Matematiska institutionen
Stockholms universitet
Avd. Matematik
Examinator: Olof Sisask

Tentamensskrivning
Kurskod: MM5013

2020-01-13 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. Problemen är INTE ordnade i svårighetsgrad.*

1. (a) (1p) Lös, i ringen $\mathbb{Z}_{17}$ (heltalen modulo 17), ekvationssystemet

$$\begin{aligned} 6x + y &= 3 \\ 10x + 2y &= 1. \end{aligned}$$

   (b) (1p) Bestäm ett heltal $k \geq 1$ sådant att $11^k = 1$ i $\mathbb{Z}_{17}$.

   (c) (3p) Ett RSA-krypto har offentlig modulo $n = 91$ och offentlig krypteringsnyckel $e = 31$. Bestäm dekrypteringsnyckeln d, och dekryptera meddelandet $b = 10$.

2. (5p) Hur många omordningar av bokstäverna i `MOROTSSOPPA` innehåller inte några av delorden `ROT`, `MOS` eller `STORM`? T.ex. är `STOROMOPPAS` ett sådant ord, men inte `MOPPSOROTAS` (för detta ord innehåller `ROT`). (Ditt svar får uttryckas med hjälp av heltal, plus, minus, gånger, delat med och fakulteter, och behöver inte förenklas.)

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

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

   (a) (2p) Finns det en permutation $\pi \in S_8$ sådan att

$$\sigma^3 \circ \pi^{-1} = \sigma^4?$$

   Om det finns en sådan permutation π, skriv ned en. Förklara annars varför inga sådana π finns. (Permutationer får skrivas med valfri notation från kursen.)

   (b) (3p) Finns det en permutation $\tau \in S_8$ sådan att

$$\tau^2 \circ \sigma^6 = \sigma \circ \tau^2?$$

   Om det finns en sådan permutation τ, skriv ned en. Förklara annars varför inga sådana τ finns. (Permutationer får skrivas med valfri notation från kursen.)

4. (5p) Du har 10 olika böcker, och bland dessa ska du välja ut 5 som du ska dela ut mellan barnen Agnes, Bertil och Cecilia, så att varje barn får åtminstone en bok. På hur många sätt kan detta ske? (Ditt svar får innehålla kombinatorisk standardnotation från kursen, som ej behöver beräknas eller förenklas, men måste motiveras tydligt. Om du vill kolla om ditt svar är rimligt: svaret ligger mellan 30 000 och 40 000.)

Var god vänd...

5. (a) (3p) Visa att om G är en grupp, och H och K är delgrupper till G, då är snittet $H \cap K$ en delgrupp till G.

   (b) (2p) Visa att om G är en cyklisk grupp, och $G = H_1 \cup H_2 \cup \cdots \cup H_k$ för några delgrupper $H_1, H_2, \ldots, H_k$ till G, då måste $H_i = G$ för något i. Du kan få delpoäng om du lyckas visa detta endast i fallet då $G = \mathbb{Z}$ och operationen är addition.

6. (a) (2p) Finn värden $x, y \in \{0, 1\}$ sådana att

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

   är en checkmatris för en linjär 1-felsrättande kod C. Förklara ditt val av x och y.

   (b) (3p) För en kod C som uppfyller kraven i (a): Bland de tre orden

$$\texttt{000111}, \quad \texttt{011101}, \quad \texttt{100001}$$

   finns det ett som ligger i koden C, ett som kan rättas av koden, och ett som inte kan rättas av koden. Bestäm, med motivering, vilka som är vilka, samt rätta det ord som kan rättas.

Kom ihåg att kolla att du inkluderat tydlig motivering i samtliga svar. Förklaringar är vad matematik mestadels handlar om, och de spelar också stor roll i poängsättningen.