

Lösningar tenta SF1679 DISKRET MATEMATIK, F3 m.fl.

5 april 2018

Tryckfel kan förekomma.

1) (3p) Vi söker alla $x \in \mathbb{Z}$ som uppfyller $x^{1682} + 22x \equiv 1652 \pmod{3599}$ [$3599 = 59 \cdot 61$].

Lösning:

Enligt kinesiska restsatsen är $\mathbb{Z}_{3599} \cong \mathbb{Z}_{59} \times \mathbb{Z}_{61}$, med isomorfin $x \mapsto ([x]_{59}, [x]_{61})$, så vi börjar med att lösa ekvationen mod 59 och mod 61 var för sig.

$\mathbb{Z}_{59}$: $1682 = 58 \cdot 29$, $1652 = 59 \cdot 28$, så ekvationen blir i $\mathbb{Z}_{59}$ $(x^{58})^{29} + 22x = 0$ och eftersom 59 är ett primtal ger Fermats lilla sats att $x^{58} = \begin{cases} 0, & \text{då } x = 0, \\ 1, & \text{annars.} \end{cases}$

Lösningar blir alltså dels $x = 0$ och dels alla lösningar till $1 + 22x = 0$, dvs $x = -22^{-1}$.

Euklides algoritm: $59 = 22 \cdot 2 + 15$, $22 = 15 \cdot 1 + 7$, $15 = 7 \cdot 2 + 1$,

så $1 = 15 - 2 \cdot (22 - 15) = -2 \cdot 22 + 3 \cdot (59 - 2 \cdot 22) = 3 \cdot 59 - 8 \cdot 22$ och $22^{-1} = -8$.

Så, **mod 59** blir alla lösningar $x \equiv_{59} 0$ och $x \equiv_{59} 8$.

$\mathbb{Z}_{61}$: $1682 = 60 \cdot 28 + 2$, $1652 = 61 \cdot 27 + 5$, så ekvationen blir i $\mathbb{Z}_{61}$ $x^{60 \cdot 28 + 2} + 22x = 5$ och eftersom 61 är ett primtal ger Fermats lilla sats att $x^{28 \cdot 60 + 2} = x^2$ för alla $x \in \mathbb{Z}_{61}$.

Ekvationen blir här alltså $x^2 + 22x = 5 \Leftrightarrow (x + 11)^2 = 121 + 5 = 2^2 \Leftrightarrow (x + 9)(x + 13) = 0$.

mod 61 blir lösningarna $x \equiv_{61} -9$ och $x \equiv_{61} -13$ (61 är primtal, så $61 \mid a \cdot b \Leftrightarrow 61 \mid a$ eller $61 \mid b$).

Vi finner lösningarna i $\mathbb{Z}$ med $y_1 \equiv_{59} 1, \equiv_{61} 0$ och $y_2 \equiv_{59} 0, \equiv_{61} 1$,

$y_1 = 61s \equiv_{59} 1 \Leftrightarrow 2s \equiv_{59} 1$ och vi kan ta $s = 30$, så $y_1 = 61 \cdot 30 = 1830$ och

$y_2 = 59t \equiv_{61} 1 \Leftrightarrow 2t \equiv_{61} -1$ och vi kan ta $t = 30$, så $y_2 = 59 \cdot 30 = 1770$.

Alla lösningar (kinesiska restsatsen): $x \equiv_{3599} 0 \cdot 1830 - 9 \cdot 1770 = -15\,930 \equiv_{3599} 2065$,

$x \equiv_{3599} 0 \cdot 1830 - 13 \cdot 1770 = \dots \equiv_{3599} 2183$, $x \equiv_{3599} 8 \cdot 1830 - 9 \cdot 1770 = \dots \equiv_{3599} 2309$,

$x \equiv_{3599} 8 \cdot 1830 - 13 \cdot 1770 = \dots \equiv_{3599} 2427$.

Svar: Alla sådana $x = y + 3599 \cdot n$, $n \in \mathbb{Z}$, där $y = 2065, 2183, 2309$ eller 2427 .

