

Matematik, KTH

B.Ek

Tentamen TENB i kurs SF1630(/5B1203), SF1631(/5B1204),
DISKRET MATEMATIK för D (m.fl.)

tisdagen den 11 december 2012, klockan 8.00–13.00.

Examinator: Bengt Ek, tel 7906951.

Tillåtna hjälpmedel: Inga, inte ens räknedosa.

Högsta möjliga poäng på skrivningen är 37p. Till poängen från skrivningen läggs bonus från lappskrivningarna 1B, 2B och 3B ht 2012, högst 6p.

Betygsgränser:

För betyg	A	B	C	D	E
krävs	32	27	22	18	15

poäng (inklusive bonus)

13–14 poäng ger omdömet Fx och rätt att delta i en komplettering för betyg E.

För att ge full poäng måste lösningarna vara ordentligt motiverade.

Satser från kursen får (utom då annat sägs) användas utan bevis, om det klart anges vad de säger.

DEL I

1) (3p) Ett (pytte-)RSA-system har de offentliga parametrarna $n = 143$ och $e = 103$. Dekryptera meddelandena 2, 3 och 4, dvs finn $D(2)$, $D(3)$ och $D(4)$.

2) (3p) Låt $G = U(\mathbb{Z}_{697})$, dvs mängden av (under multiplikationen $\cdot$) inverterbara element i $\mathbb{Z}_{697}$. Avgör, med motivering, om $32(= 2^5)$ genererar $(G, \cdot)$.
[697 = 17 · 41]

3) (3p) Låt $(G, \cdot)$ vara en grupp. Visa att om $a \in G$ är det enda elementet i G som har ordning k , så ligger a i G 's centrum, dvs $ga = ag$ för alla $g \in G$.

4) (3p) Låt $(R, +, \cdot)$ vara en ring, sådan att $(R, +)$ är en cyklisk grupp. Visa att R är kommutativ under multiplikationen, dvs $a \cdot b = b \cdot a$ för alla $a, b \in R$.

5) En linjär binär kod $\mathcal{C}$ definieras av kontrollmatrisen

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

a) (1p) Hur många kodord innehåller koden $\mathcal{C}$?
b) (2p) Vilka kodord sändes om man tar emot 10110, 11011, 01101 och högst en bit i varje ord blivit fel?

Vänd!

DEL II

6) Betrakta i $\mathbb{Z}_5[x]$ de båda polynomen

$$f(x) = x^4 + 3x^3 + x^2 + x + 3,$$

$$g(x) = x^4 + 4x^3 + 3x^2 + 2x + 4.$$

a) (2p) Bestäm den monadiska (dvs med högstgradskoefficienten = 1) största gemensamma delaren $k(x)$ till $f(x)$ och $g(x)$.

b) (2p) Finn $\lambda(x), \mu(x) \in \mathbb{Z}_5[x]$ så att $k(x) = \lambda(x)f(x) + \mu(x)g(x)$.

Ange koefficienterna i $k(x), \lambda(x), \mu(x)$ som element i $\mathbb{Z}_5$, dvs utan t.ex. minustecken.

7) (4p) En kub skall smyckas med en enfärgad kula i varje hörn. På hur många väsentligt olika sätt (dvs så att de inte blir lika hur man än vrider kuben i rummet) kan det göras om man får använda högst en röd kula och godtyckliga antal kulor med k andra färger (dvs utöver rött)?

8) Låt G vara en grupp och $a, b \in G$ ha ordningar $o(a) = m, o(b) = n$, där $\text{sgd}(m, n) = 1$.

a) (1p) Visa att om $a^r = b^s$ för några $r, s \in \mathbb{Z}$ så är $a^r = b^s = 1$, G :s identitets-element.

b) (3p) Visa att alla $a^i b^j, 0 \leq i < m, 0 \leq j < n$ är olika.

I b) får man använda resultatet i a), även om man inte gjort den uppgiften.

Man får inte förutsätta att $ab = ba$.

DEL III

För full poäng på dessa uppgifter krävs särskilt väl strukturerade och presenterade lösningar.

9a) (1p) Visa att polynomet $k(x) = x^2 + x + 1$ är irreducibelt i $\mathbb{Z}_2[x]$.

b) (1p) Ställ upp additions- och multiplikationstabellerna för kroppen $(F, +, \cdot)$, där $F = \{0, 1, \alpha, \beta\}$ och består av ekvivalensklasser modulo $k(x)$ (polynomet i uppgift a) och α, β är x :s respektive $x + 1$:s klasser.

c) (3p) Faktorisera polynomet $f(x) = x^4 + \beta x^3 + \alpha x^2 + \alpha x + \beta$ i irreducibla faktorer i $F[x]$, där F är kroppen i uppgift b.

10) (5p) Låt $(G, \cdot)$ vara en grupp. Visa att för varje funktion $f : G \rightarrow G$ är

$$\mathcal{Z}_f = \{g \in G \mid f(g \cdot x) = f(x \cdot g) \text{ för alla } x \in G\}$$

en delgrupp till G .