STOCKHOLMS UNIVERSITET
MATEMATISKA INSTITUTIONEN
Avd. Matematik
Föreläsare: P. Alexandersson
Examinator: S. Lundqvist

Tentamen i
Algebra och kombinatorik
17 maj 2023 kl $14^{00} - 19^{00}$

Enbart skrivdon tillåtna. Alla svar ska motiveras noga.

Uppgift 1. Svara på följande frågor.

(a) Finn alla lösningar till $2x + 2y = 1$ i $\mathbb{Z}_3$.

(b) Från primtalen $p = 7$ och $q = 11$, bestäm en krypteringsnyckel e för användning i RSA.

(c) Hur många delgrupper har $\mathbb{Z}_{29}$?

(d) Ge exempel på en permutation i S_5 som har ordning 6. Ange svaret på tvåradsform.

(e) Rita en graf med kromatiskt tal 4 och som saknar Hamiltonstig.

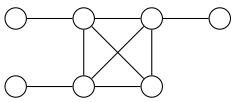
Lösning. (a) Vi multiplicerar båda led med 2. Detta leder till $x + y = 2$, så $x = 2 - y$. I $\mathbb{Z}_3$ har vi då de tre lösningarna $(x, y) = \{(0, 2), (1, 1), (2, 0)\}$.

(b) Med dessa två primtal beräknar vi $m = (7 - 1)(11 - 1) = 60$. Vi måste då välja e så att $\mathrm{sgd}(e, 60) = 1$, så vi kan ta t.ex $e = 7$.

(c) Lagranges sats säger att en delgrupps storlek måste dela gruppens storlek. Eftersom bara 1 och 29 delar 29, så finns bara två delgrupper; den med enbart identitetselementet, samt hela $\mathbb{Z}_{29}$.

(d) Vi kan ta permutationen (1 2)(3 4 5). På tvåradsform blir den $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{bmatrix}$.

(e) Man kan ta följande graf.



Uppgift 2. (a) För vilka värden på parametern $b \in \mathbb{Z}_3$ är polynomet $x^2 + 2x + b \in \mathbb{Z}_3[x]$ irreducibelt?

(b) Låt X vara mängden av moniska andragradspolynom i $\mathbb{Z}_3[x]$. Definiera relationen $\sim$ på X där $P, Q \in X$ uppfyller

$$P \sim Q \text{ precis då } P(1)^2 = Q(1)^2.$$

Visa att $\sim$ är en ekvivalensrelation samt skriv ned alla polynom i X som är i relation med polynomet $x^2 + x + 1$.

Lösning. (a) x^2+2x+b är irreducibelt om det saknar nollställen i $\mathbb{Z}_3$. För $b=0$ faktoriseras polynomet som $x(x+1)$, för $b=1$ faktoriseras polyomet till $(x+1)^2$ men för $b=2$ blir polynomet x^2+2x+2, vilket saknar nollställen (man testar $x=0,1,2$). Så $b=2$ är det enda värde då polynomet är irreducibelt.

(b) Relationen är uppenbarligen reflexiv och symmetrisk. Vidare, om $P(1)^2=Q(1)^2$ och $Q(1)^2=R(1)^2$, gäller $P(1)^2=R(1)^2$ så vi har också transitivitet.

Låt $P(x)=x^2+x+1$. Då gäller $P(1)^2=(1+1+1)^2=0$ i $\mathbb{Z}_3$. Nu,

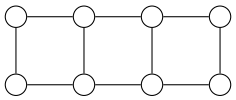
$$P\sim Q \iff Q(1)^2=0 \iff Q(1)=0 \iff (x+2)\mid Q.$$

Alltså måste $Q=(x+2)(x+c)$, för $c\in\mathbb{Z}_3$. Dessa polynom är

$$(x+2)x=x^2+2x,\quad (x+2)(x+1)=x^2+2,\quad (x+2)(x+2)=x^2+x+1,$$

och är då de polynom som är ekvivalenta med P. Alternativt kan man beräkna $Q(1)^2$ för var och en av de 9 polynomen $Q\in X$ och se vilka som ger resultatet 0.

Uppgift 3. Tre kvadrater har placerats i rad, så att en graf med 8 hörn har bildats.



