Matematiska Institutionen
KTH

Lösningar till tentamensskrivning i Diskret Matematik för IT2, CL2 och Media 1, SF1610 och 5B1118, torsdagen den 20 december 2007.

1. Euklides algoritm ger

$$\begin{aligned} 654 &= 1 \cdot 573 + 81 \\ 573 &= 7 \cdot 81 + 6 \\ 81 &= 13 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

   Svar: 3.

2. Vi placerar först ut pojkarna, vilket går på $5!$ olika sätt. Sedan placerar vi i tur och ordning ut flickorna i mellanrummen mellan pojkarna, vilket går på $4!$ olika sätt. Multiplikationsprincipen ger nu oss

   Svar: $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 4 \cdot 3 \cdot 3 \cdot 2 \cdot 1$

3. Gruppen G består av 10 element och en genrator till gruppen skall ha ordning 10. Vi vet att ordningen av varje element i gruppen är en delare till antalet element i gruppen, i detta fall 10. Så nu provar vi oss fram tills vi hittar en generator:

$$2^2 = 4 \neq 1, \quad 2^5 = -1 \neq 1$$

   Alltså har elementet 2 varken ordning 2 eller 5. Alltså har elementet 2 ordning 10 och är en generator till G

   Svar: 2

4. (a)

$$2^7 \pmod{39} = 128 \pmod{39} = 11.$$

   Svar: 11.

   (b) Då $n = 3 \cdot 13$ skall det gälla att $e \cdot d = 1$ i ringen $Z_{2 \cdot 12}$. Med $e = 7$ gissar vi att $d = 7$ vilket stämmer då $7 \cdot 7 \equiv 1 \pmod{24}$.

   Svar: $d = 7$.

   (c)

$$3^7 \pmod{39} = 3^4 \cdot 3^2 \cdot 3 \pmod{39} = 3 \cdot 9 \cdot 3 \pmod{39} = 3.$$

   Svar: 3.

5. En alternerande stig börjar i en omatchad nod, t ex b, som har en kant till 3, så vi börjar med kanten $b3$. Från noden 3 måste vi, om den noden är matchad ta en kant i givnma matchningen dvs kanten $a3$. Vi väljer nu att från noden a välja kanten $a1$ och då 1 är omatchad så är vi klar.

   Svar: $b - 3 - a - 1$.

DEL II

6. (a)
$$(1\ 3)(1\ 2)(1\ 3) = (1)(2\ 3) = (2\ 3)$$
(b) T ex har vi att givna permutationen är på cykelform lika med
$$(2\ 3\ 4\ 5)$$
som vi ju kan skriva som
$$(2\ 5)(2\ 4)(2\ 3).$$
Utnyttjar vi nu lösningen i (a) uppgiften får vi
$$(2\ 5)(2\ 4)(2\ 3) = (1\ 2)(1\ 5)(1\ 2)(1\ 2)(1\ 4)(1\ 2)(1\ 2)(1\ 3)(1\ 2) = (1\ 2)(1\ 5)(1\ 4)(1\ 3)(1\ 2).$$
(c) Välkänt är att varje permutation kan skrivas som en produkt av transpositioner typ $(a\ b)$, och varje permutation $(a\ b)$ kan skrivas som
$$(a\ b) = (1\ a)(1\ b)(1\ a).$$
Alltså kan alla permutationer skrivas som en produkt av transpositioner av typ $(1\ x)$.

7. Vi väljer att konstruera en linjär kod och beskriva den med hjälp av en kontrollmatris. Antalet kolonner i denna matris är 9 eftersom ordlängden är 9.

Kravet (a) ger, då antalet ord skall vara $16 = 2^4$, att matrisen skall ha precis fem rader.

Kravet (b) ger att alla rader skall innehålla ett jämnt antal ettor.

Kravet (c) tillfredsställer vi om låter 111000000 vara ett kodord och kravet (d) om vi låter 100011100 vara ett kodord, dvs summan av de tre första kolonnerna är nollkolonnen resp summan av den första och kolonnerna nummer 5, 6 och 7 blir nollkolonnen.

Vi prövar oss fram lite och finner
$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

8. Totala antalet surjektioner är $6!S(6,3)$. Från detta antal skall vi dra de surjektioner som uppfyller kravet (a) resp (b). Vi beräknar nu antalet surjektioner i respektive fall:

(a) I detta fall kan A, B och C identifieras some ett element och vi skall beräkna antalet surjektioner från $\{ABC, D, E, F\}$ till mängden $\{1, 2, 3\}$. Detta antal är $3!S(4,3)$.

