MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator:

Övningstenta i
Algebra och Kombinatorik
7,5 hp
2015-11-24

*Exempel på hur tentan skulle kunna se ut om alla uppgifter var från dag 1-7 i kursen.*

1. Låt $\sigma = (135)(28746)$ och låt $\tau = (18)(27)(36)(45)$ vara två permutationer i $S_8$.

   (a) Beräkna $\sigma^{-1}$, $\tau^{-1}$, $\sigma\tau$ samt $\tau^{-1}\sigma^{-1}$. Svara i cykelnotation. (2 p)

   (b) Bestäm tecknet av $\sigma$, $\tau$, $\sigma^{-1}$, $\tau^{-1}$, $\sigma\tau$ samt $\tau^{-1}\sigma^{-1}$. (1 p)

   (c) Hur många permutationer i $S_8$ är konjugerade med $\sigma$? (2 p)

   *Lösning:*

   (a) Man får inversen av en permutation genom att skriva varje cykel baklänges. Inversen till $\sigma\tau$ är $\tau^{-1}\sigma^{-1}$. Detta (samt lite beräkning) ger

   $$\begin{aligned} \sigma^{-1} &= (531)(64782), \\ \tau^{-1} &= (18)(27)(36)(45), \\ \sigma\tau &= (178324)(56), \\ \tau^{-1}\sigma^{-1} &= (423871)(56). \end{aligned}$$

   (b) Tecknet av en cykel av udda längd är 1 och tecknet av en cykel av jämn längd är $-1$. Vi har också att $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$. Detta och resultatet från uppgift (a) ger

   $$\begin{aligned} \operatorname{sgn}(\sigma) &= 1, \\ \operatorname{sgn}(\tau) &= 1, \\ \operatorname{sgn}(\sigma^{-1}) &= 1, \\ \operatorname{sgn}(\tau^{-1}) &= 1, \\ \operatorname{sgn}(\sigma\tau) &= 1, \\ \operatorname{sgn}(\sigma^{-1}\tau^{-1}) &= 1. \end{aligned}$$

   (c) Permutationen $\sigma$ har cykeltyp $[3, 5]$. Alltså innehåller konjugatklassen av $\sigma$

   $$\frac{8!}{3 \cdot 5} = 8 \cdot 7 \cdot 6 \cdot 4 \cdot 2,$$

   enligt formel från kursen.

2. Du tjuvlyssnar på Alice och Bob, som använder RSA med den publika nyckeln $e = 13$ och $n = 253$, och snappar upp det krypterade meddelandet $M = 2$ från Bob.

   (a) Beräkna $\phi(253)$. (1 p)

   (b) Bestäm det dekrypterade meddelandet. Svara på uträknad form. (4 p)

*Lösning:*

(a) $253 = 11 \cdot 23$ så $\phi(253) = (11-1)(23-1) = 220$.

(b) Vi vill bestämma $d = e^{-1}$ modulo $\phi(253)$. Vi använder först Euklides algoritm

$$\begin{aligned} 220 &= 16 \cdot 13 + 12 \\ 13 &= 1 \cdot 12 + 1. \end{aligned}$$

Vi kan nu använda Euklides algoritm baklänges för att uttrycka 1 i termer av 220 och 13:

$$\begin{aligned} 1 &= 13 - 12 = \\ &= 13 - (220 - 16 \cdot 13) = 17 \cdot 13 - 220. \end{aligned}$$

Alltså gäller $d = 17$.

Vi vill nu beräkna $M^d = 2^17$ modulo 253. Vi har att $2^8 = 256$ så

$$\begin{aligned} 2^{17} &\equiv 2^8 \cdot 2^8 \cdot 2 \equiv \\ &\equiv 256 \cdot 256 \cdot 2 \equiv \\ &\equiv 3 \cdot 3 \cdot 2 \equiv \\ &\equiv 18 \,(\mathrm{mod}\, 253). \end{aligned}$$

Det dekrypterade meddelandet är alltså 18.