Hörnen kan färgas vita eller svarta och grannar får ha samma färg.

(a) Hur många färgläggningar finns det totalt?

(b) Hur många färgläggningar uppfyller att den vänstra kvadraten är *monokromatisk*, dvs. alla fyra hörn har samma färg?

(c) Hur många färgläggningar uppfyller att ingen av de tre kvadraterna är monokromatisk?

Alla svar ska beräknas till ett heltal.

Lösning. (a) Hörnen färgas oberoende av varandra, så $2^8=256$.

(b) Val av kvadratfärg samt färg på 4 ytterligare hörn ger $2^5=32$ färgläggningar

(c) Låt V, M och H vara de färgläggningar med vänster, mitten och höger kvadrat monokromatisk, respektive. Vi söker $2^8-|V\cup M\cup H|$. Enligt föregående beräkning (samt symmetri) har vi

$$|V|=|M|=|H|=2^5.$$

Vidare, $|V\cap M|=|M\cap H|=2^3$ då 6 av hörnen tvingas ha samma färg. Vi har också $|V\cap H|=2^2$, då de två disjunkta kvadraterna ska färgas. Slutligen, $|V\cap M\cap H|=2$ då alla hörn ska ha samma färg. Inklusion-exklusion ger nu att antalet färgläggningar som sökes är

$$2^8-3\cdot 2^5+2\cdot 2^3+2^2-2=256-96+16+4-2=178.$$

Vänligen vänd!

Uppgift 4. Låt G vara mängden av matriser på formen $\begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix}$ där $x \in \mathbb{Q} \setminus \{0\}$ och $y \in \mathbb{Q}$.

(a) Visa att G är en grupp under matrismultiplikation.

(b) Visa att det inte finns något element i G som har ordning 3.

Lösning. (a) Alla matriser i G har determinant 1, så G är en delgrupp till mängden av inverterbara 2×2-matriser med rationella tal. Det räcker då att G är sluten under multiplikation samt invers. Nu,

$$\begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix} \cdot \begin{bmatrix} z & w \\ 0 & z^{-1} \end{bmatrix} = \begin{bmatrix} xz & xw + yz^{-1} \\ 0 & (xz)^{-1} \end{bmatrix}, \qquad \begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} x^{-1} & -y \\ 0 & x \end{bmatrix}$$

så G är sluten under multiplikation samt invers.

(b) Om en matris $A \in G$ har ordning 3, måste $A^3 = 1$. Vi har att

$$\begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix}^3 = \begin{bmatrix} x^2 & y(x + x^{-1}) \\ 0 & x^{-2} \end{bmatrix} \begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix} = \begin{bmatrix} x^3 & y(x^2 + 1 + x^{-2}) \\ 0 & x^{-3} \end{bmatrix}.$$

Om detta ska vara lika med identitetsmatrisen, måste vi ha

$$x^3 = 1 \text{ och } y(x^2 + 1 + x^{-2}) = 0.$$

Den första ekvationen tvingar $x = 1$, vilket insatt i den andra ger att $y = 0$. Dvs. identitetsmatrisen själv är den enda matris som uppfyller $A^3 = I$, men identitetsmatrisen har ordning 1. Alltså finns inga element i G med ordning 3.

Uppgift 5. Låt X vara mängden som består av alla sätt att fylla de 8 rutor arrangerade i en kvadrat med någon av symbolerna i $\{\times, \circ, \bullet\}$. Ett exempel på en sådan figur är följande:

○	●	×
○		●
×	○	●

Mittenrutan är alltid tom.

(a) Bestäm det totala antalet element i X.

(b) Den cykliska gruppen $G = \{e, r, r^2, r^3\}$ verkar på X genom att r roterar figuren 90° moturs. Rita en figur som tillhör $\mathrm{Fix}(r^2)$ men som inte tillhör $\mathrm{Fix}(r)$.

(c) Bestäm antalet banor under G. Svaret behöver inte förenklas.

Lösning. (a) Varje ruta kan anta 3 olika värden, så det blir $3^8 = 81^2 = (80 + 1)^2 = 6400 + 160 + 1 = 6561$ i X.

