Matematik, KTH
B.Ek

Lösningar tenta SF1679 DISKRET MATEMATIK, F3 m.fl.
11 januari 2018

Tryckfel kan förekomma.

1) För hur många $x \in \mathbb{Z}_{4851}$ är $x^{292} = 196$? [$4851 = 3^2 \cdot 7^2 \cdot 11$]

Lösning:
Enligt kinesiska restsatsen är $\mathbb{Z}_{4851} \cong \mathbb{Z}_9 \times \mathbb{Z}_{49} \times \mathbb{Z}_{11}$, med isomorfin $x \mapsto ([x]_9, [x]_{49}, [x]_{11})$.
$196 \equiv_9 7, \equiv_{49} 0, \equiv_{11} 9$, så $x^{292} \equiv_{4851} 196$ omm $x^{292} \equiv_9 7, \equiv_{49} 0, \equiv_{11} 9$.
För $a \in \mathbb{Z}_9$ är $a^k = 0$ om $3 \mid a$ och $k \geq 2$, $a^6 = 1$ annars (sgd$(a, 9) = 1$; Eulers sats, ty $\phi(9) = 6$).
Eftersom $292 \equiv_6 4$ är $a^{292} = a^4$ för alla $a \in \mathbb{Z}_9$. Det ger:

a	0	1	2	3	4	5	6	7	8
a^{292}	0	1	7	0	4	4	0	7	1

,

så $a^{292} = 7$ för **2 st $a \in \mathbb{Z}_9$**.
För $a \in \mathbb{Z}_{49}$ är $a^k = 0$ omm $7 \mid a$, $k \geq 2$ (övriga a är inverterbara), så $a^{292} = 0$ för **7 st $a \in \mathbb{Z}_{49}$**.
För $a \in \mathbb{Z}_{11}$ är $a^k = 0$ om $a = 0$ och $k \geq 1$, $a^{10} = 1$ annars (Fermats lilla sats, 11 primtal).
Eftersom $292 \equiv_{10} 2$ är $a^{292} = a^2$ om $a \in \mathbb{Z}_{11}$. Det ger för $a \in \mathbb{Z}_{11}$:

a	0	1	2	3	4	5	6	7	8	9	10
a^{292}	0	1	4	9	5	3	3	5	9	4	1

,

så $a^{292} = 9$ för **2 st $a \in \mathbb{Z}_{11}$**.
Enligt ovan ges elementen i $\mathbb{Z}_{4851}$ precis av element i $\mathbb{Z}_9 \times \mathbb{Z}_{49} \times \mathbb{Z}_{11}$, så det finns $2 \cdot 7 \cdot 2 = 28$ $x \in \mathbb{Z}_{4851}$ som uppfyller $x^{292} = 196$.

Svar: Det sökta antalet är 28.

---

2) (3p) $f\colon X \rightleftarrows X$ är en bijektion på en ändlig mängd X. Vi skall avgöra om relationen $\mathcal{R}$ på X, för $x, y \in X$ given av $x\mathcal{R}y \Leftrightarrow y = f^n(x)$ för något $n \in \mathbb{Z}_+$, är en ekvivalensrelation.

Lösning:
f är en permutation av X (en bijektion av X på X), så varje $x \in X$ ingår i en cykel (ty $|X| < \infty$).
$\mathcal{R}$ är reflexiv, dvs $x\mathcal{R}x$ är sant för alla $x \in X$, ty om x tillhör en k-cykel är $f^k(x) = x$,
$\mathcal{R}$ är symmetrisk, dvs $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ för alla $x, y \in X$, ty om x tillhör en k-cykel och $y = f^i(x)$, $i \in \mathbb{Z}_+$, är $x = f^j(y)$ för alla j med $k \mid (i + j)$ (och sådana j finns i $\mathbb{Z}_+$),
$\mathcal{R}$ är transitiv, dvs ($x\mathcal{R}y$ och $y\mathcal{R}z$) $\Rightarrow x\mathcal{R}z$ för alla $x, y, z \in X$, ty om $y = f^n(x)$ och $z = f^m(y)$ med $m, n \in \mathbb{Z}_+$ är $z = f^{m+n}(x)$ och $m + n \in \mathbb{Z}_+$.
$\mathcal{R}$ är alltså reflexiv, symmetrisk och transitiv, så (enligt definition) en ekvivalensrelation.

Svar: Ja, $\mathcal{R}$ är en ekvivalensrelation på X.

---

3) $A = \{1, 2, \ldots, 7\}$, $B = \{1, 2, \ldots, 13\}$ och vi söker (a, 2p) antalet $f\colon A \to B$ som antar precis 4 olika värden och (b, 1p) antalet av dem (de i a) som antar minst ett udda värde.

