				- ~	\sim
A	PΡ	' H'I	٠,	.(()

Roma, 30 GENNAIO 2015

<i>COGNOME</i>	<i>NOME</i>	MATRICOLA	
Pigolyoro il maggimo numoro d	i osorajzi nagomnognondo lo rignosto	aon aniogazioni chiara ad agganziali	Incomire la rienasta nos

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.

FIRMA	1	2	3	4	5	6	7	8	9	10	

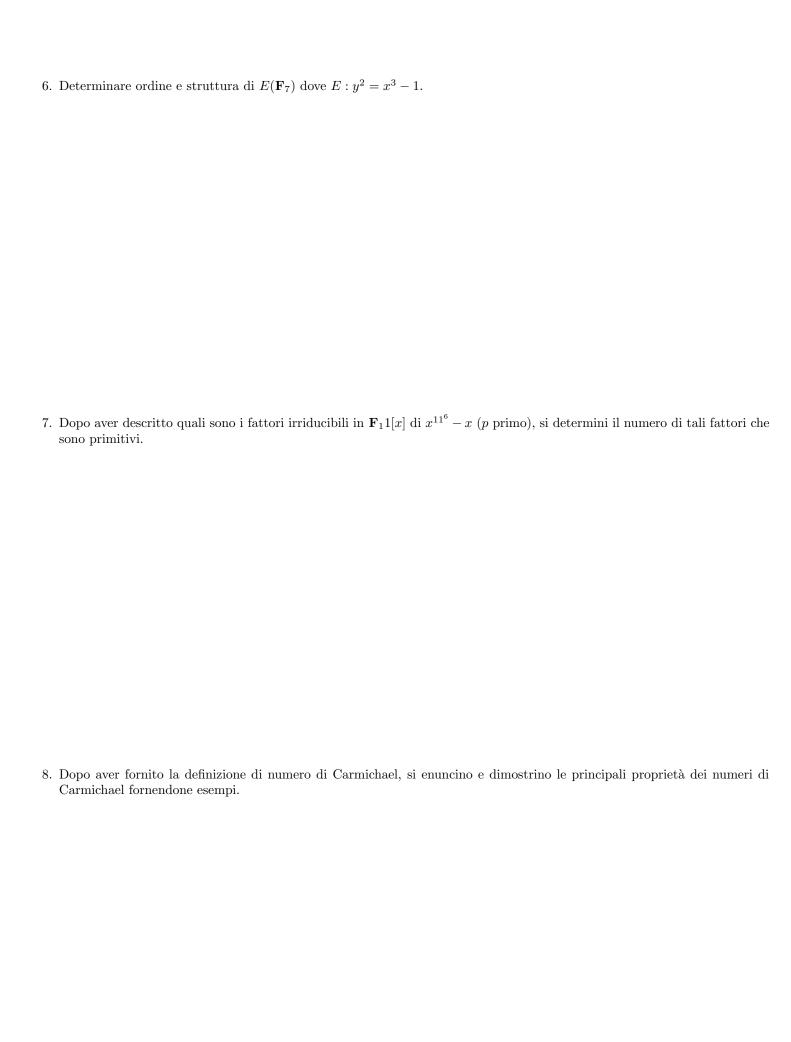
⁻ Si descrivano:

-2- Gli algoritmi per la moltiplicazione degli interi a la loro complessità;

-3- L'algoritmo Baby Steps Giant Steps per il calcolo dell'ordine di una curva ellittica su un campo finito;

⁻¹⁻ L'algoritmo di Euclide (per l'identit'a di Bezout) e suo il tempo di esecuzione.;

-4- L'algorimo di Pholig-E	Hellman per il calcolo dei logaritmi discreti;	
-5- La varie definizioni di j	pseudo primi e le loro principali proprietà.	



9. Dimostrare che su ${f F}_q, q$ dispari, c'è sempre una curva ellittica con gruppo dei punti razionali non cicli	ico.
0. Si descrivano i principali algoritmi di cifratura e decifratura.	