Matematiska institutionen
Stockholms universitet
Avd. Matematik
Examinator: Olof Sisask

Tentamensskrivning, omtenta
Kurskod: MM5013

2020-02-14 09:00–14:00

Tentamen i Algebra och Kombinatorik

Motivera dina svar noggrant. *Inga hjälpmedel är tillåtna. Tentan har 6 frågor, värda 5 poäng var. Totalt 15 poäng (med eventuella bonuspoäng) garanterar godkänt betyg.*

Lösningsförslag

1. (a) Ange definitionen av den multiplikativa inversen till ett tal a i $\mathbb{Z}_m$ (heltalen modulo m), där en sådan invers finns.
   (b) Bestäm den multiplikativa inversen till 5 i $\mathbb{Z}_{33}$. Ange ditt svar bland $\{0, 1, \ldots, 32\}$.
   (c) Sats: Ett tal $a \in \mathbb{Z}_m$ är multiplikativt inverterbart om och endast om $\text{sgd}(a, m) = 1$. Förklara varför detta är sant. (Obs: det finns två riktningar att förklara. Du behöver inte ge ett formellt bevis, men samtliga huvudidéer måste finnas med för full poäng.)

Lösning (a) Inversen av $a \in \mathbb{Z}_m$ är ett element $x \in \mathbb{Z}_m$ sådant att $ax = 1$, om ett sådant x finns.

(b) Eftersom $20 \cdot 5 = 100 \equiv 1 \pmod{33}$ så är $5^{-1} = 20$ i $\mathbb{Z}_{33}$.

(c) **Endast om**: om a är inverterbart, då finns det ett element $x \in \mathbb{Z}_m$ sådant att $ax = 1$. Per definition av ringen $\mathbb{Z}_m$ motsvarar detta att $ax = 1 + my$ för något heltal y. Varje gemensam delare till a och m delar också kombinationen $ax - my = 1$, och därmed är $\text{sgd}(a, m) = 1$.
Om: Om $\text{sgd}(a, m) = 1$ så finns det enligt den förlängda Euklidiska algoritmen/Euklides algoritm 'baklänges' heltal x, y sådana att

$$ax + my = 1.$$

Om vi reducerar detta modulo m så får vi att $ax = 1$ i $\mathbb{Z}_m$, dvs att a är inverterbart i $\mathbb{Z}_m$.

2. I denna fråga får dina svar uttryckas med hjälp av heltal och operationerna plus, minus, gånger, delat med och fakultet, och behöver inte förenklas.
   (a) Från en grupp med 20 studenter ska 12 väljas ut och delas upp i 4 lag: ett problemlösningslag med 5 studenter, ett redovisningslag med 3 studenter, ett grafiklag med 3 studenter, samt ett ledarlag med 1 student. På hur många sätt kan dessa lag formas?
   (b) Säg att Alice och Bob är bland de 12 studenterna som valts ut. På hur många sätt kan de 4 lagen formas från dessa 12 studenter, om Alice och Bob vägrar vara i samma lag?

Lösning (a) Vi väljer först de 12 studenterna och räknar sedan antalet sätt att kombinera dem, och får fram det slutliga svaret mha multiplikationsprincipen. Det finns $\binom{20}{12}$ sätt att välja de 12 studenterna på, enligt definition av binomialkoefficienter. För varje av dessa sätt finns det sedan

$$\binom{12}{5,\ 3,\ 3,\ 1} = \frac{12!}{5!\,3!\,3!\,1!}$$

sätt att dela upp dessa i de 4 lagen, per definition av multinomialkoefficienter samt sats för deras uträkning. Enligt multiplikationsprincipen är det totala antalet sätt

$$\frac{20!}{12!\,8!} \cdot \frac{12!}{5!\,3!\,3!\,1!} = \frac{20!}{8!\,5!\,3!\,3!\,1!}.$$

Att svaret är $\binom{20}{8,\,5,\,3,\,3,\,1}$ kan också ses direkt genom att tänka på ett femte 'icke-deltagar'-lag.

Var god vänd...

