Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE, CL och CMETE, SF1610 och 5B1118, måndagen den 17 oktober 2011, kl 08.00-13.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

DEL I

Var och en av nedanstående uppgifter svarar mot en kontrollskrivning. Godkänt resultat på en kontrollskrivning ger automatiskt full poäng på motsvarande uppgift. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Bestäm
$$17^{2011} \pmod{10} .$$

   Lösning: Då $17 \equiv_{10} 7$ och $7^2 = 5 \cdot 10 - 1 \equiv_{10} -1$ så
   $$17^{2011} \equiv_{10} 7^{2011} \equiv_{10} (7^2)^{1005} \cdot 7 \equiv_{10} (-1)^{1005} \cdot 7 \equiv_{10} (-1) \cdot 7 \equiv_{10} 3 ,$$
   varur

   SVAR: 3.

2. (3p) En klass med de 10 flickorna F_1, F_2, ..., F_{10} och de 10 pojkarna P_1, P_2, ..., P_{10} skall utse en grupp om sex klassrepresentanter med lika många pojkar som flickor. På hur många olika sätt kan man sätta samman en sådan grupp om pojken P_3 deltar endast på villkor att minst en av flickorna F_4 och F_8 blir med i gruppen. För full poäng krävs att svaret ges i formen av ett heltal.

   Lösning: Eftersom det skall vara tre pojkar och tre flickor i gruppen blir totala antalet möjliga grupper, om P_3 inte ställer några krav, lika med
   $$\binom{10}{3} \cdot \binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} \cdot \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 120 \cdot 120 = 14400 .$$
   Antalet otillåtna grupper är de där P_3 är med men ingen av flickorna F_4 eller F_8. Då skall man utse ytterligare två pojkar förutom P_3 samt tre flickor bland de övriga åtta flickorna. Antalet sätt detta går på är
   $$\binom{9}{2} \cdot \binom{8}{3} = \frac{9 \cdot 8}{1 \cdot 2} \cdot \frac{8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3} = 36 \cdot 56 = 1680 + 336 = 2016 .$$

   SVAR: $14400 - 2016$ dvs 12384.

3. (3p) Bestäm fyra cykliska delgrupper till gruppen $G = (Z_{30}, +)$.

   Lösning: Förutom $G = \langle 1 \rangle$ har vi t ex

$$\begin{aligned} \langle 0 \rangle &= \{0\}\,, \\ \langle 15 \rangle &= \{15, 0\}\,, \\ \langle 10 \rangle &= \{10, 20, 0\} \end{aligned}$$

4. (a) (2p) Ett RSA-krypto har parametrarna $n = 95$, $e = 29$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.

   Lösning: Då $n = 5 \cdot 19$ så $m = (5-1)(19-1) = 72$. För den dekrypterande nyckeln d gäller att $d \cdot 29 \equiv_{72} 1$. Vi bestämmer nu d med hjälp av Euklides algoritm:

$$\begin{aligned} 72 &= 2 \cdot 29 + 14 \\ 29 &= 2 \cdot 14 + 1 \end{aligned}$$

   så

$$1 = 29 - 2 \cdot 14 = 29 - 2(72 - 2 \cdot 29) = 5 \cdot 29 - 2 \cdot 72\,,$$

   så $29 \cdot 5 \equiv_{72} 1$ och $d = 5$. Det dekrypterade meddelandet ges av $D(3) = 3^5 \pmod{95}$ som vi beräknar nu:

$$D(3) = 3^5 = 81 \cdot 3 \equiv_{95} (-14) \cdot 3 \equiv_{95} -42 \equiv_{95} 53\,.$$

   SVAR: 53.

   (b) (1p) Vilka värden på parametern n kan ett RSA-kryto ha om $45 \leq n \leq 55$.

   Lösning: n skall vara en produkt av två olika primtal så möjliga ärden på n är 46, 51 och 55.

5. (3p) Rita en komplett bipartit graf $K_{n,m}$ med totalt 8 noder, dvs $n+m = 8$, som har en Eulerkrets men inte har någon Hamiltoncykel.

   Lösning: Vi ritar den kompletta bipartita grafen $K_{2,6}$.

DEL II

6. (3p) Förklara varför en graf, som har 30 noder med valens 1, 15 noder med valens 2 och minst 30 noder med valens minst 3, måste ha minst en cykel.

