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

Lösningsförslag till
Tentamen i 5B1118 Diskret matematik 5p
14 augusti, 2002

1. Använd induktion för att visa att 8 delar $(2n+1)^2-1$ för alla $n \geq 0$. **(3)**

   Lösning: Vi börjar med basfallet, det vill säga $n = 0$. Då fås $(2n+1)^2-1 = 1-1 = 0$ och 8 delar som bekant 0.

   Nu till induktionssteget. Vi antar att påståendet stämmer för $n = k$ och avser visa det för $n = k+1$. Vi ska alltså visa att 8 delar $(2(k+1)+1)^2-1$. Men

   $$(2(k+1)+1)^2-1 = ((2k+1)+2)^2-1 = (2k+1)^2+4(2k+1)+4-1 = (2k+1)^2-1+8(k+1).$$

   Eftersom vi antagit att 8 delar $(2k+1)^2-1$ står det nu klart att 8 delar $(2(k+1)+1)^2-1$. Enligt induktionsprincipen är det ursprungliga påståendet visat.

2. Finns det en uppsättning delmängder av $S = \{1,2,3,4,5,6\}$ sådana att alla har fyra element och att varje element i S förekommer i precis sex av delmängderna? **(3)**

   Lösning: Om det finns en sådan uppsättning av delmängder måste det vara nio stycken Detta kan vi se genom att räkna par av element och delmängder som innehåller elementet. Vi får $6 \cdot 6 = 36$ par eftersom varje element ligger i sex delmängder och eftersom varje delmängd innehåller fyra element måste det vara $36/4 = 9$ delmängder. För att få det lättare att konstruera en uppsättning av nio delmängder med fyra element kan vi se på komplementen till mängderna. Dessa innehåller nu bara två element var och vi vill att varje element skall förekomma i tre av komplementen, eftersom $9-6 = 3$. Vi låter elementen vara rader och komplementen till delmängderna vara kolonner i en tabell. Vi kan exempelvis fylla tabellen så här

	1	2	3	4	5	6	7	8	9
1	×			×			×		
2	×				×				×
3		×		×				×	
4		×				×			×
5			×		×		×		
6			×			×		×	

   Genom att räkna antalet kryss i varje rad och varje kolonn kan vi se att vi har tre i varje rad och två i varje kolonn. För delmängderna motsvarar det sex i varje rad och fyra i varje kolonn, vilket är precis det vi vill ha. Tabellen svarar mot de nio delmängderna $\{3,4,5,6\}$, $\{1,2,5,6\}$, $\{1,2,3,4\}$, $\{2,4,5,6\}$, $\{1,3,4,6\}$, $\{1,2,3,5\}$, $\{2,3,4,6\}$, $\{1,2,4,5\}$ och $\{1,3,5,6\}$.

Svar: Det finns sådana delmängder, exempelvis $\{3,4,5,6\}$, $\{1,2,5,6\}$, $\{1,2,3,4\}$, $\{2,4,5,6\}$, $\{1,3,4,6\}$, $\{1,2,3,5\}$, $\{2,3,4,6\}$, $\{1,2,4,5\}$ och $\{1,3,5,6\}$.

3. Visa att 129 inte är ett primtal genom att utföra *Fermat-testet* med bas 2. **(3)**

   Lösning: Vi ska beräkna $2^{128} \pmod{129}$. Om detta inte blir 1 vet vi att 129 inte är ett primtal. Vi får

$$2^{128} \equiv (2^7)^{18} \cdot 2^2 \equiv (-1)^{18} \cdot 4 \equiv 4 \pmod{129}.$$

   Alltså klarar 129 inte Fermat-testet med bas 2 och kan därmed inte vara ett primtal.

4. Faktorisera polynomet $x^4 + 2x^3 + x + 1$ i irreducibla faktorer i $\mathbf{Z}_7[x]$. **(3)**

   Lösning: Eftersom 7 är ett primtal är $\mathbf{Z}_7$ en kropp. Vi börjar med att leta efter irreducibla faktorer av grad ett. Enligt faktorsatsen räcker det att se på nollställena till polynomet. Vi beräknar polynomets värde i alla sju punkter.