(b) För vart och ett av elementen A, B och C skall vi välja ett unikt bildelement $f(A)$, $f(B)$ resp $f(C)$, vilket kan ske på $3! = 6$ olika sätt. För vart och ett av elementen D, E och F skall vi välja om dessa skall avbildas på samma element som A, eller B, eller C avbildas på (X avbildas på $f(X)$ kan man säga om man vill). Så antalet möjligheter är $3^3 = 27$.

Nu återstår att beräkna $S(6,3)$ och $S(4,3)$, som vi gör med hjälp av rekursionen
$$S(n,k) = S(n-1,k-1) + kS(n-1,k), \qquad S(n,n) = 1, \quad S(n,1) = 1.$$
$$S(6,3) = S(5,2) + 3S(5,3), \quad S(5,3) = S(4,2) + 3S(4,3), \quad S(5,2) = S(4,1) + 2S(4,2)$$
$$S(4,2) = S(3,1) + 2S(3,2), \quad S(4,3) = S(3,2) + 3S(3,3), \quad S(3,2) = S(2,1) + 2S(2,2).$$
Alltså
$$S(3,2) = 3, \quad S(4,3) = 6, \quad S(4,2) = 7, \quad S(5,2) = 15, \quad S(5,3) = 25, \quad S(6,3) = 90.$$

Svar: $3! \cdot 90 - 3! \cdot 6 - 3^3 \cdot 6 = 345$.

DEL III

9. (a) Först ser vi att

$$n(1-\frac{1}{p})(1-\frac{1}{q}) = n\frac{(p-1)(q-1)}{pq} = (p-1)(q-1).$$

Ett tal är relativt primt till n precis då det varken delas av p eller q. Inklusion exklusion ger nu med A_p som mängden av tal delbara med p och A_q som talen delbara med q att antalet tal mellan 1 och n som är relativt prima till n som

$$n - |A_p| - |A_q| + |A_p \cap A_q|.$$

Vart p:te tal är delbart med p så $|A| = n/p = q$ och $|B| = n/q = p$. Det är endast n som är delbart med både p och q, dvs $|A_p \cap A_q| = 1$, så

$$n - p - q + 1 = pq - p - q + 1,$$

som ju är lika med $(p-1)(q-1)$.

(b) Antag

$$n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_k^{e_k},$$

där $p_1, p_2, \ldots, p_k$ är olika primtal och talen $e_1, e_2, \ldots, e_k$ alla är större än noll.
Låt A_i beteckna mängden av tal mellan 1 och n som är delbara med p_i. Vi finner att

$$|A_i| = \frac{n}{p_i}, \quad |A_i \cap A_j| = \frac{n}{p_i p_j}, \quad |A_i \cap A_j \cap A_s| = \frac{n}{p_i p_j p_s}, \quad \ldots.$$

Principen om inklusion exklusion ger nu att antalet tal i intervallet 1 till n, somär relativt prima till n blir

$$n - \sum_{i=1}^{n} \frac{n}{p_i} + \sum \frac{n}{p_i p_j} - \sum \frac{n}{p_i p_j p_s} + \ldots = n[1 - \sum_{i=1}^{n} \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_s} + \ldots],$$

som man kan trolla om till formeln

$$n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k}).$$

10. Betrakta gruppen S_3 av permutationer på mängden med tre element $\{1,2,3\}$. De två 2-cyklerna $(1\ 2)$ och $(1\ 3)$ har båda ordning två men deras produkt som är $(1\ 2)(1\ 3) = (1\ 3\ 2)$ har ordning 3 som ju inte delar $mgm(2,2) = 2$. Så formeln går alltså inte att generalisera generellt till det icke abelska fallet.

Låt nu $N = mgm(\sigma(a), \sigma(b))$. Då gäller $N = k_1\sigma(a)$ och $N = k_2\sigma(b)$. Vi får då, pga kommutativiteten att

$$(a \circ b)^N = a^N \circ b^N = (a^{\sigma(a)})^{k_1} \circ (b^{\sigma(b)})^{k_2} = e^{k_1} \circ e^{k_2} = e,$$

om e betecknar gruppens identitetselement.

Låt nu d beteckna ordningen av elementet $a \circ b$ och antag $N = k \cdot d + r$ där $0 \leq r < d$. Vi får då

$$e = (a \circ b)^N = (a \circ b)^{kd+r} = ((a \circ b)^d)^k (a \circ b)^r = e^k (a \circ b)^r = (a \circ b)^r,$$

men $r < d$ och d var ordningen av elementet $a \circ b$, dvs det minsta tal d sådant att $(a \circ b)^d = e$. Enda möjligheten är att $r = 0$ och alltså att d delar N vilket skulle visas.