Institutionen för matematik, **KTH**
Mats Boij och Niklas Eriksen

Lösningsförslag till
Tentamen i 5B1118 Diskret matematik 5p
11 april, 2002

1. Bestäm det minsta positiva heltal n sådant att $31n + 13$ är delbart med 27. **(3)**

   Lösning: Vi söker det minsta positiva heltal n så att $31n + 13 = 27k$ för något heltal k. Skriver vi om det lite får vi den diofantiska ekvationen

   $$27k - 31n = 13.$$

   Med hjälp av Euklides algoritm kan vi först bestämma en lösning till ekvationen $27k - 31n = 1$, om n och k saknar gemensamma delare. Vi får

   $$\begin{aligned} 31 &= 1 \cdot 27 + 4 \\ 27 &= 6 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

   och om vi räknar baklänges får vi

   $$\begin{aligned} 1 &= 4 - 1 \cdot 3 = 4 - 1(27 - 6 \cdot 4) \\ &= 7 \cdot 4 - 1 \cdot 27 = 7(31 - 1 \cdot 27) - 1 \cdot 27 \\ &= 7 \cdot 31 - 8 \cdot 27 \end{aligned}$$

   Alltså är $n = -7$ och $k = -8$ en lösning till $27k - 31n = 1$. Multiplicerar vi detta med 13 får vi en lösning till $27k - 31n = 13$ som $n = -91$, $k = -104$. Eftersom 31 och 27 är relativt prima ges nu den allmänna lösningen av $n = 27m - 91$ och $k = 31m - 104$, där m är ett godtyckligt heltal. Det minsta positiva n fås genom att välja m som 4, eftersom $3 \cdot 27 = 81 < 91$, och $27 \cdot 4 - 91 = 108 - 91 = 17$.

   Svar: $n = 17$ är det minsta positiva heltal sådant att $31n + 13$ är delbart med 27.

2. Den booleska funktionen f ges av $f(x, y, z) = (x + y)z + xy$. Skriv f och $\overline{f}$ på disjunktiv normalform. **(3)**

   Lösning: En funktion befinner sig på disjunktiv normalform om den består av en summa av produkter, som alla består av lika många termer som antalet ingående variabler, i detta fall tre. Varje term svarar mot en tilldelning av värden till variablerna. Exempelvis svarar $xy\bar{z}$ mot att funktionen är 1 om $x = 1$, $y = 1$ och $z = 0$. 0.

Vi får

$$\begin{aligned} f(x,y,z) &= (x+y)z + xy = xz + yz + xy \\ &= xz(y+\bar{y}) + yz(x+\bar{x}) + xy(z+\bar{z}) \\ &= xyz + x\bar{y}z + xyz + \bar{x}yz + xyz + xy\bar{z} \\ &= xyz + x\bar{y}z + \bar{x}yz + xy\bar{z}. \end{aligned}$$

Funktionen $\bar{f}$ utgörs av komplementet till f, det vill säga de termer som inte var med i f. Dessa ges av

$$\bar{f}(x,y,z) = \bar{x}\bar{y}z + \bar{x}y\bar{z} + x\bar{y}\bar{z}z + \bar{x}\bar{y}\bar{z}.$$

Svar: $f(x,y,z) = xyz + x\bar{y}z + \bar{x}yz + xy\bar{z}$ och $\bar{f}(x,y,z) = \bar{x}\bar{y}z + \bar{x}y\bar{z} + x\bar{y}\bar{z} + \bar{x}\bar{y}\bar{z}$.