$$\begin{aligned}
&p(0) = 0^4 + 2\cdot 0^3 + 0 + 1 = 1\\
&p(1) = 1^4 + 2\cdot 1^3 + 1 + 1 \equiv 1+2+1+1 \equiv 5 \pmod{7}\\
&p(2) = 2^4 + 2\cdot 2^3 + 2 + 1 \equiv 16+16+2+1 \equiv 35 \equiv 0 \pmod{7}\\
&p(3) = 3^4 + 2\cdot 3^3 + 3 + 1 \equiv 81+54+3+1 \equiv 139 \equiv 6 \pmod{7}\\
&p(4) = (-3)^4 + 2\cdot(-3)^3 + (-3) + 1 \equiv 81-54-3+1 \equiv 25 \equiv 4 \pmod{7}\\
&p(5) = (-2)^4 + 2\cdot(-2)^3 + (-2) + 1 \equiv 16-16-2+1 \equiv -1 \equiv 6 \pmod{7}\\
&p(6) = (-1)^4 + 2\cdot(-1)^3 + (-1) + 1 \equiv 1-2-1+1 \equiv -1 \equiv 6 \pmod{7}
\end{aligned}$$

   Det finns alltså en linjär faktor $x-2$. Vi dividerar x^4+2x^3+x+1 med $x-2$ och får

$$\begin{array}{r|lllll}
 & x^3 & +4x^2 & +x & +3 \\ \hline
x-2 & x^4+2x^3 & & +x & +1 \\
 & x^4-2x^3 & & & \\ \hline
 & 4x^3 & & +x & +1 \\
 & 4x^3 & -x^2 & & \\ \hline
 & & x^2 & +x & +1 \\
 & & x^2 & -2x & \\ \hline
 & & & 3x & +1 \\
 & & & 3x & -6 \\ \hline
 & & & & 0
\end{array}$$

   Vi vet redan att kvoten $q(x) = x^3+4x^2+x+3$ inte har något nollställe utom möjligen $x=2$. Vi sätter in $x=2$ och får

$$q(2) = 2^3 + 4\cdot 2^2 + 2 + 3 = 8 + 16 + 2 + 3 = 29 \equiv 1 \pmod{7}.$$

Alltså finns inga nollställen till $q(x)$ och eftersom graden är tre måste det därmed vara irreducibelt. Faktoriseringen av x^4+2x^3+x+1 är alltså $(x-2)(x^3+4x^2+x+3)$ i $\mathbf{Z}_7[x]$.

Svar: Faktoriseringen av x^4+2x^3+x+1 i irreducibla faktorer i $\mathbf{Z}_7[x]$ är $(x-2)(x^3+4x^2+x+3)$.

5. I England bedrivs sedan länge en speciall sorts klockringning, där n olika stämda kyrkklockor används. Man ringer dessa i sekvenser, där alla klockor ingår exakt en gång i varje sekvens (varje sekvens svarar mot en permutation av klockorna). Permutationerna för två sekvenser i följd får bara skilja sig åt med en granntransposition (två element bredvid varandra byter plats). En tillåten följd av sekvenser med tre klockor är exempelvis `ABC, ACB, CAB, CBA, BCA, BAC`. Klockringningen är slut när man hunnit med samtliga permutationer.

   Betrakta problemet att finna en sådan följd av sekvenser, för godtyckligt n. Modellera detta som ett grafproblem, med permutationerna som hörn. Vad svarar en giltig klockringning mot i grafteoretiska termer? Är det i allmänhet lätt att finna en lösning till sådana problem? **(3)**

   Lösning: Vi skapar en graf med permutationerna som hörn. Två hörn är grannar, det vill säga att det går en kant mellan dem, om dessa permutationer skiljer sig åt med en granntransposition. Vi vill finna en stig i denna graf sådan att varje hörn besöks exakt en gång. Detta kallar vi en *Hamiltonstig*. Det är i allmänhet ett svårt problem att finna en Hamiltonstig i en graf.

6. Förklara hur en latinsk rektangel kan utvidgas till en latinsk kvadrat med hjälp av kantfärgning av bipartita grafer. Illustrera metoden genom att fylla ut rektangeln

$$\begin{array}{ccccc} A & B & C & D & E \\ E & A & D & C & B \end{array}$$

   (4)

   Lösning: Vi associerar en bipartit graf till den latinska rektangeln genom att införa hörnen $\{A,B,C,D,E\}$ och $\{1,2,3,4,5\}$ och kanter mellan hörnen om symbolen inte står i motsvarande kolonn. Vi får då kanterna

$$\{A3, A4, A5, B1, B3, B4, C1, C2, C5, D1, D2, D5, E2, E3, E4\}.$$

   Om vi lyckas kantfärga denna graf med tre färger kan vi låta de tre färgerna svara mot de tre rader som fattas för att rektangeln skall bli en kvadrat. Att samma färg används precis en gång för varje hörn innebär att kvadraten kommer att ha den latinska egenskapen att varje symbol står precis en gång i varje rad och varje kolonn. Den ursprungliga rektangeln svarar mot en kantfärgning av den komplementära bipartita grafen och sammantaget ger det en kantfärgning av den fullständiga bipartita grafen.

