KTH Matematik

Tentamen
5B1118 Diskret Matematik
22 maj, 2006

- tid:**8:00-13:00**
- Tillåtna hjälpmedel: Miniräknare. Inga böcker/anteckningar får användas.
- **Allt ska motiveras.** Ett svar utan förklaring är värt 0 poäng!
- Minst 3 poäng frn varje del krävs för godkänt.

DEL 1

(1) (3 p.) Visa med hjälp av induktion att:

$$1^2 + 3^2 + 5^2 + 7^2 + ... + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}.$$

för $n \geq 1$.

- $n = 1 : 1^2 = \frac{1(2-1)(2+1)}{3}$.

$$1^2 + 3^2 + 5^2 + 7^2 + ... + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}.$$

- Antag att formeln gäller till $n-1$.

$$1^2+3^2+5^2+7^2+...(2(n-1)-1)+(2n-1)^2 = \frac{(n-1)(2(n-1)-1)(2n-2+1)}{3}+(2n-1)^2 =$$

$$= (2n-1)(\frac{2n+n^2}{3}) = \frac{n(2n-1)(2n+1)}{3}.$$

(2) (3 p.) Låt f, g vara två fuktioner från $\mathbb{R}$ till $\mathbb{R}$, definierade av:

$$f(x) = ax + b \;\; g(x) = 1 - x + x^2.$$

Bestäm talen a, b sådan att $(g \circ f)(x) = 4x^2 - 6x + 3$. $g \circ f(x) = g(ax+b) = 1 - (ax+b) + (ax+b)^2 = 1 - ax - b + a^2x^2 + 2axb + b^2 = a^2x^2 + x(2ab - a) + (1 - b + b^2)$. Vi vill att: $a^2x^2 + x(2ab-a) + (1-b+b^2) = 4x^2 - 6x + 3$.

$$\begin{array}{rcl} a^2 & = & 4 \\ a(2b-1) & = & -6 \\ 1-b+b^2 & = & 3 \end{array}$$

lösninsgarna är $(a, b) = (-2, 2), (2, -1)$.

(3) (3 p.) Ange ett tal d sådan att ekvationen:

$$889x + 4473y = 3d.$$

har minst en lösning.
En sådan diofantiska ekvation har en lösning om och endast om $(889, 4473)/3d$. Man ser att $(889, 4473) = 7$ och $7/3d$ om $7/d$. Det betyder att d ska vara en multipel av 7, till exempel $7, 14, 21, ...$

DEL 2

(1) (3 p.) 15 likadana gula kulor skall läggas i tre fack A,B,C, så att A innehåller 2 eller 4 kulor, B minst 3 och C ett jämnt antal. På hur många sätt kan detta ske?
Vi först tar tre kulor för B. Om A ska innehålla två kulor då kan C innehålla $2, 4, 6, 8$ eller 10 kulor. Om C innehåller mindre än 10 lägger vi resten i B. Totalt har vi 5 möligheter beroende på hur många kulor finns i B. Om A ska innehålla fyra kulor då kan C innehålla $2, 4, 6$ eller 8 kulor. Det ger 4 möligheter. Totalt har vi $5 + 4 = 9$.

(2) (3 p.) Bestäm summan av koefficienterna i utveklingen av

$$(x + y)^{17}.$$

$$(x+y)^{17} = \sum_{k=0}^{17} \binom{17}{k} x^k y^{17-k}$$

summan av kofficienterna är

$$\sum_{k=0}^{17} \binom{17}{n} = (1+1)^{17}.$$

(3) (3 p.) Bestäm antalet heltal lösningar till ekvationen

$$x_1 + x_2 + x_3 + x_4 = 15$$

sådan att $x_1 \geq 5, x_2, x_3 \geq 0, x_4 \geq 7$. Låt $y_1 = x_1 - 5, y_2 = x_2, y_3 = x_3, y_4 = x_4 - 7$. Frågan är ekvivalent med att hitta alla icke-negativa heltal lösningar av

$$y_1 + y_2 + y_3 + y_4 = 15 - 5 - 7 = 3$$

Svaret är då $\binom{3+4-1}{3} = \binom{6}{3} = 20$.

DEL 3

(1) (3 p.) Låt $A_4 \subset \mathcal{S}_4$ vara delmängden av alla jämna permutationer:

$$A_4 = \{\sigma \in \mathcal{S}_4 \text{ med } sign(\sigma) = 1\}.$$

(a) Skriv alla elementerna av A_4. A_4 har 12 element. än jämn permutation kan vara av typ $[1^4], [2^2], [13]$:
- $(1)(2)(3)(4)$ är den enda av typ $[1^4]$
- $(12)(34), (13)(24), (14)(23)$ är alla av typ $[2^2]$.
- $(1)(234), (1)(243), (2)(123), (2)(132), (3)(124), (3)(142), (4)(123), (4)(132)$ är alla av typ [13].

(b) Låt $\cdot$ vara multiplikationen av två permutationer. Bevisa att $(A_4, \cdot)$ är en grupp.
- Multiplicationen är en binär operation på A_4 eftersom $sign(\sigma \cdot \eta) = sign(\sigma) \cdot sign(\eta)$. som vill säga att produkten av två jämna permutation är jämn.
- Produkten är associativ.
- $id = (1)(2)(3)(4)$ är jämn.
- Om σ är jämn då är $\sigma = \tau_1\tau_2...\tau_{2k}$. Man ser att $\sigma^{-1} = \tau_{2n}^{-1}...\tau_1^{-1}$. och då är σ^{-1} jämn.

(c) Är $(A_4, \cdot)$ kommutativ? Multiplitationen av två permutationer är inte kommutativ då är gruppen inte kommutativ.

