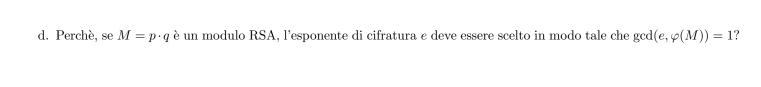
| <i>Cognome</i> | Nome | | atricola | |
|--------------------------|---|------------------------|-------------------------|-----------------------|
| Risolvere il massimo num | ero di esercizi fornendo spiegazioni chia | re e sintetiche. it Ir | nserire le risposte neg | li spazi predisposti. |
| NON SI ACCETTANO I | RISPOSTE SCRITTE SU ALTRI FOG | LI. 1 Eesrcizio = 4 | punti. Tempo previst | to: 2 ore. Nessuna |
| domanda durante le prim | a ora e durante gli ultimi 20 minuti. | | | |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | TOT. |
|---|---|---|---|---|---|---|---|---|------|
| | | | | | | | | | |
| | | | | | | | | | |

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:

| b. È vero che $X^{97} - X + 3$ non ha radici monulo 97? | |
|---|--|
| | |
| | |

| c. | Quanti sono i polinomi primitivi di grado 7 su \mathbf{F}_7 ? |
|----|---|
| | |
| | |
| | |





| 5. Si illustri il funzionamento del metodo di fattorizzazione ρ di Pollard. |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| 6. Dopo aver descritto il crittosistema ElGamal su \mathbf{F}_p , se ne illustri il funzionamento con un esempio con $p=29$. |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| 7. Realizzare il campo ${\bf F}_{25}$ e determinare l'ordine di tutti i suoi elementi. |
| 7. Realizzare il campo r 25 e determinare i ordine di tutti i suoi elementi. |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

| 8. Data una curva ellittica E , definita su \mathbf{F}_p , si spieghi il metodo per calcolare l'ordine del gruppo $E(\mathbf{F}_{p^{100}})$. |
|--|
| |
| |
| |
| |
| |
| 9. Dopo aver dimostrato che è una curva ellittica su \mathbf{F}_7 , calcolare la struttura del gruppo dei punti razionali di $y^2 = x^3 + x + x^2$ |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

.