(b) Vi räknar antalet sätt där Alice och Bob hamnar i samma lag, och tar sedan bort detta från totalen $\binom{12}{5,3,3,1}$ uträknad ovan.

Om Alice och Bob ska vara i problemlösningslaget så finns det $\binom{10}{3,3,3,1}$ sätt att dela upp de resterande 10 studenterna i lagen.

Om Alice och Bob ska vara i redovisningslaget så finns det $\binom{10}{5,1,3,1}$ sätt att dela upp de resterande 10 studenterna i lagen.

Om Alice och Bob ska vara i grafiklaget så finns det $\binom{10}{5,3,1,1}$ sätt att dela upp de resterande 10 studenterna i lagen.

Alice och Bob kan inte båda vara i ledarlaget.

Alltså finns det

$$\binom{10}{3,\ 3,\ 3,\ 1} + \binom{10}{5,\ 1,\ 3,\ 1} + \binom{10}{5,\ 3,\ 1,\ 1}$$

fördelningar där Alice och Bob hamnar i samma lag.

Antalet fördelningar där Alice och Bob inte hamnar i samma lag är alltså $\binom{12}{5,3,3,1}$ minus detta, dvs

$$\frac{12!}{5!\,3!\,3!} - \frac{10!}{3!\,3!\,3!} - \frac{2\cdot 10!}{5!\,3!}.$$

3. (a) Avgör om $(x+1)^{18}(x+2)^{32} = (x^2+1)(x^3-2x^2+x+4)^{16}$ som polynom i $\mathbb{Z}_7[x]$. Motivera!

(b) Faktorisera polynomet $p(x) = x^6+1$ i $\mathbb{Z}_2[x]$ i irreducibla faktorer. Förklara varför faktorerna du skrivit ned är irreducibla.

Lösning (a) Eftersom $\mathbb{Z}_7$ är en kropp så vet vi att ringen $\mathbb{Z}_7[x]$ har unik faktorisering in i irreducibla faktorer. Polynomen $x+1$ och $x+2$ är uppenbarligen irreducibla, eftersom de har grad 1. Polynomet x^2+1 är också irreducibelt: om det kan faktoriseras som

$$x^2+1 = f(x)g(x)$$

där graden av både $f(x)$ och $g(x)$ är åtminstone 1, så måste graden av $f(x)$ och $g(x)$ vara exakt 1. Därför skulle x^2+1 ha en rot i $\mathbb{Z}_7$, men en snabb koll av de 7 olika möjligheterna $(0, \pm 1, \pm 2, \pm 3)$ för x visar att det inte har någon rot. Alltså är x^2+1 irreducibel.

Eftersom HL:et har en irreducibel faktor som inte står med bland de irreducibla faktorerna i VL:et så är polynomen ej lika.

(b) Eftersom $(f(x)+1)^2 = f(x)^2+1$ i $\mathbb{Z}_2[x]$ så är

$$x^6+1 = (x^3+1)^2.$$

Polynomet x^3+1 har $x=1$ som en rot, och är alltså delbart med $x-1$. Polynomdivision ger då

$$x^3+1 = (x-1)(x^2+x+1).$$

Den andra faktorn här är irreducibel, eftersom den har grad 2 och inte har någon rot i $\mathbb{Z}_2$. Alltså är

$$x^6+1 = (x-1)^2(x^2+x+1)^2$$

en faktorisering i irreducibla faktorer.

4. Betrakta den symmetriska gruppen $(S_8, \circ)$, som består av permutationer på mängden $\{1, 2, 3, \dots, 8\}$, och låt $\sigma, \pi \in S_8$ vara permutationerna

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 3 & 1 & 5 & 6 & 7 & 8 \end{bmatrix}, \quad \pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 6 \end{bmatrix}.$$

(a) Bestäm om σ är en jämn eller udda permutation, och detsamma för π.

(b) Bestäm ordningarna av permutationerna $\sigma\pi$, $(\sigma\pi)^2$, $(\sigma\pi)^3$ och $\sigma^{-1}\pi$.

