

Matematik, KTH
B.Ek

Ls3Ba

**Lappskrivning 3B, version a,
i SF1630(/1631) Diskret matematik, för D (m.fl.)
torsdag 3 december 2015, klockan 15.15–15.40**

Inga hjälpmedel tillåtna.

Skriv din lösning på samma blad som uppgiften (använd baksidan och delar av det sista bladet om det behövs). Lämna in alla bladen hophäftade, som de är.

Namn:

Personnummer:

Lösningar kommer att läggas ut på kurssidan efter skrivningen.

Bedömning G på denna uppgift ger full poäng på uppgift 3 på teoridelen (del T) vid TENB i januari och mars 2016.
För G krävs minst 3p.

Poäng på uppgiften: G/U:

1a. (1p) Vad menas med **karaktistiken** för en ändlig kropp (eng. field) F ?

b. (1p) Låt F vara en ändlig kropp med $|F| = 27$.
Hur många $x \in F$ uppfyller $12 \cdot x = 0$ (dvs $\underbrace{x + x + \dots + x}_{12 \text{ st } x} = 0$)?

c. (1p) Låt F vara en kropp. Vad säger **faktorsatsen** (eng. the factor theorem) för polynom i $F[x]$?

d. (1p) Låt $(F, +, \cdot)$ vara en ändlig kropp.
Beskriv strukturen för den multiplikativa gruppen $(F \setminus \{0\}, \cdot)$.

Bedömning G på denna uppgift ger full poäng på tredje uppgiften på första problemdelen (del P1), dvs uppgift 7, vid TENB i januari och mars 2016.

För G krävs minst 3p.

Poäng på uppgiften: G/U:

För full poäng krävs att svaren tydligt motiveras.

2. Låt polynomet

$$k(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x].$$

Låt vidare $R = \mathbb{Z}_3[x]/(k(x))$, ringen av ekvivalensklasser i $\mathbb{Z}_3[x]$ modulo $k(x)$. Vi representerar som vanligt varje ekvivalensklass med det ingående polynom som har lägst grad (så att t.ex. $[x+2]$ betecknar den ekvivalensklass som innehåller polynomet $x+2$). I b. och c. nedan krävs att svaren representeras så.

a. (1p) Avgör om $k(x)$ är ett irreducibelt polynom i $\mathbb{Z}_3[x]$.

b. (1p) Vad är summan $[2x^2 + 2x + 1] + [x^2 + 2x + 2]$ i R ?

c. (1p) Vad är produkten $[2x^2 + 2x + 1] \cdot [2x + 1]$ i R ?

d. (1p) Avgör om det finns några $a, b, c \in \mathbb{Z}_3$ sådana att

$$[2x^2 + 2x + 1] \cdot [ax^2 + bx + c] = [1]$$

i R . (Det räcker alltså att avgöra om sådana a, b, c finns. Om de finns behöver du ändå inte finna dem.).