrt{n} \rceil$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

4. Calcolare il massimo comun divisore tra 1235 e 1800 utilizzando l'algoritmo binario.

5. Calcolare tutte le soluzioni in $[-300, 200]$, del sistema di congruenze $\begin{cases} x^3 \equiv 1 \pmod{5} \\ x^4 \equiv 1 \pmod{8} \end{cases}$?

6. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. $b = 2^4 + 2^2 + 1$, quante moltiplicazioni in $\mathbf{Z}/m\mathbf{Z}$ sono necessarie per calcolare $2^b \pmod{m}$?

10. Definire un sistema di chiavi rsa in modo tale che: i) l'esponente di cifratura sia 5; ii) Sia possibile spedire messaggi con pacchetti di 3 lettere alla volta.

11. Calcololare il seguente simbolo di Jacobi senza fattorizzare: $\left(\frac{22348}{65431}\right)$.

12. Definire le nozioni di pseudo primo, pseudo primo di Eulero e pseudo primo forte. E spiegare le connessioni tra le tre nozioni.

13. Carlo scopre il valore di $\varphi(n)$ dove n è il modulo RSA che Alice e Bernardo stanno usando per comunicare. Come può usare questa informazione per decifrare i messaggi?