För att finna en kantfärgning av vår graf börjar vi med att försöka med den första färgen. Vi väljer till symbolerna A, B, C, D, E det första hörn på motsvarande sida som fortfarande inte är upptaget. Vi börjar med $A3$ och går vidare med $B1$, $C2$, $D5$ och $E4$. Vi har nu lyckats med en färg, och den graf som återstår om vi tar bort dessa fem kanter är tvåvalent, och kan därmed enkelt kantfärgas genom att följa cyklerna och ge kanterna alternerande färger. Vi får då $A4$ i ena färgen, $B4$ i andra, osv. De två sista färgerna ges av $\{A4, B3, E2, D1, C5\}$ och $\{B4, E3, D2, C1, A5\}$. Den utfyllda kvadraten blir nu

$$\begin{matrix} A & B & C & D & E \\ E & A & D & C & B \\ B & C & A & E & D \\ D & E & B & A & C \\ C & D & E & B & A \end{matrix}$$

7. En linjär kod ges av matrisen

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

Hur många fel rättar den? Hur många kodord innehåller den? Om ordet 0110011 mottas, vilket kan vi då anta skickades? **(4)**

Lösning: Koden som ges av H är en Hammingkod, eftersom matrisen innehåller alla möjliga kolonner utom den med enbart nollor. Den rättar därför ett fel. Antalet kodord ges av formeln 2^{2^r-r-1}, där r är antalet rader i matrisen. I detta fall får vi $2^4 = 16$ kodord.

Om vi multiplicerar H på vektorn (0110011) får vi vektorn (111). Vi letar reda på den kolonn som är (111), nämligen den andra. Det innebär att det har blivit fel i andra positionen i det skickade ordet. Det som skickades var således 0010011.

Svar: Koden rättar ett fel och innehåller 16 kodord. Det ord som skickades är 0010011.

8. Om sex personers namn skrivs på lappar som slumpvis fördelas till de sex personerna, så att alla får var sin, är sannolikheten att ingen får sitt eget namn 53/144. Bevisa detta, exempelvis med hjälp av sållprincipen. **(4)**

Lösning: Vi betraktar de $6! = 720$ permutationer som fås genom alla möjliga sätt att fördela lapparna. Vi är ute efter att räkna de permutationer som saknar fixpunkter och sedan dela med det totala antalet permutationer. För att räkna antalet permutationer utan fixpunkter använder vi sållprincipen. Låt A_i vara de permutationer som fixerar i, för $i = 1, 2, 3, 4, 5, 6$. Vi vill beräkna kardinaliteten hos komplementet till unionen av dessa.

När vi använder sållprincipen behöver vi kunna beräkna skärningar av flera A_i. Skärningen av k av mängderna består av permutationer som fixerar motsvarande k element. Vi får $(6-k)!$ olika permutationer som fixerar k givna element eftersom de resterande $6-k$ punkterna får permuteras fritt. Antalet sätt att välja ut k av delmängderna är $\binom{6}{k}$. För att beräkna antalet element i unionen bestämmer vi

$$\begin{aligned}
\alpha_1 &= |A_1| + |A_2| + |A_3| + |A_4| + |A_5| + |A_6| = 5! \cdot \tbinom{6}{1} = 6! = 720 \\
\alpha_2 &= |A_1 \cap A_2| + \cdots + |A_5 \cap A_6| = 4! \cdot \tbinom{6}{2} = 24 \cdot 15 = 360 \\
\alpha_3 &= |A_1 \cap A_2 \cap A_3| + \cdots + |A_4 \cap A_5 \cap A_6| = 3! \cdot \tbinom{6}{3} = 6 \cdot 20 = 120 \\
\alpha_4 &= |A_1 \cap A_2 \cap A_3 \cap A_4| + \cdots + |A_3 \cap A_4 \cap A_5 \cap A_6| = 2! \cdot \tbinom{6}{4} = 2 \cdot 15 = 30 \\
\alpha_5 &= |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5| + \cdots + |A_2 \cap A_3 \cap A_4 \cap A_5 \cap A_6| = 1! \cdot \tbinom{6}{5} = 6 \\
\alpha_6 &= |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5 \cap A_6| = 0! \cdot \tbinom{6}{6} = 1 \cdot 1 = 1
\end{aligned}$$