2) För $f: X \rightarrow Y$, ges $f^{\llcorner}: \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ av $f^{\llcorner}(A) = \{f(a) \mid a \in A\}$. Vi skall avgöra vilka av ' $=$ ', ' $\subseteq$ ', ' $\supseteq$ ' som säkert gäller mellan (a, 1p) $f^{\llcorner}(A \cup B)$ och $f^{\llcorner}(A) \cup f^{\llcorner}(B)$, (b, 1p) $f^{\llcorner}(A \cap B)$ och $f^{\llcorner}(A) \cap f^{\llcorner}(B)$, (c, 1p) $f^{\llcorner}(A \setminus B)$ och $f^{\llcorner}(A) \setminus f^{\llcorner}(B)$.

Lösning:

a. $y \in f^{\llcorner}(A \cup B) \Leftrightarrow y = f(x)$ för något $x \in A \cup B \Leftrightarrow y = f(x)$ för något $x \in A$ och/eller $y = f(x)$ för något $x \in B \Leftrightarrow y \in f^{\llcorner}(A)$ och/eller $y \in f^{\llcorner}(B) \Leftrightarrow y \in f^{\llcorner}(A) \cup f^{\llcorner}(B)$,

så ' $=$ ' (och därmed ' $\subseteq$ ', ' $\supseteq$ ') gäller i a.

b. $y \in f^{\llcorner}(A \cap B) \Leftrightarrow y = f(x)$ för något $x \in A \cap B \Rightarrow y \in f^{\llcorner}(A) \cap f^{\llcorner}(B)$,

men $X = Y = \{a, b\}$, $A = \{a\}$, $B = \{b\}$, $f(a) = f(b) = a$ ger $f^{\llcorner}(A \cap B) = f^{\llcorner}(\emptyset) = \emptyset$ och $f^{\llcorner}(A) \cap f^{\llcorner}(B) = A \cap A = A \neq \emptyset$, så ' $\subseteq$ ', men varken ' $=$ ' eller ' $\supseteq$ ' gäller säkert i b.

c. $y \in f^{\llcorner}(A) \setminus f^{\llcorner}(B) \Leftrightarrow y \in f^{\llcorner}(A)$, $y \notin f^{\llcorner}(B) \Leftrightarrow y = f(x)$ för något $x \in A$, men inte för något $x \in B$ (så för ett $x \in A \setminus B) \Rightarrow y \in f^{\llcorner}(A \setminus B)$,

men X, Y, f som i b. ger $f^{\llcorner}(A \setminus B) = f^{\llcorner}(A) = A$ och $f^{\llcorner}(A) \setminus f^{\llcorner}(B) = A \setminus A = \emptyset \neq A$, så ' $\supseteq$ ', men varken ' $=$ ' eller ' $\subseteq$ ' gäller säkert i c.

Svar a: $=, \subseteq, \supseteq$, **b:** $\subseteq$, **c:** $\supseteq$ måste gälla, övriga inte.

3) (3p) Vi söker antalet sätt att placera fyra flickor och fem pojkar på tre röda och sex vita stolar, så att minst en flicka sitter på en röd stol (särskiljbara barn och stolar).

Lösning:

Det sökta antalet är det totala antalet sätt att placera barnen minus antalet sätt med alla flickor på vita stolar (additionsprincipen), dvs $9! - (6)_4 \cdot 5! = 9! - \frac{6!}{2!} \cdot 5!$ sätt (antalet bijektioner 9 -mängd $\rightarrow$ 9 -mängd respektive (multiplikationsprincipen) antalet injektioner 4 -mängd (flickorna) $\rightarrow$ 6 -mängd (de vita stolarna) $\cdot$ antalet bijektioner 5 -mängd (pojkar) $\rightarrow$ 5 -mängd (de flickfria stolarna)).

Svar: På $9! - \frac{6! \cdot 5!}{2}$ ($= 319\,680$) sätt.

