БЕЏ ПРОБЛЕМ

Шести семинар „Математика и примени“, 17 март 2023

Институт за математика, Природно-математички факултет,

Универзитет „Св. Кирил и Методиј“, Скопје

Теа Наумовска, Мелиса Мулиќ

СОДРЖИНА

ВОВЕД

- Група од n-луѓе седат околу маса и пред секој од нив има бељ со име. Точно еден го има своето име на бељот пред себе. Секој од n-те луѓе го додава бељот на личноста од својата лева страна. Интересно, повторно само еден од нив го има своето име на бељот, различен од претходниот. Навистина, секоја ротација го означува точниот бељ со име на точно една нова личност до n-тата ротација, при што секое лице го добило точниот бељ со име само еднаш. Прашањето на проблемот кој ќе го наречеме Бељ Проблем гласи: Доколку имаме произволна група на луѓе како можеме да ги распоредиме бељовите со имиња така да се репродуцира оваа ситуација?

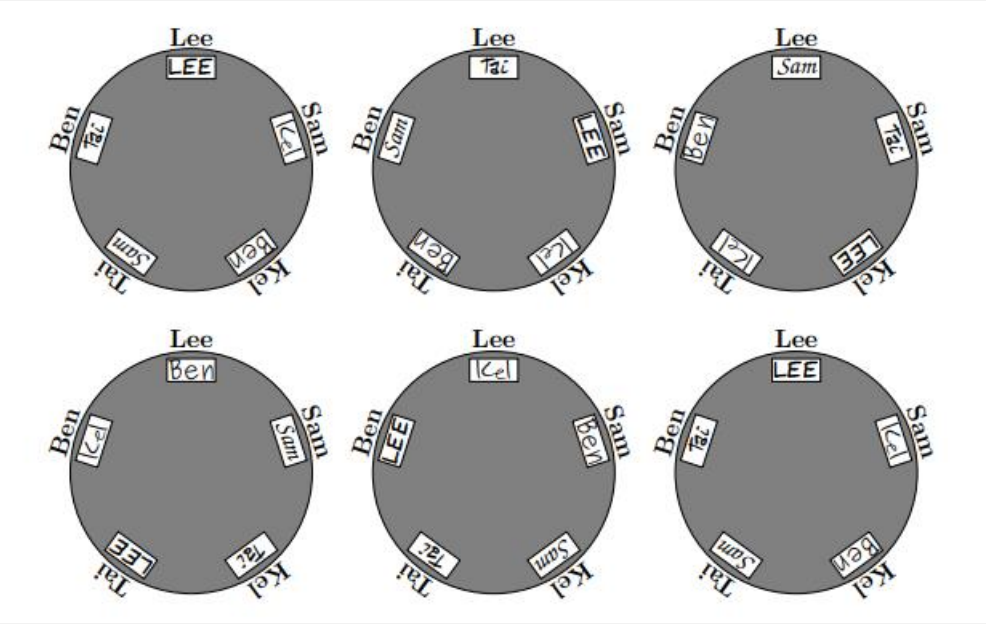
ОПИС

- Бидејќи имаме n луѓе, природно е да се означи секоја личност и беџот со 0,…,n - 1 , соодветно. Ако ги означиме луѓето како домен, а беџовите како кодомен, тогаш имаме функција f која доделува имиња што делува на $(\mathbb{Z}/n\,\mathbb{Z})$. Така сликата $f(\mathbb{Z}/n\,\mathbb{Z})$ на f ни ја дава почетната распределба на беџовите. Ако концентрично ги ориентираме елементите на доменот и кодоменот како часовници, како на Сл. 1, можеме да го претставиме пренесувањето на беџовите со поместување на сликата на функцијата на десно што создава ротација на сликата во насока на стрелките на часовникот. Врз основа на овој опис, „$f(x) = x$“ би гласело „ на личноста x е доделен бец x“ и затоа „$f(x - y) = x$“ е изразот за правилно доделен бец под одредена ротација y. Се разбира, ова значи дека, ако $f(x - y) \neq x$, тогаш лицето x не го добива точниот бец под ротација y.

