

(Diskret matte D, ht13: F30, den sista, må 16 dec 2013)

Några problem (de flesta gamla tentauppgifter) som repetition:

1. Vilken är den största ordningen (som gruppelement) någon permutation i S_{13} har? (Gjordes inte på föreläsningen.)

För en permutation $\pi = (i_1 i_2 \dots i_k)(\dots) \dots$, skriven med disjunkta cykler, gäller $\pi^n = (i_1 i_2 \dots i_k)^n(\dots)^n \dots$ och för en cykel av längd k gäller att $(i_1 i_2 \dots i_k)^n = id$ omm $k \mid n$, så $\pi^n = id$ omm n är en multipel av **alla** cyklernas längder. Problemet blir alltså att finna en partition av 13 så att minsta gemensamma multipeln för delarna blir maximal. Lite letande ($13 = 13 = \text{mgm}(13)$; $13 = 12 + 1$, $\text{mgm}(12, 1) = 12$; $13 = 11 + 2$, $\text{mgm}(11, 2) = 22$; $13 = 11 + 1 + 1$, $\text{mgm}(11, 1, 1) = 11$; $\dots$ $13 = 5 + 4 + 3 + 1$, $\text{mgm}(5, 4, 3, 1) = 60$; $\dots$, man ser att man inte behöver gå igenom alla partitioner) ger det största värdet. **Svar: maximala ordningen är 60.**

2. Definiera den binära operationen $\circ$ på $\mathbb{Z}$ enligt $m \circ n = m + n + 3$ för $m, n \in \mathbb{Z}$. Visa att $(\mathbb{Z}, \circ)$ är en grupp och att den är isomorf med $(\mathbb{Z}, +)$.

Definitionen av $\circ$ ger att $(m - 3) \circ (n - 3) = (m - 3) + (n - 3) + 3 = (m + n) - 3$. Definiera $\beta : \mathbb{Z} \rightarrow \mathbb{Z}$ enligt $\beta(n) = n - 3$. β är en bijektion (ty den har en invers, given av $\beta^{-1}(n) = n + 3$) och enligt ovan gäller $\beta(m) \circ \beta(n) = \beta(m + n)$. Det betyder att $(\mathbb{Z}, \circ)$ har samma struktur som $(\mathbb{Z}, +)$ (speciellt är den en grupp, med identitet (nolla) $\beta(0) = -3$ och inversen till $\beta(n) = n - 3$ given av $\beta(-n) = -n - 3 = -(n - 3) - 6$, dvs inversen till n är $-n - 6$) och β är en isomorfi mellan grupperna.

Saken är klar, en isomorfi ges av $\beta(n) = n - 3$.

(Man kan förstås också verifiera gruppaxiomen för $(\mathbb{Z}, \circ)$ direkt.)

3. Visa att i en ring $(R, +, \cdot)$ där $x \cdot x = x$ för alla $x \in R$, är $x + x = 0$ för alla $x \in R$.

För ett godtyckligt $a \in R$ gäller $a \cdot a = a$ och $(a + a) \cdot (a + a) = a + a$. Med axiom för en ring (distributivitet) fås $(a + a) \cdot (a + a) = (a + a) \cdot a + (a + a) \cdot a = (a \cdot a + a \cdot a) + (a \cdot a + a \cdot a) = (a + a) + (a + a) = a + a$. Eftersom $(R, +)$ är en grupp ger detta att $a + a = 0$ för alla $a \in R$.

Saken är klar.

4. Låt p och q vara primtal så att $q \mid 2^p - 1$. Visa att $q > p$.

$q \mid 2^p - 1$ betyder att $2^p = 1$ i $\mathbb{Z}_q$, dvs $o(2) = p$ i $\mathbb{Z}_q$ (p är ju ett primtal och $o(2) \neq 1$). Men $(\mathbb{Z}_q \setminus \{0\}, \cdot)$ är en grupp av ordning $q - 1$, så $p \mid q - 1 (> 0)$. **Påståendet följer.**

5. Bestäm den moniska (dvs högstagradscoefficienten = 1) största gemensamma delaren $r(x)$ till polynomen $p(x) = x^5 + 4x^3 + 2x^2 + 3x + 3$ och $q(x) = x^4 + 4x^3 + 4x^2 + x + 2$ i $\mathbb{Z}_5[x]$.

