COGNOME*NOME*Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche*.NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. Sia N un intero di 100 cifre e sia $A = 10^{20}$.
 - (a) Quanti numeri primi ci sono approssimativamente nell'intervallo $[N - A, N + A]$?
 - (b) Quanti numeri B -smooth ci sono approssimativamente nell'intervallo $[N - A, N + A]$, se $B = 1000000$? e se $B = 2000000$?

2. Sia data la curva $E : Y^2 = X^3 + 3$.
- (a) Verificare che E definisce una curva ellittica su $\mathbf{Z}_7$.
 - (b) Determinare tutti i punti di $E(\mathbf{Z}_7)$.
 - (c) Sia $P = (1, 2) \in E(\mathbf{Z}_7)$. Calcolare $2P$ e $-P$.
 - (d) Determinare la struttura del gruppo $(E(\mathbf{Z}_7), +)$.

3. (a) Determinare la più piccola radice primitiva $\bar{g}$ di $\mathbf{Z}_{37}$.
(b) Quante radici primitive ci sono in $\mathbf{Z}_{37}$?
(c) Calcolare $\log_{\bar{g}} \overline{15}$, dove $\bar{g}$ è la radice primitiva ottenuta in (a).

4. Sia N un intero di 300 cifre. Supponiamo che dopo 10^{10} iterate dell'algoritmo ρ di Pollard non abbiamo individuato alcun fattore non banale di N . Cosa possiamo verosimilmente concludere sui fattori di N ?

5. Sia E una curva ellittica sul campo $\mathbf{Z}_{101}$. Supponiamo che $E(\mathbf{Z}_{101})$ contenga un elemento P di ordine 31.

- (a) Qual è la cardinalità del gruppo $E(\mathbf{Z}_{101})$?
- (b) Qual è la struttura del gruppo $E(\mathbf{Z}_{101})$?