Diskretne strukture UNI, vaje, 30. 12. 2022 ($9^n - 11^n$)

1. (a) Izračunaj $\varphi(1215)$ in $\varphi(1216)$.
   (b) Določi $1024^{3241} \pmod{1215}$.

(a) $\varphi(n) = \varphi(p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_m^{k_m} - p_m^{k_m-1})$.

$1215 = 3^5 \cdot 5$, $1216 = 2^6 \cdot 19$

$\varphi(1215) = \varphi(3^5 \cdot 5) = (3^5 - 3^4) \cdot (5^1 - 5^0) = 648$.

$\varphi(1216) = \varphi(2^6 \cdot 19) = (2^6 - 2^5) \cdot (19 - 1) = 576$.

(b) Eulerjev izrek: $a^{\varphi(n)} \equiv 1 \pmod{n}$, če $\gcd(a, n) = 1$.

Najprej $1024 = 2^{10}$, $1215 = 3^5 \cdot 5$, $\gcd(1024, 1215) = 1$,

po E. izreku $1024^{\varphi(1215)} \equiv 1 \pmod{1215}$

$\varphi(1215) = 648$

$a \equiv b \pmod{n}$
$c \equiv d \pmod{n}$
potem $ac \equiv bd \pmod{n}$

$3241 = 5 \cdot 648 + 1$ $\quad 3241 : 648 = 5$ ost. 1

$1024^{3241} \equiv 1024^{5 \cdot 648 + 1} \equiv (1024^{648})^5 \cdot 1024^1 \equiv 1^5 \cdot 1024 \pmod{1215} \equiv$

$\equiv 1 \pmod{1215}$ $\quad \equiv 1024 \pmod{1215}$.

3. (a) Koliko je ostanek števila $((5^9)^{13})^{17}$ pri deljenju z 11?
   (b) Koliko je ostanek števila $5^{9^{13^{17}}}$ pri deljenju z 11?

(a) $((5^9)^{13})^{17} = 5^{9 \cdot 13 \cdot 17} = 5^{1989} \equiv ? \pmod{11}$

Po Eulerjevem izreku vemo $5^{\varphi(11)} \equiv 1 \pmod{11}$ (saj $\gcd(5, 11) = 1$).

$5^{10} \equiv 1 \pmod{11}$

$5^{1989} = 5^{198 \cdot 10 + 9} = (5^{10})^{198} \cdot 5^9 \equiv 1^{198} \cdot 5^9 \pmod{11} \equiv$

$5^2 \equiv 3 \pmod{11}$
$3^3 \equiv 5 \pmod{11}$

$\equiv \underbrace{3 \cdot 3 \cdot 3} \cdot 3 \cdot 5 \pmod{11} \equiv 9 \pmod{11}$.
$\equiv 5 \pmod{11}$

Malce drugače:

$$5^{9\cdot 13\cdot 17} \equiv 5^{9} \pmod{11} \equiv \ldots \equiv 9 \pmod{11}.$$

$$9\cdot 13\cdot 17 \equiv 9\cdot 3\cdot 7 \equiv 9\cdot 1 \equiv 9 \pmod{10}$$

(b) $5^{9^{13^{17}}} \equiv ? \pmod{11}$

Po Eulerjevem izreku $5^{10} \equiv 1 \pmod{11}$.

$\varphi(10) = \varphi(2\cdot 5) = 4$

$9^{13^{17}} \equiv ? \pmod{10}$ $\quad \gcd(9,10) = 1$, zato $9^{\varphi(10)} \equiv 1 \pmod{10}$

$9^{4} \equiv 1 \pmod{10}$

$13^{17} \equiv ? \pmod{4}$ $\quad \gcd(13,4) = 1$, zato $13^{\varphi(4)} \equiv 1 \pmod{4}$

$13^{2} \equiv 1 \pmod{4}$

$\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 2$

$17 \equiv 1 \pmod{2}$,

torej $13^{17} \equiv 13^{1} \pmod{4} \equiv 1 \pmod{4}$

zato $9^{13^{17}} \equiv 9^{1} \pmod{10} \equiv 9 \pmod{10}$

zato $5^{9^{13^{17}}} \equiv 5^{9} \pmod{11} \equiv 9 \pmod{11}$

Nekoliko drugače:

$5^{1} \equiv 5 \pmod{11}$
$5^{2} \equiv 3 \pmod{11}$
$5^{3} \equiv 3\cdot 5 \equiv 4 \pmod{11}$
$5^{4} \equiv 5\cdot 4 \equiv 9 \pmod{11}$
$5^{5} \equiv 5\cdot 9 \equiv 1 \pmod{11}$

$9^{13^{17}} \equiv ? \pmod{5}$

$9^{1} \equiv 4 \pmod{5}$
$9^{2} = 9\cdot 4 \equiv 1 \pmod{5}$

Sedaj $13^{17} \equiv 1 \pmod{2}$ (saj je 13^{17} liho št.),

zato $9^{13^{17}} \equiv 9^{1} \pmod{5} \equiv 4 \pmod{5}$, zato $5^{9^{13^{17}}} \equiv 5^{4} \pmod{11} \equiv$

$\equiv 9 \pmod{11}$.

