MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Rikard Bögvad

Algebra och kombinatorik HT 2024
18 januari 2025

LÖSNINGSFÖRSLAG TILL TENTAMEN

1. a) Tag till exempel $\pi = (1234)(567)$ och $\sigma = (123)(4567)$, som uppenbarligen inte fixerar något element. (Inverser och produkter räknas lättast ut i tvåradsformen av permutationerna.)

   b) Att det är en gruppverkan följer av att G:s verkan på X är en gruppverkan, se boken för de villkor som ska vara uppfyllda. Mängden $2^X := \{Y : \ Y \subseteq X\}$ består alltså av sådana mängder som $Y = \{1, 2, 3\}$, och vi inser att det finns en permutation som tar denna mängd till vilken annan mängd som helst som har tre element. Liknande för andra delmängder—det är kardinaliteten som bestämmer banan. Möjliga kardinaliteter är $0, 1, 2...7$, d v s det finns 8 banor $O(k),\ K = 0, 1, 2...7$, där banan $O(k)$ består av alla delmängder med precis k element.

   c) Det ska alltså vara en permutation som i cykelform kan skrivas $(ab)(cd)(e)(f)(g)$. Vi kan se det som att först väljer vi de tre elementen som fixeras på $\binom{7}{3} = 35$ olika sätt.Sen ska vi välja två av de fyra återstående elementen till transpositionen (ab) vilket kan ske på $\binom{4}{2} = 6$ sätt. De resterande två elementen blir den sista transpositionen (cd). Enligt multiplikationsprincipen kan alltså detta ske på $35 \cdot 6$ sätt. Emellertid noterar vi att $(ab)(cd)$ är samma permutation som $(cd)(ab)$, så att vi har överskattat antalet permutationer med en faktor två. Svaret är alltså $35 \cdot 6/2 = 105$.

2. a) Att G uppfyller gruppaxiomen följer lätt från motsvarande egenskaper för $\mathbb{Z}_m$. Enhetselementet är $(0, 0)$ och $|G| = 5 \cdot 13$ med multiplikationsprincipen. (2p)

   b) Testa något element i gruppen, t ex $g = (1, 1)$. Ordningen av g är det minsta r så att en summa $g + g + g + ... + g = (r, r)$ med r stycken $g : n$, ska bli $e = (0, 0)$. Det innebär att $r = 0$ modulo både 5 och 13 och alltså måste r vara delbart med $5 \cdot 13 = 65$. Alltså är G en cyklisk grupp med t ex $(1, 1)$ som generator. T

Om H är en delgrupp så måste dess ordning dela G:s ordning, d v s den kan vara 1,5,13 eller 65. Den enda gruppen med ett element är förstås enhetselementet, och den enda delgruppen med 65 element är G självt. Anta nu att H är en grupp av ordning 5 med ett element (a, b)som har ordning 5(ett sådant finns ju alltid). Då är $(5a, 5b) = (0, 0)$, vilket innebär att $5a = 0$(alltid sant) och $5b = 0(mod 13)$. Den sista ekvationen innebär att $b = 0 mod 13$(Varför?). Omvänt bildar $H_1 = \{(a, 0)\ a \in \mathbb{Z}_5\}$ en delgrupp av ordning 5, som alltså är den enda möjliga. På motsvarande sätt visar man att $H_2 = \{(0, b)\ b \in \mathbb{Z}_5\}$ är den enda delgruppen av ordning 13.

c) Kalla grupphomorfin f. Då gäller $f(13 \cdot a) = f(a + a + ...a) = 0$, eftersom homomorfin tar enhetselement $0 = 13 \cdot a$ till enhetselementet i $\mathbb{Z}_5$. Men eftersom f är en grupphomomorfi, så gäller att $f(a + a + ...a) = f(a) + f(a) + ..f(.a) = 13f(a)$. Alltså har vi $0 = 13f(a)$, vilket ger $f(a) = 0$ eftersom multiplikation med 13 är inverterbart modulo 5.