   Lösning: Vi bestämmer först antalet kanter i grafen med hjälp av sambandet summan av nodernas valenser är två gånger antalet kanter. Antag

först att antalet noder med valens minst tre är precis 30 och att alla dessa 30 noder har valensen 3. Vi finner då att valenssumman är

$$30 \cdot 1 + 15 \cdot 2 + 30 \cdot 3 = 150 = 2 \cdot 75 \, .$$

En graf utan cykler är en skog, dvs en graf bestående av träd. Antalet kanter i ett träd är ett mindre än antalet noder, så om grafen skulle bestå av enbart träd skulle antalet kanter vara färre än antalet noder. Då antalet noder är

$$30 + 15 + 30 = 75 \, ,$$

dvs lika många som antalet kanter, så kan grafen alltså inte enbart bestå av träd.

Nu betraktar vi de generella fallet med $30 + a$ noder av valens minst tre, utöver de noder som har valens 1 resp 2. Antalet noder blir då $75 + a$ och antalet kanter blir, med standardbeteckningar

$$\frac{1}{2} \sum_{v \in V} \delta(v) \geq \frac{1}{2}(30 \cdot 1 + 15 \cdot 2 + (30 + a) \cdot 3) = 75 + \frac{3}{2}a \geq 75 + a \, ,$$

och resonemanget ovan ger återigen att grafen inte kan vara en skog.

7. (3p) Bestäm antalet positiva hela tal som delar både talet 2156 och talet 2548.

Lösning: Den största gemensamma delaren D till två tal n och m har egenskapen att om talet d delar både n och m så gäller att d delar D. Givetvis gäller också att om d' delar D så delar d' både n och m.

Vi börjar med att bestämma $\text{sgd}(2156, 2548)$ med hjälp av Euklides algoritm:

$$\begin{aligned} 2548 &= 2156 + 392 \\ 2156 &= 5 \cdot 392 + 196 \\ 392 &= 2 \cdot 196 \end{aligned}$$

Alltså är $\text{sgd}(2156, 2548) = 196$, ett tal som vi nu lätt faktoriserar:

$$196 = 2 \cdot 98 = 2 \cdot 2 \cdot 49 = 2 \cdot 2 \cdot 7 \cdot 7 \, .$$

Enligt aritmetikens fundamentalsats gäller då att

$$d \mid 196 \qquad \Longleftrightarrow \qquad d = 2^a 7^b \, ,$$

där $(a, b) \in \{0, 1, 2\} \times \{0, 1, 2\}$. Denna direkta produkt av mängder innehåller totalt nio element så

SVAR: 9.

8. (a) (2p) Bestäm antalet sätt som elementen i mängden $\{1, 2, 3, 4, 5, 6\}$ kan delas in i fyra icketomma delmängder så att elementen 1 och 2 hamnar i olika delmängder. Svaret skall ges i formen av ett heltal.

Lösning: De otillåtna fördelningarna är de där 1 och 2 hamnar i samma delmängd. Vi skall då fördela de fem elementen $\{\{1, 2\}, 3, 4, 5, 6\}$ i fyra icketomma delmängder vilket går på $S(5, 4)$ olika sätt. Totala antalet sätt att fördela de sex elementen i fyra icketomma delmängder är $S(6, 5)$. Så svaret ges av uttrycket

$$S(6, 4) - S(5, 4) \, .$$

Stirlingtalen beräknas rekursivt enligt nedan:

$$\begin{array}{rcl} S(6,4) & = & S(5,3) + 4S(5,4) \\ S(5,4) & = & S(4,3) + 4S(4,4) = S(4,3) + 4 \\ S(5,3) & = & S(4,2) + 3S(4,3) \\ S(4,3) & = & S(3,2) + 3S(3,3) = 3 + 3 = 6 \\ S(4,2) & = & S(3,1) + 2S(3,2) = 1 + 6 = 7 \end{array}$$

så

$$S(5,3) = 7{+}3{\cdot}6 = 25, \; S(5,4) = 6{+}4 = 10, \; S(6,4) = 25{+}4{\cdot}10 = 65.$$

SVAR: 55.

(b) (3p) Bestäm antalet sätt som de 10 elementen i mängden $\{1, 2, 3, \ldots, 10\}$ kan delas in i fem icketomma delmängder så att elementen 1, 2 och 3 hamnar i olika delmängder. Svaret får innehålla beteckningar och symboler som presenterats i kursen.

Lösning: Låt x beteckna det sökta antalet sätt att fördela de 10 elementen i 5 icketomma delmängder så att 1, 2 och 3 hamnar i olika delmängder. Då kommer antal sätt att placera ut de 10 elementen i de icketomma fem etiketterade delmängderna M_1, M_2, M_3, M_4 och M_5 så att elementet 1 hamnar i M_1, elementet 2 i M_2 och elementet 3 hamnar i M_3 att vara lika med $x \cdot 2!$, eftersom det finns 2! sätt att sätta etiketter på de två mängder som inte innehåller något av elementen 1, 2 eller 3. Vi bestämmer nu antalet sätt att fördela elementen i de 5 etiketterade delmängderna.

