PERMUTACIJSKA POTENČNA ENAČBA

Pod drobnogled bomo vzeli enačbo

$$\pi^k = \alpha, \tag{1}$$

kjer je α znana permutacija, medtem ko je π permutacija-neznanka v enačbi. Poiskati želimo permutacije π, ki zadoščajo zgornji enačbi. Lepo bi bilo, če bi znali poiskati vse rešitve. Dejansko se bomo zadovoljili že z eno, oziroma informacijo, da enačba (1) nima rešitve.

Kakšen pa je lahko eksponent v enačbi (1)? Če je $k = 1$, je rešitev na dlani. V primeru, ko je $k = 0$, je enačba rešljiva le v primeru, ko je $\alpha = \mathrm{id}$, ko *vsaka* permutacija zadošča enačbi.

Enačba (1) svojo pravo podobo pokaže šele za večje eksponente. Torej privzamemo, da je $k \geq 2$.

Za analizo enačbe bo odločilnega pomena naslednji izrek, ki ga poznamo s predavanj. Permutacija je *ciklična*, če je sestavljena iz enega samega cikla.

Izrek 1. *Naj bo γ ciklična permutacija dolžine n. Potem je permutacija γ^k sestavljena iz* $\gcd(n,k)$ *disjunktnih ciklov, ki so* vsi *iste dolžine* $n/\gcd(n,k)$.

Permutacija α je ciklična

Oglejmo si najprej primer, ko je α *ciklična permutacija*, tj. sestavljena iz enega samega cikla dolžine n. Kakšna je ciklična struktura morebitne rešitve? Po Izreku 1 se disjunktni cikli v rešitvi π pri potenciranju ne morejo združiti v enega samega. Torej lahko sklepamo, da je tudi permutacija π ciklična z dolžino cikla enako n.

Obstoj rešitve enačbe (1) pa je v tem primeru odvisen od eksponenta k. Potenciranje n-cikla na k-to potenco začetni cikel razbije na več strogo krajših ciklov natanko tedaj, ko je $\gcd(n,k) > 1$. Če torej velja $\gcd(n,k) > 1$, enačba (1) rešitve nima. Če pa je $\gcd(n,k) = 1$, potem lahko poiščemo naravni števili r in s, ki zadoščata zvezi $k \cdot s = 1 + r \cdot n$. Računamo

$$\pi = \pi^{1+r\cdot n} = \pi^{k\cdot s} = (\pi^k)^s = \alpha^s$$

in pridelamo enolično rešitev enačbe (1).

Permutacija α je sestavljena iz ℓ disjunktnih ciklov iste dolžine d

Izrek 1 trdi, da je permutacija π sestavljena iz disjunktnih ciklov, katerih dolžine so večkratniki števila d. Njihova skupna dolžina pa mora biti enaka $\ell \cdot d$. Možnosti je pri velikem ℓ veliko (particije števila ℓ), toda tipično bo ℓ majhen.

Kot primer. Če je α sestavljena iz petih ciklov dolžine tri, potem so možne ciklične strukture za π naslednje: $[15]$, $[12,3]$, $[9,6]$, $[9,3,3]$, $[6,6,3]$, $[6,3,3,3]$ in $[3,3,3,3,3]$.

Šele zdaj pride na vrsto eksponent k. Za vsako od možnih cikličnih struktur preverimo, ali pri potenciranju na potenco k ustreza strukturi permutacije α. Tedaj pravimo, da je struktura *dobra*. Lahko se zgodi, da nobena izmed možnih struktur ni dobra in enačba nima rešitve.

Če primer nadaljujemo. Če je $k = 7$, potem je $[3,3,3,3,3]$ edina dobra ciklična struktura za π. Če je $k = 8$, potem so za π dobre strukture $[12,3]$, $[6,6,3]$, $[6,3,3,3]$ in $[3,3,3,3,3]$.

In če najdemo kakšno dobro strukturo? Vsako dobro strukturo zapišemo z neznanimi koeficienti, permutacijo potenciramo, in primerjamo s koeficienti permutacije α. Vsaki dobri strukturi ustreza vsaj ena rešitev enačbe (1).

V permutaciji α nastopajo disjunktni cikli različnih dolžin

V tem primeru nalogo razcepimo na več manjših nalog prejšnjega tipa.

Permutacijo α pišemo kot produkt permutacij

$$\alpha = \alpha_{d_1} * \alpha_{d_2} * \cdots * \alpha_{d_\ell},$$

kjer z α_{d_i} označimo produkt vseh ciklov dolžine d_i iz zapisa permutacije α.