ДЕФИНИЦИЈА 1

- Нека a и n се цели броеви т.ш $n \geq 1$ и нека $f: (\mathbb{Z}/n\,\mathbb{Z}) \to (\mathbb{Z}/n\,\mathbb{Z})$ е линеарна функција дефинирана со $f(x) = ax(\mathrm{mod}\, n)$. Велиме дека f е линеарно решение за БП ако се исполнети следните услови:

  1. за секој $y \in \mathbb{Z}/n\,\mathbb{Z}$, постои единствен $x \in \mathbb{Z}/n\,\mathbb{Z}$ т.ш $f(x-y) = x$.
  2. за секој $x \in \mathbb{Z}/n\,\mathbb{Z}$, постои единствен $y \in \mathbb{Z}/n\,\mathbb{Z}$ т.ш $f(x-y) = x$.



Сл. 1

Со првиот часовник, исто така почетната распределба $f(x)$, воочуваме дека само Lee го има точниот бец. Со вториот часовник, исто така првата ротација $f(x-1)$, воочуваме дека само Kel го добива точниот бец. Шемата продолжува се додека Lee не го добие точниот бец при ротацијата број 5.

СВОЈСТВА НА ЛИНЕАРНИ РЕШЕНИЈА НА БП

- Согледувајќи ја дефиницијата 1, гледаме дека за решението на БП, потребно е да се разгледа равенката

$$f(x-y)=x \qquad (1)$$

во однос на соодвентите квантификатори над x и y. Бидејќи равенката (1) е еквивалентна на линеарната конгруенција

$$a(x-y)\equiv x(\mathrm{mod}\, n) \qquad (2)$$

проблемот на одредување дали f го задоволува БП се сведува на решавање на линеарната конгруенција (2), во однос на соодвентите квантификатори.

Затоа е очигледно дека за да се утврди дали f го задоволува БП, мора да сме запознаени со општите услови под кои една произволна линеарна конгруенција има решение.

Забелешка 1: Нека a, b и n се цели броеви и $n\geq 1$ и нека $g=\mathrm{НЗД}(a,n)$.

1) ако $g\nmid b$, тогаш $ax\equiv b(\mathrm{mod}\, n)$ нема решение

2) ако $g\mid b$, тогаш $ax\equiv b(\mathrm{mod}\, n)$ има точно g инконгруентни решенија.

ТЕОРЕМА 1

- Нека a и n се цели броеви $n \geq 1$, $f: (\mathbb{Z}/n\,\mathbb{Z}) \to (\mathbb{Z}/n\,\mathbb{Z})$ е линеарна функција дефинирана со $f(x) = ax(\mathrm{mod}\, n)$.

а) Функцијата f го задоволува првото својство на БП акко

$$\text{НЗД}(\text{a} - 1, n) = 1$$

б) Функцијата f го задоволува второто својство на БП акко

$$\text{НЗД}(\text{a}, n) = 1$$

Тогаш, f е линеарно решение на БП акко

$$\text{НЗД}(\text{a} - 1, n) = \text{НЗД}(\text{a}, n) = 1$$

ДОКАЗ:

а) Прво, f го задоволува условот 1 од Деф.1 акко $\forall y \in \mathbb{Z}/n\,\mathbb{Z}$ има единствено решение за линеарната конгруенција (2). Нека $y \in \mathbb{Z}/n\,\mathbb{Z}$ е даден и $(a-1)y \equiv ay(mod n)$.

