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. Costruire tutte le soluzione dell'equazione diofantea $3X + 9Y + 6Z = -6$.
2. Mostrare che se $a \in \mathbf{Z}$, $m_1, m_2, n \in \mathbf{N}$ sono tali che $m_1 \equiv m_2 (\mathrm{mod} \varphi(n))$ e n non ha fattori quadratici, allora $a^{m_1} \equiv a^{m_2} (\mathrm{mod} n)$.
3. Determinare le soluzioni di $X^4 + 3X^2 + X \equiv 0 \bmod 9$.
4. Enunciare e dimostrare il Lemma di Gauss per il calcolo del simbolo di Legendre.
5. Dimostrare che se p e q sono primi dispari distinti, allora non esiste una radice primitiva modulo pq.
6. Determinare le soluzioni (se esistono) della congruenza polinomiale $X^4 \equiv 8 \bmod 31$.
7. Calcolare il seguente simbolo di Jacobi/Legendre: $\left(\frac{1731}{2431}\right)$.
8. Mostrare che se $n, m \in \mathbf{N}$ sono tali che $(n, m) = 1$ e se $f \in \mathbf{Z}[X]$, allora $\#\mathcal{N}(f, nm) = \#\mathcal{N}(f, n) \cdot \#\mathcal{N}(f, m)$ dove $\mathcal{N}(f, m) = \{z \in \mathbf{Z} \mid f(z) \equiv 0 (\mathrm{mod} m), z \in [0, m)\}$.
9. Enunciare e dimostrare la formula di inversione di Möbius e usarla per dimostrare che $\mu * \mathbb{1} = u$.
10. Mostrare che $x^4 + y^4 = z^2$ non ha soluzioni non banali.
11. Siano p e q primi distinti tali che $q \equiv p \equiv 1 \bmod 4$. Mostrare che l'equazione $pq = x^2 + y^2$ ammette almeno due soluzioni distinte $(x, y) \in \mathbf{N}^2$ con $x \leq y$.
12. Mostrare che se $e, k \in \mathbf{N}$, allora $4^e(7 + 8k)$ non si può scrivere come somma di tre quadrati.