Institutionen för matematik
KTH
B.Ek

Lösningar tentamen 5B1204 Diskret matematik för D2, 7 mars 2002

Teoridel

1a) $a_n = A \cdot 4^n + B \cdot 2^n$, se stencilen. **b)** Se Biggs 8.3.
c) 12, se Biggs 8.5. **d)** 5, se Biggs 10.2.
2a) Se Biggs 10.6. **b)** Se Biggs 1.7. **c)** Se Biggs 2.2.
3a) Se Biggs 3.1. **b)** Se Biggs 4.3. **c)** Se Biggs 4.2.4.
4a) Se Biggs 5.2. **b)** Se Biggs 5.3. **c)** Se Biggs 5.5.
5a) Se Biggs 13.3. **b)** Se Biggs 16.4.

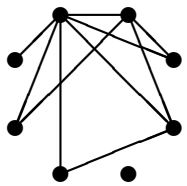
Problemdel

6a) Om de mottagna orden (som kolonnvektorer) kallas z' fås $Hz' = \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}$ resp. $\begin{bmatrix}0\\0\\0\end{bmatrix}$. Vi känner igen den första som kolonn 2 och den andra som kolonn 5 i H, så fel har uppstått i position 2, position 5 resp. ingenstans. De sända orden var alltså $(001101), (101011), (100110)$.
b) Eftersom alla kolonner i H är olika och skilda från noll, rättar koden **minst ett** fel (enligt känd sats i boken). Enligt a) är (001101) ett kodord. Med två fel i det eller ett fel i kodordet (000000) fås (000001). Koden rättar alltså inte två fel, så svaret blir **ett fel**.
c) Det gäller $n = pq$, där p och q är olika primtal, och $(ed =)9 \cdot 49 \equiv 1 \pmod m$, där $m = (p-1)(q-1)$. Vi har alltså $9 \cdot 49 = 441 = k(p-1)(q-1)+1$, för något heltal k. p och q måste alltså vara primtal med $(p-1) \mid 440 (= 2^3 \cdot 5 \cdot 11)$ och $(q-1) \mid 440$.
Alla sådana primtal: $1+1=2$, $2+1=3$, $2^2+1=5$, $2\cdot5+1=11$, $2^3\cdot5+1=41$, $2\cdot11+1=23$, $2^3\cdot11+1=89$. Det största möjliga pq blir (obs att $(p-1)(q-1) \mid 440$) $\boldsymbol{n = 11\cdot23 = 253}$.

7a) Låt X vara mängden av alla placeringar i ledet och A_1 mängden placeringar **med** två flickor längst fram. Då är det sökta antalet: $|X| - |A_1| = 20! - 11 \cdot 10 \cdot 18! = (20 \cdot 19 - 11 \cdot 10) \cdot 18! = \mathbf{270 \cdot 18!}$.
b) Med A_2 = mängden placeringar **med** Lasse och Bosse intill varandra ger sållprincipen det sökta antalet (antalet placeringar med Lasse och Bosse intill varandra = $2\cdot$ antalet med Lasse och Bosse som en pojke): $|X \setminus (A_1 \cup A_2)| = |X| - |A_1| - |A_2| + |A_1 \cap A_2| = 20! - 11\cdot10\cdot18! - 2\cdot19! + 2\cdot11\cdot10\cdot17! = (20\cdot19\cdot18 - 11\cdot10\cdot18 - 2\cdot19\cdot18 + 2\cdot11\cdot10)\cdot17! = \mathbf{4396\cdot17!}$.
c) $\alpha\sigma = \sigma\alpha \Leftrightarrow (14)(2839)(5107) = \alpha = \sigma\alpha\sigma^{-1} = (\sigma(1)\sigma(4))(\sigma(2)\sigma(8)\sigma(3)\sigma(9))(\sigma(5)\sigma(10)\sigma(7))$.
Vi ser att vi måste ha $\sigma(1) = 1$ eller 4 och då $\sigma(4) = 4$ resp. 1 och motsvarande för de andra cyklerna (eftersom alla α:s cykler har olika längd måste σ ta varje cykel till densamma). Totalt kan $\sigma(1), \sigma(2), \sigma(5)$ väljas fritt i motsvarande cykel och detta val bestämmer σ helt. Anatalet olika σ blir $2 \cdot 4 \cdot 3$, dvs **svar: 24 stycken**.

