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.*

Lösningsförslag

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

$$6x + y = 3$$
$$10x + 2y = 1.$$

(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 $b = 10$.

Lösning (a) Eftersom $\mathbb{Z}_{17}$ är en kropp så kan vi lösa systemet på vilket som av de vanliga sätten. T.ex. kan vi byta ut den andra ekvationen mot ($2 \cdot$ (första ekvationen) $-$ andra ekvationen), dvs

$$2x = 5.$$

Inversen till 2 i $\mathbb{Z}_{17}$ är $(17 + 1)/2 = 9$, så denna ekvation är ekvivalent (i $\mathbb{Z}_{17}$) med

$$x = 9 \cdot 5 = 45 = 11.$$

Den första ekvationen är sedan ekvivalent med $y = 3 - 66 = -63 = 5$. Så lösningen är

$$(x, y) = (11, 5).$$

(b) Enligt Fermats lilla sats gäller detta för $k = 16$, eftersom 17 är ett primtal.

(c) Vi kan faktorisera $n = 91 = 7 \cdot 13$, så den privata modulon u ges av

$$u = (p - 1)(q - 1) = 6 \cdot 12 = 72.$$

Dekrypteringsnyckeln d är enligt definition den multiplikativa inversen till e modulo u, dvs lösningen till $ed \equiv 1 \pmod{u}$, vilket i vårt fall är

$$31d \equiv 1 \pmod{72}.$$

Detta motsvarar heltalsekvationen $31d + 72k = 1$, som vi löser med hjälp av Euklides algoritm:

$$72 = 2 \cdot 31 + 10$$
$$31 = 3 \cdot 10 + 1,$$

varifrån

$$1 = 31 - 3 \cdot 10 = 31 - 3 \cdot (72 - 2 \cdot 31) = 7 \cdot 31 - 3 \cdot 72.$$

Alltså är $d = 7$.

För att dekryptera $b = 10$ beräknar vi enligt känd metod

$$a = b^d = 10^7 \mod n.$$

Eftersom $n = 91$ har vi

$$\begin{aligned} 10^2 &\equiv 9 \pmod{91} \\ 10^4 &\equiv 81 \equiv -10 \pmod{91}, \end{aligned}$$

så

$$10^7 = 10 \cdot 10^2 \cdot 10^4 \equiv 10 \cdot 9 \cdot (-10) \equiv (-1)(-10) \equiv 10 \pmod{91}.$$

Det dekrypterade meddelandet är alltså 10.
Svar: $(d, a) = (7, 10)$.

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.)

Lösning: Vi räknar först det totala antalet omordningar, och sedan använder vi inklusion-exklusion för att räkna bort de förbjudna orden.

Enligt lärd sats om multinomialkoefficienter är det totala antalet omordningar

$$\binom{11}{3,2,2,1,1,1,1} = \frac{11!}{3!\,2!\,2!},$$

då det finns 3 `O`, 2 `P`, 2 `S` och 1 var av `A`, `M`, `R`, `T`.

Låt $F_{\texttt{ROT}}$ vara mängden av ord som innehåller ordet `ROT`, och liknande för $F_{\texttt{MOS}}$ och $F_{\texttt{STORM}}$. De ord vi vill räkna bort är precis dem i unionen $F_{\texttt{ROT}} \cup F_{\texttt{MOS}} \cup F_{\texttt{STORM}}$. Enligt principen om inklusion-exklusion kan storleken på denna union beräknas genom

$$\begin{aligned} |F_{\texttt{ROT}} \cup F_{\texttt{MOS}} \cup F_{\texttt{STORM}}| = {} & |F_{\texttt{ROT}}| + |F_{\texttt{MOS}}| + |F_{\texttt{STORM}}| \\ & - |F_{\texttt{ROT}} \cap F_{\texttt{MOS}}| - |F_{\texttt{ROT}} \cap F_{\texttt{STORM}}| - |F_{\texttt{MOS}} \cap F_{\texttt{STORM}}| \\ & + |F_{\texttt{ROT}} \cap F_{\texttt{MOS}} \cap F_{\texttt{STORM}}|. \end{aligned}$$

Storleken $|F_{\texttt{ROT}}|$ kan beräknas på ett enkelt sätt: mängden består av alla omordningar av de 9 symbolerna `ROT`, `O`, `O`, `P`, `P`, `S`, `S`, `A`, `M`, och det finns, precis som förut,

$$|F_{\texttt{ROT}}| = \binom{9}{2,2,2,1,1,1} = \frac{9!}{2!\,2!\,2!}$$

sådana omordningar. På samma sätt har vi

$$\begin{aligned} |F_{\texttt{MOS}}| &= \binom{9}{2,2,1,1,1,1,1} = \frac{9!}{2!\,2!} \\ |F_{\texttt{STORM}}| &= \binom{7}{2,2,1,1,1} = \frac{7!}{2!\,2!}. \end{aligned}$$

Mängden $F_{\texttt{ROT}} \cap F_{\texttt{MOS}}$ består av alla ord som är omordningar av `ROT`, `MOS`, `O`, `P`, `P`, `S`, `A`, varav det finns

$$|F_{\texttt{ROT}} \cap F_{\texttt{MOS}}| = \binom{7}{2,1,1,1,1,1} = \frac{7!}{2!}.$$

