Diszkrét matematika II. feladatok

9.

Bemelegítő feladatok

1. Legyen $f = x^2 + 2 \in \mathbb{Z}_3[x]$, $g = 2x^2 + 4x + 1 \in \mathbb{Z}_3[x]$, $h = x^3 + x + 4 \in \mathbb{Z}_3[x]$. Számítsa ki a következő értékeket:

   a) $(f + g)^2 \mod x^2 + 2x + 2$;

   b) $g \cdot h \mod x^2 + 2x + 2$;

   c) $(f - g)(g - h)(f - h) \mod x^2 + 2x + 2$;

   d) $(f - g)^3 \mod x^2 + 2x + 2$.

2. Legyen $f = x^2 + x + 1 \in \mathbb{Z}_5[x]$, $g = 3x^2 + 4x + 1 \in \mathbb{Z}_5[x]$, $h = x^3 + x + 4 \in \mathbb{Z}_5[x]$. Számítsa ki a következő értékeket:

   a) $(f + g)^2 \mod x^3 + 1$;

   b) $f \cdot g + g \cdot h + f \cdot h \mod x^3 + 1$;

   c) $(f - g)(g - h)(f - h) \mod x^3 + 1$.

Gyakorló feladatok

3. Keresse meg az összes másodfokú irreducibilis polinomot $\mathbb{Z}_3$-ban.

4. Mutassa meg, hogy a következő polinomok irreducibilisek:

$$x^3 + x + 1,\ x^3 + x^2 + 1,\ x^3 + 4x^2 + 4x + 4 \in \mathbb{Z}_5[x].$$

5. Írja fel az $f = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ irreducibilis polinom segítségével az $\mathbb{F}_9$ műveleti tábláit $(+, \times)$!

Érdekes feladatok

6. Legyen $f = x^3 + x + 1 \in \mathbb{Z}_5[x]$ irreducibilis polinom és legyen $\mathbb{F}_{125} = \{g \mod f : g \in \mathbb{Z}_5[x]\}$. Legyen $a = x$, $b = x^2 + 1$, $c = 4x + 1$. Számítsa ki a következő értékeket $\mathbb{F}_{125}$-ben:

   a) $a \cdot b \cdot c$; b) $(a + b + c)^2$; c) a^{-1}; d) b^{-1};
   e) c^{-1}; f) a/b; g) $(b + c)^{-1}$; h) $(a + b)/(b + c)$.

Vegyes gyakorló feladatok

7. Legyen $f = x^5 + x + 1 \in \mathbb{Z}_2[x]$, $g = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$, $h = x^3 + x \in \mathbb{Z}_2[x]$. Számítsa ki a következő értékeket:

   a) $(f + g)^2 \mod x^3 + x + 1$;

   b) $f \cdot g + g \cdot h + f \cdot h \mod x^3 + x + 1$;

   c) $(f - g)(g - h)(f - h) \mod x^3 + x + 1$;

   d) $(f - g)^8 \mod x^3 + x + 1$.

8. Mutassa meg, hogy a következő polinomok irreducibilisek:

$$x^3 + x + 1,\ x^3 + x^2 + 1,\ x^3 + 4x^2 + 4x + 4 \in \mathbb{Z}_5[x].$$

9. Mutassa meg, hogy az

   a) $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ nem irreducibilis;

   b) $x^4 + x + 1 \in \mathbb{Z}_2[x]$ irreducibilis.

10. Lagrange interpolációval konstruálja meg a következő feltételnek eleget tevő polinomokat:

    a) $f \in \mathbb{C}[x]$, $\deg f \leq 5$ és $f(1) = 2 + 3i$, $f(-1) = 3i$, $f(i) = 1 - 2i$, $f(-i) = 1 - 4i$, $f(2i) = 1 + 20i$, $f(2) = 33 + 12i$.

    b) $f \in \mathbb{Z}_7[x]$, $\deg f \leq 5$ és $f(1) = 5$, $f(2) = 0$, $f(3) = 6$, $f(4) = 1$, $f(5) = 5$.

11. Legyen $f = x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$ irreducibilis polinom és legyen $\mathbb{F}_{27} = \{g \mod f : g \in \mathbb{Z}_3[x]\}$. Legyen $a = x^2$, $b = x^2 + 2$, $c = 2x^3 + 1$. Számítsa ki a következő értékeket $\mathbb{F}_{27}$-ben:

    a) $a \cdot b \cdot c$; b) $(a + b + c)^2$; c) a^{-1}; d) b^{-1};
    e) c^{-1}; f) a/b; g) $(b + c)^{-1}$; h) $(a + b)/(b + c)$.

Szorgalmi feladatok

12. A $p = 19$ használatával egy titok lett szétosztva tizenhárom ember között. Alice a $(3, 12)$, Bob a $(6, 14)$, Cecile a $(9, 17)$, Donna a $(14, 4)$, Eve a $(17, 10)$ párt kapta. Tudják, hogy közösen meg tudják fejteni a szétosztott titkot. Mi volt az?

13. Legyen $f = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ irreducibilis polinom és legyen $\mathbb{F}_9 = \{g \mod f : g \in \mathbb{Z}_3[x]\}$. Oldja meg a $z^2 + z + 2 = 0$ egyenletet $\mathbb{F}_9$-ben!