Låt X beteckna de fördelningar av de 10 elementen, i delmängder med etiketterna M_1, M_2, ..., M_5, sådana att M_4 blir tom och Y mängden av fördelningar där M_5 blir tom.

När vi lagt ut elementen 1, 2 och 3 återstår 7 element att fördela i fem etiketterde mängder vilket går på 5^7 olika sätt. Antalet fördelningar i X och Y är 4^7 och antalet fördelningar i $X \cap Y$ är 3^7. Principen om inklusion exklusion ger alltså att

$$x \cdot 2! = 5^7 - 2 \cdot 4^7 + 3^7 \, ,$$

så
SVAR: $(5^7 - 2 \cdot 4^7 + 3^7)/2$.

DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigvis ordagrant, där de används i lösningen.

9. Mängden av alla permutationer av elementen i mängden $\{1, 2, 3, 4\}$ bildar på sedvanligt sätt, dvs under operationen sammansättning av permutationer, en grupp som vi betecknar med $\mathcal{S}_4$.

   (a) (1p) Bestäm en ickecyklisk delgrupp till $\mathcal{S}_4$ med fyra element.

   Lösning: Vi kombinerar permutationer av elementen 1 och 2 med permutationer av elementen 3 och 4 och får då följande delgrupp med fyra element:
   $$H = \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}\ .$$
   Eftersom inget element i gruppen har ordning 4 så kan inte gruppen vara cyklisk.

   (b) (2p) Visa att mängden av alla jämna permutationer i $\mathcal{S}_4$ bildar en delgrupp till $\mathcal{S}_4$ och att denna delgrupp har 12 element.

   Lösning: En permutation är jämn om den kan skrivas som en produkt av ett jämnt antal 2-cykler.
   Vi konstaterar att en produkt av ett jämnt antal 2-cykler med en produkt av ett jämnt antal 2-cykler bildar en produkt av ett jämnt antal 2-cykler. Alltså
   (i) Mängden av jämna permutationer är sluten under operationen sammansättning av permutationer.
   Eftersom associativitet gäller generellt i $\mathcal{S}_4$ så gäller det också speciellt i varje delmängd till $\mathcal{S}_4$. Alltså
   (ii) I mängden av jämna permutationer gäller associativa räknelagen.
   Då identiteten är en produkt av noll 2-cykler, (alternativt id. $=$ $(1\ 2)(1\ 2)$) så
   (iii) id. tillhör mängden av jämna permutationer.
   Om inversen till en jämn permutation φ vore en udda permutation skulle $\varphi \circ \varphi^{-1}$ vara en produkt av ett udda antal 2-cykler, vilket strider mot att id. är en jämn permutation. Alltså,
   (iv) Om φ tillhör mängden av jämna permutationer så kommer också φ^{-1} att tillhöra denna mängd.
   Egenskaperna (i), (ii), (iii) och (iv) ger nu tillsammans att mängden av jämna permutationer bildar en grupp, som vi betecknar med $\mathcal{A}_4$. Låt $\mathcal{B}_4$ beteckna de udda permutationerna i $\mathcal{S}_4$.

Låt γ vara en fix udda permutation. Eftersom produkten av en jämn permutation med en udda permutation är en udda permutation så gäller att γ definierar en funktion

$$\Gamma : \mathcal{A}_4 \quad \longrightarrow \quad \mathcal{B}_4$$

genom tillordningen

$$\varphi \mapsto \gamma\varphi \, .$$

Eftersom för varje udda permutation ψ gäller att $\gamma^{-1}\psi$ är en jämn permutation och

$$\gamma^{-1}\psi \mapsto \psi$$

så är Γ surjektiv. Då

$$\gamma\varphi' = \gamma\varphi \qquad \Longrightarrow \qquad \varphi' = \varphi \, ,$$

så är Γ också injektiv.
Funktionen Γ är således en bijektion från $\mathcal{A}_4$ till $\mathcal{B}_4$ och vi kan alltså sluta att mängderna $\mathcal{A}_4$ och $\mathcal{B}_4$ är lika stora. Var och en av de 24 permutationerna i $\mathcal{S}_4$ är antingen udda eller jämn, så

$$|\mathcal{A}_4| + |\mathcal{B}_4| = 24, \qquad |\mathcal{A}_4| = |\mathcal{B}_4|$$

vilket ger att

$$|\mathcal{A}_4| = 12 \, .$$

(c) (2p) Bestäm den minsta delgrupp till $\mathcal{S}_4$ som innehåller permutationerna (1 2 3) och (3 4).

