Matematiska Institutionen,
KTH

Problem till övning nr 7 den 23 april, Diskret matematik CINTE, SF1610, vt 14.

OBS. Efter kontrollskriving nr 2 mellan kl 13.00 och 14.00 gör vi en kort paus, varefter följande problem diskuteras. Om vi inte hinner med uppgift nummer 5 så kommer den på nästa övning.

1. (E) Skriv permutationen φ nedan på cykelform, dvs som en produkt av disjunkta cykler:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 6 & 1 & 5 & 8 & 2 \end{pmatrix}.$$

   Skriv permutationen $\psi = (1\ \ 5\ \ 2\ \ 7\ \ 3)(6\ \ 4)$ i tablåform. Bestäm också ordningen av dessa permutationer samt avgör om permutationerna är udda eller jämna.

2. (E) Låt nu $\varphi = (1\ \ 5\ \ 4)(2\ \ 3)$ och $\psi = (1\ \ 3\ \ 5\ \ 4)$. Bestäm ordningen av permutationerna $\psi\varphi$, $\varphi\psi$ och $\varphi\psi\varphi$ samt avgör vilka som är udda resp jämna permutationer.

3. Låt φ och ψ vara som i föregående uppgift.

   (a) (E) Bestäm en permutation x sådan att

$$\psi x = \varphi.$$

   (b) (D) Undersök om det finns någon permutation γ sådan att

$$\gamma^2\psi = \varphi^2.$$

4. (B) Mängden av alla permutationer av elementen i mängden $\{1, 2, 3, 4\}$ bildar en grupp som brukar betecknas $\mathcal{S}_4$. Bestäm den minsta delgrupp H till gruppen $\mathcal{S}_4$ som är sådan att permutationerna $(1\ \ 2\ \ 3)$ och $(3\ \ 4)$ tillhör H.

5. (E) Ett RSA-krypto har de offentliga nycklarna $n = 55$ och $e = 7$. Kryptera meddelandet $a = 2$ och dekryptera meddelandet $b = 2$.

SVAR.

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

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 4 & 2 & 4 & 3 \end{pmatrix}$$

   φ har ordning 4 och är jämn. ψ har ordning 10 och är udda.

2. $\psi\varphi = (1\ \ 4\ \ 3\ \ 2\ \ 5)$ så av ordning 5 och jämn.
   $\varphi\psi = (1\ \ 2\ \ 3\ \ 4\ \ 5)$ så av ordning 5 och jämn.
   $\varphi\psi\varphi = (2\ \ 4)$ så ordning 2 och udda.

3. (a) $x = (1\ \ 3\ \ 2)(4)(5)$
   (b) Finns ingen sådan permutation γ.

4. $\mathcal{S}_4$.

5. Elementet 2 krypteras till $E(2) = 18$, och $D(2) = 2^{23} = 8$