4) $\pi, \sigma \in S_9$ ges av tabellen till höger. Vi söker (a, 1p) π, σ och $\pi\sigma$ på cykelform och skall (b, 2p) visa att om gruppen G innehåller π och σ måste G 's ordning vara delbar med 180.

i	1	2	3	4	5	6	7	8	9
$\pi(i)$	2	3	1	5	6	7	4	9	8
$\sigma(i)$	4	8	1	9	2	3	7	5	6

Lösning:

a. $\pi(1) = 2, \pi(2) = 3, \pi(3) = 1$ etc. ger $\pi = (1\ 2\ 3)(4\ 5\ 6\ 7)(8\ 9)$ och $\sigma = (1\ 4\ 9\ 6\ 3)(2\ 8\ 5)$. Sammansättning (först σ sedan π) ger $(\pi\sigma)(1) = \pi(\sigma(1)) = \pi(4) = 5$ osv, så $\pi\sigma = (1\ 5\ 3\ 2\ 9\ 7\ 4\ 8\ 6)$.

b. G är en grupp som innehåller π och σ och således också $\pi\sigma$. Ordningen för en grupp är en multipel av ordningen för varje element (följer ur Lagranges sats) och ordningen för en permutation är den minsta gemensamma multipeln av cykellängderna. Vi ser att ordningarna för $\pi, \sigma, \pi\sigma$ är $\text{mgm}(3, 4, 2) = 12, \text{mgm}(5, 3, 1) = 15, \text{mgm}(9) = 9$. $|G|$ är delbar med alla tre, således också med $\text{mgm}(12, 15, 9) = 180$. **Saken är klar.**

Svar a: $\pi = (1\ 2\ 3)(4\ 5\ 6\ 7)(8\ 9), \sigma = (1\ 4\ 9\ 6\ 3)(2\ 8\ 5), \pi\sigma = (1\ 5\ 3\ 2\ 9\ 7\ 4\ 8\ 6)$,

b: Visat ovan.

5) Ett RSA-system har offentliga (n, e) , där $n = 4331 [= 61 \cdot 71]$. Vi söker (a, 1p) de av $205, \dots, 209$ som är möjliga för e och (b, 2p) ett motsvarande d -värde för något av de e :na.

Lösning:

a. Villkoret på e är att $\text{sgd}(m, e) = 1$, där (om $n = p \cdot q$ med p, q olika primtal)

$$m = \phi(n) = (p-1)(q-1) = 60 \cdot 70 = 4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Eftersom $2 \mid 206, 208$ och $3 \mid 207$ och $5 \mid 205$ och $2, 3, 5, 7 \nmid 209$ är det enda möjliga $e = 209$.

b. Ett motsvarande d bestäms av $e \cdot d \equiv_m 1$.

Euklides algoritim: $4200 = 209 \cdot 20 + 20, 209 = 20 \cdot 10 + 9, 20 = 9 \cdot 2 + 2, 9 = 2 \cdot 4 + 1$, så $1 = 9 - 4 \cdot 2 = 9 - 4(20 - 2 \cdot 9) = -4 \cdot 20 + 9 \cdot 9 = -4 \cdot 20 + 9(209 - 10 \cdot 20) = 9 \cdot 209 - 94 \cdot 20 = 9 \cdot 209 - 94(4200 - 20 \cdot 209) = -94 \cdot 4200 + 1889 \cdot 209$ och vi kan ta $d = 1889$.

Svar a: Det enda möjliga $e = 209$, b: Ett motsvarande $d = 1889$.

(I själva verket räcker det att $e \cdot d \equiv_{\text{mgm}(p-1, q-1)} 1$, så alla $d = 209 + 420k, k \in \mathbb{Z}_+$ fungerar.)

6) (4p) $G = (V, E), G_i = (V_i, E_i), V = V_1 \cup V_2, V_1 \cap V_2 = \emptyset$ och $E_i = \{\{x, y\} \in E \mid x, y \in V_i\}$. Vi skall visa att för de kromatiska polynomen gäller $P_G(\lambda) \leq P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$ då $\lambda \in \mathbb{N}$.