3. Låt $P$ vara en mängd bestående av $n$ primtal. Låt $M$ vara mängden av tal som kan skrivas som en produkt av 4 tal i $P$, d.v.s.

$$M = \{x_1 \cdot x_2 \cdot x_3 \cdot x_4 | x_1, x_2, x_3, x_4 \in P\}.$$

Observera att faktorerna inte behöver vara olika.

(a) Hur många primtal måste $P$ innehålla för att $|M| \geq 5$? (1 p)

(b) Bestäm $|M|$ som ett uttryck av $n$. (4 p)

*Lösning:*

(a) Om $|P| = 1$ så är $|M| = 1$. Om $P = \{p_1, p_2\}$ så är

$$M = \{p_1^4, p_1^3 p_2, p_1^2 p_2^2, p_1 p_2^3, p_2^4\}.$$

Alltså är svaret 2.

(b) Elementen $y$ i $M$ har formen

$$y = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n},$$

där $k_1 + k_2 + \cdots + k_n = 4$. Vi kan skapa en bijektion mellan $M$ och mängden av sekvenser av ettor och nollor med precis fyra ettor och längd $n - 1 + 4 = n + 3$ genom att till $y$ associera sekvensen

$$\underbrace{1 \cdots 1}_{k_1 \text{ ettor}} 0 \underbrace{1 \cdots 1}_{k_2 \text{ ettor}} 0 \cdots 0 \underbrace{1 \cdots 1}_{k_n \text{ ettor}}.$$

Exempelvis: om $n = 5$ och $y = p_1^2 p_3 p_4$ så svarar $y$ mot sekvensen 11001010.

Vi kan alltså räkna sekvenser av denna typ istället. Vi ska alltså bland $n+3$ tecken välja precis 4 som är ettor. Detta kan göras på

$$\binom{n+3}{4},$$

sätt.

4. (a) Beräkna antalet surjektioner $f : \mathbb{N}_6 \to \mathbb{N}_4$. (2 p)

   (b) Hur många surjektioner $f : \mathbb{N}_6 \to \mathbb{N}_4$ uppfyller att $x < y$ medför $f(x) > f(y)$ för alla $x, y \in \mathbb{N}_6$? (1 p)

   (c) Hur många surjektioner $f : \mathbb{N}_6 \to \mathbb{N}_4$ uppfyller att $x \leq y$ medför $f(x) \geq f(y)$ för alla $x, y \in \mathbb{N}_6$? (2 p)

*Lösning:*

(a) Antalet surjektioner $\mathbb{N}_6 \to \mathbb{N}_4$ ges av $4! \cdot S(6,4)$. Stirlingtal uppfyller $S(n,1) = S(n,n) = 1$ samt $S(n,k) = S(n-1,k-1) + kS(n-1,k)$. Detta ger

$$S(6,4) = S(5,3) + S(5,4) = S(4,2) + S(4,3) + S(4,3) + S(4,4) = \ldots = 65.$$

Svaret är alltså $4! \cdot 65$.

(b) Om $x < y$ medför $f(x) > f(y)$ så följer det att $f(x) \neq f(y)$ om $x \neq y$. Alltså måste $f$ vara en injektion. Men det finns inga injektioner från $\mathbb{N}_6$ till $\mathbb{N}_4$.

(c) Låt $f : \mathbb{N}_6 \to \mathbb{N}_4$ vara en surjektiv funktion sådan att $x \leq y$ medför att $f(x) \geq f(y)$. Beteckna talen $f(1), \ldots, f(6)$ med $a_1, \ldots, a_6$. Mellan varje par av tal $a_i, a_{i+1}$ sätter vi in tecknet $=$ eller $>$ beroende på om $a_i = a_{i+1}$ eller $a_i = a_{i+1}+1$. Funktionen $f$ är avtagande och surjektiv så dessa är de enda möjligheterna och vi måste ha $f(1) = 4$ och $f(6) = 1$. Vi måste använda symbolen $>$ precis 3 gånger. Exempelvis kan vi få sekvensen $4 = 4 > 3 > 2 = 2 > 1$.

