MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Dan Petersen
Kontrollant: Sofia Tirabassi

Tentamensskrivning i
Algebra och Kombinatorik, MM5013
7.5 hp
2019-08-21

Inga hjälpmedel är tillåtna. 15 poäng (inräknat eventuella bonuspoäng) garanterar godkänt betyg. Motivera lösningarna noggrant. Problemen är INTE sorterade i svårighetsordning.

1. (a) Hur många ord med 11 bokstäver kan bildas genom att ordna om bokstäverna i ordet AUSTRALASIA? 2 poäng.

   (b) Hur många ord med 5 bokstäver kan bildas genom att använda[1] bokstäver från ordet AUSTRALASIA? 2 poäng.

   Lösning:

   (a) Det finns 11 bokstäver i AUSTRALASIA, 4 av dem är A och 2 är S. Alltså är svaret $\frac{11!}{4!\cdot 2!}$.

   (b) Vi har 5 platser som vi kan fylla med 4 A, 2 S och med bokstäverna U, T, R, L, I. Vi delar in i flera olika fall:

   - Antal ord med högst ett A och högst ett S $= \binom{7}{5} \cdot 5! = \frac{7!}{2!}$, eftersom vi ska välja fem av sju bokstäver och sedan ordna dessa fem bokstäver godtyckligt.
   - Antal ord med två A och högst ett S $= \binom{5}{2} \cdot \binom{6}{3} \cdot 3!$, eftersom vi ska välja två platser för A, och sedan blir resten ett ord med tre bokstäver av sex möjliga.
   - Antal ord med tre A och högst ett S $= \binom{5}{3} \cdot \binom{6}{2} \cdot 2!$, enligt samma princip som ovan.
   - Antal ord med fyra A och högst ett S $= \binom{5}{4} \cdot \binom{6}{1} \cdot 1!$, enligt samma princip som ovan.
   - Antal ord med två S och högst ett A $= \binom{5}{2} \cdot \binom{6}{3} \cdot 3!$, enligt samma princip som ovan.
   - Antal ord med två A och två S $= \binom{5}{2,2,1} \cdot 5$, eftersom vi ska välja två platser för A, två platser för S, och en av fem möjliga bokstäver på sista platsen.
   - Antal ord med tre A och två S $= \binom{5}{2,3}$
   - Antal ord med fyra A och två S $= 0$.

   Lösningen till problemet är summan av alla antal!

2. (a) Vad är det största antalet kanter som en graf med 5 noder kan ha? 1 poäng.

   (b) Ge exempel på två icke-isomorfa grafer med 5 noder och 8 kanter. Förklara varför de inte kan vara isomorfa med varandra. 2 poäng.

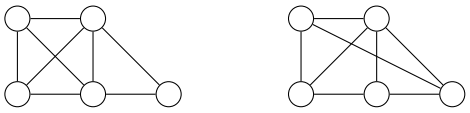
[1] Till exempel är SAAIT ett sådant ord, men inte SLLIT: ordet kan som mest innehålla ett "L".

(c) Visa att varje graf med 5 noder och 8 kanter är isomorf med en av de två graferna du konstruerade i del (b). 3 poäng.

Lösning:

(a) Det största antalet är $\binom{5}{2} = 10$.

(b) Betrakta följande två grafer:



Dessa har båda fem noder och åtta kanter. Man kan t.ex. se att graferna inte är isomorfa eftersom den vänstra har en nod av grad två och den högra inte har det.

(c) För att skapa en graf med fem noder och åtta kanter kan man starta från den kompletta grafen K_5, d.v.s. grafen med fem noder och där varje par av noder är förbundna med en kant, och sedan ta bort exakt två av kanterna. Men upp till att numrera om noderna finns det nu bara två möjligheter: antingen tar vi bort två kanter som möts i en nod, eller så tar vi bort två kanter som inte möts. Dessa två möjligheter ger upphov till de två graferna ovan.

3. Betrakta permutationen $\alpha = (12345)(24567)(1872)$ i S_8.

(a) Skriv α som en produkt av disjunkta cykler, och hitta inversen till α. 2 poäng.

(b) Vad är ordningen av α? 2 poäng.

(c) Avgör om α är udda eller jämn. 2 poäng.