3. Illustrera metoden med successiv kvadrering genom att beräkna $3^{28} \pmod{77}$. **(3)**

Lösning: Vi börjar med att skriva exponenten på binär form genom att successivt dividera med två.

$$\begin{aligned} 28 &= 2 \cdot 14 + 0 \\ 14 &= 2 \cdot 7 + 0 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Därmed är 11100 den binära formen för 28 som alltså kan skrivas som $16 + 8 + 4$. Vi beräknar nu successiva kvadrater av 3 modulo 77.

$$\begin{aligned} 3^2 &\equiv 9 \pmod{77} \\ 3^4 &\equiv 9^2 \equiv 81 \equiv 4 \pmod{77} \\ 3^8 &\equiv 4^2 \equiv 16 \pmod{77} \\ 3^{16} &\equiv 16^2 \equiv 256 \equiv 25 \pmod{77} \end{aligned}$$

Vi kan nu beräkna 3^{28} genom

$$3^{28} = 3^{16+8+4} \equiv 25 \cdot 16 \cdot 4 \equiv 400 \cdot 4 \equiv 15 \cdot 4 \equiv 60 \pmod{77}.$$

Svar: Resten vid division av 3^{28} med 77 är 60.

4. Bestäm samtliga delgrupper av ordning tre i den symmetriska gruppen S_4. **(3)**

Lösning: Eftersom 3 är ett primtal måste samtliga element förutom *id* i delgruppen ha ordning 3. Permutationer av ordning 3 består av ett antal cykler av längd 3 och cykler av längd 1. För en permutation i S_4 är summan av cyklernas längd 4, så permutationer av ordning 3 består av en cykel av längd 3 och en cykel av längd 1.

I en permutation $(a\ b\ c)(d)$ ges dess invers av $(a\ c\ b)(d)$. Dessa två permutationer bildar tillsammans med id en delgrupp till S_4. Det finns 4 sätt att välja d till permutationen ovan, och för varje sådant sätt finns bara ett par av permutationer $(a\ b\ c)(d)$ och $(a\ c\ b)(d)$. Delgrupperna blir således $\{id,\ (1\ 2\ 3)(4),\ (1\ 3\ 2)(4)\}$, $\{id,\ (1\,2\,4)(3),\ (1\,4\,2)(3)\}$, $\{id,\ (1\,3\,4)(2),\ (1\,4\,3)(2)\}$ och $\{id,\ (2\,3\,4)(1),\ (2\,4\,3)(1)\}$.

Svar: Delgrupperna är $\{id,\ (1\ 2\ 3)(4),\ (1\ 3\ 2)(4)\}$, $\{id,\ (1\ 2\ 4)(3),\ (1\ 4\ 2)(3)\}$, $\{id,\ (1\ 3\ 4)(2),\ (1\ 4\ 3)(2)\}$ och $\{id,\ (2\ 3\ 4)(1),\ (2\ 4\ 3)(1)\}$.

5. Låt G vara en graf med sex hörn som svarar mot de sex sidorna i en kub och vars kanter svarar mot de par av sidor som har en gemensam kant. Avgör om G har någon Eulerväg och om G har någon Hamiltoncykel. **(3)**

   Lösning: Om vi numrerar sidorna i kuben som en tärning och använder motsvarande numrering för hörnen i grafen G får vi kanter mellan alla hörn utom de som svarar mot motstående sidor i kuben, dvs inte kanterna 16, 25 och 34. Vi kan hitta en Hamiltoncykel genom $1, 2, 3, 5, 6, 4, 1$. Vi går då efter kanterna 12, 23, 35, 56, 46 och 14. Eftersom vi hittat en Hamiltoncykel måste grafen vara sammanhängande och alla hörn har valens fyra, eftersom det bara är en av de fem möjliga kanterna som inte är med i grafen. Alltså finns en Eulerväg, och vi kan också hitta en genom att fortsätta Hamiltoncykeln med $1, 3, 6, 2, 4, 5, 1$. De tolv kanterna i grafen används nu i ordningen $12, 23, 35, 56, 45, 14, 13, 36, 26, 24, 45, 15$.

   Svar: Grafen har både en Eulerväg och en Hamiltoncykel.

6. Grafen G ges av nedanstående granntabell. Vilket är det minsta antalet färger som krävs för att hörnfärga, respektive kantfärga, grafen G?