Lösning:

Låt $G' = (V, E_1 \cup E_2)$ (dvs G med alla kanter med hörn i både V_1 och V_2 borttagna, så G' består av delarna G_1 och G_2 , utan kanter mellan). Då är färgningar av delarna G_1 och G_2 oberoende, så $P_{G'}(\lambda) = P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$ då $\lambda \in \mathbb{N}$ (för varje färgning av G_1 finns $P_{G_2}(\lambda)$ färgningar av G_2). Men färgningarna av G utgör en delmängd av dem av G' , så $P_G(\lambda) \leq P_{G'}(\lambda)$. **Saken är klar.**

7) X är en oändlig mängd och $G = \{f: X \rightrightarrows X\}$. Vi skall visa att (a, 1p) $(G, \circ)$ är en grupp ($\circ$ sammansättning), med (b, 2p) $H = \{f \in G \mid |\{x \in X \mid f(x) \neq x\}| < \infty\}$ en delgrupp, och (c, 1p) avgöra om H är en normal delgrupp.

Lösning:

a. $(G, \circ)$ är en grupp, ty (definitionen av en grupp)

- $f, g \in G \Rightarrow f \circ g \in G$ (slutenhet, sammansättningen av två bijektioner är en bijektion),
- $f, g, h \in G \Rightarrow f \circ (g \circ h) = (f \circ g) \circ h$ (associativitet, för alla funktioner (om båda led definierade)),
- $f \in G \Rightarrow f \circ id = id \circ f = f$, där $id \in G$ är identitetsfunktionen ($id(x) = x$, alla $x \in X$) (identitets-element) och
- $f \in G \Rightarrow f^{-1} \in G$ och $f \circ f^{-1} = f^{-1} \circ f = id$ (inverselement, finns, ty f en bijektion). $\square$

b. H är en delgrupp till G , ty (känd sats)

- $H \subseteq G$ (enligt definitionen av H), $H \neq \emptyset$ ($id \in H$),
- $f, g \in H \Rightarrow f \circ g \in H$ (ty $\{x \in X \mid (f \circ g)(x) \neq x\} \subseteq \{x \in X \mid f(x) \neq x\} \cup \{x \in X \mid g(x) \neq x\}$ och A, B ändliga, $C \subseteq A \cup B \Rightarrow C$ ändlig) och
- $f \in H \Rightarrow f^{-1} \in H$ (ty $\{x \in X \mid f^{-1}(x) \neq x\} = \{x \in X \mid f(x) \neq x\}$). $\square$

c. H är en normal delgrupp, ty $f \in G, h \in H \Rightarrow f \circ h \circ f^{-1} \in H$ (ty $\{x \in X \mid f(h(f^{-1}(x))) \neq x\} = \{f(x) \mid x \in X, h(x) \neq x\}$) och $fHf^{-1} \subseteq H, f^{-1}Hf \subseteq H \Rightarrow fH = Hf$.

Svar a,b: Visade ovan, c: H är en normal delgrupp.

8) (4p) $G = (V, E)$ är en graf, $\mu(x)$, för $x \in V$, medelvärde av x :s grannars valenser (= 0 om $\delta(x) = 0$). Vi skall visa att $\sum_{x \in V} \mu(x) \geq \sum_{x \in V} \delta(x)$.

