Diskretne strukture UNI
Vaje 11

1. S pomočjo malega Fermatovega izreka pokaži, da

   (a) 23 deli $a^{154} - 1$ za vse $a \in \mathbb{N}$, za katere je $\gcd(a, 23) = 1$.

   (b) 17 deli $a^{80} - 1$ za vse $a \in \mathbb{N}$, za katere je $\gcd(a, 17) = 1$.

Fermatov mali izrek:

$p \in \mathbb{P} \Rightarrow \forall a \in \mathbb{Z}: \; a^p \equiv a \pmod{p}$

Eulerjev izrek

a, m tuji $\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{m}$

a) $p = 23 \rightsquigarrow a^{23} \equiv a \pmod{23} \quad \Big/ : a \quad$ (lahko, ker $\gcd(a,23)=1$)

$a^{22} \equiv 1 \pmod{23}$

$a^{154} = a^{7 \cdot 22} = (a^{22})^7 \equiv 1^7 = 1 \pmod{23}$

$a^{154} \equiv 1 \pmod{23} \Rightarrow a^{154} - 1 \equiv 0 \pmod{23} \Rightarrow 23$ deli $a^{154} - 1$ $\blacksquare$

b) $p = 17 \rightsquigarrow a^{17} \equiv a \pmod{17} \quad \Big/ : a \qquad \gcd(a,17)=1$

$a^{16} \equiv 1 \pmod{17} \quad \Big/ \,{}^{\wedge}5$

$(a^{16})^5 \equiv 1^5 \pmod{17}$

$a^{80} \equiv 1 \pmod{17}$

$a^{80} - 1 \equiv 0 \pmod{17} \rightsquigarrow 17$ deli $a^{80} - 1$

2. (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?

Eulerjev izrek

a, n tuji $\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$5, 11$ tuji $\Rightarrow 5^{10} \equiv 1 \pmod{11}$

a) $$((5^9)^{13})^{17} = 5^{9\cdot 13\cdot 17} = 5^{1989} = 5^{1980}\cdot 5^9 = (5^{10})^{198}\cdot 5^9 \equiv$$

$$\equiv 1^{198}\cdot 5^9 = 5^9 = (5^3)^3 = 125^3 \equiv 4^3 = 64 \equiv 9 \pmod{11}$$

$125 = 121 + 4$

$125 \equiv 4 \pmod{11}$

$64 = 66 - 2 = 55 + 9$

$64 \equiv 9 \pmod{11}$

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

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

ta vzorec se ponavlja mod 5

k	0	1	2	3	4	5	6	7	8	9	10
$5^k \% 11$	1	5	3	4	9	1	5	3	4	9	1

$\cdot 5$ $\quad 5\cdot 5 = 25$, $25 \% 11 = 3$

$\cdot 5$ $\quad 3\cdot 5 = 15$, $15 \% 11 = 4$

$\cdot 5$ $\quad 4\cdot 5 = 20$, $20 \% 11 = 9$

$\cdot 5$ $\quad 9\cdot 4 = 45$, $45 \% 11 = 1$

} lažje

ali $\quad 5^3 = 125$, $125 \% 11 = 4$

ali $\quad 5^4 = 625$, $625 \% 11 = 9$

} težje, večje številke, kmalu nemogoče

$5^{10} \equiv 1 \pmod{11}$ vemo iz Eulerjevega izreka (je pa že prej $5^5 \equiv 1 \pmod{11}$, $\varphi(n)$ ni nujno prvi tak eksponent)

$\Rightarrow 9^{(13^{17})} \% 5 = ?$

ponavlja mod 2

k	0	1	2	3	4	5
$9^k \% 5$	1	4	1	4	1	4

$\cdot 9$, $\%5$ $\quad \cdot 9$, $\%5$

$\Rightarrow 13^{17} \% 2 = ? = 1$ (ker je 13 liho)

Ker je $13^{17} \% 2 = 1$, je $9^{(13^{17})} \% 5 = 4$ in zato $5^{(9^{(13^{17})})} \% 11 = 9$.

Slučajno isto kot pri a).
Rezultata sta lahko različna.

