COGNOME .... *NOME* .... *MATRICOLA* ....

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.

1. Si determinino tutte le soluzioni intere della seguente equazione: $2X + 3Y + 5Z = 100$.

2. Per quali valori del parametro λ il seguente sistema di congruenze ammette un unica soluzione? $\begin{cases} 2x - 4y \equiv 0 \bmod 7 \\ 3x + \lambda^2 y \equiv 1 \bmod 7. \end{cases}$

3. Dimostrare il piccolo Teorema di Fermat.

4. Dimostrare che per ogni primo p la seguente congruenza è verificata: $(p-4)! \equiv 6^* \bmod p$ dove 6^* è l'inverso aritmetico modulo p.

5. Calcolare il numero delle soluzioni modulo 125 della seguente congruenza polinomiale: $X^3 - 11X^2 + 24X - 14 \equiv 0 \bmod 125$.

6. Calcolare le soluzioni del sistema di congruenze: $\begin{cases} X \equiv 4 \bmod 5 \\ X \equiv 3 \bmod 7 \end{cases}$ nell'intervallo $[100, 250]$.

7. Si enunci il Teorema del sollevamento per soluzioni di congruenze polinomiali.

8. Sia p un primo dispari tale che $q = 2p + 1$ è anche primo. Mostrare che se un intero a, $2 \leq a \leq p - 2$ è tale che $a^p \equiv -1 \bmod q$ se e solo se a è una radice primitiva modulo q.

9. Quante e quali soluzioni ha la congruenza $X^{15} \equiv 5 \bmod 93$? *Suggerimento: lavorare modulo primi*

10. Mostrare direttamente che non esiste una radice primitiva modulo 24.

11. Illustrare l'algoritmo di Gauss per il calcolo di una radice primitiva.

12. Usare una radice primitiva per mostrare che se p è primo e m è un intero, allora

$$1^m + 2^m + \cdots + (p-1)^m \equiv \begin{cases} 0 \bmod p & \text{se } (p-1) \nmid m \\ -1 \bmod p & \text{se } p-1 \mid m. \end{cases}$$