Lösning: Vi betecknar den sökta delgruppen med H. Eftersom H är sluten m a p operationen i $\mathcal{S}_4$ så gäller att

$$(1\ 2\ 3)(3\ 4) = (1\ 2\ 3\ 4) \in H \, .$$

Nu vet vi att H innehåller element vars ordning är tre och vars ordning är fyra så då måste, enligt Lagranges sats, 3 och 4 dela antalet element i H, och antalet element i H måste dela antalet element i $\mathcal{S}_4$. Då $|\mathcal{S}_4| = 24$ så antingen är $H = \mathcal{S}_4$ eller så har H 12 element.
(Om vi hade ägt kunskapen att $\mathcal{A}_4$ är den enda delgruppen till $\mathcal{S}_4$ med 12 element hade uppgiften nu varit löst eftersom H innehåller (3 4) som är udda, så skulle inte H kuna vara lika med $\mathcal{A}_4$, den enda delgruppen med 12 element.)
Låt K beteckna nedanstående delgrupp till H:

$$K = \langle (1\ 2\ 3\ 4) \rangle = \{\mathrm{id.}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$$

och betrakta följande två sidoklasser till K i H:

$$(3\ 4)K = \{(3\ 4), (1\ 2\ 4), (1\ 4\ 2\ 3), (1\ 3\ 2)\}$$

och

$$(1\ 2\ 3)K = \{(1\ 2\ 3), (1\ 3\ 4\ 2), (2\ 4\ 3), (1\ 4)\}\ .$$

Observera att sidoklasserna är delmängder till H, så totalt har vi nu funnit 12 olika element i H, bland annat permutationen

$$\gamma = (1\ 3\ 4\ 2) \in (1\ 2\ 3)K \subseteq H\ .$$

Men elementet $\gamma^2 = (1\ 4)(2\ 3)$ i H finns inte med bland de ovan 12 redan uppräknade elementen från H, alltså måste H ha fler element än 12. Enligt vår tidigare diskussion har vi alltså

SVAR: $\mathcal{S}_4$

10. Under kursen fick ni se hur en 1-felsrättande kod C kan konstrueras med hjälp av en så kallad kontrollmatris (parity check-matris) $\mathbf{H}$, och där C ges av $\mathbf{H}$ enligt nedan:

$$c = (c_1, c_2, \ldots, c_n) \in C \qquad \Longleftrightarrow \qquad \mathbf{H}c^T = 0^T\ .$$

(a) (2p) Vilka egenskaper måste $\mathbf{H}$ ha för att en kod C, konstruerad enligt ovanstående recept, skall vara 2-felsrättande?

Lösning: Om c och c' är två ord i C på avstånd d så gäller att antalet ettor i ordet $c - c'$ är lika med d. Detta ger att för nollkolonnen 0^T gäller att

$$0^T = 0^T - 0^T = \mathbf{H}c^T - \mathbf{H}c'^T = \mathbf{H}(c - c')^T$$

dvs, nollkolonnen är en summa av d stycken kolonner, de kolonner som svara mot de koordinatpositioner i vilka c och c' skiljer sig åt. Enligt känd sats gäller att en kod är e-felsrättande om kodens minimiavstånd är $d = 2e + 1$. Enligt resonemanget ovan gäller för en kod C, konstruerad med hjälp av en kontrollmatris $\mathbf{H}$, att C är e-felsrättande precis då ingen summa av färre än $2e + 1$ kolonner i $\mathbf{H}$ blir nollkolonnen. Så

SVAR: Ingen suma av en, två, tre eller fyra kolonner blir nollkolonnen.

(b) (1p) Vilka egenskaper måste $\mathbf{H}$ ha för att en kod C, konstruerad enligt ovanstående recept, skall vara e-felsrättande?

Lösning: Enligt lösningen ovan får vi

SVAR: Ingen suma av en, två, ..., $2e$ kolonner blir nollkolonnen.

(c) (2p) Konstruera en 2-felsrättande kod med åtta ord. (Antalet poäng du får beror bland annat på ordlängden n. T ex kan du få 1p för en 2-felsrättande kod med 8 ord och med ordlängden $n = 15$.)

Lösning: Vi finner att nedanstående matris $\mathbf{H}$ genererar, enligt receptet ovan, en 2-felsrättande kod med 8 ord:

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

Nämligen, antalet kolonner är 10 och antalet rader är 7, och då dessa är "linjärt oberoende", så blir antalet ord i C lika med $2^{10-7} = 8$. Ingen summa av fyra, tre, två eller en kolonn blir nollkolonnen. Alltså kommer koden att vara 2-felsrättande.