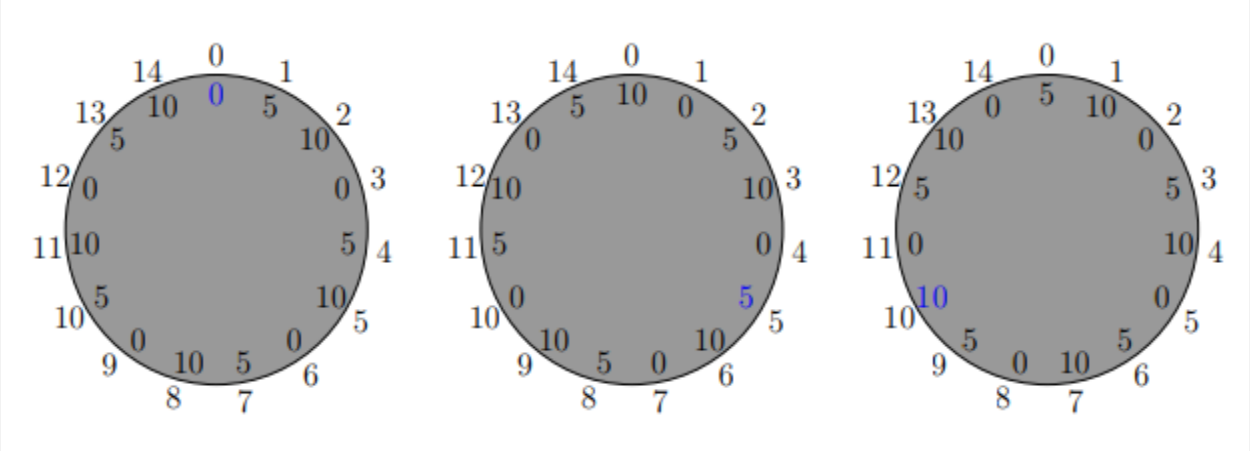
Од забелешката 1, постои единствено решение акко $\text{НЗД}(\text{a} - 1, n) = 1$.

б) Слично, ако конгруенцијата (2) ја запишеме како

$$ay \equiv (a-1)x\ (mod n)$$

согледуваме дека за било кој $x \epsilon\ \mathbb{Z}/n\ \mathbb{Z}$, од забелешката 1, постои единствено решение акко $\text{НЗД}(a,n) = 1$.

ПРИМЕР 1: Нека $n = 15$, $a = 5$, $\text{НЗД}(\text{a} - 1, n) = \text{НЗД}(14{,}5) = 1$ и $\text{НЗД}(\text{a}, n) = \text{НЗД}(5{,}15) = 5$. Значи f го задоволува условот 1 од Деф.1, а не го задоволува условот 2.



Сл.2 $n = 15$, $a = 5$

На Сл.2 гледаме дека на „масата“ се појавуваат само множители на 5 и така повторно стигнуваме до прашањето за еквивалентноста на условот 2 од Деф.1 и f е биективна фукција. Започнуваме со решавање на проблемот дали бројот на секој бец е множител на 5. Бидејќи f се дефинира како решение на линеарната конгруенција

$$ax \equiv f(x)(modn)$$

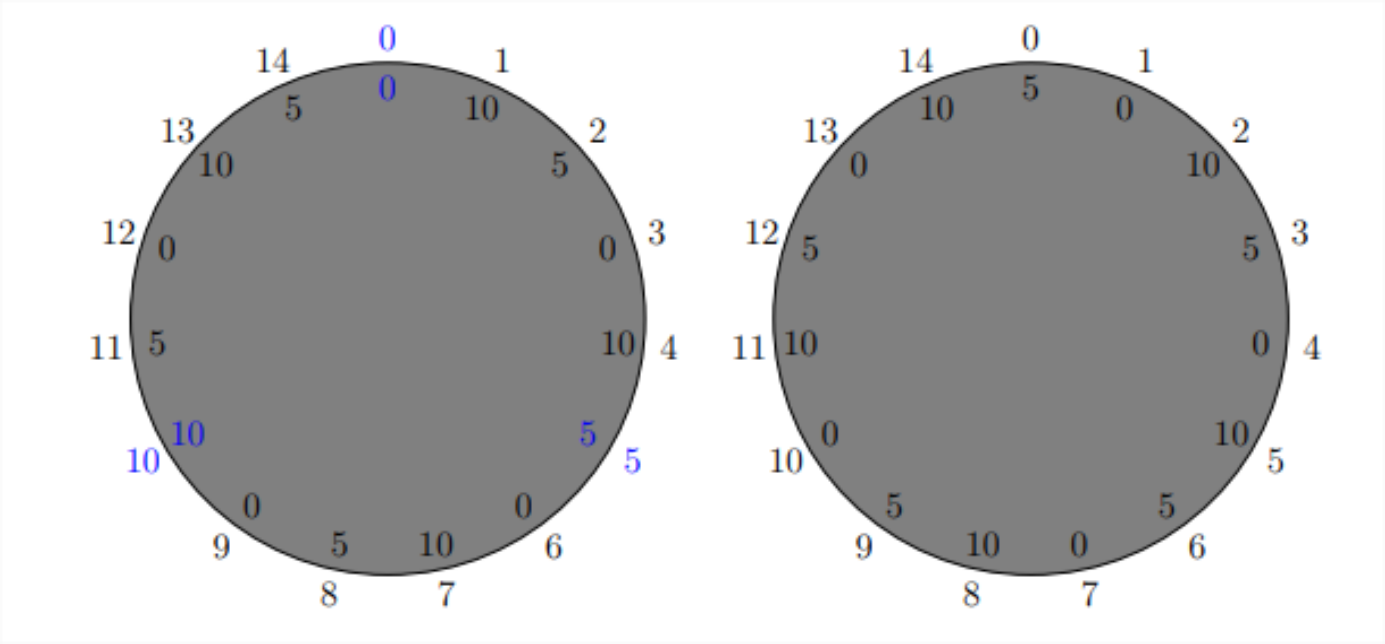
мора $f(x)$ да е множител на $\text{НЗД}(\text{a}, n)$ за секој x. Така, секое решение на овој пример е множител на 5.

