Kryptografia z elementami algebry

ćwiczenia

Zadanie 1. Sprawdzić, czy następujące zbiory z działaniem zwykłego dodawania i mnozenia liczb zawężonego do tego zbioru są pierścieniami przemiennymi. Czy są to ciała?

(a) $n\mathbb{Z}$, $n \in \mathbb{N}$,

(b) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$,

(c) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$,

Zadanie 2. Wyznaczyć dzielniki zera i elementy odwracalne w pierścieniach:

$$\mathbb{Z}_{21}, \qquad \mathbb{F}_{13}, \qquad \mathbb{Z}[i]$$

Który z powyższych pierścieni jest dziedziną całkowitości?

Zadanie 3. Niech $f, g \in \mathbb{Z}_8[X]$, gdzie $f(X) = 2X^2 + 6X + 5$, $g(X) = X^3 + 7X^2 + 4X + 3$. Oblicz $g(X) - f(X) + f(X)g(X)$.

Zadanie 4. Wykonać następujące dzielenia z resztą:

(a) $2X^4 + X^3 + X^2 + 3X + 3$ przez $3X^2 + X + 4$ w $\mathbb{F}_5[X]$,

(b) $2X^5 + 8X^4 + 7X^3 + 3X + 5$ przez $3X^3 + 7X^2 + 5X + 1$ w $\mathbb{F}_{11}[X]$,

(c) $X^{13} + X^{12} + X^{11} + X^9 + X^8 + X^6 + X^4 + X^3 + X^2 + 1$ przez $X^2 + X + 1$ w $\mathbb{F}_2[X]$,

(d) $X^{12} + X^4 + 1$ przez $X^8 + X^4 + X^3 + X + 1$ w $\mathbb{F}_2[X]$.

Zadanie 5. Wyznaczyć warstwy pierścienia $\mathbb{F}_3[X]$ względem ideału $I = (X^2 + 1)\mathbb{F}_3[X]$ oraz utworzyć tabelki działań. Oblicz element przeciwny i odwrotny do $(X + 1) + I$.

Zadanie 6. Czy pierścień ilorazowy $\mathbb{F}_5[X]/(X^2 + 1)\mathbb{F}_5$ jest dziedziną całkowitości?

Zadanie 7. W pierścieniu ilorazowym $\mathbb{F}_5[X]/I$, gdzie $I = (X^4 + 1)\mathbb{F}_5[X]$, obliczyć element przeciwny i odwrotny do $(X^2 + 4X + 3) + I$.

Zadanie 8. W pierścieniu ilorazowym $\mathbb{F}_2[X]/I$, gdzie $I = (X^6+X^4+X^2+X+1)\mathbb{F}_2[X]$, obliczyć element przeciwny i odwrotny do $(X^4 + X^2 + X) + I$.

Zadanie 9. W pierścieniu ilorazowym $\mathbb{F}_3[X]/I$, gdzie $I = (2X^3 + X + 1)\mathbb{F}_3[X]$, rozwiązać równanie $((2X + 1) + I)t = (X^2 + 2X + 2) + I$ o niewiadomej t.