MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Rikard Bögvad

Algebra och kombinatorik HT 2024
Tentamen 18 januari 2025

För godkänt är det tillräckligt med 15 av de 30 poängen, inklusive bonuspoäng, någorlunda jämnt fördelade över problemen. *Samtliga svar måste motiveras utförligt! Ange för säkerhets skull hur många bonuspoäng du har uppnått!*

Lycka till!

TENTAMEN

1. Elementen i gruppen $G = S_7$ verkar på $X = \{1, 2, 3, ...7\}$ som permutationer.

   a) Välj två element π, σ i G, som inte har några fixpunkter, och inte kommuterar och räkna på cykelform ut π^2, $\sigma\pi$ och π^{-1}. (1 p)

   b) G verkar också på mängden $2^X := \{Y : Y \subseteq X\}$ genom $\pi(Y) = \{\pi(y) : y \in Y\}$. Visa att detta är en gruppverkan, och beräkna antalet banor som denna verkan har och beskriv dem. *Ledning: Använd INTE Burnsides lemma....* (2p)

   c) Hur många element finns det i G med cykeltyp

   $$[1]^3[2]^2[3]^0[4]^0[5]^0[6]^0[7]^0?$$

   (Obs: Svaret får innehålla kombinatoriska uttryck av den typ som förekommit i kursen —fakulteter, binomialkoefficienter, etc—och dessa behöver inte räknas ut!) (1p)

2. Låt

   $$G := \mathbb{Z}_5 \times \mathbb{Z}_{13} = \{(a, b) \ : a \in \mathbb{Z}_5, \ b \in \mathbb{Z}_{13}\}.$$

   a) Visa att G är en grupp med gruppoperation

   $$(a, b) * (c, d) = (a + c, b + d).$$

   Vad är enhetselementet? Vad är $|G|$? (2p)

   b) Visa att G är en cyklisk grupp och ange explicit en generator. Visa sedan att det bara finns fyra delgrupper till G. Vilka är de? (2p)

c) Visa att den enda grupphomorfin från den additiva gruppen $\mathbb{Z}_{13}$ till den additiva gruppen $\mathbb{Z}_5$ är den som tar alla element i $\mathbb{Z}_{13}$ till $0 \in \mathbb{Z}_5$. (2p)

3. En ändlig grupp G verkar på en ändlig mängd X. Gruppens ordning är ett primtal p, och för varje $x \in X$ finns det åtminstone ett element $g \in G$ så att $gx \neq x$.

   a) Vilka är möjliga ordningar av stabilisatordelgrupper (alltså $|G_x|$, $x \in X$)? Hur många element kan en bana innehålla? (1p)

   b) Visa att antalet element i fixpunktsmängden $|X^g| = 0$ om och endast om g inte är enhetselementet i gruppen. (2p)

   c) Använd Burnsides sats för att visa att antalet banor är $|X|/|G|$. (Obs:Burnsides sats måste användas.) (1p)

4. Hur många ord kan man bilda med alla bokstäverna i ordet MINDREBRATENTA om orden MINDRE,BRA och TENTA inte får förekomma som delord i ordet? (MIBREDRATNETA är alltså ok men inte BRATEMTANINDRE..) (5p)

5. a) En RSA-kod är baserad på talet $n = 55$. Den offentliga nyckeln är e=11, budskapet 2. Vad är det krypterade meddelandet? Vad är den privata nyckeln d? (2p)

   b) Ange explicit en paritetscheckmatris för en lineär kod som rättar ett fel. Ange vilka resultat om lineära koder som du använder för att inse att din kod verkligen rättar ett fel. (3p)

6. a) Visa att polynomet $p(x) := x^4 + x + 1 \in \mathbb{Z}_2[x]$ är irreducibelt. (Ledning: Vilka irreducibla andragradspolynom finns det i $\mathbb{Z}_2[x]$? (2p)

   b) Definiera en relation $\equiv$ mellan polynom i $\mathbb{Z}_{17}[x]$ på följande sätt:

   $$r(x) \equiv s(x) \iff x - 1 | (r(x) - s(x)).$$

   Visa att detta är en ekvivalensrelation. (1p)

   c) Visa att det finns precis 17 ekvivalensklasser, för ekvivalensrelationen i b), och ange ett element av minimal grad i varje klass. (2p)