Lösning:

a. Värdena som antas kan väljas på $\binom{13}{4} = \frac{13!}{4! \cdot (13-4)!}$ (antalet 4-delmängder till en 13-mängd) sätt och för varje sådant val finns $4! \cdot S(7, 4) = 4! \cdot 350$ (stirlingtalet $S(7, 4) = 350$ enligt "triangeln" t.h.) surjektioner av A på mängden av de fyra värdena. Multiplikationsprincipen ger det sökta antalet som produkten av dem, $\frac{13! \cdot 350}{9!}$.

			1			
		1		1		
	1		3		1	
1		7		6		1
	15		25		10	
		90		65		
			350			

b. Enligt additionsprincipen fås det sökta antalet genom att dra antalet sådana funktioner som bara antar jämna värden ($\binom{6}{4} \cdot 4! \cdot S(7, 4) = \frac{6! \cdot 350}{(6-4)!}$) från svaret i a. Det ger $(\frac{13!}{9!} - \frac{6!}{2!}) \cdot 350$.

Svar a: $\frac{13! \cdot 350}{9!}$ (= 6 006 000) st, b: $\left(\frac{13!}{9!} - \frac{6!}{2!}\right) \cdot 350$ (= 5 880 000) st.

4) (3p) $(G,\cdot)$ är en grupp och $\varphi\colon G\to G$ ges av $\varphi(g)=g^{-1}$, alla $g\in G$.
Vi skall visa att φ är en isomorfi omm G är abelsk.

Lösning:
φ är en isomorfi omm den är en bijektion och $\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)$ för alla $g_1,g_2\in G$.
Vi visar först "om", så antag att gruppen G är abelsk (dvs kommutativ).
φ är en bijektion, ty den har inversen $\varphi^{-1}=\varphi$ (eftersom $(g^{-1})^{-1}=g$ för alla $g\in G$).
Om $g_1,g_2\in G$ är $\varphi(g_1g_2)=(g_1g_2)^{-1}=g_2^{-1}g_1^{-1}=\varphi(g_2)\varphi(g_1)\overset{G\text{ abelsk}}{=}\varphi(g_1)\varphi(g_2)$. □
För att visa "endast om", antag att φ är en isomorfi och låt g_1,g_2 vara godtyckliga i G.
Eftersom φ är en bijektion finns $h_1,h_2\in G$ med $g_i=\varphi(h_i)$ $(i=1,2)$ och $g_1g_2=\varphi(h_1)\varphi(h_2)\overset{\varphi\text{ iso}}{=}$
$=\varphi(h_1h_2)=(h_1h_2)^{-1}=h_2^{-1}h_1^{-1}=\varphi(h_2)\varphi(h_1)=g_2g_1$. □ **Saken är klar.**

---

5) $\pi,\sigma\in S_{13}$ ges av tabellen:

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$\pi(i)$	9	8	12	7	2	6	11	4	1	13	5	3	10
$\sigma(i)$	11	2	12	3	5	1	4	8	13	9	6	7	10

Vi söker (a, 1p) π:s och σ:s pariteter och (b, 2p) alla $n\in\mathbb{Z}$ som uppfyller $\tau\pi^n=\sigma^n\tau$ för något $\tau\in S_{13}$.

Lösning:
a. På cykelform är $\pi=(1\ 9)(2\ 8\ 4\ 7\ 11\ 5)(3\ 12)(6)(10\ 13)$ (ty $\pi(1)=9$, $\pi(9)=1,\ldots$) och $\sigma=(1\ 11\ 6)(2)(3\ 12\ 7\ 4)(5)(8)(9\ 13\ 10)$. Cykelstrukturer för $\pi:\ [1\,2^3\,6]$, $\sigma:\ [1^3\,3^2\,4]$.
Pariteterna är π: jämn (4 (jämnt) cykler av jämn längd), σ: udda (1 (udda) cykel av jämn längd).
b. $\tau\pi^n=\sigma^n\tau\Leftrightarrow\sigma^n=\tau\pi^n\tau^{-1}$, så vi söker $n\in\mathbb{Z}$ som gör π^n och σ^n konjugerade, dvs med samma cykelstruktur (enligt känd sats).
Den n:e potensen av en k-cykel är d st $\frac{k}{d}$-cykler, $d=\gcd(k,n)$, men det räcker med fallen $k=1,2,3,4,6$ för att ställa upp följande tabell över cykelstrukturerna:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
π^n	$[1^{13}]$	$[12^36]$	$[1^73^2]$	$[12^6]$	$[1^73^2]$	$[12^36]$	$[1^{13}]$	$[12^36]$	$[1^73^2]$	$[12^6]$	$[1^73^2]$	$[12^36]$	$[1^{13}]$
σ^n	$[1^{13}]$	$[1^33^24]$	$[1^32^23^2]$	$[1^94]$	$[1^73^2]$	$[1^33^24]$	$[1^92^2]$	$[1^33^24]$	$[1^73^2]$	$[1^94]$	$[1^32^23^2]$	$[1^33^24]$	$[1^{13}]$