4. Reši enačbe:

(a) $11x \equiv 242 \pmod{21}$,

(b) $5x \equiv 270 \pmod{25}$,

(c) $((6^7)^8)^9 \equiv x \pmod{13}$,

(d) $6^{7^{8^9}} \equiv x \pmod{13}$.

(d) $6^1 \equiv 6 \pmod{13}$

$6^2 \equiv 10 \pmod{13} \equiv -3 \pmod{13}$

$6^3 \equiv -3 \cdot 6 \equiv 8 \pmod{13} \equiv -5 \pmod{13}$

$6^4 \equiv -5 \cdot 6 \equiv -4 \pmod{13}$

$6^5 \equiv -4 \cdot 6 \equiv 2 \pmod{13}$

$6^6 \equiv 2 \cdot 6 \equiv 12 \pmod{13} \equiv -1 \pmod{13}$

$36 = 2 \cdot 13 + 10 = 3 \cdot 13 - 3$

$-18 = -1 \cdot 13 - 5 = -2 \cdot 13 + 8$

$-30 = -2 \cdot 13 - 4$

$-24 = -2 \cdot 13 + 2$

$12 = 0 \cdot 13 + 12 = 1 \cdot 13 - 1$

$\vdots$

$(6^6)^2 \equiv (-1)^2 \pmod{13}$

$6^{12} \equiv 1 \pmod{13}$

(Iz E izreka dobimo $6^{12} \equiv 1 \pmod{13}$.)

$7^{8^9} \equiv ? \pmod{12}$

$7^1 \equiv 7 \pmod{12}$

$7^2 \equiv 1 \pmod{12}$

$8^9 \equiv ? \pmod{2}$ ... $8^9 \equiv 0 \pmod{2}$ (8^9 je sodo št.)

$7^{8^9} \equiv 7^0 \pmod{12} \equiv 1 \pmod{12}$

$6^{7^{8^9}} \equiv 6^1 \pmod{13} \equiv 6 \pmod{13}$.

$\alpha, \beta : \{1,2,..,8\} \to \{1,2,..,8\}$ bijekciji

5. Dani sta permutaciji

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 8 & 1 & 7 & 4 & 6 \end{pmatrix} \quad \text{in} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

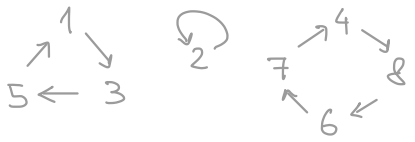
(a) Zapiši α in β kot produkt disjunktnih ciklov.

(b) Zapiši permutacijo $\alpha * \beta * \alpha^{-1}$.

(c) Poišči najmanjše število k, za katerega je $\alpha^k = \mathrm{id}$.

(d) Poišči najmanjše število k, za katerega je $\beta^k = \mathrm{id}$.

(a) $\alpha = (1\,3\,5)(2)(4\,8\,6\,7)$, $\beta = (1\,8)(2\,7)(3\,6)(4\,5)$



(b) $\alpha * \beta * \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 8 & 1 & 7 & 4 & 6 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 7 & 3 & 8 & 6 & 4 \end{pmatrix} =$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 4 & 1 & 8 & 2 & 5 & 3 \end{pmatrix} * \left(\quad \right) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 6 & 7 & 5 & 4 & 2 & 3 & 1 \end{pmatrix}$

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

$\alpha * \beta * \alpha^{-1} = (1\,3\,5)(4\,8\,6\,7) * (1\,8)(2\,7)(3\,6)(4\,5) * (5\,3\,1)(7\,6\,8\,4) =$

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

(c,d) $\alpha^k = id$, $\beta^k = id = \begin{pmatrix} 1 & 2 & \dots & 8 \\ 1 & 2 & .. & 8 \end{pmatrix}$ k je red permutacije

$k = \mathrm{lcm}$ ("dolžin ciklov")

$\mathrm{red}(\alpha) = \mathrm{lcm}(3,1,4) = 12$

$\mathrm{red}(\beta) = \mathrm{lcm}(2,2,2,2) = 2$

$\beta^1 = \beta \neq id$

$\beta^2 = \beta * \beta = (1\,8)(2\,7)(3\,6)(4\,5) * (1\,8)(2\,7)(3\,6)(4\,5) =$

$= (1)(2) \dots (7)(8) = id.$

8. Poišči vsaj dve permutaciji $\pi \in S_6$, za kateri je

$$\pi^3 = (1\ 2)(3\ 4)(5\ 6).$$

$\pi = (1\ 2\ 3\ 4\ 5\ 6)$

Naivno: recimo $\pi = (a\ b)(c\ d)(e\ f)$ ← zapis π kot prod disj.

Tedaj $\pi^3 = \big((ab)(cd)(ef)\big)^3 = (ab)^3(cd)^3(ef)^3 = (ab)(cd)(ef)$ ciklov

↑ ker imamo disj. cikle

Torej $\pi^3 = (ab)(cd)(ef) = (12)(34)(56)$ ... $\pi = (12)(34)(56)$.

Kaj pa $\pi = (a\ b\ c\ d\ e\ f)$?

Tedaj $\pi^3 = (a\ d)(b\ e)(c\ f) = (1\ 2)(3\ 4)(5\ 6)$

ali $\pi = (1\ 3\ 5\ 2\ 4\ 6)$.