1	2	3	4	5	6	7
2	1	2	2	1	1	4
5	3	4	3	2	7	5
6	4		7	7		6
	5					

(4)

   Lösning: Vi börjar med att titta på lägre gränser för färgningarna. Vi ser att grafen innehåller en triangel (t.ex. hörnen 1, 2 och 5 med kanter mellan sig), så åtminstone 3 färger behövs i hörnfärgningen. Detta för att samtliga hörn i triangeln måste färgas med olika färger. Vi ser även att hörn 2 har valens 4, så kantfärgningen kräver minst 4 färger. Detta för att samtliga kanter utgående från detta hörn måste ha olika färg.

   För att demonstrera att det räcker med tre respektive fyra färger ger vi exempel på sådana färgningar.

   En variant för hörnfärgning ges av hörn 2 rött, hörn 1, 3, 7 blå och hörn 4, 5, 6 gula. Det är en tillåten hörnfägning eftersom kanterna (1 3), (1 7) och (3 7) inte förekommer och inte heller kanterna (4 5), (4 6) och (5 6).

En kantfärgning ges av $(2\ 5), (3\ 4), (6\ 7)$ röda, $(1\ 2), (4\ 7)$ svarta, $(1\ 6), (2\ 4), (5\ 7)$ gredelina och $(1\ 5), (2\ 3)$ chockrosa. Kantfärgningen är tillåten eftersom samma hörn inte förekommer flera gånger i listan över kanter med en given färg.

Svar: 3 respektive 4 färger.

7. Låt $\pi = 136542$ och $\sigma = 216354$ vara två permutationer i S_6 angivna i enradsnotation.

   (a) Visa att π och σ är *konjugerade* genom att bestämma en permutation τ sådan att $\pi\tau = \tau\sigma$.

   (b) Hur många permutationer τ i S_6 uppfyller $\pi\tau = \tau\sigma$?

(4)

Lösning: Vi skriver först permutationerna på cykelnotation genom att följa elementen och får $\pi = (1)(236)(45)$ och $\sigma = (12)(364)(5)$. Permutationerna är konjugerade eftersom de har samma typ [123] och vi kan välja τ genom att avbilda de olika cyklerna i σ på motsvarande cykel i π. Vi får då exempelvis $\tau(1) = 4$, $\tau(2) = 5$, $\tau(3) = 2$, $\tau(4) = 6$, $\tau(5) = 1$ och $\tau(6) = 3$. Vi kan verifiera att $\pi\tau = (15)(24)(3)(6) = \tau\sigma$.

Eftersom τ måste avbilda cykler i σ på cykler av samma längd i π och det inte finns två cykler av samma längd i σ har vi inget val för $\tau(5)$, men två val för $\tau(1)$, nämligen 4 eller 5, och tre val för $\tau(3)$, nämligen 2, 3 eller 6. När vi väl bestämt $\tau(5)$, $\tau(1)$ och $\tau(3)$ är resterande värden helt bestämda. Vi får $\tau(2) = \tau(\sigma(1)) = \pi(\tau(1))$, $\tau(6) = \tau(\sigma(3)) = \pi(\tau(3))$ och $\tau(4) = \tau(\sigma(6)) = \pi(\tau(6)) = \pi(\pi(\tau(3)))$.

Vi får alltså $1 \cdot 2 \cdot 3 = 6$ olika möjliga τ.

Svar: Det finns 6 olika τ som uppfyller $\pi\tau = \tau\sigma$.

8. Låt a och b vara element i en abelsk (kommutativ) grupp och antag att ordningarna för a och b är m respektive n. Visa att ordningen för ab är en delare i

$$\frac{mn}{\mathrm{sgd}(m,n)}$$

och visa dessutom genom ett exempel att detta inte behöver gälla om gruppen inte är abelsk. **(4)**

Lösning: Sätt

$$d = \frac{mn}{\mathrm{sgd}(m,n)}$$

Eftersom $\mathrm{sgd}(m,n)$ delar såväl m som n är $k = m/\mathrm{sgd}(m,n)$ och $l = n/\mathrm{sgd}(m,n)$ heltal. Vi får därför att

$$(ab)^d = a^d b^d = a^{km} b^{ln} = id \cdot id = id,$$

det vill säga ordningen för ab delar d, ty om så inte vore fallet skulle $(ab)^d \neq id$.