Tabellen har åt båda håll (π, π^{-1} har samma cykelstruktur) period 12 ($o(\pi)=6$, $o(\sigma)=12$) och vi ser att π^n och σ^n har samma cykelstruktur omm $4\mid n$.

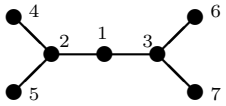
Svar a: π är jämn och σ är udda, b: Alla $n=4k$, $k\in\mathbb{Z}$.

---

6) (4p) $G=(V,E)$ är en plan, sammanhängande graf med $\delta(x)\geq 3$ för alla $x\in V$ och den duala grafen $G^\perp=(V^\perp,E^\perp)$ har $|V^\perp|\leq 11$. Vi skall visa att $\delta^\perp(x)\leq 4$ för något $x\in V^\perp$.

Lösning:
Antag (för att få en motsägelse) att $\delta^\perp(x)\geq 5$ för alla $x\in V^\perp$.
Summan av valenserna i en graf är (gängse beteckningar) $2\,|E|$, så $3v\leq\sum_{x\in V}\delta(x)=2e$ och $5v^\perp\leq\sum_{x\in V^\perp}\delta^\perp(x)=2e^\perp=2e$ ($e=e^\perp$ enligt definitionen av $G^\perp$).
Med Eulers polyederformel (plan, sammanhängande graf) och att antalet ytor $r=v^\perp$ (enligt definitionen av $G^\perp$): $2=v-e+r=v-e+v^\perp\leq v^\perp-\frac{e}{3}$, så $\frac{2e}{5}\geq v^\perp\geq 2+\frac{e}{3}$. Det ger $\frac{2e}{5}\geq 2+\frac{e}{3}$, dvs $(\frac{2}{5}-\frac{1}{3})e=\frac{e}{15}\geq 2$, så $e\geq 30$, och $v^\perp\geq 2+\frac{e}{3}\geq 12$, motsägelse. **Saken är klar.**

7) (4p) Vi söker antalet väsentligt olika (så att de inte blir lika hur man än vrider en del av eller hela anordningen i rummet) sätt att färga pärlorna med precis två röda och resten med någon av k andra färger.



Lösning:
Med pärlorna numrerade som i figuren är gruppen av "tillåtna" permutationer av dem $G = \{(1), (45), (67), (45)(67), (23)(46)(57), (23)(47)(56), (23)(4657), (23)(4756)\}$, $|G| = 8$.
Enligt Burnsides lemma (Thm 21.4 i boken) är antalet väsentligt olika färgningar = antalet banor för gruppens verkan på färgningarna = $\frac{1}{|G|}\sum_{g\in G}|F(g)|$.

g	cykelstruktur	antal g	$\lvert F(g)\rvert$
id	$[1^7]$	1	$\binom{7}{2}\cdot k^5 = 21\,k^5$
$(4\,5), (6\,7)$	$[1^5\,2]$	2	$1\cdot k^5 + \binom{5}{2}\cdot k^4 = k^5 + 10\,k^4$
$(4\,5)(6\,7)$	$[1^3\,2^2]$	1	$\binom{2}{1}\cdot k^4 + \binom{3}{2}\cdot k^3 = 2\,k^4 + 3\,k^3$
$(2\,3)(4\,6)(5\,7), (2\,3)(4\,7)(5\,6)$	$[1\,2^3]$	2	$\binom{3}{1}\cdot k^3 = 3\,k^3$
$(2\,3)(4\,6\,5\,7), (2\,3)(4\,7\,5\,6)$	$[1\,2\,4]$	2	k^2

$|F(g)|$ fås av att alla pärlor i samma cykel måste ha samma färg och de två röda pärlorna kan vara två 1-cykler eller en 2-cykel.
Vi finner $\frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{8}\big(21k^5 + 2(k^5+10k^4) + (2k^4+3k^3) + 2\cdot 3k^3 + 2k^2\big) =$
$= \frac{1}{8}(23\,k^5 + 22\,k^4 + 9\,k^3 + 2\,k^2)$

Svar: Det sökta antalet är $\frac{1}{8}(23\,k^5 + 22\,k^4 + 9\,k^3 + 2\,k^2)$.
($k=1$ ger 7 st, $k=2$ ger 146 st, $k=3$ ger 954 st, $k=4$ ger 3724 st etc.)