Lösning

(a) Man räknar ut att $\alpha = (1834)(567)$, $\alpha^{-1} = (576)(1438)$.

(b) Permutationen α är en produkt av två disjunkta cykler av längd 3 och 4. Ordningen till α är därmed $\operatorname{lcm}(4,3) = 12$.

(c) En k-cykel har tecknet $(-1)^{k-1}$. Alltså är $\operatorname{sgn}(\alpha) = \operatorname{sgn}(567) \cdot \operatorname{sgn}(1438) = (-1)^{3-1} \cdot (-1)^{4-1} = -1$. Därför är α udda.

4. Låt X_n beteckna mängden av positiva delare till det positival heltalet n. Givet två positiva heltal n och m låt $f : X_n \times X_m \to X_{nm}$ definieras genom $f(a,b) = ab$.

(a) Visa att f är surjektiv. 2 poäng.

(b) Visa att f inte är injektiv om $\gcd(m,n) > 1$. 1 poäng.

(c) Visa att f är injektiv om $\gcd(m,n) = 1$. 3 poäng.

Lösning: Den enklaste delen av uppgiften är del (b). Antag att $d = \gcd(m,n) > 1$. I så fall kommer $X_n \times X_m$ innehålla båda elementen $(d,1)$ och $(1,d)$. Men vi har $f(d,1) = f(1,d) = d$. Så f är inte injektiv.

Del (a) och (c) är svårare och vi presenterar två olika lösningsalternativ.

(Alternativ 1.) Antag att vi har primtalsfaktoriseringarna $n = \prod_i p_i^{a_i}$ och $m = \prod_i p_i^{b_i}$, vilket alltså ger $nm = \prod_i p_i^{a_i+b_i}$. Obs: här tillåter vi att vissa av talen a_i och b_i är noll, så vi antar alltså inte att det är exakt samma primtal som delar både n och m.

Ett tal s ligger i X_n om och endast om $s = \prod_i p_i^{d_i}$ med $0 \leq d_i \leq a_i$ för alla i. På samma sätt är varje $t \in X_m$ unikt på formen $t = \prod_i p_i^{e_i}$ med $0 \leq e_i \leq b_i$, och produkten st får primtalsfaktoriseringen $st = \prod_i p_i^{d_i+e_i}$.

Tag ett element $r \in X_{nm}$, som alltså kan skrivas som $r = \prod_i p_i^{c_i}$, där $0 \leq c_i \leq a_i + b_i$ för alla i. Vi vill visa att f är i bilden av f, d.v.s. att vi kan skriva $r = st$ där $s \in X_n$ och $t \in X_m$. Men eftersom $r = \prod_i p_i^{c_i}$ och $st = \prod_i p_i^{d_i+e_i}$ är detta samma sak som att skriva varje tal c_i som en summa $d_i + e_i$, där $0 \leq d_i \leq a_i$ och $0 \leq e_i \leq b_i$. Men det är klart att om $c_i \leq a_i + b_i$ kan c_i skrivas som en summa av två tal som är högst lika med a_i respektive b_i. Alltså går det att skriva r som en produkt av ett element i X_n och ett element i X_m, så f är surjektiv.

Antag nu dessutom att $\gcd(n, m) = 1$. I så fall har n och m inga gemensamma primtalsfaktorer, så om $a_i > 0$ är $b_i = 0$ och vice versa. Antag t.ex. att $a_i = 0$ och att vi ska välja d_i och e_i som i föregående paragraf. Vi får då $0 \leq d_i \leq 0$, så $d_i = 0$, och om $c_i = d_i + e_i$ finns då endast möjligheten $e_i = c_i$. Alltså finns det endast en lösning för d_i och e_i, så det finns exakt ett val av element (s, t) sådana att $f(s, t) = r$. Alltså är f även injektiv.

(Alternativ 2.) Tag $r \in X_{nm}$. Låt $s = \gcd(r, n)$ och $t = r/\gcd(r, n)$. Det är klart att $s \cdot t = r$ och att $s \in X_n$, så för att visa att f är surjektiv räcker att visa att $t \in X_m$, d.v.s. att $m \equiv 0 \pmod{t}$.

Notera att $n/\gcd(r, n)$ och $r/\gcd(r, n)$ saknar gemensamma delare, eftersom om d vore en gemensam delare till dessa tal skulle $d \cdot \gcd(r, n)$ vara en större genemsam delare till r och n. Så n/s är en enhet modulo t.