Lösning:

För alla $x \in V$ är $\mu(x) = \sum_{y \in V_x} \frac{1}{\delta(x)} \delta(y)$, där $V_x = \{y \in V \mid \{x, y\} \in E\}$, x :s grannar, så $\sum_{x \in V} \mu(x) = \sum_{x \in V, y \in V_x} \frac{\delta(y)}{\delta(x)} = \sum_{\{x, y\} \in E} \left(\frac{\delta(y)}{\delta(x)} + \frac{\delta(x)}{\delta(y)} \right) \geq \sum_{\{x, y\} \in E} 2 = 2|E| = \sum_{x \in V} \delta(x)$, där vi använt att $a^2 + \frac{1}{a^2} \geq 2$ för alla $a \in \mathbb{R} \setminus \{0\}$ (ty $(a - \frac{1}{a})^2 \geq 0$). **Saken är klar.**

9) Vi skall (a, 1p) med $D: F[[x]] \rightarrow F[[x]]$ (F en kropp) given av $D(A(x)) = \sum n a_n x^{n-1}$ för $A(x) = \sum a_n x^n \in F[[x]]$ visa att $D(A(x)B(x)) = D(A(x))B(x) + A(x)D(B(x))$, alla $A(x), B(x) \in F[[x]]$, (b, 2p) finna koefficienterna i $p_n(x)$ då $E(x) = \sum \frac{1}{n!} x^n \in \mathbb{R}[[x]]$ och $p_0(x) = 1$, $p_{n+1}(x)E(x) = x D(p_n(x)E(x))$ för $n \in \mathbb{N}$, och (c, 2p) uttrycka beltalet B_n (antalet olika ekvivalensrelationer på en n -mängd) med en konvergent oändlig serie.

Lösning:

a. Om $A(x) = \sum a_n x^n$, $B(x) = \sum b_n x^n$ är koefficienten för x^n i $A(x)B(x)$: $\sum_{k=0}^n a_k b_{n-k}$. Koefficienten för x^{n-1} är i VL: $n \sum_{k=0}^n a_k b_{n-k}$ och i HL: $\sum_{k=0}^n k a_k b_{n-k} + \sum_{k=0}^n a_k (n-k) b_{n-k} = \sum_{k=0}^n (k + (n-k)) a_k b_{n-k} =$ den i VL, så VL=HL. $\square$

b. Låt $p_n(x) = \sum p_{n,k} x^k$. Då är $p_{0,0} = 1$, $p_{0,k} = 0$ för $k > 0$ och a. ger att $p_{n+1}(x)E(x) = x(\sum k p_{n,k} x^{k-1} + \sum p_{n,k} x^k)E(x) = (\sum_{k=1}^{\infty} (k p_{n,k} + p_{n,k-1}) x^k)E(x)$ (ty $D(E(x)) = E(x)$). Så för alla $n \in \mathbb{N}$ är $p_{n+1,0} = 0$, $p_{n+1,k} = p_{n,k-1} + k p_{n,k}$ för $k > 0$.

Med $p_{0,k}$ enligt ovan ger det $p_{n+1,k} = 0$ för $k = 0$ och $k > n+1$, $p_{n+1,1} = p_{n+1,n+1} = 1$ och $p_{n+1,k} = p_{n,k-1} + k p_{n,k}$ för $1 < k < n+1$, så $p_{n,k} = S(n, k)$, stirlingtalen (av andra slaget). $p_n(x)$ är för $n \in \mathbb{Z}_+$ alltså polynomet $\sum_{k=1}^n S(n, k) x^k$ (stirlingtalens genererande polynom).

c. Ekvivalensrelationerna på en mängd motsvarar bijektivt partitionerna av mängden (i ekvivalensklasser), så $B_n = \sum_{k=1}^n S(n, k) = p_n(1)$, antalet olika partitioner av en n -mängd.

Enligt b. är $p_n(x)E(x) = (x D)^n E(x) = (x D)^{n-1} \sum_{k=1}^{\infty} \frac{k}{k!} x^k = \dots = \sum_{k=1}^{\infty} \frac{k^n}{k!} x^k$.

$x = 1$ ger att $p_n(1) \cdot E(1) (= B_n \cdot e) = \sum_{k=1}^{\infty} \frac{k^n}{k!}$ (HL konvergent eftersom VL är det).

Svar a: Visat ovan, b: x^k -koefficienten i $p_n(x)$ är $S(n, k)$ (och = 0 då $k = 0$ eller $> n$),

c: $B_n = \frac{1}{e} \sum_{k=1}^{\infty} \frac{k^n}{k!}$ (Dobińskis formel).