(b) Man kan ta följande figur. Den fixeras av r^2 (rotation 180°) men blir annorlunda om man roterar ett kvarts varv.

○	○	×
○		○
×	○	○

(c) Vi använder Burnsides lemma, så vi behöver räkna ut antalet fixpunkter för varje element i G. Vi får följande beräkning

g	$\mathrm{Fix}(g)$
e	3^8
r	3^2
r^2	3^4
r^3	3^2

$\mathrm{Fix}(r)$, $\mathrm{Fix}(r^3)$:

a	b	a
b		b
a	b	a

$\mathrm{Fix}(r^2)$:

a	d	c
b		b
c	d	a

där bokstäverna indikerar element som måste vara lika för att vara en fixpunkt. Burnside's lemma säger nu att antalet banor är

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{4}\left(3^8 + 2\cdot 3^2 + 3^4\right) = 1665.$$

Uppgift 6. Kom ihåg att $\mathbb{N} = \{1, 2, 3, \dots\}$. En funktion $f : \mathbb{N} \to \mathbb{N}$ kallas för *ökande* om $f(n) \leq f(n+1)$ för alla $n \geq 1$.

(a) Hur många ökande funktioner $f : \mathbb{N} \to \{1, 2\}$ finns det som uppfyller $f(1) = 1$ och $f(5) = 2$?

(b) Visa att mängden av ökande funktioner $f : \mathbb{N} \to \{1, 2\}$ är uppräknelig.

(c) Visa att mängden av ökande funktioner $f : \mathbb{N} \to \mathbb{N}$ *inte* är uppräknelig.

Notera att i (c) får nu f anta värden i $\mathbb{N}$.

Lösning. (a) Eftersom $f(5) = 2$ och funktionen är ökande, gäller det också att $f(n) = 2$ då $n \geq 5$. Det räcker då att beskriva $f(2), f(3), f(4)$ och dessa kan då vara något av de fyra alternativen $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 2)$ eller $(2, 2, 2)$.

(b) Om $f : \mathbb{N} \to \{1, 2\}$ är ökande, gäller det antingen att f är konstant (lika med 1 eller 2), eller så finns det ett positivt heltal k så att

$$f(n) = \begin{cases} 1 & \text{om } n \leq k \\ 2 & \text{annars.} \end{cases}$$

Eftersom antalet olika k är uppräknelig (i bijektion med $\mathbb{N}$) så är också antalet funktioner uppräknelig.

(c) Vi använder ett diagonaliseringsargument. Antag att vi har en (uppräknelig) lista med ökande funktioner,

$$f_1, f_2, f_3, f_4, \dots .$$

Vi definierar då en ny funktion f^* enligt följande rekursiva formel;

$$f^*(1) = f_1(1) + 1 \qquad f^*(n) = \max\left(f_n(n) + 1, f^*(n-1)\right) \text{ då } n \geq 2.$$

Notera att för $n \geq 1$ har vi att $f^*(n+1) \geq f^*(n)$ så f^* är ökande. Vi ser också att $f^*(n)$ är strikt större än $f_n(n)$, så f^* kan inte vara samma funktion som f_n, för något n. Med andra ord, f^* finns inte i listan. Detta visar att det är omöjligt att lista alla ökande funktioner, så denna mängd är inte uppräknelig.

Alternativ lösning: Man kan också konstruera en surjektion från mängden ökande funktioner till någon mängd som inte är uppräknelig, t.ex $\mathcal{P}(\mathbb{N})$ eller de reella talen mellan 0 och 1.

Givet en ökande funktion f, vi kan associera ett reellt tal $0.b_1b_2b_3\dots$ (binära decimalutveckingen) genom att låta

$$b_i = \begin{cases} 1 \text{ om } f(i) < f(i+1) \\ 0 \text{ om } f(i) = f(i+1). \end{cases}$$

Till exempel, det reella talet som börjar med de binära siffrorna $0.10110101\dots$ fås bland annat från

$$(f(1), f(2), f(3), \dots) = (0, 1, 1, 2, 3, 3, 4, 4, 5, \dots).$$

Det är då ganska klart att vi har en surjektion från ökande funktioner till reella tal i intervallet $[0, 1)$, så mängden ökande funktioner måste vara överuppräknelig.