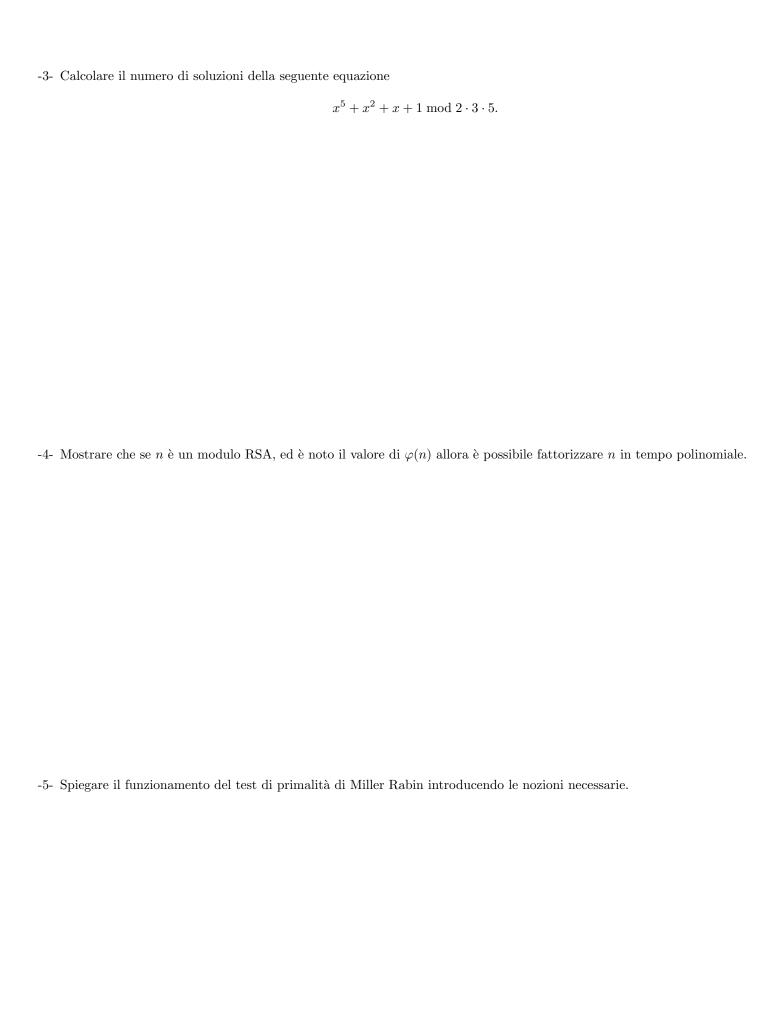
Risolvere il massimo numero di esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Scrivere il proprio nome anche nell'ultima pagina. 1 Esercizio = 4 punti. Tempo previsto: 2 ore. Nessuna domanda durante la prima ora e durante gli ultimi 20 minuti.

FIRMA	1	2	3	4	5	6	7	8	9	TOT.

-1- Determinare una stima per il numero di operazioni bit necessarie a moltiplicare due matrici  $n \times n$  i cui coefficienti sono minori di  $e^n$ .

-2- Descrivere un algoritmo per calcolare i massimo comun divisore di due interi e descriverne la complessità.



-6-	Calcolare la probabilità che un polinirriducibile e non primitivo.	omio irriducibile di gr	ado 11 su ${f F}_7$ risulti p	rimitivo. Dare un es	sempio di polinomio
-7-	Simulare uno scambio delle chiavi all $polinomio\ x^2+1$	a Diffie–Hellmann in u	n campo finito con 49	elementi $su$	ggerimento: Usare il

-8- Enunciare l'algoritmo Pohlig-Hellmann per calcolare i logaritmi discreti in un gruppo ciclico f	inito dimostrandone la validità.
-9- Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la rispo gruppo dei punti razionali della curva ellittica su ${\bf F}_7$ $y^2=x^3+x+1.$	sta) l'ordine e la struttura del