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.* Ogni esercizio vale 7.5 punti.

1. Fattorizzare $5^{24} - 1$ giustificando attentamente tutti i calcoli.

2. Sia $n = 1042387$. Usare il fatto che

$$1021^2 \equiv 54 \bmod n, \quad 1027^2 \equiv 12342 \bmod n, \quad 1030^2 \equiv 18513 \bmod n$$

per trovare un fattore proprio di n.

3. Dimostrare che, se $2^m + 1$ è primo, allora $m = 2^\alpha$, ovvero è una potenza di due. Dare un esempio di α per cui $2^{2^\alpha} + 1$ non è primo.

---

4. Mostrare che un polinomio di grado tre a coefficienti in un campo è irriducibile se e solo se non ha radici nel campo.

---

3. (Quickies): Scrivere **solo** la risposta delle seguenti domande:
   i. Quali tra i seguenti valori sono fattori di $50000^{111} - 50000$?

$$500,\ 541,\ 1111,\ 49999,\ 9,\ 5^5.$$

   ii. Quale è un valore di B per cui il metodo $p-1$ con parametro B fattorizza 47053?

---

i.
ii.