Paskaita 4.

Lyginių skaičiavimo pvz. – Ferma hipotezės fiktyvumas (pratybos)

Hipotezė: Skaičius $2^{2^n}+1$ yra pirminis.

Motyvacija: Ferma patikrino šią hipotezę, kai $n = 0, 1, 2, 3, 4$.

$n=0$ $\quad F_0 = 2^1 + 1 = 3$ (pirminis)

$n=1$ $\quad F_1 = 2^2 + 1 = 5$ (pirminis)

$n=2$ $\quad F_2 = 2^4 + 1 = 17$ (pirminis)

$n=3$ $\quad F_3 = 2^8 + 1 = 257$ (pirminis)

(užtenka patikrinti dalikliams $d \le \sqrt{257}$

$n=4$ $\quad F_4$ – sudėtinis pirminis (patikrinta laboratoriniame darbe)

$n = 5 \qquad F_5 = 2^{32} + 1$

Vėl galime patikrinti viską dalykliu (laboratorinis darbas), bet rezultato gausime naudodami lyginių skaičiavimo metodus.

Hipotezė – 641 yra F_5 daliklis

$$641 = 640 + 1 = 5 \cdot 2^7 + 1.$$

Todėl $5 \cdot 2^7 \equiv -1 \mod 641.$

Skaičiuojame 4 laipsnį abiejų lygybės pusių (lyginių skaičiavimo taisyklės).

$$5^4 \cdot 2^{28} \equiv 1 \mod 641$$

(Čia galime pastebėti, kad $2^{32} = 2^4 \cdot 2^{28}$!

Taip pat teisinga lygybė

$$641 = 625 + 16 = 5^4 + 2^4$$

Tada trivialiai gaunama lygybė

$$5^4 \equiv -2^4 \mod 641$$

Iš čia $5^4 \cdot 2^{28} \equiv 1 \mod 641$ gaunama

$$-2^4 \cdot 2^{28} \equiv 1 \mod 641$$

$$\boxed{2^{32} + 1 \equiv 0 \mod 641}$$

Taigi 641 yra daliklis. Reiškia F_5 nėra pirminis, Fermat hipotezė yra neteisinga.

Apibrėžkime naujas algebrines struktūras.

* $(X, \circ)$, čia operacija

$$\circ : X \times X \to X.$$

$X = \mathbb{Z}/m\mathbb{Z}$ lyginių mod m ekvivalentumo klasių aibė.

Imkime $a+m\mathbb{Z}$, $b+m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ šios aibės du elementus (klases).

Def. Apibrėžkime + (sumos) ir · (daugybos) operacijas

$$(a+m\mathbb{Z}) + (b+m\mathbb{Z}) = (a+b)+m\mathbb{Z}$$
$$(a+m\mathbb{Z}) \cdot (b+m\mathbb{Z}) = (a \cdot b)+m\mathbb{Z}$$

T.y. dviejų ~~ekvivalentu~~ lyginių klasių suma yra klasė, kuriai priklauso elementas $a+b$, o sandauga - yra klasė, kuriai priklauso elementas $a \cdot b$.

Taigi apibrėžimuose panaudojame atitinkamų liekanų klasių atstovus.

Svarbu įsitikinti, kad pakeitus atstovus sumos ir daugybos liekanų klasės nepasikeičia. Tai įrodome remdamiesi lygინių savybėmis

Jeigu $a \equiv c,\ b \equiv d$ $\overline{\mathrm{mod}\ m}$ Tai

1) $a + b \equiv c + d \mod m$

2) $a \cdot b \equiv c \cdot d \mod m.$

Pvz. $(3 + 5\mathbb{Z}) + (2 + 5\mathbb{Z}) = 5 + 5\mathbb{Z}.$

$= 5\mathbb{Z},$

nes $5 \equiv 0 \mod 5.$

$(3 + 5\mathbb{Z}) \cdot (2 + 5\mathbb{Z}) = 6 + 5\mathbb{Z}$

$= 1 + 5\mathbb{Z},$

nes $6 \equiv 1 \mod 5.$

Ap. Operacija $\circ$ yra asociatyvi, jei
$\forall a, b, c \in X$ teisinga lygybė

$$(a \circ c) \circ b = a \circ (b \circ c)$$

Operacija yra komutatyvi, jei

$$a \circ b = b \circ a.$$

Pav. 1) Jei $X = M$ - $n \times n$ matricos, $m_{ij} \in \mathbb{R}$,

tai $+$ yra asociatyvi ir komutatyvi operacija

2) ~~Nr~~ daugyba $\cdot$ yra asociatyvi operacija, bet bendrąja atveju ji nėra komutatyvi