Za vajo: a) $((7^3)^{17})^{23} \% 10 = ?$

b) $7^{(3^{(17^{23})})} \% 10 = ?$

Rešitev: a) $\underline{\underline{7}}$ b) $17^{23} \% 2 = 1 \Rightarrow$

$3^{(17^{23})} \% 4 = 3 \Rightarrow$

$7^{3^{17^{23}}} \% 10 = \underline{\underline{3}}$

3. Reši enačbe:

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

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

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

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

$$ax \equiv ay \pmod{n} \quad \Big|:a \qquad \gcd(a,n)=1$$
$$x \equiv y \pmod{n}$$

$$ax \equiv ay \pmod{an} \quad \Big|:a$$
$$x \equiv y \pmod{n}$$

$$6x \equiv 6 \pmod 9 \quad \Big|:3$$
$$2x \equiv 2 \pmod 3 \quad \Big|:2 \qquad \gcd(3,2)=1$$
$$\underline{\underline{x \equiv 1 \pmod 3}}$$

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

$$210 + 32 = \underbrace{210}_{0} + \underbrace{21}_{0} + 11$$

$$11x \equiv 11 \pmod{21} \quad \Big|:11 \qquad \gcd(11,21)=1$$
$$\underline{\underline{x \equiv 1 \pmod{21}}}$$

Rešitve v $\mathbb{Z}$: $\ldots, -41, -20, 1, 22, 43, \ldots$

Rešitve v $\mathbb{Z}_{21} = \{0, 1, \ldots, 20\}$: 1

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

$$\underbrace{250}_{0} + 20$$

$$5x \equiv 20 \pmod{25} \quad \Big|:5 \qquad (5 \text{ deli } 25)$$
$$\underline{\underline{x \equiv 4 \pmod 5}}$$

Rešitve v $\mathbb{Z}$: $\ldots, -6, -1, 4, 9, 14, \ldots$

Rešitve v $\mathbb{Z}_{25}$: $4, 9, 14, 19, 24$

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

Euler: $a = 6,\ n = 13,\ \varphi(n) = 12 \rightsquigarrow 6^{12} \equiv 1 \pmod{13}$

$$x = 6^{7\cdot 8\cdot 9} = 6^{4\cdot 3\cdot 2\cdot 3\cdot 7} = (6^{12})^{42} \equiv 1^{42} = 1 \pmod{13} \rightsquigarrow \underline{\underline{x \equiv 1 \pmod{13}}}$$

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

$7^{8^9} \% 12 = ? = 1$

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$6^k \% 13$	1	6	10	8	9	2	12	7	3	5	4	11	1
							−1	−6	−10	−8	−9	−2	−12

$\cdot 6$ $\%13$ $\quad$ $\cdot 6$ $\%13$

$8^9 \% 2 = ? = 0$

k	0	1	2	3	4	...						
$7^k \% 12$	1	7	1	7	1	...						

$\cdot 7$ $\%12$ $\quad$ $\cdot 7$ $\quad 49 \% 12$

4. 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) Zapiši α in β kot produkt disjunktnih ciklov.

α^{-1}

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

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

$*$

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

v splošnem $\alpha * \beta \neq \beta * \alpha$
(množenje permutacij ni komutativno)

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

$\boxed{\text{red permutacije } \alpha = \text{najmanjši } k \in \mathbb{N} \setminus \{0\}, \text{ za katerega je } \alpha^k = \mathrm{id}}$

$\boxed{\text{red}(\alpha) = \text{lcm dolžin ciklov z zapisu } \alpha \text{ z disjunktnimi cikli}}$

ciklična struktura α: $3+1+4$

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

$\Rightarrow \alpha^1, \alpha^2, \ldots, \alpha^{11} \neq \mathrm{id}$ in $\alpha^{12} = \mathrm{id}$

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

cikl. struktura β: $2+2+2+2$

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

$\Rightarrow \text{red}(\beta) = 2$

5. Dana je permutacija

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

(a) Določi π^{-1}.

(b) Zapiši π kot produkt disjunktnih ciklov.

(c) Zapiši π kot produkt samih transpozicij.

(d) Določi π^2 in π^{2018}.

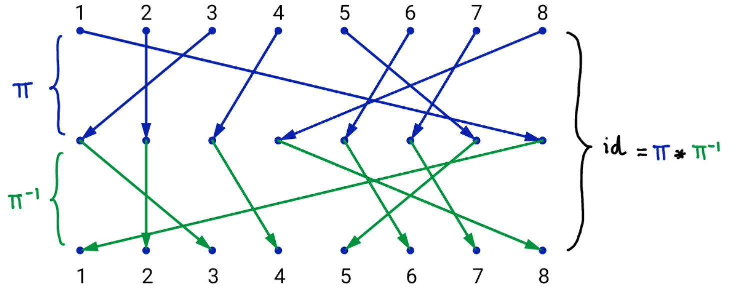
flip

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

sort

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 8 & 6 & 7 & 5 & 1 \end{pmatrix}$$

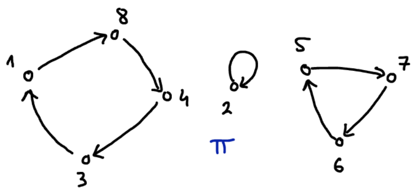
(a) Določi π^{-1}.

