Institutionen för matematik, **KTH**
Mats Boij

Lösningsförslag till
Tentamen i 5B1118 Diskret matematik 5p
22 augusti, 2001

1. Ange kvot och rest vid division av $5BE$ med $1F$ där båda talen är angivna i hexadecimal form. **(3)**

   Lösning: Vi kan använda den vanliga algoritmen för division och utföra alla räkningar hexadecimalt.

$$\begin{array}{r|l}
 & 2\,F \\ \cline{2-2}
1F & 5BE \\ \cline{1-1}
 & \underline{3E} \\
 & 1DE \\
 & \underline{1D\,1} \\
 & D
\end{array}$$

   där vi behövt utföra multiplikationerna $2 \cdot 1F$ och $F \cdot 1F$. Dessa kan utföras i vanliga uppställningar.

$$\begin{array}{r}
1F \\
\cdot\, 2\ \cancel{1} \\ \hline
3E
\end{array}
\qquad
\begin{array}{r}
1\,F \\
\cdot\, F\cancel{E} \\ \hline
1D\,1
\end{array}$$

   Svar: Kvoten är $2F$ och resten är D i hexadecimal form. (I decimal form blir det 47 respektive 13.)

2. Bestäm den största gemensamma delaren mellan $x^4+x^3+2x^2+x+1$ och x^4+x^2+1 i $\mathbf{Z}_3[x]$. **(3)**

   Lösning: Vi beräknar den största gemensamma delaren med Euklides algoritm.

$$\begin{aligned}
x^4+x^3+2x^2+x+1 &= 1\cdot(x^4+x^2+1)+x^3+x^2+x \\
x^4+x^2+1 &= (x+2)\cdot(x^3+x^2+x)+x^2+x+1 \\
x^3+x^2+x &= x\cdot(x^2+x+1)+0
\end{aligned}$$

   där den mellersta raden fås genom följande polynomdivision:

$$\begin{array}{r|lllll}
 & & & & x & +2 \\ \cline{2-6}
x^3+x^2+x & x^4 & & +x^2 & & +1 \\ \cline{1-1}
 & x^4 & +x^3 & +x^2 & & \\ \cline{2-4}
 & & 2x^3 & & & +1 \\
 & & 2x^3 & +2x^2 & +2x & \\ \cline{3-6}
 & & & x^2 & +x & +1
\end{array}$$

Den största gemensamma delaren ges av den sista icke-försvinnande resten som i det här fallet är $x^2 + x + 1$.

Svar: $\mathrm{sgd}(x^4 + x^3 + 2x^2 + x + 1, x^4 + x^2 + 1) = x^2 + x + 1$ i $\mathbf{Z}_3[x]$.

3. Bestäm det minsta antal färger som krävs för att kantfärga den bipartita grafen G har hörnmängd $\{1, 2, 3, 4, 5\} \cup \{A, B, C, D, E\}$ och kantmängd

$$\{1B, 1D, 1E, 2A, 2B, 2C, 3A, 3B, 3D, 4B, 4C, 4D, 5A, 5D, 5E\}.$$

(3)

Lösning: Det minsta antalet färger som krävs för att färga en bipartit graf ges av den största valensen för något hörn i grafen. Hörnen $1, 2, 3, 4$ och 5 har alla valens 3, medan valenserna för hörnen A, B, C, D och E är $3, 4, 2, 4, 2$. Alltså är den maximala valensen 4 och den krävs fyra färger för att kantfärga G.

Svar: Det krävs 4 färger för att kantfärga G.

4. De två permutionerna α och β ges i tvåradsnotation av

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$$

Avgör vilka av permutationerna α^{-1}, $\alpha\beta$ och $\alpha^2\beta^3$ som är udda och vilka som är jämna. **(3)**

Lösning: Vi skriver först permutationerna med cykelnotation. Vi får $\alpha = (1534)(2)$ och $\beta = (14352)$. Eftersom en cykel av udda längd är jämn och tvärtom får vi att α är udda och β jämn.

Inversen av en udda permutation är udda eftersom sammansättningen av permutationen och dess invers skall ge identitetspermutationen som är jämn. Alltså är α^{-1} udda.

Sammansättningen av en udda permutation med en jämn är udda, och därmed är $\alpha\beta$ udda.

En jämn potens av en permutation är alltid jämn och alla potenser av jämna permutationer är jämna. Därmed är $\alpha^2\beta^3$ jämn.

Svar: Permutationerna α^{-1} och $\alpha\beta$ är udda medan $\alpha^2\beta^3$ är jämn.