(2) (3 p.)
(a) Ange en delgrupp H av $(A_4, \cdot)$, med 3 element. En permutation av typ [13] har grad 3 och då har delgruppen genererad av en sådan permutation 3 element. Till exempel är $H =< (1)(234) >= \{(1)(2)(3)(4), (1)(234), (1)(243)\}$.
(b) Har $(A_4, \cdot)$ en delgrupp med 5 element? Låt H vara en del grupp av $(A_4, \cdot)$. Enligt Lagranges sats ska antalet element i H dela $12 = |A_4|$. Det finns då ingen delgrupp med 5 element.

(3) (3 p.) Betrakta gruppen $G = (\mathcal{S}_5 \times \mathbb{Z}_8, *)$, där

$$(\sigma, [k]_8) * ((\tau, [t]_8) = (\sigma \cdot \tau, [t + k]_8).$$

(a) Bestämma $ord((14)(325), [3]_8)$. $ord((14)(325)) = l.c.m(2, 3) = 6$ som element av $\mathcal{S}_5$.
$ord([3]_8) = 8)$ som element av $\mathbb{Z}_8$. Det följer att $ord((14)(325), [3]_8) = l.c.m(6, 8) = 24$.
(b) Är G cyklisk? G är cyklisk om det finns ett element $a = (\sigma, n) \in G$ av order $|G| = 5! \cdot 8$. Det vill säga att $5!8 = 2^6 35) = l.c.m(ord(\sigma), ord(n))$. Detta innebär att $2^6 / ord(\sigma)$ eller att $2^6 / ord(n)$. Både är omöjliga.

DEL 4

(1) (3 p.) Visa att det inte finns någon graf med 7 noder vilka alla har grad 3. Låt $G = (V, E)$ en graf med $|V| = 7$ och $deg(v) = 3$ för alla noder $v \in V$. Enligt förmeln

$$\sum_{v \in V} deg(v) = 2E$$

skulle summan av alla grader vara jämn. Men $3 \cdot 7$ är odda.

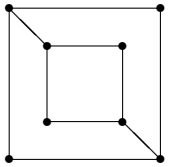
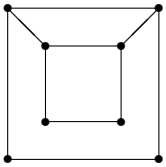
(2) (3 p.) Låt G vara en graf med 11 noder och 53 kanter.
(a) Bevisa att det finns minst en nod av grad 10. Sätt en ordning på noderna $v_1, ..., v_{11}$ så att $deg(v_1) \leq deg(v_2) \leq ... \leq (v_{11})$. Enligt

$$11 \deg(v_{11}) \geq \sum_{v \in V} deg(v) = 2E = 106$$

är $\deg(v_{11}) \geq \frac{106}{11}$. Eftersom $deg(v_{11})$ är ett heltal är $\deg(v_{11}) \geq 10$. Men grafen har bara 11 noder som betyder att graden av en nod kan inte vara större än 10. Då är $deg(v_{11}) = 10$.
(b) Bevisa att G inte är en Eulergraf.
G är Eulersk om och endast om alla noderna har jämn grad. Från formeln

$$11 \deg(v_1) \leq \sum_{v \in V} deg(v) = 2E = 106$$

vi ser att $deg(v_1) \leq 9$. Om alla noderna ska ha jämn grad då är $(deg(v_1), ..., deg(v_{11})) = (8, 8, 10, 10, ..., 10)$. Det betyder at v_i är förbunda till alla andra för $i = 3, 4, ..., 11$, men detta innebär att $grad(v_1) \geq 9$.

(3) (3 p.) Betrakta graferna G:  G': 
Är de isomorfa?
Om två grafer är isomorfa då har de lika många cyklar av givet längd. Man ser att G' hat två cyklar av längd 4, men G har bara en sådan cykel.

DEL 5

(1) (3 p.) Bevisa att polynomet $x^7 + x^2 + 1$ är reducerbart över $\mathbb{Z}_2$.

$$x^7 + x^2 + 1 = (x^5 + x^4 + x^2 + x + 1)(x^2 + x + 1).$$

(2) (3 p.) Hur många inverterbara matriser

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}_5$$

finns? (En matris A över $\mathbb{Z}_5$ är inverterbar om och endast om $det(A) \neq 0$.)
$det(A) = ad - bc \neq 0$ över $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Antag att $a, b, c, d \neq 0$. Eftersom 5 är primtal är alla elementen, utom 0, inverterbara. Om $d = 0$ då är $ad - bc = bc = 0$ när $b = 0$ eller $c = 0$. Om $d \neq 0$ då är

$$ad - bc = 0 \Rightarrow a = bcd^{-1}$$

Lösningarna är

- $(a, b, c, d) = (a, 0, c, 0), a, c \in \mathbb{Z}_5, b \neq 0; (a, b, 0, 0), a, b \in \mathbb{Z}_5; b \neq 0$ totalt $25 + 20 = 45$.
- $(bcd^{-1}, b, c, d), b, c \in \mathbb{Z}_5, d \in \mathbb{Z}_5 - \{0\}$. Totalt $5 \cdot 5 \cdot 4 = 100$.

Svar: 145

(3) (3 p.) Antag given ett RSA-system med kripteringsnyckel $n = 217$ och $e = 11$. Dekryptera meddelandet 5.
Här är $n = 217 = 31 \cdot 7$ och $m = 30 \cdot 6 = 180$. Eftersom $(180, 11) = 1$ har vi att:

$$1 = 3 \cdot 180 - 49 \cdot 11$$

Det följer att $d = [11]_{180}^{-1} = 49$.

$$D(5) = 5^{49}.$$