Institutionen för matematik, **KTH**
Mats Boij

Lösningsförslag till
Tentamen i 5B1118 Diskret matematik 5p
25 april, 2001

1) Bestäm den största gemensamma delaren mellan 407 och 594. **(3p)**

Lösning: Vi använder Euklides algoritm för att bestämma den största gemensamma delaren.

$$\begin{aligned} 594 &= 1 \cdot 407 + 187 \\ 407 &= 2 \cdot 187 + 33 \\ 187 &= 5 \cdot 33 + 22 \\ 33 &= 1 \cdot 22 + 11 \\ 22 &= 2 \cdot 11 + 0 \end{aligned}$$

och vi får $\text{sgd}(407, 594)$ som den sista nollskillda resten, dvs 11.

Svar: $\text{sgd}(407, 594) = 11$.

2) Skriv upp cykelnotationen för sammansättningen $\tau^{-1}\sigma\tau$ där $\sigma = (135)(64)$ och $\tau = (24)(356)$. **(3p)**

Lösning: Vi bestämmer τ^{-1} genom att se vad som står före de respektive elementen i cykelnotationen. Ett annat sätt är att invertera varje cykel för sig själv. Inversen ges därmed av $\tau^{-1} = (24)(365)$. Vi får sammansättningen genom att sätta in resultatet av en permutation i nästa.

$$\begin{aligned} \tau^{-1}\sigma\tau(1) &= \tau^{-1}(\sigma(\tau(1))) = \tau^{-1}(\sigma(1)) = \tau^{-1}(3) = 6 \\ \tau^{-1}\sigma\tau(2) &= \tau^{-1}(\sigma(\tau(2))) = \tau^{-1}(\sigma(4)) = \tau^{-1}(6) = 5 \\ \tau^{-1}\sigma\tau(3) &= \tau^{-1}(\sigma(\tau(3))) = \tau^{-1}(\sigma(5)) = \tau^{-1}(1) = 1 \\ \tau^{-1}\sigma\tau(4) &= \tau^{-1}(\sigma(\tau(4))) = \tau^{-1}(\sigma(2)) = \tau^{-1}(2) = 4 \\ \tau^{-1}\sigma\tau(5) &= \tau^{-1}(\sigma(\tau(5))) = \tau^{-1}(\sigma(6)) = \tau^{-1}(4) = 2 \\ \tau^{-1}\sigma\tau(6) &= \tau^{-1}(\sigma(\tau(6))) = \tau^{-1}(\sigma(3)) = \tau^{-1}(5) = 3 \end{aligned}$$

Cykelnotationen får vi nu genom att följa de olika elementen genom permutationen, och resultatet blir $\tau^{-1}\sigma\tau = (163)(25)$.

Svar: Cykelnotationen för sammansättningen blir $\tau^{-1}\sigma\tau = (163)(25)$.

3) Kryptera meddelandet $x = 25$ om den öppna nyckeln i ett RSA-system är $n = 55$ och $e = 9$. **(3p)**

Lösning: Krypteringsalgoritmen ger $E(x) = x^e \pmod{n}$ och i detta fall behöver vi beräkna $25^9 \pmod{55}$. Med successiv kvadrering fås $25^2 = 625 \equiv 20 \pmod{55}$, $25^4 = (25^2)^2 \equiv 20^2 \equiv 400 \equiv 15 \pmod{55}$, $25^8 = (25^4)^2 \equiv 15^2 \equiv 225 \equiv 5 \pmod{55}$ och därmed

$$25^9 \equiv 25^1 \cdot 25^8 \equiv 25 \cdot 5 \equiv 125 \equiv 15 \pmod{55}.$$

Svar: Det krypterade meddelandet är 15.

