

Några övningar inför lappskrivning nummer 3 på moment B, Diskret matematik för D2 och F, vt09.

1. Betrakta den kropp med 8 element man får med hjälp av polynomet $p(x) = x^3 + x + 1$, dvs mängden

$$GF(8) = \{a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in Z_2\},$$

och där man räknar som om $p(x) = 0$ dvs som om $x^3 = x + 1$.

- Beräkna $(1 + x + x^2)(1 + x^2) + x + x^2$.
 - Bestäm inverserna till elementen $1 + x$, x och $x + x^2$.
 - Lös ekvationen $(1 + x)z + x^2 = x$.
 - Bestäm tre olika generatorer till kroppens multiplikativa grupp.
2. Kunstruera kroppar, eller motivera varför de inte går att konstruera, om kropparna skall ha
- 119 element.
 - 120 element.
 - 121 element.
3. En kropp $F = GF(27)$ med 27 element konstrueras med hjälp av det i polynomringen $Z_3[x]$ irreducibla polynomet $p(x) = x^3 + 2x + 2$.
- Bestäm x^4 , x^5 och x^6 .
 - Är $p(x)$ ett primitivt polynom i ringen $Z_3[x]$.
 - Bestäm en generator α för kroppens multiplikativa grupp.
 - Bestäm k sådant att $\alpha^k = x^2 + 2$.
 - Har ekvationen $z^2 + xz + 1 = 0$ några rötter i kroppen? Lös den i sådana fall.
4. Bestäm ett primitivt polynom $p(x)$ av grad två i ringen $Z_5[x]$. Detta polynom kan på sedvanligt sätt användas för att definiera en kropp F .
- Hur många element kommer denna kropp att ha?
 - Bestäm tre olika generatorer för kroppens multiplikativa grupp.
 - Bestäm samtliga lösningar i F till ekvationen $z^3 = 1$.
 - Bestäm samtliga lösningar i F till ekvationen $z^5 = 1$.
5. Kan en kropp med 64 element ha en delkropp med
- 2 element?
 - 32 element?
6. Konstruera en kropp med 64 element som har en delkropp med 8 element. Kommer varje kropp med 64 element att ha en delkropp med 8 element?