Matematiska institutionen
KTH

Lösningar till tentamensskrivning på kursen Diskret Matematik, 5B1118, för IT, den 7 juni 2006.

1. I ringen Z_{34} gäller att $7x - 32 = 25$ ger att $7x = 25 + 32 = 23$. Då $5 \cdot 7 = 1$ får vi då att $x = 5 \cdot 23 = 13$ eftersom $115 \equiv 13 \pmod{34}$.

   Svar $x = 13$.

2. Både 5 och 6 ligger i samtliga mängder. Vi klistrar ihop dessa element med varandra. Hur vi än manövrerar med mängdoperationerna delas inga element upp i bitar. Alltså kan elementet 56 ej splittras upp och en mängd med enbart elementet 5 kan ej erhållas.

3. Låt A, B och C beteckna de av talen 1,2,...,120 som är delbara med 2, 3 respektive 5. Enligt principen om inklusion exklusion gäller att vi får svaret med hjälp av formeln

$$120 - (|A| + |B| + |A|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|\,.$$

   Vartannat tal är delbart med 2 så $\mid A \mid = 60$, vart tredje delbart med 3 så $\mid B \mid = 40$ osv. Alltså

   Svar $120 - (60 + 40 + 24) + (20 + 12 + 8) - 4 = 32$.

4. Vi skriver upp additionstabellerna för $(Z_2, +)$ och $(Z_3, +)$:

$+$	0	1
0	0	1
1	1	0

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

   Mängden av permutationer på en mängd med tre element bildar en icke abelsk grupp med sex element.

5. (a) $4 + 5 \notin \{0, 1, 2, 3, 4, 5\}$ medför att mängden inte är sluten med avseende på addition. Mängden är då inte en delgrupp.

   (b) Eftersom talet 15 inte delar talet 24 kan inte, enligt Lagranges sats, G ha en delgrupp med 15 element.

   (c) Sidoklasserna blir

$$H + 0 = \{0, 4, 8, 12, 16, 20\}$$

$$H + 1 = \{0 + 1, 4 + 1, 8 + 1, 12 + 1, 16 + 1, 20 + 1\} = \{1, 5, 9, 13, 17, 21\}$$

$$H + 2 = \{0 + 2, 4 + 2, 8 + 2, 12 + 2, 16 + 2, 20 + 2\} = \{2, 6, 10, 14, 18, 22\}$$

$$H + 3 = \{0 + 3, 4 + 3, 8 + 3, 12 + 3, 16 + 3, 20 + 3\} = \{3, 7, 11, 15, 19, 23\}$$

6. Vi har att $n = 77 = 7 \cdot 11$ så $m = 6 \cdot 10 = 60$. Dekrypteringsnyckeln d erhålls nu ur sambandet $e \cdot d \equiv 1 \pmod{60}$ med hjälp av Euklides algoritm: $60 = 2 \cdot 37 - 14$, $37 = 3 \cdot 14 - 5$ och $14 = 3 \cdot 5 - 1$, varur

   $$1 = 3 \cdot 5 - 14 = 3(3 \cdot 14 - 37) - 14 = 8 \cdot 14 - 3 \cdot 37 = 8(2 \cdot 37 - 60) - 3 \cdot 37 = 13 \cdot 37 - 8 \cdot 60.$$

   Vi sluter att $13 \cdot 37 \equiv 1 \pmod{60}$ och därmed att $d = 13$. Då $2^{13} \equiv 30 \pmod{77}$ så

   Svar 37.

7. (a) Operation nummer 1: Placera A_1 i en kö och A_2 i den andra kön. Två möjligheter.

   Operation nummer 2: Välj ut de fyra personer bland de åtta återstående som skall stå i samma kö som A_1. Finns $\binom{8}{4}$ möjligheter.

   Operation nummer 3: Ordna den första kön. Finns 5! möjligheter.

   Operation nummer 4: Ordna den andra kön. Finns 5! möjligheter.

   Enligt multiplikationsprinipen finns nu $2 \cdot \binom{8}{4} 5!5!$ olika köer.

   (b) Operation 1: Klistra ihop A_1 och A_2 till antingen A_1A_2 eller A_2A_1. Två möjligheter.

   Operation 2: Välj kö åt dessa: Två möjligheter.

   Operation 3: Välj kökamrater till dem: $\binom{8}{3}$ möjligheter.

   Operation 4: Ordna den kön: 4! olika möjligheter.

   Operation 5: Ordna den andra kön: 5! olika möjlighere.

   Enligt multiplikationsprinipen finns nu $2 \cdot \binom{8}{3} 4!5!$ olika köer.

8. (a) Låt alla kanter som går från en av noderna ha vikten 1. Fördela vikten godtyckligt bland de övriga och kanterna med vikt 1 bildar ett minimalt spännade träd med vikten 5.

   (b) Låt alla kanter som går från en av noderna ha vikten 3. Varje spännade träd måste då innehålla en kant med vikten 3. Låt nu alla övriga kanter från en annan nod v ha vikten 1. Fördela vikten godtyckligt bland de övriga. Kanterna från noden v bildar nu ett minimalt spännade träd med vikten 7.

9. (a) Den cykliska gruppen med 143 element består av elementen

   $$< a >= \{a, a^2, a^3, \ldots, a^{143} = 1\}.$$

   Följande mängder bildar delgrupper med 11 respektive 13 element.

   $$H =< a^{13} >= \{a^{13}, (a^{13})^2, (a^{13})^3, (a^{13})^4 \ldots, (a^{13})^{11} = 1\}.$$

   $$K =< a^{11} >= \{a^{11}, (a^{11})^2, (a^{11})^3, (a^{13})^4 \ldots, (a^{13})^{13} = 1\}.$$

(b) Vi skall visa att för varje t med $1 \leq t \leq 143$ finns tal x och y med $1 \leq x \leq 13$ och $1 \leq y \leq 11$ så att

$$a^t = (a^{11})^x (a^{13})^y = a^{11x+13y}.$$

Likheten ovan ger nu att

$$t \equiv 11x + 13y \pmod{143}.$$

Eftersom 11 och 13 är relativt prima finns för varje värde på talet t och talet n minst en lösning (x, y) till den diofantiska ekvationen

$$t = 11x + 13y.$$

Betrakta en sådan lösning. Vi vet också att övriga lösningar kan skrivas

$$(x', y') = (x + k13, y - k11).$$

Välj nu k så att $1 \leq x + k13 \leq 13$ och sedan väljer vi n så att $1 \leq y - k11 - 11n \leq 11$. Låt nu $x' = x + k13$ och $y' = y - k11 - n11$. Då gäller att

$$t + n143 = 11x' + 13y'.$$

10. Betrakta den kontrollmatris H som varje linjär kod har och speciellt den kod C som vi söker. Om avståndet mellan orden c och c' i C är ett gäller att

$$0 = Hc - Hc' = H(c - c') = k_i$$

där k_i är kolonn nummer i och orden c oh c' skiljer i precis position i. Så detta inträffar aldrig, dvs att $0 = k_i$, precis då H saknar en nollkolonn.

Antal ord i koden C är 2^{8-r} där vi kan låta r beteckna antalet rader i H. Med $r = 1$ och en matris utan nollkolonn får vi som enda möjlighet

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Men då innehåller koden ordet 11000000. Alltså kan vi utesluta möjligheten att C innehåller 2^7 stycken ord. Alltså $|C| \leq 2^6$. Men t ex med

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

får vi en kod med 2^6 ord men utan ordet 11000000.