4) Bestäm ordningen av den multiplikativa gruppen av inverterbara element i $\mathbf{Z}_{24}$. **(3p)**

Lösning: Ordningen av en grupp är antalet element i gruppen. Den multiplikativa gruppen av inverterbara element i $\mathbf{Z}_{24}$ består av de restklasser $[a]_{24}$ där $\text{sgd}(a, 24) = 1$. Eftersom $24 = 2^3 \cdot 3$ ges dessa precis av de a som inte är delbara med varken 2 eller 3. Vi kan räkna upp dessa restklasser genom att stryka alla multipler av 2 och 3:

$$\not{0}, \mathbf{1}, \not{2}, \not{3}, \not{4}, \mathbf{5}, \not{6}, \mathbf{7}, \not{8}, \not{9}, \not{10}, \mathbf{11}, \not{12}, \mathbf{13}, \not{14}, \not{15}, \not{16}, \mathbf{17}, \not{18}, \mathbf{19}, \not{20}, \not{21}, \not{22}, \mathbf{23}$$

Kvar blir $\{[1], [5], [7], [11], [13], [17], [19], [23]\}$, dvs åtta olika restklasser.

Svar: Ordningen av den multiplikativa gruppen av inverterbara element i $\mathbf{Z}_{24}$ är åtta.

5) Grafen G ges av nedanstående granntabell. Avgör om det går att lägga till en kant i grafen G så att den resulterande grafen G' har en eulerväg.

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

(3p)

Lösning: Det finns en eulerväg i en graf precis om grafen är sammanhängande och antalet hörn med udda valens är högst två. Vi kan se att alla hörn i grafen G har jämn valens. När vi lägger till en kant kommer de två hörnen som är ändpunkter till denna kant att få udda valens, men övriga hörn kommer fortfarande att ha jämn valens. Alltså blir det två hörn med udda valens oavsett vilken kant vi lägger till. Det återstår att se ifall vi kan lägga till en kant så att grafen G' blir sammanhängande. I grafen G bildar hörnen 2, 3 och 6 en sammanhängande komponent som inte har någon förbindelse med övriga hörn. Hörnen 4, 5, 7 och8 har kanter till hörnet 1 och hörnet 9 har kanter till 4 och 5. Alltså bildar hörnen $\{1, 4, 5, 7, 8, 9\}$ en sammanhängande komponent och G består av två komponenter. Därmed blir grafen sammanhängande om vi lägger till en kant mellan dessa två komponenter, exemepelvis kanten 12.

Svar: Det går att lägga till en kant i grafen G så att den resulterande grafen har en eulerväg.

6) Ett barn har sex klossar i olika färger. På hur många sätt kan barnet lägga klossarna i tre likadana lådor så att det kommer minst en kloss i varje låda? **(4p)**

Lösning: Att lägga de sex olika klossarna i tre identiska lådor så att det kommer minst en i varje är detsamma som att ge en partition av mängden av klossar i precis tre delar. Antalet sådana partitioner ges av Stirlingtalet $S_{6,3}$. För att beräkna detta kan vi använda rekursionsformeln $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$, och startvärdena $S_{n,1} = S_{n,n} = 1$, för alla $n \geq 1$. Om vi ställer upp det i något som liknar Pascals triangel får vi

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 3 & & 1 & & & & \\
 & 1 & & 7 & & 6 & & 1 & & & \\
1 & & 5 & & 25 & & 10 & & 1 & & \\
1 & & 31 & & 90 & & 65 & & 15 & & 1
\end{array}$$

och vi kan läsa av att $S_{6,3} = 90$.

Svar: Barnet kan lägga klossarna i tre likadana lådor på 90 olika sätt.

7) Bestäm den genererande funktionen för lösningen till rekursionen

$$a_{n+2} = a_{n+1} - 3a_n, \qquad n \geq 0$$

med begynnelsevärdena $a_0 = 2$ och $a_1 = 3$. **(4p)**

Lösning: Den genererande funktionen för talföljden a_n är $\sum_{n=0}^{\infty} a_n x^n$. Eftersom talföljden uppfyller rekursionen $a_{n+2} = a_{n+1} - 3a_n$ för $n \geq 0$ får vi att

$$\begin{aligned}
(1 - x + 3x^2)\sum_{n=0}^{\infty} a_n x^n &= a_0 + (a_1 - a_0)x + (a_2 - a_1 + 3a_0)x^2 + \cdots \\
&= a_0 + (a_1 - a_0)x + 0 = 2 + (3 - 2)x = 2 + x.
\end{aligned}$$

Alltså kan vi skriva den genererande funktionen som $\sum_{n=0}^{\infty} a_n x^n = \frac{(2+x)}{(1-x+3x^2)}$.

