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

Lösningsförslag till kontrollskrivningar
5B1118 Diskret matematik 5p
9 april, 2002

KS 1

1. Bestäm en lösning till den diofantiska ekvationen $456n + 347m = 3$. **(3)**

   Lösning: Använd Euklides algoritm på 456 och 347. Det ger $156 \cdot 456 - 205 \cdot 347 = 1$ och multiplikation med 3 ger en lösning $x = 468$, $y = 615$. Övriga lösningar fås genom $x = 468 - 347k$, $y = 456k - 205$.

2. Formulera aritmetikens fundamentalsats och använd den för att visa att $\sqrt{3}$ inte är rationellt, dvs att det inte finns positiva heltal m och n sådana att $m/n = \sqrt{3}$. **(3)**

   Lösning: Aritmetikens fundamentalsats säger att varje positivt heltal har en primtalsfaktorisering som är unik sånär som på ordningen av faktorerna. $m/n = \sqrt{3}$ innebär att $m^2 = 3n^2$. Vi kan anta att m och n saknar gemensamma primtalsfaktorer, eftersom vi annars skulle kunnat förkorta m/n. Nu förekommer alla primtalsfaktorer på vänster sida ett jämnt antal gånger, medan faktorn 3 förekommer ett udda antal gånger på höger sida. Detta ger en motsägelse och därför måste $\sqrt{3}$ vara irrationellt.

KS 2

1. Hur många permutationer i S_8 har typ $[2^2 4]$? **(3)**

   Lösning: En permutation av typ $[2^2 4]$ består av två cykler av längd två och en cykel av längd fyra. Om vi skriver permutationen som $(x_1x_2)(y_1y_2)(z_1z_2z_3z_4)$ ser vi att det finns 8! sätt att göra detta eftersom alla symboler skall förekomma precis en gång. Däremot kommer varje permutation representeras på flera sätt, eftersom det finns 2 sätt att skriva vardera av de två tvåcyklerna och 4 sätt att skriva fyrcykeln. Dessutom kan vi byta plats på de två tvåcyklerna. Detta ger totalt $8!/(2 \cdot 2 \cdot 4 \cdot 2) = 1260$ permutationer på den givna formen.

2. Visa att summan av talen i en rad i Pascals triangel är 2^n för något n. **(3)**

Lösning: Summan i en rad i Pascals triangel ges av

$$\sum_{k=0}^{n} \binom{n}{k}$$

och enligt binomialsatsen har vi att

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Med $x = y = 1$ ger detta

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$$

Vi kan också se det rent kombinatoriskt eftersom summan representerar antalet sätt att välja ut en delmängd med k element ur en mängd med n element när k går över alla tal från 0 till n. Då får vi det totala antalet delmängder av en mängd med n element, dvs 2^n.

KS 3

1. Kryptera meddelandet $x = 4$ i ett RSA-system med öppen nyckel $n = 91$ och $e = 47$ **(3)**

   Lösning: Vi behöver beräkna $E(4) = 4^{47}$ modulo 91. Detta kan göras exempelvis med successiv kvadrering. $4^2 = 16$, $4^4 = 16^2 = 256 \equiv -17 \pmod{91}$, $4^8 \equiv (-17)^2 \equiv 16 \pmod{91}$, $4^{16} \equiv 16^2 \equiv -17 \pmod{91}$ och $4^{32} \equiv (-17)^2 \equiv 16 \pmod{91}$. Till slut får vi

   $$4^{47} = 4^{1+2+4+8+32} \equiv 4 \cdot 16 \cdot (-17) \cdot 16 \cdot 16 \equiv 4 \cdot 1 \cdot (-17) \equiv -68 \equiv 23 \pmod{91}.$$

2. Förklara hur man kan använda Stirlingtal för att beräkna antalet surjektiva funktioner från en mängd med n element till en mängd med k element och beräkna detta antal om $n = 7$ och $k = 5$. **(3)**

   Lösning: Antalet surjektiva funktioner från en mängd X med n element till en mängd Y med k element ges av $k!S_{n,k}$, eftersom varje surjektiv funktion ger upphov till en partition av X i k delar, medan alla funktioner som fås från en given funktion genom att permutera elementen i Y ger upphov till samma partition.

Speciellt för $n = 7$ och $k = 5$ får vi $5!S_{7,5}$ surjektiva funktioner och vi kan beräkna $S_{7,5}$ genom rekursionsformeln

$$S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$$

i uppställningen

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 1 & & & & \\
 & & & 1 & & 7 & & 6 & & 1 & & & \\
 & & 1 & & 15 & & 25 & & 10 & & 1 & & \\
 & 1 & & 31 & & 90 & & 65 & & 15 & & 1 & \\
1 & & 63 & & 301 & & 350 & & 140 & & 21 & & 1
\end{array}$$

Alltså finns det $5! \cdot 140 = 120 \cdot 140 = 16800$ surjektiva funktioner från en mängd med sju element till en mängd med fem element.

KS 4

1. Bestäm den största gemensamma delaren mellan $x^4+x^3-x^2-2x+4$ och x^4+2x^3-x+1 i $\mathbf{Z}_5[x]$. **(3)**

   Lösning: Med Euklides algoritm fås

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

   Alltså är $3x^2+x+4$ den största gemensamma delaren mellan $x^4+x^3-x^2-2x+4$ och x^4+2x^3-x+1 i $\mathbf{Z}_5[x]$. Om ledande koefficienten skall vara ett blir det x^2+2x+3.

2. Visa att en grupp av ordning fyra måste vara isomorf med C_4 eller $C_2 \times C_2$. **(3)**

   Lösning: I en grupp av ordning fyra måste alla element ha en ordning som är en delare i $4 = 2 \cdot 2$. Om det finns ett element av ordning fyra är gruppen cyklisk, och därmed isomorf med C_4. Annars måste alla element ha ordning 1 eller 2. Eftersom bara identitetselementet kan ha ordning 1 måste de övriga tre elementen ha ordning 2. Om vi kallar elementen för $\{e, a, b, c\}$ där e är identitetselementet får vi genast följande partiellt ifyllda grupptabell.

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

För de övriga positionerna finns nu endast en möjlighet eftersom grupptabellen måste vara en latinsk kvadrat. Exempelvis måste $ab = c$, eftersom de övriga tre elementen förekommer i samma rad, eller i samma kolonn som ab. Den fullständiga grupptabellen blir

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Alltså måste alla grupper av ordning fyra som inte är cykliska vara isomorfa med varandra och eftersom $C_2 \times C_2$ är en sådan grupp är de isomorfa med $C_2 \times C_2$.

KS 5

1. Bestäm antalet kanter i en skog med 117 hörn och 13 komponenter. **(3)**

   Lösning: En skog med 13 komponenter består av 13 disjunkta träd. Ett träd med n hörn har $n-1$ kanter. Det kan vi se genom induktion, genom att ta bort ett löv i taget från trädet tills det inte finns några kanter kvar, men fortfarande ett hörn. För varje träd är alltså antalet kanter ett mindre än antalet hörn. Vi får därför $117 - 13 = 104$ kanter i en skog med 13 komponenter.

2. Förklara hur och varför algoritmen med alternerande stigar fungerar för att hitta en fullständig matchning i en bipartit graf där Halls kriterium är uppfyllt. **(3)**

   Lösning: Se avsnitt 10.4 i kursboken.