MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Rikard Bøgvad
Kursansvarig: Magnus Carlson

Tentamensskrivning i
Algebra och kombinatorik
7.5 hp
15 februari 2024

Lösningsförslag

1. (5p) Svara på följande frågor

   (a) Låt G vara en grupp och låt $g \in G$ vara ett element så att g har ordning m, där m är ett positivt heltal. Bestäm alla positiva heltal n så att $g^n = e$, där e är identitetselementet i G.

   (b) Lös ekvationen $5x + 7 = 13$ i $\mathbb{Z}_{23}$.

   (c) Hitta koefficienten framför x^5y^{45} som fås om man expanderar uttrycket $(15x + 7y)^{50}$. Svaret får anges i kombinatorisk standardform.

   (d) Beräkna ordningen av permutationen $(123)(456789)(10\ 11)$ i S_{11}.

   (e) Hur många omordningar kan man bilda av bokstäverna i "ordet" $AABBCDEFG$?

   Lösning: För a) ser vi att heltalen n vi söker är de som är multiplar av m. För att lösa ekvationen $5x+7 = 13$ så subtraherar vi och får $5x = 6$. Denna kan vi lösa genom att lösa ekvationen $5x+23y = 6$ och den löser vi med hjälp av Euklides algoritm och ser att $x = 15$ är en lösning till ekvationen. För att hitta koefficienten så använder vi bonimalsatsen och får att koefficienten är $\binom{50}{5}15^57^{45}$. Ordningen av permutationen ges som minsta gemensamma multiplen av cykellängderna, så ordningen är 6. Slutligen, antalet omordningar ges av multinomialtalet $\binom{9}{2,2}$.

2. Låt G vara en grupp och låt H, K vara delgrupper av G. Definiera snittet av H och K som $H \cap K := \{g \in G | g \in H, g \in K\}$, dvs. de element av G som både ligger i H och K.

   (a) Visa att $H \cap K$ är en delgrupp av G. 3p

   (b) Låt H ha ordning 13 och låt K ha ordning 51. Vilka ordningar är möjliga för $H \cap K$? 2p

   Lösning: För att visa att $H \cap K$ är en delgrupp så behöver vi visa att för alla $h_1, h_2 \in H \cap K$ så gäller att $h_1 \cdot h_2^{-1} \in H \cap K$. Eftersom att $h_1, h_2 \in H$ så gäller att $h_1 \cdot h_2^{-1} \in H$ och eftersom $h_1, h_2 \in K$ så gäller även att produkten ligger i K. Således gäller att $h_1 \cdot h_2^{-1} \in H \cap K$. Så snittet är en delgrupp. Eftersom att $H \cap K$ är en delgrupp av både H och K så måste ordningen, av Lagrange, dela både 13 och $51 = 17 \cdot 3$. Men det enda talet som delar både 13 och 51 är 1. Således är $H \cap K$ den triviala gruppen.

3. En glassbar har 13 olika smaker på sina glasstrutar. En familj med tre barn kommer in och skall beställa glass. Barnen har de ovanliga namnen A,B och C. På hur många vis kan familjen beställa 7 glasstrutar med *olika* smaker och sedan dela ut dessa till de tre barnen så att varje barn får åtminstone en glasstrut? För att förtydliga så spelar det roll vilket barn som får vilka glassar, och hur många glassar varje barn får, så t.ex. så är fördelningen där barn A får en vaniljstrut och en jordgubbsstrut, barn B hallon och citron, och barn C en chokladstrut, en pistagestrut och en melonstrut, annorlunda än fördelningen där barn A får en chokladstrut, pistagestrut och en melonstrut, barn B får vanilj och jordgubb och barn C hallon och citron.
   5p *Lösning:* Vi följer först 7 smaker från de 13 på $\binom{13}{7}$ vis. Vi ska sedan distribuera dessa till barnen så att ingen är utan någon glasstrut. Detta är samma som att räkna antalet surjektioner från en mängd av storlek 7 till en mängd av storlek 3 och det finns $S(7,3) \cdot 3!$ sådana surjektioner. Således finns det $\binom{13}{7} \cdot S(7,3) \cdot 3!$ olika sätt.

4. (Denna uppgift hade tyvärr ett misstag—$n = 17$ är inte av formen $n = pq$ för två olika primtal. Så den utgick. Men det kan, i efterhand vara instruktivt att ändå titta på lösningen och se hur mycket som går igenom. Men samtidigt är idén att ta $n = p$, ett primtal, helt idiotiskt som krypteringsmetod. Varför då?) Ett RSA-krypto har offentlig nyckel $n = 17$ och $e = 5$.