(Man kan visa att $\sum_{k=2n+1}^{\infty} \frac{k^n}{k!} < e$, så $B_n = \lceil \frac{1}{e} \sum_{k=1}^{2n} \frac{k^n}{k!} \rceil$ (Comtets formel) ($\lceil a \rceil$ = det minsta heltal $\geq a$).

Genom att skriva $x = e^t$ fås för $n \in \mathbb{Z}_+$ att $\sum_{k=1}^n S(n, k) e^{kt} \cdot e^{e^t} = \frac{d^n}{dt^n} e^{e^t}$.)

10) Grafen $G = (X \cup Y, E)$ är bipartit och för $A \subseteq X$ är $r(A)$ det största antalet element i A som samtidigt kan matchas med element i Y . Vi skall (a, 3p) visa att för alla $A, B \subseteq X$ gäller $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ och (b, 2p) ge ett exempel med $<$ i olikheten.

Lösning:

a. Låt M, N vara matchningar mellan $A \cup B$ respektive $A \cap B$ och Y med $|M| = r(A \cup B)$, $|N| = r(A \cap B)$.

Det finns en matchning M' mellan $A \cup B$ och Y med $|M'| = |M|$ och $N \subseteq M'$,

ty om $x \in A \cap B$ och $\{x, y\} \in N \setminus M$,

- lägg till $\{x, y\}$ i M och tag bort andra kanter i M som innehåller x eller y ,
- om $\{x, y'\}, \{x', y\} \in M$, lägg också till $\{x', y'\}$ i M .

Det ger en ny, lika stor ($\times |M|$ ($|M|$ störst möjlig), så minst en kant tas bort i första steget; om två tas bort, läggs ytterligare en till i det andra), matchning av $A \cup B$ som innehåller $\{x, y\}$ och om det upprepas för alla kanter i N fås den utlovade M' (redan tillförda N -kanter påverkas ju inte mer). $\square$

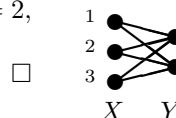
Låt matchningarna M_A, M_B mellan A, B och Y bestå av de kanter i M' som innehåller hörn från A respektive B . Då är $M_A \cup M_B = M'$ och $M_A \cap M_B = N$ (ty $|N| = r(A \cap B)$), så (inklusion/exklusion) $r(A \cup B) + r(A \cap B) = |M| + |N| = |M'| + |N| = |M_A| + |M_B| \leq r(A) + r(B)$. $\square$

b. Med $G = K_{3,2}$ enligt figuren och $A = \{1, 2\}$, $B = \{2, 3\}$ fås $r(A \cup B) = 2$,

$r(A \cap B) = 1$, $r(A) = r(B) = 2$, så

$r(A \cup B) + r(A \cap B) = 2 + 1 < 2 + 2 = r(A) + r(B)$. $\square$

(Det går lika bra med $G = K_{2,1}$ och $A = \{1\}$, $B = \{2\}$.)



Svar a: Visat ovan, b: Exempel ovan.

(En ändlig mängd $X \neq \emptyset$ med en funktion $r: \mathcal{P}(X) \rightarrow \mathbb{N}$ som (liksom r ovan) för alla $A, B \in \mathcal{P}(X)$ uppfyller de tre villkoren 1. $r(A) \leq |A|$, 2. $A \subseteq B \Rightarrow r(A) \leq r(B)$ och 3. olikheten i uppgiften, kallas **en matroid**.)

Andra exempel på matroider:

1. X en delmängd till ett vektorrum, med $r(A)$ = dimensionen av delrummet A spänner upp,
2. $X = E$ för en graf $G = (V, E)$, med $r(A)$ = maximala antalet kanter i A som inte innehåller någon cykel.

Ett $A \in \mathcal{P}(X)$ som uppfyller $r(A) = |A|$ kallas en **oberoende mängd**.)