Vi betraktar nu de icke-abelska gruppen S_3. Låt $a = (1\ 2)$ och $b = (2\ 3)$. Vi får att

$$ab = (1\ 2)(2\ 3) = (1\ 2\ 3)$$

och därmed har ab ordning 3 medan

$$\frac{mn}{\text{sgd}(m,n)} = \frac{2 \cdot 2}{2} = 2.$$

Eftersom 3 inte delar 2 följer att S_3 inte är abelsk.

9. Visa att ett positivt heltal är delbart med tre om och endast om dess siffersumma är delbar med tre när talet skrivs i hexadecimal form. Exempelvis är den hexadecimala formen för tjugoett 15 och vi får då siffersumman $1 + 5 = 6$, vilken är delbar med tre. **(4)**

   Lösning: Betrakta talet $x = (x_n x_{n-1} \ldots x_1 x_0)_{16} = x_n 16^n + x_{n-1} 16^{n-1} \ldots x_1 16 + x_0$. Dess siffersumma är $x_n + x_{n-1} + \ldots + x_1 + x_0$. Vi räknar nu modulo 3. Då fås

$$x - \sum_{k=0}^{n} x_k \equiv \sum_{k=0}^{n} x_k 16^k - \sum_{k=0}^{n} x_k \equiv \sum_{k=0}^{n} x_k - \sum_{k=0}^{n} x_k \equiv 0 \pmod 3$$

   eftersom $16^k \equiv 1^k \equiv 1 \pmod 3$ för alla heltal k. Detta innebär i klartext att 3 delar $x - \sum_{k=0}^{n} x_k$, vilket är ekvivalent med att x är delbar med 3 om och endast om siffersumman är delbar med 3.

   Svar:

10. Med en linjär kod C av längd fem som rättar ett fel har följande bitström mottagits:

$$10110001000011111111011001.$$

    Rätta meddelandet om det uppstått så få fel som möjligt. Detta är ett rimligt antagande om störningen är relativt liten, exempelvis om sannolikheten för fel i en given bit är en hundradel. **(4)**

    Lösning: Först använder vi Sfärpackningssatsen för att bestämma vilken dimension koden kan ha. Vi har att $|C|(1+5) \leq 2^5 = 32$, vilket ger $|C| \leq 5$. Eftersom en linjär kod av dimension k har 2^k kodord får vi att k är 0, 1, eller 2 och det finns maximalt fyra olika kodord, varav ett är 00000. Vi har mottagit fem olika ord, varav inget är 00000, och därmed måste det uppstått fel i minst två ord. Vi antar därför först att det uppstått precis två fel. Då kan de inte ha uppstått i samma ord, eftersom minst två ord är felaktiga. Alltså har vi högst ett fel i varje ord.

    Det andra mottagna ordet är 00100. Eftersom koden skall kunna rätta ett fel, och det uppstått högst ett fel i detta ord måste det riktiga ordet vara 00000, som är ett kodord.

Det återstår ett fel och fyra nollskilda ord. Vi jämför orden med varandra och ser att avståndet mellan det första och det fjärde ordet är 1, varför något av dem måste vara fel. (I en kod som rättar ett fel är minsta avståndet minst 3.) Om vi jämför dessa två med de övriga ser vi att avståndet mellan det första och det tredje är två. Alltså måste det vara det första som är fel. Vi har nu kvar tre nollskilds ord, 00111, 11110 och 11001. Vi ser att det tredje av dessa är summan av de två första och därmed bildar de fyra orden 00000, 00111, 11110 och 11001 en linjär kod. Denna rättar ett fel eftersom minsta vikten av ett nollskilt ord är tre.

Svar: Det korrigerade meddelandet lyder 111100000000011111111011001.