vale 3 punti.

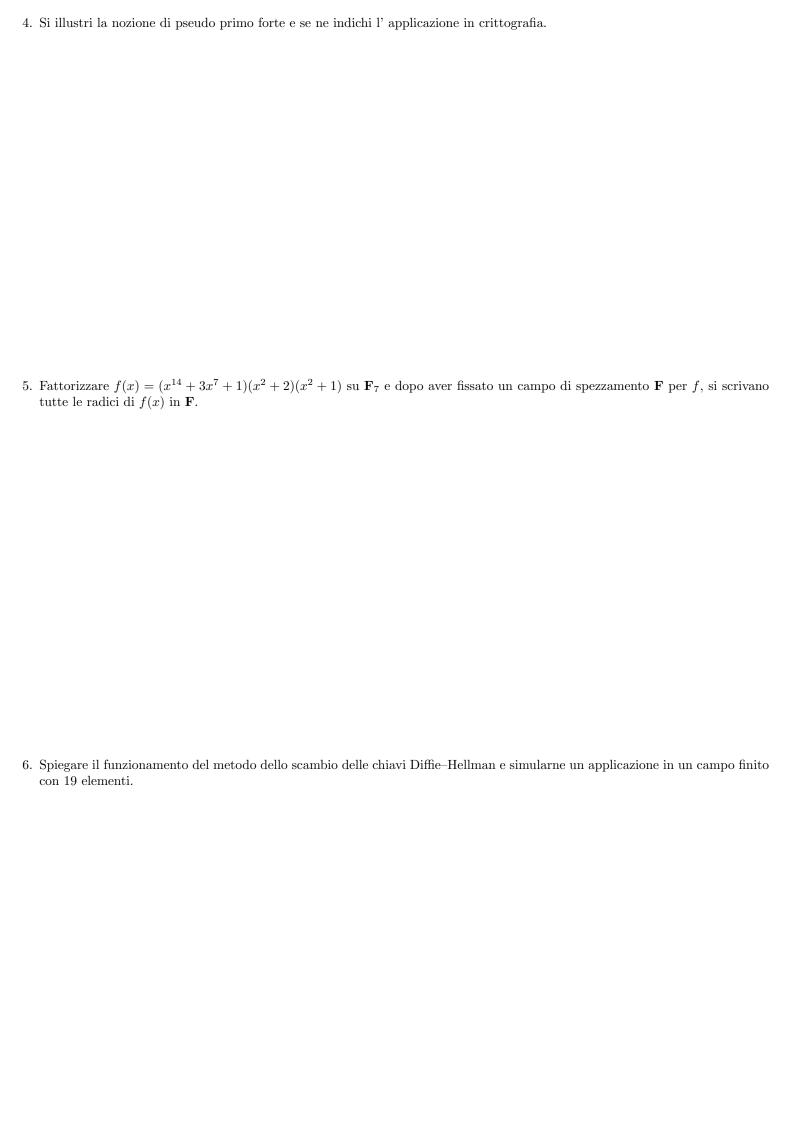
1. Si stimi il numero di operazioni bit necessarie a calcolare l'integrale a di un polinomio di grado n in cui tutti i coefficienti sono

1. Si stimi il numero di operazioni bit necessarie a calcolare l'integrale a di un polinomio di grado n in cui tutti i coefficienti sono minori di e^n .

2. Si risolva il seguente sistema di equazioni di congruenze

$$\begin{cases} x^2 \equiv 4 \bmod 11 \\ x^3 \equiv 2 \bmod 5 \end{cases}.$$

3. Quale è la probabilità che un polinomio irriducibile f di grado 6 su \mathbf{F}_{11} risulti primitivo?



7. Dopo aver verificato che si tratta di una curva el	tica, determinare l'ordine e la struttura del gruppo dei punti razionali	i della
curva ellittica su \mathbf{F}_5		

$$y^2 = x^3 - x + 1.$$

8. Si calcoli il seguente simbolo di Jacobi: $\binom{983932}{72637}.$

9. Scrivere in una sola riga il codice (in PARI) per ottenere: a Numero di cifre decimali di x; b Il resto della divisione euclidea di a per b; c Un più piccolo numero primo con 100 cifre binarie.

10. Scrivere un programma per almeno una base rai	in PARI	per otte	nere un	vettore c	ontenent	e i nume	ri minor	i di 10 ²⁰	che sono	o pseudop	rimi di Eulero,
NOME E COGNOME	1		3	4	5	6	7	8	9	10	TOTALE
TOTAL L COUTOME	1						'		<u>.</u>	10	10111111