Vi använder Euklides algoritm. Polynomdivision (i $\mathbb{Z}_5[x]$) ger $p(x) = x^5 + 4x^3 + 2x^2 + 3x + 3 = (x + 1)(x^4 + 4x^3 + 4x^2 + x + 2) + x^3 + 2x^2 + 1 = (x + 1)q(x) + s(x)$, $q(x) = x^4 + 4x^3 + 4x^2 + x + 2 = (x + 2)(x^3 + 2x^2 + 1) = (x + 2)s(x)$, så $r(x) = s(x)$.

Svar: Största gemensamma delaren $r(x) = x^3 + 2x^2 + 1$.

6. Visa att $g(x) = x^2 + 1$ är irreducibelt i $\mathbb{Z}_3[x]$ och finn ett primitivt element i den ändliga kropp som kan konstrueras med $\mathbb{Z}_3[x]$ och $g(x)$.

$g(x) = x^2 + 1$ är irreducibelt, ty om det vore reducibelt skulle det ha en linjär faktor och därmed ett nollställe i $\mathbb{Z}_3$, men $g(0) = 1$, $g(1) = g(2) = 2$.

Låt $F = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$ vara motsvarande kropp. I F gäller $x^2 = x^2 + 1 + 2 = 2$, $x^3 = x^2x = 2x$, $x^4 = x^3x = 2x^2 = 2 \cdot 2 = 1$, så x är inte ett primitivt element i F . Eftersom $F \setminus \{0\}$ har $8 = 2^3$ element, har vart och ett av dess element multiplikativ ordning 1, 2, 4 eller 8. Elementen $f = x, 2, 2x, 1$ uppfyller $f^4 = 1$, vilken har exakt 4 lösningar. Övriga nollskilda element i F har alltså ordning 8 och är därmed primitiva element.

Svar: (t.ex.) $x + 1$ är ett primitivt element.

7. Av sex sugrör formas en käck prydnad i form av en tetraeder (med sugrören som kanter). På hur många väsentligt olika sätt (dvs så att de inte blir lika hur man än vrider dem i rummet) kan det göras, om man har sugrör av k olika färger att tillgå?

Vi använder Burnsidess lemma (Thm 21.4 i Biggs).

(Den regelbundna) tetraederns grupp av symmetrirotationer har 12 element: Identitets-elementet (bevarar alla konfigurationer, $|F(id)| = k^6$), åtta rotationer $\pm \frac{2\pi}{3}$ kring axlar genom ett hörn och mittpunkten av motstående sidoyta (bevarar konfigurationer med samma färg på kanterna vid hörnet och samma på kanterna vid sidoytan, $|F(g)| = k^2$) och tre rotationer π kring axlar genom mittpunkterna av motstående kanter (bevarar konfigurationer med övriga fyra kanter parvis likfärgade, $|F(g)| = k^4$).

Lemmat ger antalet banor = antalet väsentligt olika färgningar, $\frac{1}{|G|} \sum_{g \in G} |F(g)|$. **Svar: $\frac{1}{12}(k^6 + 3k^4 + 8k^2)$**

8. Finn en kontrollmatris H för en linjär binär kod $\mathcal{C}$ som rättar ett fel, med $|\mathcal{C}| = 16$, $1011010 \in \mathcal{C}$, $0011000 \notin \mathcal{C}$. (Det sista följer av att koden rättar ett fel.)

Koden har tydligen längd 7 och dimension 4 ($16 = 2^4$), så H 's rang skall vara 3. Vi tar alltså H som en 3×7 -matris.

$1011010 \in \mathcal{C}$ ger att summan av kolonnerna 1, 3, 4 och 6 är $\mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$. $0011000 \notin \mathcal{C}$ ger att summan av kolonnerna 3 och 4 inte är $\mathbf{0}$.

Så man kan ta (summan av 1 och 6)=(summan av 3 och 4) $\neq \mathbf{0}$ och fylla ut med alla kolonner olika och $\neq \mathbf{0}$ (för att koden skall rätta ett fel). **Svar: Man kan (t.ex.) ta $H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$.**

9. 100 numrerade lådor med 100 lappar med 100 personers namn, slumpmässigt fördelade, en lapp i varje låda, står i ett rum.

De går i tur och ordning in i rummet, läser lappen i en valfri låda och lägger tillbaks den, läser lappen i en annan låda osv. Var och en får läsa högst 50 lappar.

Om **alla** finner sina egna namn får de alla ett storslaget pris.

a. Vad är sannolikheten att de lyckas om de saknar gemensam strategi?

b. Visa att det finns en gemensam strategi som ger sannolikheten över 30%(!).

Gjordes på föreläsningen. Inte där? Fundera själv!