Lösning (a) I cykelnotation har vi

$$\sigma = (1\ \ 2\ \ 4) \quad \text{och} \quad \pi = (1\ \ 2\ \ 4)(3\ \ 5)(6\ \ 7\ \ 8).$$

Eftersom en cykel av längd 3 kan skrivas som en produkt av två 2-cykler, t.ex. $(1\ \ 2\ \ 4) = (1\ \ 2)(2\ \ 4)$, så kan σ skrivas som en produkt av 2 2-cykler, och är därmed jämn, medans π kan skrivas som en produkt av 5 2-cykler och är därmed udda.

(b) Vi har att

$$\sigma\pi = (1\ \ 4\ \ 2)(3\ \ 5)(6\ \ 7\ \ 8).$$

Enligt sats från kursen ges ordningen av en permutation, skriven som en produkt av disjunkta cykler, av den minsta gemensamma multipeln av ordningen av cykellängderna; alltså är

$$\text{ord}(\sigma\pi) = \text{lcm}(3, 2, 3) = 6.$$

Enligt sats från gruppteori, eller via direkt beräkning, är

$$\text{ord}((\sigma\pi)^2) = 6/2 = 3$$

och

$$\text{ord}((\sigma\pi)^3) = 6/3 = 2.$$

Slutligen har vi att

$$\sigma^{-1}\pi = (3\ \ 5)(6\ \ 7\ \ 8)$$

har ordning 6, av samma anledning som förut.

5. Betrakta gruppen $G = (\mathbb{Z}_{100}, +)$ av heltalen modulo 100 med operationen plus.

(a) Bestäm en delgrupp H till G där varje nollskilt element har ordning 5.

(b) Låt H vara den delgrupp till G som innehåller både elementen 25 och 8, men som annars har så få element som möjligt. Bestäm hur många element H har.

Lösning (a) Ordningen av ett element $g \in G$ är det minsta talet n så att $ng = \text{id} = 0$. Elementen av ordning 5 är alltså 20, 40, 60, 80. Tillsammans med 0 bildar dessa en delgrupp:

$$H = \{0, 20, 40, 60, 80\}.$$

(b) Eftersom delgruppen innehåller 8 och 25 och är sluten under addition och att ta inverser, så måste den innehålla $25 - 8 - 8 - 8 = 1$. Därför innehåller den också alla multiplar av 1, eftersom den är sluten under addition. Därför är

$$H = G$$

och har 100 element.

6. (a) För var och en av följande talföljder, bestäm om det finns en graf med 5 noder med dessa tal som grader. Om det finns det, rita en sådan graf; om det inte finns, förklara varför.

(i) 2, 3, 3, 4, 4, (ii) 2, 3, 4, 4, 4, (iii) 4, 4, 4, 4, 4.

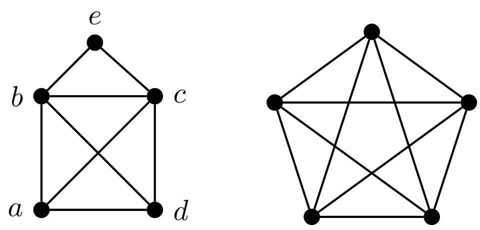
(b) Ange, för någon av graferna i del (a), en Eulerväg i grafen. Skriv ditt svar som en följd av noder, där nodnamnen står med i din ritning.

(c) Om en graf har en Eulerkrets (dvs en sluten Eulerväg) så måste varje nod i grafen ha jämn grad. Förklara varför.

Lösning (a)

(i) Ja, (ii) Nej, (iii) Ja.

För (i) och (iii), se diagram. För (ii): summan av alla talen är udda här, medans för graderna i en graf är summan alltid jämn, enligt handskakningslemmat.



(i) (iii)

(b) För (i): t.ex. $a\ b\ e\ c\ d\ a\ c\ b\ d$.

(c) Låt v vara en godtycklig nod i grafen. Varje gång en kant leder in till noden v längs Eulerkretsen så finns det en unik kant som leder ut längs Eulerkretsen. Eftersom alla kanter förekommer i Eulerkretsen (enligt definition av Eulerkrets) så förekommer alla kanter intill v i par av in- och ut-kanter, med inget överlapp mellan paren. Alltså har varje nod jämn grad.