Svar: Den genererande funktionen för lösningen kan skrivas som $(2+x)/(1-x+3x^2)$.

8) Använd stark induktion för att bevisa att varje positivt heltal kan skrivas som en produkt av primtal. **(4p)**

Lösning: Vi börjar med att repetera definitionen av primtal; ett primtal är ett heltal större än ett som inte kan skrivas som en produkt av mindre positiva heltal. För att påståendet vi skall bevisa skall kunna vara sant måste vi acceptera att en produkt av primtal kan bestå av ett eller inget primtal.

Vi konstaterar nu att 1 kan skrivas som en produkt av (noll) primtal. Vi kan nu göra induktionsantagandet att varje positivt heltal mindre än n kan skrivas som en produkt av primtal, och vi vill visa att även n kan skrivas som en produkt av

primtal. Eftersom $n > 1$ är n antingen ett primtal eller ett sammansatt tal. Om n är ett primtal är det en produkt av (ett) primtal. Om n är sammansatt kan det skrivas som en produkt av två positiva heltal som är strikt mindre än n. Enligt induktionsantagandet är dessa produkter av primtal, och eftersom en produkt av produkter av primtal är en produkt av primtal följer att n är en produkt av primtal. Enligt induktionsprincipen gäller därmed att alla positiva heltal är produkter av primtal.

9) Använd metoden med alternerande stigar för att från matchningen $\{1A, 2B, 3C\}$ få en fullständig matchning i den bipartita grafen med hörnmängd $\{1, 2, 3, 4\} \cup \{A, B, C, D, E\}$ och kantmängd $\{1A, 1D, 2B, 2E, 3A, 3C, 4B, 4C\}$. **(4p)**

Lösning: Vi börjar med att se på det enda hörnet 4 i $X = \{1, 2, 3, 4\}$ som inte är med i matchningen. Vi väljer en kant som utgår från 4, tex $4B$. Eftersom B är matchat med 2 går vi vidare till 2. Vi ser nu att det också går en kant från 2 till E, så vi går vidare till E. Nu är inte E matchat med något hörn och vi kan gå tillbaka längs stigen och byta ut kanterna i matchningen mot de som inte är med i matchningen. Vi får då matchningen $\{1A, 2E, 3C, 4B\}$ som är fullständig eftersom varje hörn i X är med i matchningen.

10) Bevisa eller ge motexempel till identiteten

$$2|A \cup B \cup C| - 2|A \cap B \cap C| = |A \cup B| + |B \cup C| + |C \cup A| - |A \cap B| - |B \cap C| - |C \cap A|.$$

där A, B och C är ändliga delmängder av en mängd S. **(4p)**

Lösning: Identiteten är sann och vi kan bevisa den genom att använda sållprincipen. För tre ändliga delmängder A, B och C av en mängd S har vi

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Om vi sätter in detta i vänsterledet av identiteten får vi

$$2(|A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|) - 2|A \cap B \cap C|$$

vilket kan förenklas till

$$2|A| + 2|B| + 2|C| - 2|A \cap B| - 2|B \cap C| - 2|C \cap A| \tag{1}$$

Sållprincipen för två av mängderna i taget ger att

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ |B \cup C| &= |B| + |C| - |B \cap C| \\ |C \cup A| &= |C| + |A| - |C \cap A| \end{aligned}$$

och lägger vi ihop dessa tre får vi

$$|A \cup B| + |B \cup C| + |C \cup A| = 2|A| + 2|B| + 2|C| - |A \cap B| - |B \cap C| - |C \cap A|.$$

Om vi löser ut $2|A| + 2|B| + 2|C|$ ur detta och sätter in i (1) får vi att vänsterledet i den givna identiteten är lika med

$$|A \cup B| + |B \cup C| + |C \cup A| - |A \cap B| - |B \cap C| - |C \cap A|.$$

vilket är lika med högerledet. Därmed är identiteten bevisad.