Ова исто така имплицира дека f е сурјективна функција акко $\text{НЗД}(\text{a}, n) = 1$.

Допуштајќи $\text{НЗД}(\text{a}, n) = g$, воочуваме дека забелешката 1 имплицира дека има избор на само g вредности што $f(x)$ може да прими.

ПРИМЕР 2

- Нека n= 15, a= 10, НЗД(a, n)=НЗД(10,15)=5 и НЗД(a -1, n)=НЗД(9,15)=3. Значи, f не ги исполнува двата услови истовремено. Сликата 3 го потврдува тоа дека на масата се појавуваат само множители на 5, при што почетната конфигурација доделува 3 точни беџови додека првата ротација не доделува ниту една.



Сл.3

ДЕФИНИЦИЈА 2

Го дефинираме подмножеството $\mu_n \subseteq \mathbb{Z}/n\,\mathbb{Z}$ како $\{x \in \mathbb{Z}, n\mathbb{Z} | НЗД(x, n) = НЗД(x-1, n) = 1\}$. Со други зборови μ_n е подмножество на $\mathbb{Z}/n\,\mathbb{Z}$ така што $a \in \mu_n$ значи дека

$f(x) = ax(\mathrm{mod}\, n)$ е решение на БП.

- ТЕОРЕМА 2:

Нека n е позитивен цел број. Тогаш:

i) $\mu_n \neq \emptyset$ ако и само ако n е непарен

ii) $\mu_1 = \mathbb{Z}/1 \cdot \mathbb{Z} = \{0\}$ и $0 \notin \mu_n$ за сите n > 1.

Доказ:

i) Ако n е парен тогаш за секој $a \in \mathbb{Z}/n\,\mathbb{Z}$, НЗД($a$, n) ≥ 2 или НЗД(a -1, n) ≥ 2. Ако n е непарен, тогаш (2(mod n)) $\epsilon\ \mu_n$бидејќи НЗД(2, n)=НЗД(1, n)=1.

ii) Ова е лесно да се види бидејќи НЗД(x,1)=1 и НЗД(0, n)= n за секој x и n и бидејќи $\mathbb{Z}/1 \cdot \mathbb{Z} = \{0\}$. .

БРОЕЊЕ ЛИНЕАРНИ РЕШЕНИЈА НА БП

- За било кој зададен n може да го најдеме множеството линеарни решенија со наоѓање на сите елементи на μ_n, но многу брзо станува неефикасно. Сепак, можеме да најдеме начин за броење на колку линеарни решенија постојат за било кое дадено $n > 1$. Значи во овој дел даваме формула за $|\mu_n|$, кога $n > 1$.
- ДЕФИНИЦИЈА 3: Нека $n > 1$ и k се цели броеви и дефинираме подмножесво $M_n^k \subseteq \mu_n$ т.ш ги содржи оние елементи на μ_n кои се наоѓаат помеѓу $k - \text{тите}$ последователни целобројни множители на производ на единствените прости фактори на n.

$$M_n^k = \left\{ x \in \mu_n \middle| k\left(\prod_{p|n} p\right) < x < (k+1)\left(\prod_{p|n} p\right) \right\}$$