---

8) (4p) $G = (V, E)$ är en sammanhängande graf.
Vi skall visa att dess kanter kan riktas så att högst ett hörn har udda utvalens.

Lösning:
En orientering av kanterna som minimerar $|\{x \in V \mid \delta^+(x) \text{ udda}\}|$ (en sådan finns, ty antalet $\in \mathbb{N}$) uppfyller villkoret, ty om $x, y \in V$, $x \neq y$, $\delta^+(x), \delta^+(y)$ udda, vänd riktningen för alla kanter i en stig mellan x and y. Då blir $\delta^+(x), \delta^+(y)$ jämna och pariteten för alla andra hörns utvalens oförändrad, så antalet $x \in V$ med $\delta^+(x)$ udda minskar, omöjligt. **Saken är klar.**

---

9) (5p) Vi söker värdet av $\sum_{n=0}^{\infty} 2^{-n}\cdot F_n$, där fibonaccitalen $\{F_n\}_{n=0}^{\infty}$ som vanligt definieras av att $F_0 = 0$, $F_1 = 1$ och $F_{n+2} = F_{n+1} + F_n$ för $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$.

Lösning:
Vi visar att serien som fås då vi sätter $x = \frac{1}{2}$ i den genererande funktionen $\sum_{n=0}^{\infty} F_n\,x^n$ (formell potensserie) konvergerar och finner dess värde.
Låt $\phi = \frac{1+\sqrt{5}}{2}$ (gyllene snittet). Det uppfyller $1+\phi = \phi^2$ och $1 < \phi < 2$ (ty $1 < 5 < 9 \Rightarrow 1 < \sqrt{5} < 3$), så med induktion får vi att $F_n < \phi^n$ för alla $n \in \mathbb{N}$:

- Bas: $F_0 = 0 < 1 = \phi^0$, $F_1 = 1 < \phi = \phi^1$,
- Steg: Om $F_n < \phi^n$, $F_{n+1} < \phi^{n+1}$ är $F_{n+2} = F_{n+1} + F_n < \phi^{n+1} + \phi^n = \phi^{n+2}$. □

För att se konvergensen, betrakta partialsumman av den genererande funktionen ($N \in \mathbb{Z}_+$):
$(1 - x - x^2)\cdot\sum_{n=0}^{N} F_n\,x^n = F_0\,x^0 + (F_1 - F_0)x^1 + 0 + \ldots - (F_{N-1} + F_N)x^{N+1} - F_N\,x^{N+2}$,
som med $x = \frac{1}{2}$ ger $\sum_{n=0}^{N} 2^{-n}F_n = 2 - 2^{-(N-1)}(F_{N-1} + F_N) - 2^{-N}F_N$. Det visar (eftersom $2^{-n}F_n < (\frac{\phi}{2})^n \to 0$ då $n \to \infty$) att $\sum_{n=0}^{N} 2^{-n}F_n \to 2$ då $N \to \infty$.

Svar: Seriens värde är 2.

---

10) Vi skall (a, 1p) visa att x är udda om $x, y \in \mathbb{Z}$ och $y^3 = x^2 + 2$, (b, 2p) visa att $R = \mathbb{Z}[\sqrt{2}\,i] = \{a + b\sqrt{2}\,i \mid a, b \in \mathbb{Z}\}$ har entydig faktorisering i "primtal" (bortsett från faktorernas ordning och faktorer ± 1) och (c, 2p) finna alla $x, y \in \mathbb{Z}$ med $y^3 = x^2 + 2$.

Lösning:

a. Om x är jämnt är $x^2 + 2 \equiv_4 2$, men $y^3 \equiv_4 0, 1$ eller 3. □

b. Låt $\boldsymbol{z, w \in R,\ w \neq 0}$. Vi skall visa att det finns $\boldsymbol{q, r \in R}$ med $\boldsymbol{z = wq + r,\ |r|^2 < |w|^2}$, dvs **division med rest**, så att **resten är (strikt) mindre än divisorn**, mätt i en storhet som tar **värden i** $\mathbb{N}$ (en välordnad mängd).

Det räcker för att (som i $\mathbb{Z}$, med Euklides algoritm, i ett ändligt antal steg) visa att det för alla $z, w \in R$ finns en entydig (bortsett från faktorer ± 1) $\text{sgd}(z, w) = mz + nw$ för några $m, n \in R$.