Palyginkite su lygybe Jeigu abi simetrinės matricos A, B sandauga $A \cdot B$ yra simetrinė matrica, tai ~~tik~~ tokios matricos komutuoja $A \cdot B = B \cdot A$ $\left((A \cdot B)^T = B^T \cdot A^T, \right.$

$A^T = A, B^T = B \Rightarrow$ $\left. (A \cdot B = B \cdot A \right)$ |

Nagrinėkime algebrinę struktūrą $(A, \circ)$, čia A yra elementų aibė, $\circ$ – operacija $\circ : A \times A \to A$

Ap. Pora $(A, \circ)$ yra <u>pusgrupė</u>, jei $\circ$ yra <u>asociatyvi operacija</u>.

Ap. Jei $\circ$ yra <u>ir</u> komutatyvi operacija, tai tokia pusgrupė vadinama <u>Abelio</u> pusgrupe.

<u>Pav</u> 1. Komutatyvios pusgrupės $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, \cdot)$

2. $(M, \overset{\circ}{\uparrow})$ yra pusgrupė, bet daugyba ne Abelio pusgrupė.

Pažymėkime $a^1 = a$., $(X, \circ)$.

Def. $a^{n+1} = a \circ a^n$, $\forall a \in X$.

Tada teisingos lygybės

$$a^n \circ a^m = a^{n+m}, \quad (a^n)^m = a^{nm}$$

(įrodyti pratybose).

T. Jeigu $a \circ b = b \circ a$, tai

$$\boxed{(a \circ b)^n = a^n \circ b^n.}$$

◀ Įrodysime matematinės indukcijos metodu.

$n = 1$ (patikrinti, ar teiginys teisingas, kada nors).

$$(a \circ b)^1 \overset{\text{def}}{=} a \circ b \left(\overset{\text{def}}{=} a^1 \circ b^1\right).$$

Tarkime, kad teiginys teisingas $\forall k$: $1 \le k \le n$.

$$(a \circ b)^{n+1} \overset{def}{=} (a \circ b) \circ (a \circ b)^n$$

$$\overset{\text{индукц. пр.}}{=} (a \circ b) \circ (a^n \circ b^n)$$

$$\overset{\text{асоциат.}}{=} a \circ (b \circ a^n) \circ b^n$$

Надграждане $(a \circ b)^{n-1}$

$$b \circ a^n \overset{def}{=} b \circ (a \circ a^{n-1}) \overset{\text{комут?}}{=} a \circ (b \circ a^{n-1})$$

$$= a \circ (a \circ (b \circ a^{n-2})) = a^2 \circ (b \circ a^{n-2})$$

$$= \ldots = a^n \circ b$$

Тада даденото:

$$(a \circ b)^{n+1} = a \circ (a^n \circ b) \circ b^n$$

$$= (a \circ a^n) \circ (b \circ b^n) \overset{def}{=} a^{n+1} \circ b^{n+1} \blacktriangleright$$

Ap. Neutralus pusgrupės $(X, \circ)$ elementas e, yra toks $e \in X$, kad

$$\boxed{e \circ a = a \circ e = a, \quad \forall a \in X}$$

e komutuoja su $\forall a$, nors X nebūtinai yra Abelio pusgrupė.

Ap. Jeigu toks elementas e egzistuoja, tai pusgrupė yra vadinama monoidu.