Inga ord innehåller både `ROT` och `STORM`, så

$$|F_{\texttt{ROT}} \cap F_{\texttt{STORM}}| = 0 = |F_{\texttt{ROT}} \cap F_{\texttt{MOS}} \cap F_{\texttt{STORM}}|.$$

Till slut har vi mängden $F_{\texttt{MOS}} \cap F_{\texttt{STORM}}$. Eftersom det bara finns 1 `M` så måste alla ord som innehåller både `MOS` och `STORM` innehålla ordet `STORMOS`. Resterande symboler är då `O`, `P`, `P`, `A`, och vi får

$$|F_{\texttt{MOS}} \cap F_{\texttt{STORM}}| = \binom{5}{2,1,1,1} = \frac{5!}{2!}.$$

Svar:

$$\frac{11!}{3!\,2^2} - \frac{9!}{2^3} - \frac{9!}{2^2} - \frac{7!}{2^2} + \frac{7!}{2} + \frac{5!}{2}.$$

(Detta kan även skrivas som 1 528 440.)

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.)

Lösning (a) Vi bearbetar ekvationen, vilket vi kan göra med kancellerings- och inverslagarna från gruppteori:

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

Alltså finns det precis en sådan permutation, nämligen

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

(b) Vi använder konceptet av jämna och udda permutationer, som beskriver partiteten av antalet 2-cykler som behövs för att skriva en permutation, men det finns många sätt att lösa denna fråga. Oavsett vad τ är för permutation så är τ^2 en jämn permutation. Permutationen σ är däremot en udda permutation, eftersom den kan skrivas som en produkt av ett udda antal 2-cykler:

$$\sigma = (1\ 3)(3\ 5)(5\ 7)(2\ 6)(4\ 8).$$

I ekvationen $\tau^2 \circ \sigma^6 = \sigma \circ \tau^2$ så är vänsterledet alltså en jämn permutation (som en sammansättning av två jämna permutationer), oavsett vad τ faktiskt är, medans högerledet är en udda permutation, oavsett τ. Alltså har ekvationen ingen lösning.

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.)

Lösning: Vi kan välja ut de 5 böckerna på $\binom{10}{5}$ sätt. För varje av dessa sätt finns det sedan $S(5,3)$ sätt att partitionera böckerna in i 3 o-ordnade icke-tomma mängder, enligt definitionen av Stirlingtalen av andra ordningen. För varje sådan partition finns det sedan 3! att ordna ut delarna bland de 3 barnen. Enligt multiplikationsprincipen blir alltså svaret

$$\binom{10}{5} \cdot S(5,3) \cdot 3! = \frac{10!}{(5!)^2} \cdot 25 \cdot 6 = 37\,800.$$

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.

Lösning (a) Det räcker, enligt delgruppstestet, att kolla

- att $H \cap K$ är en icke-tom delmängd till G och
- att

$$ab^{-1} \in H \cap K \quad \text{för alla } a, b \in H \cap K.$$

Eftersom $H \subset G$ och $K \subset G$, och båda innehåller identitetselementet, så gäller det första kravet. För det andra kravet: eftersom $a, b \in H$, så gäller $ab^{-1} \in H$, eftersom H är en delgrupp. På samma sätt gäller $ab^{-1} \in K$, eftersom $a, b \in K$. Alltså gäller $ab^{-1} \in H \cap K$.

(b) Enligt definitionen av termen 'cyklisk grupp' så finns det en generator x för G:

$$G = \langle x \rangle.$$

Om $G = H_1 \cup H_2 \cup \cdots \cup H_k$, då måste denna generator x ligga i något H_i (för annars skulle den inte finnas med i unionen). Men, eftersom H_i är en delgrupp så måste den även då innehålla $\langle x \rangle$, gruppen som genereras av x. Eftersom x genererar hela G, så är då $H_i = G$. I specialfallet $G = \mathbb{Z}$ så kan man ta $x = 1$ som generator: Om $\mathbb{Z} = H_1 \cup \cdots \cup H_k$ för några delgrupper $H_1, \ldots, H_k \subset \mathbb{Z}$, då måste talet 1 ligga i någon H_i. Men eftersom H_i är en delgrupp och därmed sluten under + så ligger $1+1$, $1+1+1$ osv också i H_i, samt 0, samt -1, $-1-1$ osv. Med andra ord är $H_i = \mathbb{Z}$.

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

`000111`, `011101`, `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.

Lösning (a) Att koden är 1-felsrättande motsvarar, enligt lärd sats, att den inte har någon kolonn som består enbart av 0:or, och att inga två kolonner är lika. Alltså måste $x = 1$, och sedan $y = 1$.

(b) Vi testar att multiplicera matrisen med orden.

- Första ordet:
$$\mathbf{H}\begin{pmatrix}0\\0\\0\\1\\1\\1\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix},$$
vilket är matrisens första kolonn. Enligt lärd metod så går detta ord alltså att rätta, och vi kan göra det genom att flippa ordets första bit (motsvarande att detta var den första kolonnen): ordet rättas till
$$\texttt{100111}.$$
- Andra ordet:
$$\mathbf{H}\begin{pmatrix}0\\1\\1\\1\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}.$$
Eftersom detta är 0-vektorn så ligger ordet `011101` i koden C, per definition.
- Tredje ordet: ordet `100001` går inte att rätta: det har inte avstånd 1 till något kodord, och det har avstånd 2 till båda kodorden `100111` och `000000`.

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.