Om man definierar att $p \in R$ är ett "R-primtal" omm det bara har delarna ± 1 och $\pm p$, kan man som i $\mathbb{Z}$ visa att varje $z \in R$ är en (väsentligen) unik produkt av "R-primtal".

(Eftersom $z \mid w \Rightarrow |z|^2 \mid |w|^2$ för $z, w \in \mathbb{C}$ är $p = a + b\sqrt{2}\,i$ ett "R-primtal" om $|p|^2 = a^2 + 2b^2$ är ett (vanligt) primtal, t.ex. $1 + \sqrt{2}\,i$, $3 + 4\sqrt{2}\,i$. Däremot behöver inte vanliga primtal vara "R-primtal", t.ex. är $2 = -\sqrt{2}\,i \cdot \sqrt{2}\,i$, $3 = (1 + \sqrt{2}\,i)(1 - \sqrt{2}\,i)$, men 5 är ett "$R$-primtal".)

Återstår att visa resultatet om division med rest ovan, så låt $z, w \in R$, $w \neq 0$.

Division i $\mathbb{C}$ ger $\frac{z}{w} \in \mathbb{Q}[\sqrt{2}\,i] = \{s + t\sqrt{2}\,i \mid s, t \in \mathbb{Q}\}$ (ty $\frac{a+b\sqrt{2}\,i}{c+d\sqrt{2}\,i} = \frac{ac+2bd}{c^2+2d^2} + \frac{bc-ad}{c^2+2d^2}\sqrt{2}\,i$).

Tag $q = u + v\sqrt{2}\,i$ det tal i R som ligger närmast $\frac{z}{w}$ ($u \in \mathbb{Z}$ närmast $\frac{ac+2bd}{c^2+2d^2}$ och $v \in \mathbb{Z}$ närmast $\frac{bc-ad}{c^2+2d^2}$).

Då är $|\frac{z}{w} - q|^2 \leq (\frac{1}{2})^2 + (\frac{\sqrt{2}}{2})^2 = \frac{3}{4} < 1$, så $z = wq + r$ med $r \in R$ och $|r|^2 = |\frac{z}{w} - q|^2 |w|^2 < |w|^2$.

Därmed är (skissen av) beviset för (väsentligen) entydig faktorisering i R klar. □

c. Vi söker $x, y \in \mathbb{Z}$ med $y^3 = x^2 + 2 = (x + \sqrt{2}\,i)(x - \sqrt{2}\,i)$ och vet att x är udda.

$\text{sgd}(x + \sqrt{2}\,i, x - \sqrt{2}\,i) = d = (\pm)1$, ty $\text{sgd}(x + \sqrt{2}\,i, x - \sqrt{2}\,i) = \text{sgd}(x - \sqrt{2}\,i, 2\sqrt{2}\,i)$, så $d \in R$ delar $x + \sqrt{2}\,i$ och $2\sqrt{2}\,i$ och därmed $|d|^2 \mid (x^2 + 2)$ och $|d|^2 \mid |2\sqrt{2}|^2 = 8$, men $x^2 + 2$ är udda, så $|d| = 1$. (Alternativt, med Euklides algoritm, $(4k \pm 1) - \sqrt{2}\,i = 2\sqrt{2}\,i(-k\sqrt{2}\,i) + (\pm 1 - \sqrt{2}\,i)$; $2\sqrt{2}\,i = (\pm 1 - \sqrt{2}\,i)(-1 \pm \sqrt{2}\,i) \mp 1$.)

Det ger att $x + \sqrt{2}\,i = (a + b\sqrt{2}\,i)^3$ för några $a, b \in \mathbb{Z}$, ty varje "R-primtal" p i $x + \sqrt{2}\,i$ ingår i y, så p^{3k} (något $k \in \mathbb{Z}_+$) är en faktor i y^3, således i $x + \sqrt{2}\,i$ (ty inte i $x - \sqrt{2}\,i$).

$x + \sqrt{2}\,i = (a + b\sqrt{2}\,i)^3$ ger $a(a^2 - 6b^2) = x$ och $b(3a^2 - 2b^2) = 1$. Andra ekvationen ger $b \mid 1$, så $b = \pm 1$ och $3a^2 - 2 = b = \pm 1$, så $a^2 = b = 1$ och alltså $a = \pm 1$, $b = 1$ som ger $x = a(a^2 - 6b^2) = \pm(1 - 6) = \mp 5$. Det ger till sist $y^3 = x^2 + 2 = 3^3$, så $y = 3$.

Svar a,b: Visade ovan, c: De enda lösningarna är $\boldsymbol{x = \pm 5,\ y = 3}$.