

# ლამაზების მეთოდები

- ვაჩიანუების გადასახელვით  
ლამაზების ხამრებიდან ეცავთაღ რაყოფა და სალიცალია  
ლამცაისები.
- კონცხაპოზიციი  
თუ  $P$ , მაშინ  $Q$   
 $\downarrow$  (მცხოვრება ეპივალენტურობა ფუნქციების სტრუქტურის  
თუ ან  $Q$ , მაშინ ან  $P$
- საწინააღმდეგოს ლამაზებით ლამცაისები  
მაგ. ლამცაისები, ხოდ  $\sqrt{2}$  იხადონალოგია  
 $\downarrow$   
ლამაზები  $\sqrt{2}$  ხადონალოგია ...



- მინიმალური კლემუნტის შინაგანი

სამარტინო

ყ. მ. მ.  $P(n)$  სხელდება უკეთ ი-სავის ( $N$ -ში)

II

სამინიმარტინოს დაშვება

ასევე 1 ი პირ, რომ  $P(n)$  არ საკონფიდენციალური

III

მინიმალური კლემუნტის მემკვანეობა

ასევე 1  $N$  (მინიმალური ნაკუთხეფის რიცხვი),  
რომელისთვის  $P(n)$  არ საკონფიდენციალური

IV

ვადგენილება, რომ  $N$  ასევე 1 (ან ჩვენს

მიზან მოიხველოთ პაროვანება მეტა  $n < N$ ),

რომ  $P(n)$  სხელდება

## ★ • ინდუქციის მეთოდი

მ. ე.  $P(n)$  სხეულის ყველა  $n$ -სივრცის ( $N$ -ში)

- $P(0)$  სხეულის (ან გინიმარტები), ხათა დავხერხეთ რამდენიმე ასეთი.
- დავამცეკიცოთ  $P(n+1)$ -სივრცის (თუ  $P(n)$  მაგრა  $P(n+1)$ )

მაგ. ესავ., რამდენიმე  $0+1+2+3+\dots+n = \frac{n(n+1)}{2}$  ( $n \in N$ )

### • საბაზისო

$$\begin{array}{ll} \text{თუ } n=0 & 0 = \frac{0 \cdot 1}{2} \\ & \text{გთავანი} \\ n=1 & 1 = \frac{1 \cdot 2}{2} \end{array}$$

### • გვამდვათ გებულება სამახარეოანის

$$1+2+3+\dots+m = \frac{m(m+1)}{2}$$

$$\text{მაგრა } (m+1)P \text{ სივრცის ენერგეტიკული } \rightarrow \\ 1+2+3+\dots+m+1 = \frac{(m+1)(m+2)}{2}$$

დავამცეკიცოთ, რამდენიმე ასეთი

$$1+2+3+\dots+m+m+1 = \frac{m(m+1)}{2} + m+1 = \frac{(m+1)(m+2)}{2}$$

თუ  $P(n)$ , მაგრა  $P(n+1)$

## ★ • ძლიერი ინდუქცია

მ.მ. დ.  $P(n)$  სხელდება ყველა  $n$ -სთვის

1) საბაზო

2) დავგმვა

1-სთვის, 2-სთვის, 3-სთვის ...  $n$ -სთვის სხელდება

მ.მ. , ხმა

$n+1$ -სთვისაც შესხელდება

(მაგალითები შემოწმება)

თუ  $p(0)$  და  $p(1)$  და  $p(2)$  და ... და  $p(n)$ , გამონ

$p(n+1)$

---

ყველა  $n$ -სთვის  $p(n)$   $\leftarrow$  თუ მცვალეობა ძლიერი  
ინდუქციით, გამონ

ყველა  $n$ -სთვის თუ  $m \leq n$ , გამონ  $P(m)$   $\leftarrow$   
მცვალეობა მაჩვივი ინდუქციით

## ლოგიკური მსენაციონისტი:

ქმრ.	ინგ.	ქმრ.	მათ.	შემოგ.	თანააკვეთა
და	and	^	&	( ^ პიკაბსაღ უ-ისა)	
არა/არ	not	¬	!		გაუჩინანების
ან	or	∨		( ∨ პიკაბსაღ უ-ისა)	

nand

nor

ოუ... მაშინ  
გამომდინარება. implies  $\Rightarrow$

გამომჩენება  $\oplus$  xor  $\oplus$  ^

ექვივილინგუისტი  
უზრუნველყოფილ  
equivalent  $\Leftrightarrow$

II  
օղուհեր

„ $\neg\neg$ ”-ն յշտացնելու վեհումո

Յաջականքներ

		P	Q	$P \wedge Q$	$\neg P \wedge \neg Q$	$\neg P$	$\neg Q$
		P	$\neg P$	T	F	F	F
		T	F	F	F	F	T
...		F	T	F	F	T	F
...		F	F	F	T	T	T

