H23-T1-A1

a) Seien $n \geq 1$ eine natürliche Zahl und $p \neq 2$ eine Primzahl. Zeigen Sie:

$$p|(1+2+3+\ldots+(n-1)+n) \Leftrightarrow p|n \text{ oder } p|(n+1).$$

b) Bestimmen Sie die Anzahl der Elemente der Einheitengruppe

$$(\mathbb{Z}[X]/(2, X^3+X^2+X))^*$$

des angegebenen Quotientenringes.

c) Bestimmen sie mithilfe des Chinesischen Restsatzes und unter vollständiger Angabe des Lösungsweges die kleinste natürliche Zahl $n \geq 1$, die die Kongruenzen $n \equiv 1 \mod 3, n \equiv 2 \mod 5$ und $n \equiv 0 \mod 8$ erfüllt.

Lösung

a) Wir benutzen die bekannte Gauß'sche Summenformel

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Man erhält daher $p|\sum_{k=1}^{n} k \Leftrightarrow p|\frac{n(n+1)}{2} \overset{p\neq 2}{\Leftrightarrow} p|n(n+1) \overset{\text{ggT}(n,n+1)=1}{\Leftrightarrow} p|n$ oder $p|(n+1)$.

b) Man betrachte den Ringisomorphismus (Überprüfen!)

$$\Psi : \mathbb{Z}[X]/(2, X^3+X^2+X) \to \mathbb{F}_2[X]/(X^3+X^2+X), \quad [f] \mapsto [\overline{f}] \Leftrightarrow \left[\sum_{k=0}^{n} a_k X^k\right] \mapsto \left[\sum_{k=0}^{n} \overline{a_k} X^k\right],$$

wobei $\overline{x}$ für die Klasse von x in $\mathbb{F}_2$ steht. Um nun Notation zu sparen wird der Überstrich nun weggelassen, ab sofort befinden wir uns - sofern nichts anderes behauptet wird - in $\mathbb{F}_2[X]$. Wir faktorisieren das Polynom $X^3+X^2+X = X(X^2+X^+1)$ in seine irreduziblen Faktoren in $\mathbb{F}_2[X]$. Man erhält dadurch mithilfe des Chinesischen Restsatzes folgende Isomorphie

$$\mathbb{F}_2[X]/(X^3+X^2+X) \cong \mathbb{F}_2[X]/(X) \times \mathbb{F}_2[X]/(X^2+X+1).$$

Da $\mathbb{F}_2[X] \cong \mathbb{F}_2$ und $\mathbb{F}_2[X]/(X^2+X+1) \cong \mathbb{F}_4$ hat $\mathbb{F}_2[X]/(X^3+X^2+X)$ $1 \cdot 3$ Einheiten, nach der ersten Isomorphie also $\left|(\mathbb{Z}[X]/(2, X^3+X^2+X))^*\right| = 3$.

c) Wiederum nach dem Chinesischen Restsatz erhält man die folgende Isomorphie

$$\Phi : \mathbb{Z}/120\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \quad [n] \mapsto ([1],[2],[0]).$$

Wir gehen nun Schritt für Schritt vor, zunächst berechnet man mithilfe des euklidischen Algorithmus, dass $1 = 2 \cdot 8 - 3 \cdot 5$ gilt. Hieraus erhält man die folgende Abbildung

$$\eta : \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/40\mathbb{Z}, \quad ([x],[y]) \mapsto [2 \cdot 8 \cdot x - 3 \cdot 5 \cdot y].$$

Aus $1 = 40 - 3 \cdot 13$ (ebenfalls euklidischer Algorithmus) erhält man

$$\zeta : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/120\mathbb{Z}, \quad ([x],[y]) \mapsto [40 \cdot x - 3 \cdot 13 \cdot y].$$

Aus η und ζ erhält man

$$\Phi^{-1} : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/120\mathbb{Z}, \quad ([x],[y],[z]) \mapsto [40x - 624y + 585z].$$

Folglich gilt also $\Phi^{-1}([1],[2],[0]) = [112]$. 112 ist also die gesuchte natürliche Zahl n.