   (a) Kryptera meddelandet 10. 2p

   (b) Dekryptera meddelandet 2. 3p

   Lösning: För att kryptera meddelandet 10 så beräknar vi 10^5 modulo 17. Vi ser att $10^5 = 10 \cdot (10^2)^2$ och då $100 = 15$ i $\mathbb{Z}_{17}$ så ser vi att $10^5 = 10 \cdot 15^2 = 10 \cdot 225$ och $225 = 4$ så det krypterade meddalandet är $40 = 6$. För att dekryptera meddelandet 13 så vill vi alltså hitta ett g så att $g^5 = 2$. Vi söker då först ett d så att $5d = 1$ modulo 16, så en lösning ges av 13. Vi beräknar sen att $(g^5)^{13} = g = 2^{13} = 15$. Så det meddelandet som dekrypterades var 15.

5. Låt $\sigma = (29)(357)(18)$ och $\tau = (457)(28)$ i S_9.

   (a) Beräkna $\sigma\tau$ och σ^{-1} och skriv ner svaret på cykelform. Vad är ordningen av $\sigma\tau$? 2p

   (b) Finns det ett $k \geq 0$ och ett $\gamma \in S_9$ så att $\gamma\sigma^k\gamma^{-1} = (4\ 9)(5\ 2)$? 3p

   Lösning: En beräkning visar att $\sigma\tau = (281)(35)(47)$ och att $\sigma^{-1} = (29)(753)(18)$. Ordningen är $\sigma\tau$ är 6, då det är minsta gemensamma multipeln av cykellängderna. Den andra frågan är ekvivalent med att fråga huruvida det finns ett k så att σ^k har samma cykeltyp som $(4\ 9)(5\ 2)$. Vi ser att om $k = 3$ så gäller att trecykeln försvinner, medan två cyklerna fortfarande kvarstår. Således finns en lösning för $k = 3$.

6. Betrakta grafen G som ges $G = (V, E)$ där $V = \{v_1, v_2, v_3, v_4\}$ och

$$E = \{(v_1, v_4), (v_1, v_2), (v_2, v_4), (v_2, v_3), (v_3, v_4)\}.$$

   (a) Bestäm automorfigruppen av G. Kom ihåg att automorfigruppen till G är de bijektioner $f : V \to V$ så att om (v_i, v_j) är en kant, $i \neq j$, så är $(f(v_i), f(v_j))$ en kant. 3p

   (b) Säg att vi har fyra färger och att vi vill färglägga kanterna i grafen med dessa färger, flera kanter får ha samma färg. Hur många ekvivalensklasser av sådana färgläggningar av grafen G finns det, om vi betraktar två färgläggningar som ekvivalenta om de skiljer sig åt med en automorfi av G? 2p

   Lösning: Kalla hörnen för v_1, v_2, v_3, v_4 där v_1 är hörnet som är längst upp, och v_2, v_3, v_4 är de resterande hörnen tagen i medurs ordning. Då ser vi att för att en bijektion av hörnmängden skall vara en grafhomomorfism att antingen så går v_1 på sig självt, eller så byter v_1 plats med v_3, och samma för v_2 och v_4. Således finns det fyra automorfier. f_1 definierad genom att $f(v_i) = v_i$ för alla hörn, f_2 definierad genom att $f_2(v_1) = v_3, f_2(v_3) = v_1, f_2(v_2) = v_2, f_2(v_4) = v_4$, f_3 definierad genom att $f_3(v_1) = v_1, f_3(v_3) = v_3, f_3(v_2) = v_4, f_3(v_4) = v_2$ och f_4 definierad genom att $f_4(v_1) = v_3, f_4(v_3) = v_1, f_4(v_2) = v_4, f_4(v_4) = v_2$. Det finns totalt fem kanter, det finns totalt 4^5 olika färgläggningar om vi inte betraktar dessa upp till automorfi. VI använder Burnside för att hitta antalet färgläggningar upp till automorfi. Det är klart att identitetselementet fixerar alla färgläggningar, medan f_2 tar kanten (v_1, v_2) på (v_3, v_2), (v_1, v_4) på (v_3, v_4), de övriga kanterna rörs ej. Vi ser således att (v_1, v_2) måste ha samma färg som (v_3, v_2) och att (v_1, v_4) måste ha samma färg som (v_3, v_4) och den andra kanten kan väljas godtyckligt. Således finns det totalt 4^3 färgläggningar som f_2 fixerar och samma resonemang fungerar för f_3. För f_4 så ser vi att (v_1, v_4) går på (v_3, v_2), (v_1, v_2) på (v_3, v_4) och de andra är fixerade, så återigen 4^3 färglägningar. Av Burnsides lemma får vi att antalet icke-ekvivalenta färgläggningar är $\frac{4^5 + 3 \cdot 4^3}{4} = 304$.