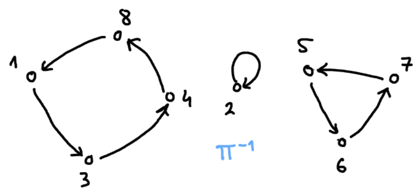


(b) Zapiši π kot produkt disjunktnih ciklov.

$$\pi = (1\ 8\ 4\ 3)(2)(5\ 7\ 6) \xrightarrow{\text{lažje}} \pi^{-1} = (6\ 7\ 5)(2)(3\ 4\ 8\ 1)$$

zapis z disjunktnimi cikli je enoličen do vrstnega reda ciklov natančno





(c) Zapiši π kot produkt samih transpozicij.

$\pi = (1\ 8)(1\ 4)(1\ 3)(5\ 7)(5\ 6)$ 5 transpozicij $\to$ liha

(ta zapis ni enoličen, to ni edina pravilna rešitev)

(d) Določi π^2 in π^{2018}.

$$\boxed{(k\text{-cikel})^n = (k\text{-cikel})^{n \% k}}$$

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

$$\pi^{2018} = \underbrace{\pi * \cdots * \pi}_{2018} = \big((1\ 8\ 4\ 3)(2)(5\ 7\ 6)\big)^{2018} = (1\ 8\ 4\ 3)^{2018}(2)^{2018}(5\ 7\ 6)^{2018} = (1\ 8\ 4\ 3)^{2018\%4}(2)(5\ 7\ 6)^{2018\%3} =$$

$2018 \% 4 = 2$

$2018 \% 3 = 2$

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

to je res samo za zapis z disjunktnimi cikli; če $\alpha\beta \neq \beta\alpha$, potem $(\alpha\beta)^2 \neq \alpha^2\beta^2, \ldots$

$$\pi^{2020} = (1\ 8\ 4\ 3)^{2020\%4}(2)(5\ 7\ 6)^{2020\%3} = (1\ 8\ 4\ 3)^0(2)(5\ 7\ 6)^1 = (1)(8)(4)(3)(2)(5\ 7\ 6)$$

6. Za $n > 3$ definiramo permutacije $\pi_n \in S_n$ kot produkt ciklov

$$\pi_n = (1 \quad 2 \quad n)(1 \quad 3 \quad n)\cdots(1 \quad n-1 \quad n).$$

(a) Zapiši permutacije π_4, π_5 in π_6.

(b) Izračunaj $\pi_n(1)$, $\pi_n(n)$, $\pi_n^{-1}(1)$ in $\pi_n^{-1}(n)$.

(c) Določi ciklično strukturo in parnost permutacije π_n.

(a) Zapiši permutacije π_4, π_5 in π_6.

$\pi_4 = (1\ 2\ 4)(1\ 3\ 4) = (1\ 2)(3\ 4)$ $\quad 2=4-2$

$\pi_5 = (1\ 2\ 5)(1\ 3\ 5)(1\ 4\ 5) = (1\ 2\ 4\ 5\ 3)$ $\quad 3=5-2$

$\pi_6 = (1\ 2\ 6)(1\ 3\ 6)(1\ 4\ 6)(1\ 5\ 6) = (1\ 2\ 4)(3\ 5\ 6)$ $\quad 4=6-2$

$\pi_7 = (1\ 2\ 7)(1\ 3\ 7)(1\ 4\ 7)(1\ 5\ 7)(1\ 6\ 7) =$
$= (1\ 2\ 4\ 6\ 7\ 3\ 5)$

(b) Izračunaj $\pi_n(1)$, $\pi_n(n)$, $\pi_n^{-1}(1)$ in $\pi_n^{-1}(n)$.

$$\pi_n = (1\ 2\ n)(1\ 3\ n)\underbrace{(1\ 4\ n)\cdots(1\ n-2\ n)(1\ n-1\ n)}_{\text{ni već } 2}$$

ni več 3

$\pi_n(1) = 2 \qquad \pi_n(n) = 3$

2. ni več $n-1$

$$\pi_n = (1\ 2\ n)(1\ 3\ n)(1\ 4\ n)\cdots(1\ n-2\ n)(1\ n-1\ n)$$

1. 2. 1.