5. Den linjära koden C ges av

$$C = \{00000000, 01100110, 11001100, 00110011, \\ 11111111, 01010101, 10101010, 10011001\}.$$

Hur många fel upptäcker, respektive rättar, koden C? **(3)**

Lösning: För att avgöra hur många fel koden upptäcker, respektive rättar, behöver vi veta det minimala avståndet δ. Eftersom koden i detta fall är linjär ges δ av den minsta positiva vikten av något kodord. Eftersom vikterna för kodorden i C är $0, 4, 4, 4, 8, 4, 4, 4, 4$, är det minimala avståndet $\delta = 4$. Koden upptäcker tre fel, eftersom $\delta \geq 3 + 1$, men $\delta < 4 + 1$. Den rättar endast ett fel eftersom $\delta \geq 2 \cdot 1 + 1$, men $\delta < 2 \cdot 2 + 1$.

Svar: Koden C upptäcker tre fel och rättar ett fel.

6. På hur många sätt kan man med k färger hörnfärga en skog med 36 hörn och 30 kanter? **(4)**

Lösning: En skog består av ett antal disjunkta träd. Vi kan välja ett hörn i varje träd som rot och sedan färga träden utifrån roten. På det sättet ser vi att vi har k valmöjligheter för varje rot, men $k - 1$ val för varje annat hörn.

Vi behöver nu veta hur många rötter skogen har, dvs antalet komponenter. Ett träd med n hörn har $n - 1$ kanter. Om skogen har m träd med $n_1, n_2, \ldots, n_m$ hörn får vi då totalt $\sum_{i=1}^{m} n_i$ hörn och $\sum_{i=1}^{m}(n_i - 1) = (\sum_{i=1}^{m} n_i) - m$ kanter. Eftersom vi nu har 36 hörn och 30 kanter måste $m = 36 - 30 = 6$. Antalet sätt att färga grafen med k färger blir därmed $k^6(k-1)^{30}$.

Svar: En skog med 36 hörn och 30 kanter kan hörnfärgas på $k^6(k-1)^{30}$ sätt med k färger.

7. Den genererande funktionen för talföljden $a_0, a_1, a_2, \ldots$ ges av

$$\frac{1+x}{(1-2x)(1-4x^2)}.$$

Bestäm ett uttryck för a_n. **(4)**

Lösning: Eftersom $(1-2x)(1-4x^2) = (1-2x)^2(1+2x)$ kan vi partialbråksuppdela den genererande funktionen som

$$\frac{1+x}{(1-2x)(1-4x^2)} = \frac{A}{(1-2x)^2} + \frac{B}{(1-2x)} + \frac{C}{(1+2x)}$$

Genom att multiplicera med $(1-2x)^2$ i båda led och sedan sätta in $x = 1/2$ får vi

$$A = \frac{1 + 1/2}{(1 + 2 \cdot (1/2))} = 3/4.$$

Om vi multiplicerar med $(1+2x)$ och sätter in $x = -1/2$ får vi

$$C = \frac{1 + (-1/2)}{(1 - 2 \cdot (-1/2))^2} = \frac{1}{8}$$

och sätter vi slutligen in $x = 0$ får vi $A+B+C = 1$, vilket ger $B = 1-3/4-1/8 = 1/8$.

Vi kan nu använda binomialsatsen för negativa exponenter för att få

$$\frac{1}{(1-2x)^2} = \sum_{i=0}^{\infty} \binom{-2}{i} (-2x)^i = \sum_{i=0}^{\infty} (-1)^i \binom{2+i-1}{i} (-2x)^i = \sum_{i=0}^{\infty} (i+1)(2x)^i.$$

De övriga två termerna är geometriska serier och vi får

$$a_n = \frac{3}{4}(n+1)2^n + \frac{1}{8}2^n + \frac{1}{8}(-2)^n = \frac{2^n}{8}(6n+7+(-1)^n) = 2^{n-3}(6n+7+(-1)^n).$$

Svar: Följden ges av $a_n = 2^{n-3}(6n+7+(-1)^n)$, för $n \geq 0$.

8. Ett barn har sex klossar i sex olika färger. På hur många sätt kan barnet lägga alla klossarna i en rad så att den gula inte hamnar bredvid den blå och inte heller den gröna bredvid den röda? **(4)**

Lösning: Det finns $6! = 720$ olika sätt att lägga klossarna i en rad till att börja med. I en del fall kommer den gula ligga bredvid den blå, i en del fall kommer den röda ligga bredvid den gröna och i en del fall både och. Vi använder sållprincipen för att räkna hur många fall vi ska ta bort.

Antalet fall då den gula ligger bredvid den blå kan vi räkna genom att först räkna de positioner de två klossarna kan ha, dvs 5. För var och en av dessa finns det två ordningar för dessa två klossar och sedan $4! = 24$ olika sätt att lägga de övriga fyra klossarna. Detta ger $5 \cdot 2 \cdot 24 = 240$ olika sätt.