S π_{d_i} označimo morebitno rešitev enačbe

$$\pi_{d_i}^k = \alpha_{d_i}. \tag{2}$$

Če obstaja rešitev rešitev enačbe (2) za vse $i = 1, \ldots, \ell$, potem je

$$\pi = \pi_{d_1} * \pi_{d_2} * \cdots * \pi_{d_\ell}$$

rešitev enačbe (1). Čim pa pri nekem $i \in \{1, \ldots, \ell\}$ enačba (2) ni rešljiva, potem tudi enačba (1) nima rešitve.

Zgled

Poišči rešitev enačbe

$$\pi^k = (1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11)(12\,13)(14), \tag{3}$$

pri $k = 543$ in $k = 544$. Enačbo razcepimo na tri enačbe:

$$\begin{aligned}
\pi_3^k &= (1\,2\,3)(4\,5\,6)(7\,8\,9)\\
\pi_2^k &= (10\,11)(12\,13)\\
\pi_1^k &= (14)
\end{aligned}$$

in opazujemo možne ciklične strukture permutacij π_1, π_2 in π_3. Možne strukture za π_3 so $[3,3,3]$, $[6,3]$ in $[9]$. Možni strukture za π_2 sta 4 in $[2,2]$, medtem ko je permutacija π_1 kar fiksna točka (14).

Obdelajmo najprej prvi eksponent: $k = 543$. Ker je $\gcd(543, 9) = 3$ in $\gcd(543, 3) = 3$, je za π_3 dobra samo struktura 9: 9-cikel namreč pri potenciranju na 543-to potenco razpade na tri disjunktne 3-cikle, 3-cikel pa razpade na tri disjunktne 1-cikle. Pišemo $\pi_3 = (x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7\, x_8\, x_9)$, računamo

$$\pi_3{}^{543} = \pi_3{}^3 = (x_1\, x_4\, x_7)(x_2\, x_5\, x_8)(x_3\, x_6\, x_9)$$

in preberemo eno možno rešitev: $\pi_3 = (1\,4\,7\,2\,5\,8\,3\,6\,9)$. Opazimo, da je 9-cikel v π_3 sestavljen iz prepletenih 3-ciklov permutacije α.

Ker je $\gcd(543, 2) = 1$, je edina dobra struktura za π_2 enaka $[2, 2]$. Pišemo $\pi_2 = (y_1\, y_2)(y_3\, y_4)$ in računamo:

$$\pi_2{}^{543} = \pi_2{}^1 = (y_1\, y_2)(y_3\, y_4).$$

Zato je $\pi_2 = (10\,11)(12\,13)$.

Produkt permutacij π_1, π_2 in π_3 je permutacija

$$\pi = (1\,4\,7\,2\,5\,8\,3\,6\,9)(10\,11)(12\,13)(14),$$

ki je rešitev enačbe (3) v primeru $k = 543$.

Če pa je eksponent $k = 544$, potem nobena izmed možnih struktur za π_2 ni dobra. Tako 4-cikel kot 2-cikel pri potenciranju na 544-to potenco razpadeta na cikle dolžine 1. Torej enačba (3) nima rešitve v primeru $k = 544$.

Vse rešitve?

Že v uvodu smo omenili, da ima lahko enačba (1) več rešitev. Oglejmo si naslednji primer:

$$\pi^2 = (1\,3\,5)(2\,4\,6) \tag{4}$$

Zgornja analiza nam pove, da imamo dve možnosti za ciklično strukturo permutacije π: dva 3-cikla ali en 6-cikel. Pa poiščimo za začetek rešitve sestavljene iz enega 6-cikla.

Zgornji postopek poišče rešitev $\pi = (1\,2\,3\,4\,5\,6)$. Dobimo jo tako, da prepletemo cikla dolžine tri iz desne strani enačbe.

Toda desno stran enačbe lahko zapišemo tudi kot $(1\,3\,5)(4\,6\,2)$ ali $(1\,3\,5)(6\,2\,4)$. V tem primeru metoda nedoločenih koeficientov pridela še drugi dve ciklični rešitvi $(1\,4\,3\,6\,5\,2)$ in $(1\,6\,3\,2\,5\,4)$.

Skupaj še z eno rešitvijo sestavljeno iz dveh 3-ciklov, namreč $(1\,5\,3)(2\,6\,4)$, ima enačba (4) kar štiri rešitve.

Problem vseh rešitev enačbe (1) je torej težji kot problem iskanja kakršne koli rešitve iste enačbe. Omenimo le, da je rešitev enačbe (1) kvečjemu ena, če v zapisu permutacije α z disjunktnimi cikli nastopajo cikli samih različnih dolžin.