3. ni več $n-2$

$\pi_n^{-1}(1) = n-2 \qquad \pi_n^{-1}(n) = n-1$

$\pi_n(n-2) = 1 \qquad \pi_n(n-1) = n$

(c) Določi ciklično strukturo in parnost permutacije π_n.

n sodo $\Rightarrow$ $\pi_n = (1\ 2\ 4\ 6\ \cdots\ 2k-2)(3\ 5\ 7\ 9\cdots 2k-1\ 2k)$
$n=2k$

$= (1\ 2\ 4\ 6\ \cdots\ n-2)(3\ 5\ 7\ \cdots\ n-1\ n)$ $\rightsquigarrow$ ciklična struktura : $\frac{n}{2} + \frac{n}{2}$

zapis z disjunktnimi cikli

$\frac{n}{2} - 1 + \frac{n}{2} - 1 = n-2$ transpozicij

$\Rightarrow$ soda

$(1 \quad 2 \quad n)(1 \quad 3 \quad n)\cdots(1 \quad n-1 \quad n)$ ni zapis z disjunktnimi cikli

$\Rightarrow 3+3+\cdots+3$ ni ciklična struktura π_n !

n liho $\Rightarrow$ $\pi_n = (1\ 2\ 4\ 6\ \cdots\ n-1\ n\ 3\ 5\ 7\cdots\ n-2)$ $\rightsquigarrow$ ciklična struktura : n

$n-1$ transpozicij $\Rightarrow$ soda

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

$$\pi^3 = \underbrace{(1\ 2)(3\ 4)(5\ 6)}_{\text{ciklična struktura}:\ 2+2+2}.$$

ciklične strukture za π: $2+2+2$, $4+2$, 6

$\boxed{(n\text{-cikel})^k \text{ razpade na } \gcd(k,n) \text{ ciklov dolžine } \frac{n}{\gcd(k,n)}}$

$(2+2+2)^3 = 2^3+2^3+2^3 = 2+2+2$ ✓

$(4+2)^3 = 4^3+2^3 = 4+2$ //

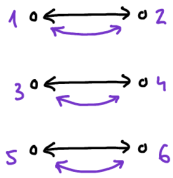
$6^3 = 2+2+2$ ✓

$\gcd(6,3)=3$

$\frac{6}{3}=2$

i) π : $2+2+2$

π^3: $2+2+2$

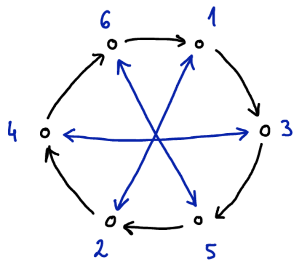


$\pi^3 = (1\ 2)(3\ 4)(5\ 6) \rightsquigarrow \pi_1 = (1\ 2)(3\ 4)(5\ 6)$

edina rešitev za to ciklično strukturo (do vrstnega reda disjunktnih ciklov natančno)

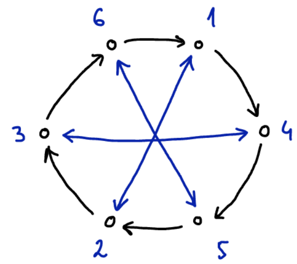
ii) π : 6

π^3: $2+2+2$

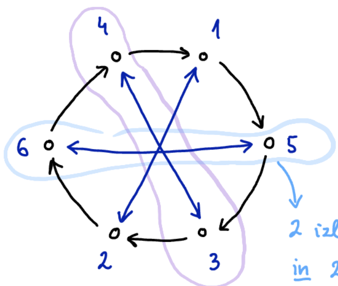


$\pi^3 = (1\ 2)(3\ 4)(5\ 6)$

$\pi_2 = (1\ 3\ 5\ 2\ 4\ 6)$



$\pi_3 = (1\ 4\ 5\ 2\ 3\ 6)$ $\quad \pi_3(1)=4,\ \pi_2(1)=3 \Rightarrow \pi_3 \neq \pi_2$



$\pi_4 = (1\ 5\ 3\ 2\ 6\ 4)$ $\quad \pi_4(1)=5 \Rightarrow \pi_4 \neq \pi_2, \pi_3$

2 izbiri transpozicije $((3,4)$ ali $(5,6))$
in 2 izbiri vrstnega reda izbrane transpozicije
2 izbiri vrstnega reda preostale transpozicije

$\Big\}\ 2\cdot 2\cdot 2 = 8$ različnih rešitev za c.str. 6

⋮