Men vi har att $st \mid nm$, vilket ger $t \mid \frac{n}{s} \cdot m$, vilket ger $(\frac{n}{s}) \cdot m \equiv 0 \pmod{t}$. Eftersom $\frac{n}{s}$ är en enhet modulo t måste då $m \equiv 0 \pmod{t}$ och f är därmed surjektiv.

Antag nu att $f(s, t) = f(s', t')$, d.v.s. $st = s't'$. Vi vill visa att $s = s'$ och $t = t'$, det räcker att visa att $s \mid s'$; genom att byta plats på s och s' får vi delbarhet i andra riktningen och likadant med t. Vi har att $\gcd(s, t') = 1$ eftersom en gemensam delare till s och t' skulle vara en gemensam delare till n och m. Men notera att $st = s't' \equiv 0 \pmod{s}$. Eftersom t' är en enhet modulo s följer att $s' \equiv 0 \pmod{s}$, d.v.s. $s \mid s'$. Det följer att f är injektiv.

5. Betrakta följande checkmatris (d.v.s. matris med koefficienter i $\mathbb{Z}/2$):

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

   (a) Lår C vara motsvarande kod (d.v.s. C är kärnan till H, $\operatorname{Ker} H$).

Avgör vilka av följande ord tillhör C.

$$111001,\ 010100,\ 101100,\ 110111,\ 100001.$$

2 poäng.

(b) Avgör vilka av orden i (a) som kan rättas genom att man ändrar exakt en bit. Rätta dessa. 2 poäng.

Lösning:

(a) Vi beräknar att

$$\begin{aligned} H \cdot (1,1,1,0,0,1)^t &= (0,0,0)^t \\ H \cdot (0,1,0,1,0,0)^t &= (1,0,0)^t \\ H \cdot (1,0,1,1,0,0)^t &= (0,1,1)^t \\ H \cdot (1,1,0,1,1,1)^t &= (0,1,0)^t \\ H \cdot (1,0,0,0,0,1)^t &= (0,1,1)^t. \end{aligned}$$

Det enda ordet som ger $(0,0,0)^t$ är 111001, så det är det enda av orden som tillhör koden.

(b) Om v har exakt ett fel, är $H \cdot v$ en kolumn i H. Från förra deluppgiften ser vi att bara 010100 och 110111 har den egenskapen. Ordet 010100 rättas till 110100 och ordet 110111 rättas till 100111.

6. Betrakta polynomet $p(x) = x^4 + 2x^3 + 3x^2 + 4x + 2$ i $(\mathbb{Z}/5)[x]$.

(a) Hitta alla rötter till $p(x)$ i $\mathbb{Z}/5$. 2 poäng.

(b) Skriv $p(x)$ som en produkt of polynom som är irreducibla i $(\mathbb{Z}/5)[x]$. 2 poäng.

Lösning:

(a) Vi har $p(0) \equiv 2 \mod 5$, $p(1) \equiv 2 \mod 5$, $p(2) \equiv 4 \mod 5$, $p(3) \equiv 1 \mod 5$ och $p(4) \equiv 0 \mod 5$, så vi har bara en rot $x = 4$.

(b) Vi delar $p(x)$ med $x - 4 = x + 1$ och vi hittar

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

Vi måste avgöra om $(x^3 + x^2 + 2x + 2)$ är irreducibelt. Eftersom det har grad mindre än 4, är det tillräckligt att avgöra om det har någon rot. Eftersom varje rot till $x^3 + x^2 + 2x + 2$ är en rot till p, och det enda nollstället till p är 4, så är $x = 4$ det enda potentiella nollstället. Vi finner dock $4^3 + 4^2 + 2 \cdot 4 + 2 \equiv 0 \mod 5$, så polynomet är inte irreducibelt. Vi delar det med $(x+1)$, och får $p(x) = (x+1)^2 \cdot (x^2+2)$. Nu måste vi kontrollera att $x^2 + 2$ saknar rötter. Igen räcker det att kontrollera $x = 4$, men nu finner vi $4^2 + 2 = 18 \not\equiv 0 \mod 5$, så $x^2 + 2$ är irreducibelt! Så $p(x) = (x+1)^2(x^2+2)$.