CR410 AA12	2/13 (	(Crittografia	1)
------------	--------	---------------	----

## APPELLO A

Roma, 7 GIUGNO 2013.

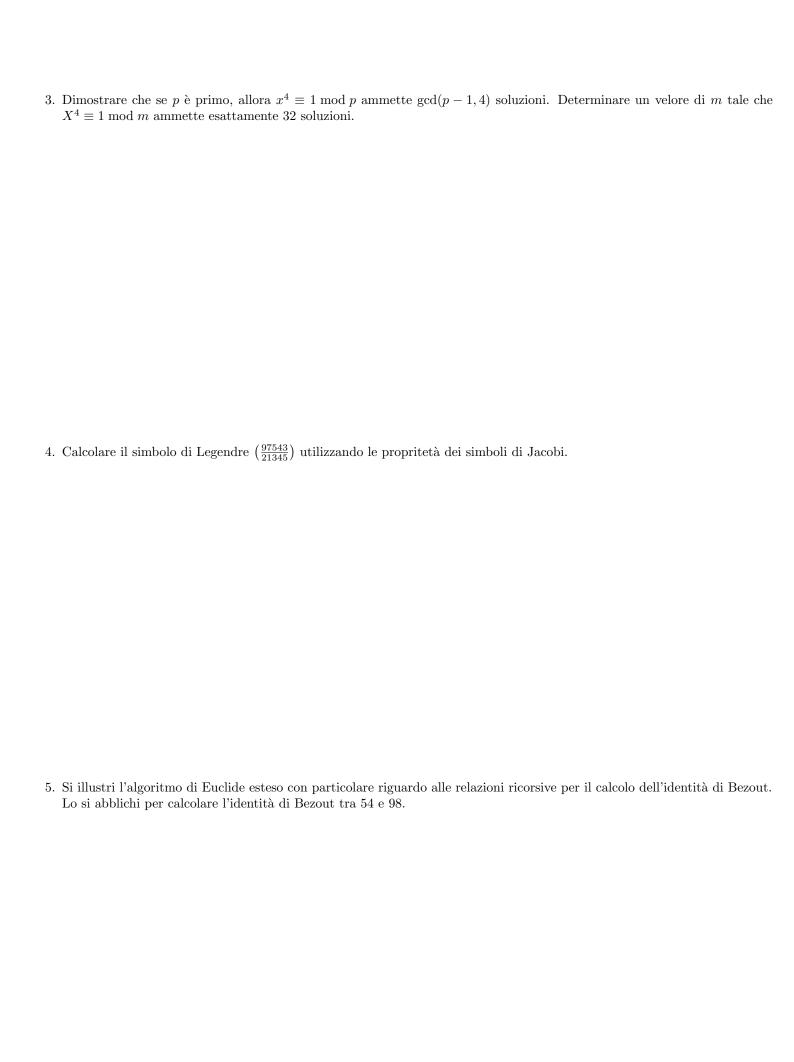
<i>COGNOME</i>	NOME	MATRICOLA
COGNOME	TVOWE	. MAIMOODA

Risolvere il massimo numero di esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. Inserire le risposte negli spazi predisposti.  $NON\ SI\ ACCETTANO\ RISPOSTE\ SCRITTE\ SU\ ALTRI\ FOGLI.\ Scrivere\ il\ proprio\ nome\ anche\ nell'ultima\ pagina.\ 1\ Esercizio = 3\ punti.\ Tempo\ previsto:\ 2\ ore.\ Nessuna\ domanda\ durante\ la\ prima\ ora\ e\ durante\ gli\ ultimi\ 20\ minuti.$ 

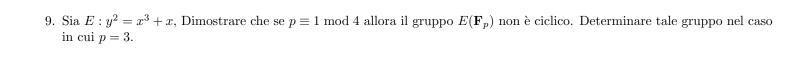
FIRMA	1	2	3	4	5	6	7	8	9	10	

1. Si descriva un algoritmo per calcolare in tempo polinomiale la parte intera di  $m^{1/5}$  per ogni intero positivo m.

2. Descrivere l'algoritmo di moltiplicazione di Karatsuba.







10. Spiegare il funzionamento di tutti i protocolli crittografici incontrati nel corso.