3. a) Enligt Lagranges sats så kan stabilisatorgrupperna ha en ordning $|G_x|$ som är 1 eller p. Om den har ordning p så fixerar hela G elementet x, vilket strider mot villkoret att det för varje $x \in X$ finns det åtminstone ett element $g \in G$ så att $gx \neq x$. Alltså har alla stabilisatorgrupper ordning 1. Det innebär(varför?) att varje bana har precis p element, .

b) Om en bana har precis lika många element som gruppen så gäller förstås att $gx \neq x$ om $g \neq e$ för alla x. Annars skulle g vara innehållen i stabilisatorgruppen till x, som bara hade ett element, d v s enhetselementet e.

c) Enligt b) säger Burnsides sats att antalet banor är lika med

$$(1/p)(\sum_{g \in G} |X^g) = |X^e|/p = |X|/p.$$

(1p)

4. Det finns 14 bokstäver i ordet, och 2 vardera av N,R,E,A,T. Alltså kan man bilda $A_0 = \binom{14}{2,2,2,2,2,1,1,1,1}$ ord av dessa totalt. Vii Räknar nu ut hur många som (i form av delord) innehåller MINDRE, BRA ,respektive TENTA(A_1, A_2, A_3), samt hur många som innehåller två av dem(A_{12}, A_{13}, A_{13} och hur många som innehåller alla tre A_{123}.

Sedan tillämpar vi principen om exklusion och inklusion, so ger att det sökta antalet är

$$A_0 - (A_1 + A_2 + A_3) + A_{12} + A_{13} + A_{13} - A_{123}.$$

Nu behöver vi bara ta reda på A_i:na. Vi nöjer oss med att exemplifiera idén med A_1. Där ser vi MINDRE som en enda bokstav och vi har alltså 9 olika bokstäver. Två av dem är lika, A och T. Alltså är

$$A_1 = \binom{9}{2,2,1,1,1,1,1}.$$

5. a) En RSA-kod är baserad på talet $n = 55$. Den offentliga nyckeln är e=11, budskapet 2. Vad är Det krypterade meddelandet är $2^11 \equiv 13(mod 55)$ och den privata nyckeln är $d = 11$, eftersom $11 \cdot 11 = 121 \equiv 1(mod \phi(55) = 40)$.

   b) Här kan man vara smart och säga

$$H = (1).$$

   Koden består då av strängen 0, och eftersom det bara finns ett möjligt meddelande så rättas alla fel automatiskt. Eller så kan man vara lite mindre trivial och såga att det gäller för alla checkmatriser som inte har någon kolonn helt lika med nollkolonnen och inte två lika kolonner, enligt en sats i boken. Samt förstås skriva upp en sådan...

6. a) Av faktorsatsen följer det att €p(x)€ inte delas av något förstagradspolynom x eller $x - 1$(som är de enda möjligheterna) eftersom varken $p(0)$ eller $p(1)$ är 0. Man visar lätt med samma teknik att det enda irreducibla moniska andragradspolynomet är $q(x) = x^2 + x + 1$. Därmed är den enda möjliga faktoriseringen av $p(x)$ att det skulle vara $q(x)^2 = x^4 + x^2 + 1 \neq p(x)$. Alltså är $p(x)$ irreducibelt.

   (2p)

   b) Beviset för att relationen är en ekvivalensrelation, är precis analogt med beviset för att likhet modulo ett tal är en ekvivalensrelation.. (1p)

   c) Enligt divisionsalgoritmen kan varje polynom $f(x) \in \mathbb{Z}_{17}[x]$ delas med $x - 1$:

$$f(x) = q(x)(x - 1) + r,$$

där r är ett polynom av grad 1 mindre än $x-1$, d v s en konstant. Ekvationen medför att $f(x) \equiv r$, och varje polynom tillhör alltså någon av de 17 ekvivalensklasserna $[r]$ som representeras av konstanterna $r = 0, 1..., 16$ i $\mathbb{Z}_{17}$. Dessa är alla olika, för om $[r] = [s]$ så innebär det att $r \equiv s$ d v s (enl.def) att $x-1|r-s \implies r-s = 0$.