T. Pusgrupė turi ne daugiau kaip vieną neutralų elementą

◁ Tarkime, kad $\exists$ du skirtingi neutralūs elementai $e_1, e_2 \in X$. Tada:

$$e_1 \circ e_2 \overset{\text{def}}{=} e_2$$

$$e_1 \circ e_2 \overset{\text{def}}{=} e_1 \quad \Rightarrow \quad \boxed{e_1 = e_2}$$

▷

Ap. Jeigu $e \in X$ yra pusgrupės neutralus elementas ir $a \in X$, tai $a' \in X$ yra simetriškas a atžvilgiu (priešingas, atvirkštinis), jei

$$a \circ a' = a' \circ a = e.$$

(a' komutuoja su a!).

Tada a vadinamas apverčiamu elementu.

Pav 1) $(\mathbb{Z}, +)$, $e = 0$, $\forall a \in \mathbb{Z}$ visada $\exists$ simetriškas elementas $(-a) = a'$

$$a + (-a) = 0.$$

(vadiname ir priešingu)

2) $(\mathbb{Z}, \cdot)$, $e = 1$. Vienintelės apverčiamieji elementai $1, -1 \in \mathbb{Z}$.

$$1 \cdot 1 = 1 \Rightarrow 1' = 1$$

$$(-1) \cdot (-1) = 1 \Rightarrow (-1)' = -1.$$

3. Liekanų klasėje pusgrupėje $(\mathbb{Z}/m\mathbb{Z}, +)$ klasė $m\mathbb{Z}$ yra neutralus elementas. Klasei $a+m\mathbb{Z}$ ~~priešinga~~ simetrinė klasė yra $(-a)+m\mathbb{Z}$.

Imkime $3+5\mathbb{Z}$ elementą. Jam simetrinė (priešinga) klasė yra

$$(-3)+5\mathbb{Z} = 2+5\mathbb{Z},$$ nes

$$-3 \equiv 2 \mod 5.$$

4. Pusgrupėje $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ neutralus elementas yra klasė $1+m\mathbb{Z}$.

$a+m\mathbb{Z}$ yra apverčiamas (jam egzistuoja simetrinis elementas ~~$\mathbb{Z}$ jei~~ $a'+m\mathbb{Z}$) jei

$$a\,a' \equiv 1 \mod m$$

Esame įrodę, kad tokia lygtis turi sprendinį tada ir tik tada, kai

$$\gcd(a, m) = 1.$$

Tada, naudodami Euklido algoritmą, sprendžiame lygtį

$$ax + my = 1 \quad \text{ir} \quad \boxed{a' = x.}$$

Imkime $3 + 5\mathbb{Z}$ ekvivalentiemo klasę. Kadangi $\gcd(3, 5) = 1$, tai simetriškas (atvirkštinis) elementas $a' + 5\mathbb{Z}$ egzistuoja. Sprendžiame lygtį

$$3x + 5y = 1. \Rightarrow x = 2,\ y = -1.$$

$a' = 2$ (atvirkštinis elementas $2 + 5\mathbb{Z}$)

Apibr. Grupė yra toks monoidas $(X, \circ)$, kuriame $\forall a \in X$ egzistuoja simetrinis elementas $a' \in X$.

Grupė yra Abelio, jei monoidas yra komutatyvus.

1. $(\mathbb{Z}, +)$ yra Abelio grupė
2. $(\mathbb{Z}, \cdot)$ nėra grupė
3. $(\mathbb{Z}/m\mathbb{Z}, +)$ yra Abelio grupė.
4. $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ ne visada grupė

Turime grupę, jei m yra pirminis skaičius, nes tada $\forall a \in \{1, \dots, m-1\}$

$$\gcd(a, m) = 1.$$

Ap. Grupės eilė (arba pusgrupės eilė) vadiname jos elementų skaičių

$(\mathbb{Z}/n\mathbb{Z}, +)$ eilė n

$(\mathbb{Z}, +)$ eilė ∞.

Pažymėkime $a^{\Delta} = a^{-1}$

Apibrėžkime: ~~a^{-n}~~

$$a^{-n} = (a^{-1})^n.$$

Patikrinkite, ar

$$(a^n)^{-1} = a^{-n}.$$