8a) $39x + 45y = 12 \Leftrightarrow 13x + 15y = 4$.
Euklides algoritm: $15 = 1\cdot13+2$, $13 = 6\cdot2+1$, $2 = 2\cdot1$ och baklänges: $1 = 1\cdot13 - 6\cdot2 = 1\cdot13 - 6\cdot(15-1\cdot13) = (-6)\cdot15 + 7\cdot13$. Således $13\cdot7 + 15\cdot(-6) = 1$, så $13\cdot28 + 15\cdot(-24) = 4$ och en lösning till ekvationen ges av $x_0 = 28, y_0 = -24$. Om x, y är en annan lösning fås $13\cdot(x_0 - x) + 15\cdot(y_0 - y) = 0$, med allmän lösning $x = x_0 + 15a, y = y_0 - 13a$, a heltal. Detta kan hyfsas till $\boldsymbol{x = -2 + 15k, y = 2 - 13k}$, k godtyckligt heltal.
b) $3x \equiv_{14} 1 \Leftrightarrow 3x \equiv_{14} 15 \Leftrightarrow x \equiv_{14} 5$ och
$4x \equiv_{13} 5 \Leftrightarrow 4x \equiv_{13} 44 \Leftrightarrow x \equiv_{13} 11 \equiv_{13} -2$.
Eftersom 13 och 14 är relativt prima och $14\cdot13 = 182$, ger kinesiska restsatsen $x \pmod{182}$: $-13 \equiv_{14} 1, -13 \equiv_{13} 0$ och $14 \equiv_{14} 0, 14 \equiv_{13} 1$, så $x \equiv_{182} 5\cdot(-13) + (-2)\cdot14 = -93 \equiv_{182} 89$.
Dvs **svar: $\boldsymbol{x = 89 + 182k}$, $\boldsymbol{k}$ heltal**.
c) Eftersom $1155 = 3\cdot5\cdot7\cdot11$ gäller $758^n \equiv_{1155} 1 \Leftrightarrow 758^n \equiv_3 2^n \equiv_3 1$ och $758^n \equiv_5 3^n \equiv_5 1$ och $758^n \equiv_7 2^n \equiv_7 1$ och $758^n \equiv_{11} 10^n \equiv_{11} (-1)^n \equiv_{11} 1$.
Genom att betrakta de multiplikativa ordningarna i $\mathbb{Z}_3$, $\mathbb{Z}_5$ etc. fås att detta gäller precis om $2 \mid n$, $4 \mid n$, $3 \mid n$ och $2 \mid n$. Det minsta möjliga värdet blir alltså **svar: $\boldsymbol{n = 12}$**.

9a) i) 0,1,2,2,2,3,4,6 : möjligt, se figuren till höger.
ii) 1,1,2,3,3,4,7,7 : omöjligt, ty hörn med valens 7 är grannar med alla andra hörn; om två hörn har valens 7 måste alla hörn ha valens minst 2. (Här användes att grafen saknar loopar och multipla kanter.)
iii) 3,3,3,4,5,5,6,6 : går inte, ty summan av valenserna är 2 gånger antalet kanter, dvs ett jämnt tal.



b) K_n innehåller alltid en hamiltoncykel (eftersom det går kanter mellan alla par av hörn, kan man gå cykliskt genom alla hörn). Om man tar bort kanterna i den, återstår en graf som är sammanhängande om $n \geq 5$ (om $n = 3$ saknar den kanter) och varje hörn har valens $n - 3$. Problemet är när det finns en sluten eulerväg i den återstående grafen. Det gör det som bekant om alla hörn har jämn valens, dvs **svar: om n är udda och ≥ 5** (om man godtar en tom väg som en sluten väg, går också $n = 3$ bra).
c) Antag att $\bar{G}$ inte är sammanhängande, vi skall visa att G då är sammanhängande. Ur detta följer påståendet.
Låt u och v vara två hörn i G. Om de ligger i olika komponenter av $\bar{G}$, är de inte grannar i $\bar{G}$, så de är grannar i G. Om de ligger i samma komponent av $\bar{G}$, tag ett hörn w i en annan komponent av $\bar{G}$. Då är uwv en väg från u till v i G. I båda fallen går det alltså en väg från u till v i G och G är sammanhängande.

10a) $p(x) = x^4 + x^3 + 4x^2 + 3x + 4$ skall faktoriseras i $\mathbb{Z}_5[x]$.
Enligt faktorsatsen finns det en förstagradsfaktor precis om $p(x)$ har ett nollställe. Prövning ger ett nollställe $x = 2$, så $x - 2 = x + 3$ är en faktor (irreducibel, förstås) till $p(x)$. Division ger $p(x) = (x + 3)q(x)$, med $q(x) = x^3 + 3x^2 + 3$.
Prövning ger sedan ett nollställe $x = 4$ till $q(x)$, så $x - 4 = x + 1$ är en (irreducibel) faktor till $q(x)$. Division ger $q(x) = (x + 1)r(x)$, med $r(x) = x^2 + 2x + 3$.
Ny prövning visar att $r(x)$ saknar nollställen, så det är irreducibelt.
Svar: $p(x) = (x + 1)(x + 3)(x^2 + 2x + 3)$.
b) $p \nmid x^2 + 1$ innebär precis att $x^2 + 1 \neq 0$ i $\mathbb{Z}_p$. Det gäller alltså att visa att det inte finns x med $x^2 = -1$ i $\mathbb{Z}_p$ om p är ett primtal av form $4k + 3$.
I gruppen $(\mathbb{Z}_p \setminus \{0\}, \times)$ skulle ett sådant x ha ordning 4 (ty $x^4 = 1$, men $x^2 \neq 1$), men $4 \nmid p - 1 = 4k + 2$, gruppens ordning. Ett sådant x finns alltså inte.
c) Nu är p ett primtal av form $4k+1$ och det gäller att visa att det finns ett x så att $x^2 = -1$ i $\mathbb{Z}_p$.
Eftersom $\mathbb{Z}_p$ är en ändlig kropp är $(\mathbb{Z}_p \setminus \{0\}, \times)$ en cyklisk grupp av ordning $p-1 = 4k$. Låt g vara en generator för denna grupp och betrakta $x = g^k$. $x^4 = g^{4k} = 1$, men $x^2 = g^{2k} \neq 1$, eftersom g har ordning $4k$. Då är $x^2 = -1$, ty i en kropp har ekvationen $y^2 = 1$ bara lösningarna $y = 1$ och $y = -1$ (ty $y^2 - 1 = (y - 1)(y + 1)$ och i en kropp kan en produkt bara vara 0 om en faktor är det) och $y = x^2 \neq 1$ är en lösning. Saken är klar.