„ $\neg\neg$ ”-ու յշտացնելու վեհումո

		P	Q	$P \vee Q$	$\neg(P \vee Q)$	հարցան զոյնու , հոմ	
		P	$\neg P$	T	F	$\neg P$	
		T	F	T	F	$\neg P$	
...		F	T	T	F	$\neg P$	
...		F	F	F	T	$\neg P$	

Յաջականքու յաջականու արշարութեա (այլուրեա)

$$\neg(P \vee Q) = \neg P \wedge \neg Q \quad (\text{և } (P \vee Q) = \neg \neg P \wedge \neg \neg Q)$$

↓

$$\neg(\neg(P \vee Q)) = \neg(\neg P \wedge \neg Q)$$

$$P \wedge Q = \neg(\neg P \vee \neg Q)$$

ოფიციალური სიტყვა (ისეთ ლოგიკურ თქმას ეძღვნეთ)

{ and, or, not }

სიმუვლე, ხომალია სტატუსი

{ and, not }

Ելքություն անհայտ

{ or, not }

զանուածքած Շյածընչընու)

{ nand }

{nor}

$\text{nand} = \text{not, and } (\exists x. a \text{ nand } b \equiv \text{not}(a \wedge b))$

nor = not, or (dog. a nor b not (a  $\vee$  b))

⇒

լույսի հմատ  $\Rightarrow$  - ու լինելու ( չընթափնչուն )

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

||

մյածածիուն և - ու լինելու  
( հարցաբ  
աւշակայեն )

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

( F պերա ազդանու  
T F - եղան  
ամուլտ լույսի հմատ )

P	Q	$\neg P \vee Q$
T	T	T
T	F	F
F	T	T
F	F	T

||

$\neg P$  ( հմատ պահանջ  
եաթի F F ամուլտ  
ու ոյ լույսի հմատ  
ամանինին Պ բանի )

$$P \Rightarrow Q = \neg P \vee Q$$

xor

$$(a \text{ xor } b) = (a \wedge \neg b) \vee (\neg a \wedge b)$$

$$(a \text{ xor } b) = (a \vee b) \wedge (\neg a \vee \neg b)$$

P	Q	$P \text{ xor } Q$
T	T	F
T	F	T
F	T	T
F	F	F

$\Leftrightarrow$

$$(P \Rightarrow Q \text{ or } Q \Rightarrow P)$$

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

$$P \Leftrightarrow Q = (P \Rightarrow Q) \wedge (Q \Rightarrow P) \quad (\text{ცხვრის განვქმნელი ღია})$$

$$P \Leftrightarrow Q = \neg (P \text{ xor } Q)$$

გვერდი 1-სთვის საყვლევები  $p(n)$

$\forall n : p(n)$

(all)

ესთ 1-სთვის დანერგვები  $p(n)$

$\exists n : p(n)$

(exists)

•  $\forall n : p(n) \Leftrightarrow \neg \exists n : \neg p(n)$  ცოდნის

$\neg \forall n \in \mathbb{N} : p(n)$

"  
 $\exists n \in \mathbb{N} : \neg p(n)$

•  $\neg \exists n : p(n) \Leftrightarrow \forall n : \neg p(n)$  ცოდნის

სიმხევლები  
სამატერიალო გარემო

•  $\forall x \exists y \forall z \dots : p(x, y, z) \Leftrightarrow \exists x \forall y \exists z \dots : \neg p(x, y, z)$  ცოდნის

# სტატისტიკა

- ალბათური სივრცე - ყველა შესაძლო ვარიანტის სიმსახული
- ჩავალის ნიმუში - ხოდესავ აუკილებლად ან საირანუ დავინურ

ასტოურებული ხდომილობა

$$\text{II} \quad P(A \cap B) = P(A) \cdot P(B)$$

$$P(A \cup B) = 1 - (P(\neg A) + P(\neg B))$$

(ან  $A \cap B$  არ არის)

$$1 - P(A' \cup B') = 1 - P(A') \cdot P(B')$$

**მარტივი მოლოდინი** - ხდომ. 1 • კონ. 1 + ხდომ. 2 • კონ. 2 + ...

- თუ გამოვიდა დარებითი რის თამაში, თუ შე არ არის
- def. ჩა იქნება ჩვენი სამართლო მოვალეობა გვიჩვენ თუ ვითარდებ

ასტოურებული ხდომილობა

$$P(A \cap B) = P(A) \cdot P(B|A)$$

↑

$P(B|A)$  -  $B$ -ს ალბათობა  $A$  სიზუსტით, ხოდ  $A$  უსხეული (სიზუსტი არ არ ხდება ვიცით, ხოდ  $A$  უკვე მოხადა)

1

მგ. • „ას”-დან გადავიღოთ „რა”-გი

• „დაბოხვება” ვამტკიცებთ „ას დაბოხვება”

