

Matematik, KTH

B.Ek

Svarsförslag för lappskrivning 3B, torsdag 3 december 2015
i SF1630(/1631) Diskret matematik, för D (m.fl.)

(Tryckfel kan förekomma.)

a-versionen (b-versionen på andra sidan):

a1a. (1p) Karakteristiken för en ändlig kropp F är det minsta $p \in \mathbb{N} \setminus \{0\}$ som uppfyller $\underbrace{1 + 1 + \dots + 1}_{p \text{ st}} = 0$ i F , dvs den additiva ordningen för elementet 1.

a1b. (1p) Då F är en kropp med $|F| = 27 = 3^3$ är F 's karakteristisk 3 (en kropp med $|F| = p^r$, p primtal, har karakteristisk p). Det betyder att $3 \cdot x = x + x + x = (1 + 1 + 1) \cdot x = 0 \cdot x = 0$ för alla $x \in F$ och därmed $12 \cdot x = 4 \cdot 3 \cdot x = 0$.

Svar: Alla $x \in F$ uppfyller ekvationen, så 27 stycken.

a1c. (1p) Faktorsatsen säger att om $f(x) \in F[x]$, där F är en kropp, gäller för alla $\alpha \in F$ att $(x - \alpha) \mid f(x)$ omm $f(\alpha) = 0$.

a1d. (1p) Om $(F, +, \cdot)$ är en ändlig kropp är den multiplikativa gruppen $(F \setminus \{0\}, \cdot)$ cyklisk.

a2. $k(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$ och $R = \mathbb{Z}_3[x]/(k(x))$. Vi ska
(a, 1p) avgöra om $k(x)$ är irreducibelt i $\mathbb{Z}_3[x]$,
(b, 1p) finna $[2x^2 + 2x + 1] + [x^2 + 2x + 2]$ i R ,
(c, 1p) finna $[2x^2 + 2x + 1] \cdot [2x + 1]$ i R och
(d, 1p) avgöra om $[2x^2 + 2x + 1] \cdot [ax^2 + bx + c] = [1]$ i R för några $a, b, c \in \mathbb{Z}_3$.

Lösning: a. Eftersom $k(x)$ har grad 3, är det irreducibelt omm det saknar nollställen i $\mathbb{Z}_3$ (en faktorisering i icke-konstanta faktorer skulle kräva en faktor av grad 1, så enligt faktorsatsen ett nollställe). $k(0) = k(1) = k(2) = 1$, så $k(x)$ är irreducibelt.

b. $[2x^2 + 2x + 1] + [x^2 + 2x + 2] = [(2x^2 + 2x + 1) + (x^2 + 2x + 2)] = [x]$.

c. $[2x^2 + 2x + 1] \cdot [2x + 1] = [(2x^2 + 2x + 1) \cdot (2x + 1)] = [x^3 + x + 1] = [(x^3 + 2x + 1) + 2x] = [k(x) + 2x] = [2x]$.

d. Eftersom $k(x)$ är irreducibelt (enligt a.), är R en kropp. $[2x^2 + 2x + 1] \neq [0]$ i R , så det har en invers i R , dvs de aktuella $a, b, c \in \mathbb{Z}_3$ finns (entydigt).

Svar a: $k(x)$ är irreducibelt, **b:** $[x]$, **c:** $[2x]$,

d: Ja, sådana a, b, c finns.

b-versionen:

b1a. (1p) Då F är en kropp med $|F| = 25 = 5^2$ är F 's karakteristik 5 (en kropp med $|F| = p^r$, p primtal, har karakteristik p). Det betyder att $5 \cdot x = x + x + x + x + x = (1 + 1 + 1 + 1 + 1) \cdot x = 0 \cdot x = 0$ för alla $x \in F$ och därmed $15 \cdot x = 3 \cdot 5 \cdot x = 0$.

Svar: Alla $x \in F$ uppfyller ekvationen, så 25 stycken.

b1b. (1p) Karakteristiken för en ändlig kropp F är det minsta $p \in \mathbb{N} \setminus \{0\}$ som uppfyller $\underbrace{1 + 1 + \dots + 1}_{p \text{ st}} = 0$ i F , dvs den additiva ordningen för elementet 1.

b1c. (1p) Om $(F, +, \cdot)$ är en ändlig kropp är den multiplikativa gruppen $(F \setminus \{0\}, \cdot)$ cyklisk.

b1d. (1p) Faktorsatsen säger att om $f(x) \in F[x]$, där F är en kropp, gäller för alla $\alpha \in F$ att $(x - \alpha) \mid f(x)$ omm $f(\alpha) = 0$.

b2. $k(x) = x^3 + 2x + 2 \in \mathbb{Z}_3[x]$ och $R = \mathbb{Z}_3[x]/(k(x))$. Vi ska

(a, 1p) avgöra om $k(x)$ är irreducibelt i $\mathbb{Z}_3[x]$,

(b, 1p) finna $[2x^2 + 2x + 1] + [x^2 + 2x + 2]$ i R ,

(c, 1p) finna $[2x^2 + 2x + 1] \cdot [2x + 1]$ i R och

(d, 1p) avgöra om $[2x^2 + 2x + 1] \cdot [ax^2 + bx + c] = [1]$ i R för några $a, b, c \in \mathbb{Z}_3$.

Lösning: a. Eftersom $k(x)$ har grad 3, är det irreducibelt omm det saknar nollställen i $\mathbb{Z}_3$ (en faktorisering i icke-konstanta faktorer skulle kräva en faktor av grad 1, så enligt faktorsatsen ett nollställe). $k(0) = k(1) = k(2) = 2$, så $k(x)$ är irreducibelt.

b. $[2x^2 + 2x + 1] + [x^2 + 2x + 2] = [(2x^2 + 2x + 1) + (x^2 + 2x + 2)] = [x]$.

c. $[2x^2 + 2x + 1] \cdot [2x + 1] = [(2x^2 + 2x + 1) \cdot (2x + 1)] = [x^3 + x + 1] = [(x^3 + 2x + 2) + 2x + 2] = [k(x) + 2x + 2] = [2x + 2]$.

d. Eftersom $k(x)$ är irreducibelt (enligt a.), är R en kropp. $[2x^2 + 2x + 1] \neq [0]$ i R , så det har en invers i R , dvs de aktuella $a, b, c \in \mathbb{Z}_3$ finns (entydigt).

Svar a: $k(x)$ är irreducibelt, **b:** $[x]$, **c:** $[2x + 2]$,

d: Ja, sådana a, b, c finns.