och enligt sållprincipen är

$$|A_1 \cup A_2 \cup \cdots \cup A_6| = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 + \alpha_5 - \alpha_6 = 720 - 360 + 120 - 30 + 6 - 1 = 455$$

och antalet element i komplementet till unionen blir $6! - 455 = 720 - 455 = 265$. Eftersom det totala antalet permutationer är $6! = 720$ är sannolikheten att det blir en permutation utan fixpunkter $265/720 = 53/144$.

Svar:

9. Låt $M \subseteq \{\{a_1, a_2, \ldots\} | a_i \in \mathbf{N}\}$ vara mängden av följder $\{a_1, a_2, \ldots\}$ av naturliga tal sådana att endast ett ändligt antal element är nollskilda. Visa med hjälp av *Aritmetikens fundamentalsats* att mängden M har samma kardinalitet som de naturliga talen. **(4)**

   Lösning: Enligt aritmetikens fundamenalsats har varje positivt heltal en unik faktorisering i primtal. Om vi numrerar primtalen som $p_1, p_2, p_3, \ldots$ kan vi nu uttrycka en sådan faktorisering som
$$p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots$$
   där exponenterna förr eller senare alla är noll. Oservera att det finns ett oändligt antal primtal, så p_i kommer att vara definierat för alla positiva heltal i.

   Vi utnyttjar detta för att få en bijektion mellan M och de positiva hela talen genom

$$a_1, a_2, a_3, \ldots \mapsto p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots$$

   Denna funktion är injektiv eftersom faktoriseringen är unik, och den är surjektiv eftersom varje positivt heltal har en sådan faktorisering. Vi har därmed att M har samma kardinalitet som de positiva heltalen. Vi kan å andra sidan finna en bijektion från de positiva hela talen till de naturliga talen genom att sända n på $n-1$. Alltså finns en bijektion mellan M och de naturliga talen och de har samma kardinalitet.

10. Vi säger att en permutation $\sigma = \sigma_1\sigma_2\ldots\sigma_n$ innehåller mönstret $\tau = \tau_1\tau_2\ldots\tau_k$, om vi kan plocka ut element $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}$, där $i_1 < i_2 < \ldots < i_k$, så att de är ordnade storleksmässigt på samma sätt som τ. Exempel: permutationen 164523 innehåller mönstret 132 på flera ställen, såsom **164**523, **16**45**2**3 och **1**64**523**. Den innehåller däremot inte mönstret 213.

    Låt L_k vara längden hos den kortaste permutationen som innehåller **alla** mönster av längd k. Visa att $L_k \geq \frac{k^2}{e^2}$ för stora k genom att visa att kortare permutationer inte kan innehålla alla mönster av längd k, eftersom det inte finns tillräckligt med delsekvenser i dem. Du får använda att $k! \geq \sqrt{2\pi}k^{k+1/2}e^{-k}$. **(4)**

    Lösning: En permutation av längd L_k innehåller $\binom{L_k}{k}$ delsekvenser av längd k. Antalet permutationer av längd k är $k!$. Vi vill alltså visa att $\binom{L_k}{k} < k!$ om $L_k < \frac{k^2}{e^2}$.

    Vi skriver om $\binom{L_k}{k} < k!$ som $L_k(L_k-1)(L_k-2)\ldots(L_k-k+1) < (k!)^2$. Eftersom $L_k(L_k-1)(L_k-2)\ldots(L_k-k+1) < L_k^k$ räcker det att visa $L_k^k \leq k!$. Men

$$(k!)^2 \geq (\sqrt{2\pi}k^{k+1/2}e^{-k})^2 = 2\pi k^{2k+1}e^{-2k} = ((2\pi k)^{1/k}\frac{k^2}{e^2})^k.$$

    Därmed står det klart att om $L_k < \frac{k^2}{e^2}$ så är

$$L_k(L_k-1)(L_k-2)\ldots(L_k-k+1) < L_k^k \leq \left(\frac{k^2}{e^2}\right)^k \leq \left((2\pi k)^{1/k}\frac{k^2}{e^2}\right)^k \leq (k!)^2,$$

    det vill säga att

$$\binom{L_k}{k} < k!.$$