Alltså är det ekvivalent att räkna sekvenser av 5 symboler där precis 3 är $>$ och övriga $=$. Det finns precis

$$\binom{5}{3} = 10,$$

sådana sekvenser.

5. Låt $M$ vara mängden av funktioner $f : \{a,b,c,d,e\} \to \{0,1\}$. För $f, g \in M$, definiera $f \sim g$ om och endast om $f(a) = g(a)$.

   (a) Visa att $\sim$ är en ekvivalensrelation på $M$. (4 p)

   (b) Beräkna storleken av ekvivalensklassen som innehåller funktionen som tar värdet 0 på samtliga element. (1 p)

*Lösning:*

(a) Vi måste visa att $\sim$ är reflexiv, symmetrisk och transitiv.
**Reflexivitet:** Vi har
$$f \sim f \Leftrightarrow f(a) = f(a).$$
Uppenbarligen gäller $f(a) = f(a)$ så $\sim$ är reflexiv.
**Symmetri:** Vi har
$$f \sim g \Leftrightarrow f(a) = g(a) \Leftrightarrow g(a) = f(a) \Leftrightarrow g \sim f.$$
Alltså är $\sim$ symmetrisk.
**Transitivitet:** Vi har
$$f \sim g, \quad g \sim h \quad \Leftrightarrow \quad f(a) = g(a), \quad g(a) = h(a).$$
Men om om $f(a) = g(a)$ och $g(a) = h(a)$ så fäljer det att $f(a) = h(a)$. Alltså implicerar $f \sim g$ och $g \sim h$ att $f \sim h$ så $\sim$ är transitiv.

(b) Beteckna funktionen som tar värdet 0 på samtliga element med $f$. Vi har $g \sim f$ om och endast om $g(a) = f(a) = 0$. Vi kan alltså fritt välja $g$'s värden på $b, c, d$ och $e$. Alltså finns det $2^4 = 16$ funktioner som är ekvivalenta med $f$ under $\sim$.

6. Bestäm antalet ord om sex bokstäver som man kan bilda från bokstäverna
$$\{A, B, C, D, E, F\}$$
så att delorden $AB$, $EF$, och $EFA$ inte förekommer i något ord. Varje bokstav får endast förekomma en gång per ord. T.ex. är $BACEDF$ ett tillåtet ord, men $ABCEDF$ är inte tillåtet eftersom delordet $AB$ förekommer i detta ord. (5 p)

*Lösning:*

Beteckna mängden av ord med sex bokstäver man kan bilda av bokstäverna $A$, $B$, $C$, $D$, $E$, $F$ med $X$. Vi har då
$$|X| = 6! = 720.$$
Beteckna delmängden av $X$ bestående av ord som innehåller delordet $AB$ med $X_{AB}$. Låt $X_{EF}$ och $X_{EFA}$ ha motsvarande betydelse. Vi kan dock observera att om ett ord innehåller delordet $EFA$ så innehåller det också delordet $EF$. Alltså behöver vi bara ta bort mängderna $X_{AB}$ och $X_{EF}$ från $X$.

Ett element i $X_{AB}$ kan ses som ett ord med fem "bokstäver" bildat av "bokstäverna"
$$AB, C, D, E, F.$$
Alltså gäller
$$|X_{AB}| = 5! = 120.$$
På liknande sätt beräknar vi
$$|X_{EF}| = 5! = 120.$$

Ett ord i $X_{AB} \cap X_{EF}$ kan ses som ett ord med fyra "bokstäver" bildat av "bokstäverna"

$$AB, EF, C, D.$$

Alltså gäller

$$|X_{AB} \cap X_{EF}| = 4! = 24.$$

Principen om inklusion och exklusion ger nu

$$|X_{AB} \cup X_{EF} \cup X_{EFA}| = 120 + 120 - 24 = 240 - 24 = 216.$$

Antalet ord som inte innehåller något av delorden $AB$, $EF$ eller $EFA$ är alltså

$$|X| - |X_{AB} \cup X_{EF} \cup X_{EFA}| = 720 - 216 = 504.$$