Antalet fall då den röda ligger bredvid den gröna blir av symmetriskäl också 240.

Det återstår att räkna de fall då både den gula ligger bredvid den blå och den röda bredvid den gröna. Om den gula och den blå ligger i ena änden av raden finns det tre möjliga positioner för den gröna och röda att ligga bredvid varandra på. Detta ger $2 \cdot 2 \cdot 3 \cdot 2$ olika fall och i var och en av dessa finns 2 möjligheter för de två sista klossarna. Alltså totalt 48 fall. Om den gula och den blå inte ligger i någon ända finns två möjliga positioner för den röda och den gröna att ligga bredvid varandra. Detta ger $3 \cdot 2 \cdot 2 \cdot 2 = 24$ fall och återigen två möjligheter för de övriga två, vilket totalt ger 48 fall. Sammanlagt finns $48 + 48 = 96$ fall när både den gula ligger bredvid den blå och den röda bredvid den gröna.

Enligt sållprincipen får vi att antalet sätt att lägga klossarna så att varken den gula hamnar bredvid den blå eller den röda bredvid den gröna är

$$720 - 240 - 240 + 96 = 336.$$

Svar: Det går på 336 sätt.

9. Bestäm lösningarna till ekvationen $x^2 + x + 60 = 0$ i kroppen $\mathbf{Z}_{101}$. **(4)**

   Lösning: För att utföra kvadratkomplettering av andragradsekvationen behöver vi kunna dela med 2. Inversen till 2 kan vi få genom Euklides algortim som i detta fall endast är ett steg, $101 = 2 \cdot 50 + 1$, vilket ger $2 \cdot (-50) \equiv 1 \pmod{101}$. Vi kan därför skriva om ekvationen som

$$(x - 50)^2 - (-50)^2 + 60 = 0$$

   vilket kan förenklas till

$$(x - 50)^2 = 2440$$

   Eftersom $2440 = 24 \cdot 101 + 16$, är detta detsamma som

$$(x - 50)^2 = 16.$$

   Eftersom ett element kan ha högst två kvadratrötter i en kropp och vi vet att $4^2 = 16$ och $(-4)^2 = 16$ får vi att lösningarna ges av $x = 50 \pm \sqrt{16} = 50 \pm 4$, dvs $x = 46$ och $x = 54$.

   Svar: Lösningarna till ekvationen är $x = 46$ och $x = 54$ i $\mathbf{Z}_{101}$.

10. För ett primtal p kan vi för varje positivt heltal a definiera en funktion $f_a : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ genom $f_a(x) = x^a$ för alla x i $\mathbf{Z}_p$. Avgör för vilka värden på a som funktionen f_a är surjektiv. **(4)**

    Lösning: Att funktionen är surjektiv är i det här fallet samma sak som att den är injektiv och bijektiv, eftersom den går från från en ändlig mängd till samma ändliga mängd.

    Eftersom $f_a(0) = 0$ och $f_a(x) \neq 0$ om $x \neq 0$ räcker det att avgöra när funktionen är bijektiv från $\mathbf{Z}_p^*$ till $\mathbf{Z}_p^*$.

    Enligt Fermats lilla sats har vi att $x^{p-1} = 1$ för alla x i $\mathbf{Z}_p^*$. Detta betyder att $x^{k(p-1)+1} = x$ för alla x i $\mathbf{Z}_p^*$ och därmed är f_a bijektiv om $a = k(p-1)+1$, eftersom f_a då är identitetsfunktionen. Vi har emellertid också att $f_a \circ f_b = f_{ab}$, och därmed kommer f_a att vara inverterbar, och därmed surjektiv, om a är inverterbart modulo $p - 1$, dvs om $\mathrm{sgd}(a, p-1) = 1$.

    Vi skall nu försöka visa att f_a inte är surjektiv om $\mathrm{sgd}(a, p-1) \neq 1$. Antag att det finns en gemensam delare $k > 1$ mellan a och $p - 1$. Då finns det ett positivt heltal $m = (p-1)/k$ så att $am = (a/k)(p-1)$ är delbart med $p - 1$ och $m < p - 1$. Vi har då att $f_a(x^m) = x^{am} = x^{(p-1)a/k} = 1^{a/k} = 1$ för alla x i $\mathbf{Z}_p^*$. Om nu f_a var bijektiv, skulle detta innebära att $x^m = 1$ för alla x i $\mathbf{Z}_p^*$, men en polynomekvation av grad m över en kropp kan inte ha mer än m rötter, och eftersom $m < p - 1$ ger detta en motsägelse. Alltså kan inte f_a vara bijektiv.

    Svar: Funktionen f_a är surjektiv precis om a och $p - 1$ är relativt prima.