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.

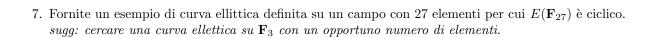
FIRMA	1	2	3	4	5	6	7	8	TOT

1. Dimostrare che se p è primo, allora  $x^5 \equiv 1 \mod p$  ammette  $\gcd(p-1,5)$  soluzioni. Determinare un valore di m tale che  $X^5 \equiv 1 \mod m$  ammette esattamente 25 soluzioni modulo m.

2. Dopo aver spiegato il funzionamento dei sistemi crittografici che usano i logaritmi discreti, si illustri il funzionamento di ElGamal utilizzando come gruppo  $\mathbf{F}_{16}^*$ .

2	Descrivoro l'algoritmo dei e	uadrati successivi in r	un qualciaci monoido moltin	licativo discutendone la complessità.	
J.	Descrivere i algoritmo dei q	uadran successivi in t	m quaisiasi monoide morup	ncativo discutendone la complessita.	
		(077.40)			
4.	Calcolare il simbolo di Lege	endre $\left(\frac{97543}{21345}\right)$ utilizzan	do le propritetà dei simboli	di Jacobi e giustificando ogni passag	gio.
4.	Calcolare il simbolo di Lege	endre $\left(\frac{97543}{21345}\right)$ utilizzan	do le propritetà dei simboli	di Jacobi e giustificando ogni passag	ggio.
4.	Calcolare il simbolo di Lege	endre $\left(\frac{97543}{21345}\right)$ utilizzan	do le propritetà dei simboli	di Jacobi e giustificando ogni passag	ggio.
4.	Calcolare il simbolo di Lege	endre $\left(\frac{97543}{21345}\right)$ utilizzan	do le propritetà dei simboli	di Jacobi e giustificando ogni passag	ggio.
4.	Calcolare il simbolo di Lege	endre $\left(\frac{97543}{21345}\right)$ utilizzan	do le propritetà dei simboli	di Jacobi e giustificando ogni passag	gio.
4.	Calcolare il simbolo di Lege	endre $\left(\frac{97543}{21345}\right)$ utilizzan	do le propritetà dei simboli	di Jacobi e giustificando ogni passag	ggio.

5. Dopo aver definito la nozione di pseudo primo forte, si illustri come utilizzarla per scrivere un test di primalità probabilistico
6. Si determini la probabilità che un polinomio irriducibile su ${\bf F}_7$ di grado 6 risulti primitivo.



8. Sia  $E: y^2 = x^3 + x$ , Dimostrare che se  $p \equiv 1 \mod 4$  allora il gruppo  $E(\mathbf{F}_p)$  non è ciclico. Determinare tale gruppo nel caso in cui p = 5.