ЛЕМИ:

- Лема 1: Нека $n > 1$ е цел број, $p_1 \ldots p_r$ бидат единствените прости фактори на n. Тогаш

$$\mu_n = \{x \in \mathbb{Z}/n\mathbb{Z} | x \not\equiv 0 (mod p_i) \text{ и } x \not\equiv 1 (mod p_i), i \in 1 \ldots . \mathrm{r}\}.$$

- Лема 2: Нека $n > 1$ и k се цели броеви и нека $m = \prod_{p,n} p$. Тогаш,

$M_n = \left\{ M_n^k \middle| 0 \leq k < \frac{n}{m} \right\}$ е партиција на μ_n. (партиција - раздвојуваат подмножества што припаѓаат на истото семејство (неговиот пресек, во парови, е празен))

- Лема 3: Нека $n > 1$ е цел број, $p_1 \ldots p_r$ бидат единствените прости фактори на n. Нека $m = \prod_{p,n} p$ е нивниот производ. Тогаш

$\left| M_n^k \right| = \prod_{p,n} (p-2)$ за сите $0 \leq k < \frac{n}{m}$.

ТЕОРЕМА 3

- Нека n е позитивен цел број.

а) $|\mu_1| = 1$

б) ако $n > 1$, тогаш $|\mu_n| = n\prod_{p,n}(1-\frac{2}{p})$.

ДОКАЗ:

а) Следува од Теорема 2

б) Од Лема 2 следува дека $|\mu_n| = \sum_{k=0}^{\frac{n}{m}-1}|M_n^k|$. Од Лема 3 следува дека

$$\sum_{k=0}^{\frac{n}{m}-1}|M_k| = \frac{m}{n}\prod_{p,n}(p-2) = n\frac{\prod_{p,n}(p-2)}{\prod_{p,n}p} = n\prod_{p,n}(1-\frac{2}{p}).$$

ОРТОМОРФИЗМИ

- Ортоморфизмите се интересен тип на пермутација на група со примени на различни математики. Овој дел го детализира односот помеѓу ортомофизмите на $\mathbb{Z}/n\,\mathbb{Z}$ и решенијата на БП.
- ДЕФИНИЦИЈА 4: Нека G е група и θ е пермутација на G. Тогаш θ е ортоморфизам на G ако $x^{-1}\theta(x)x$ е исто така пермутација на G.
- ТЕОРЕМА 4: Нека G е група и θ е пермутација на G. Тогаш θ е ортоморфизам на G акко θ^{-1} е ортоморфизам.

ДОКАЗ: Следниве услови се еквивалентни

1. θ е ортоморфизам
2. $x^{-1}\theta(x)x$ е пермутација на G
3. $(x^{-1}\theta(x)x)\circ\theta^{-1}$ е пермутација на G
4. $x^{-1}\theta^{-1}(x)$е пермутација на G

ТЕОРЕМА 5: Функцијата $f:(\mathbb{Z}/n\,\mathbb{Z}) \to (\mathbb{Z}/n\,\mathbb{Z})$ го задоволува БП ако и само ако е ортоморфизам на $(\mathbb{Z}/n\,\mathbb{Z})$.

ЗАКЛУЧОК

- Овој труд развива математички опис на БП и не запознава со конструкцијата на линеарни решенија, истакнување на уникатни карактеристики со теореми и дијаграми. Иако целта беше вежба базирана на забавен проблем, откривме дека резултатите беа интересни сами по себе и имаат врска со неколку области на математиката, вклучувајќи теорија на броеви, комбинаторика и одреден тип на групни пермутации – ортоморфизми кои имаат примери во разни други области на математиката. Заклучуваме дека на овој проблем наречен БП може да му се пријде на неколку различни начини што го прави уникатен .

ЛИТЕРАТУРА

[1] Anthony B. Evans, Orthomorphism Graphs of Groups, Springer, Berlin, Heidelberg, 1992

[2] The On-Line Encyclopedia of Integer Sequences, https://oeis.org/A006717

[3] https://mk.erf-est.org/9715-partici-n.html

ВИ БЛАГОДАРИМЕ НА ВНИМАНИЕТО!