Kryptografia z elementami algebry

ćwiczenia

1. Sprawdzić czy następujące zbiory z działaniem zwykłego dodawania i mnożenia liczb zawężonego do tego zbioru są pierścieniami przemiennymi

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

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

2. Wyznaczyć elementy odwracalne i dzielniki zera w pierścieniach:

   (a) $\mathbb{Z}_{15}$

   (b) $\mathbb{Z}_{11}$

   Który, ze zbiorów jest dziedziną całkowitości?

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

   (a) $f(X) + g(X)$

   (b) $f(X) - g(X)$

   (c) $f(X)g(X)$

4. Podzielić z resztą wielomian f przez g w $\mathbb{Z}_{10}[X]$, gdzie

   (a) $f(x) = 2X^5 + 8X^4 + 7X^3 + 3X + 5$, $g(X) = 3X^3 + 7X^2 + 5X + 1$

5. Podzielić z resztą wielomian f przez g w $\mathbb{F}_2[X]$, gdzie

   (a) $f(x) = X^{12} + X^4 + 1$, $m(X) = X^8 + X^4 + X^3 + X + 1$

6. Wyznaczyć warstwy pierścienia $\mathbb{Z}_3[X]$ względem ideału $\mathcal{A} = (X^2 + 1)\mathbb{Z}_3[X]$. Zbuduj tabelkę działań. Oblicz element odwrotny oraz przeciwny do $(x + 1) + \mathcal{A}$.

7. Wyznaczyć warstwy pierścienia $\mathbb{F}_2[X]$ względem ideału $\mathcal{A} = (X^8+X^4+X^3+X+1)\mathbb{F}_2[X]$. Zbuduj tabelkę działań. Oblicz element odwrotny oraz przeciwny do $(x^6+x^3+x^2+1)+\mathcal{A}$.