• ხოდ მიჩნა 1-1 განსაზღვრული

გადავიღოთ ან 1-გი

და მეტი ვაძლები 1-ს

• შაიგნის ფორმულა

$$P(A) \cdot P(B|A) = P(B) \cdot P(A|B)$$

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

★ პირველი 3 ლექციის მნიშ. ამონანები  
აზმათში

ლ. 3  $\rightarrow$  5, 10 ~ (კონსკიუტი ბროკნოგბი)

ლ. 2  $\rightarrow$  13, 14, 12 (15), 9

ლ. 1  $\rightarrow$  გვისეული აჩვენების ჩავალის უკლ. შეინიშნე  
(„ინიციაციური“-ში უკლ. ამონანაა)

★ ლისახეული მათემატიკის მეცნ. ლექციის  
კონსკიუტის კლ. ვებსიტი მატვ

# სიტყვლეები

- მაქსიმუმ 1 ხელ თითო კლემუნტი  $\{x\} = \{x, x\}$
- მიმღებების გნიმენელობა ან სტანდარტული  $\{x, y\} = \{y, x\}$

• სიტყვლის ჩასების ხელი  $\{x \mid p(x)\}$   
 ↑  
 obj. hmd

- $\{1, 2, 4, 8, \dots\}$
- $\{x \mid x : 2\}$

$$\{x \in \mathbb{N} \mid \exists k \in \mathbb{N} : x = 2^k\}$$

ისეთი  $x$ -ების სიტყვლე, რომელიც იყოფიან 2-ები.

$$\{x \in \mathbb{N} \mid x : 2\}$$

• სიტყვლეების

• **თანაელეთა**  $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$

• **გუერიანება**  $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$

• **დამაცემა**  $\bar{A} = A^c = \{x \in \mathbb{U} \mid x \notin A\}$   
 ↑  
 $(\setminus A)$

უნივერსუალები სიტყვლე

- ესა მიცემთ ჩვენ სიტყვლე გამოტანის. მაგარიარა ა, ჩვენ იყოს  $\mathbb{N}$  და  $A$  მყნები.  $A$ -ს დამაცემა დაგენერი ხვდებოდა იწნება.

- $A$  ქვესიმებერება  $B$ -ს

$$A \subseteq B \quad \text{თ. } \forall x : (x \in A) \Rightarrow (x \in B)$$

- $A = B$

$$\text{1) } (A \subseteq B) \wedge (B \subseteq A)$$

$$\text{2) } \forall x : (x \in A) \Leftrightarrow (x \in B)$$

სამყარო 1

კანონიური მართვა

$$\text{თ. 2) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$\text{თ. 2) } x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$$

ნიზამი ნისა რანიშმაღლი ( გუერიანება / რანცვევთა )

$$\text{თ. 3) } (x \in A) \vee (x \in (B \cap C)) \Leftrightarrow (x \in (A \cup B)) \cap (x \in (A \cup C))$$

$$\text{თ. 4) } (x \in A) \vee ((x \in B) \cap (x \in C)) \Leftrightarrow ((x \in A) \vee (x \in B)) \cap ((x \in A) \vee (x \in C))$$

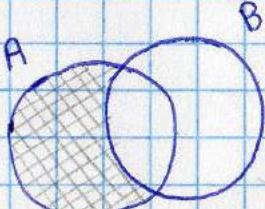
$$P \quad Q \quad R$$

$$P \vee (Q \cap R) \Leftrightarrow (P \vee Q) \cap (P \vee R) \leftarrow \text{ასევე უკარატების ფასილიტეტი}$$

სხვაობები

$$\bullet A - B \quad (A \setminus B) \quad \{x \mid (x \in A) \wedge (x \notin B)\}$$

$$A \cap \overline{B}$$



## სიმებურთო სხვაობა

$$A \Delta B = (A - B) \cup (B - A)$$

$$(A \cup B) - (A \cap B)$$

$$\Downarrow = \{ x \mid ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A)) \}$$

$\text{P}$        $\text{Q}$

$$(P \wedge \neg Q) \vee (Q \wedge \neg P) = P \text{ xor } Q$$

$$= \{ x \mid (x \in A) \text{ xor } (x \in B) \}$$

$$? \quad A = \{ \emptyset, \{3\}, \{3,4\} \}$$

$$\{3\} \in A \quad \checkmark$$

$\{3\} \subseteq A \times A$  hond ymgynnyd  $\{\emptyset, \{3\}, \{3, 4\}, 3\}$

$\emptyset \in A$  ✓

$$\emptyset \subseteq A \quad \checkmark$$

ମାତ୍ରିକ

$$\bullet \quad A \subseteq B \quad B \subseteq C$$

$$A \subseteq C$$

$$A \in B \quad B \in C$$

$$\text{A} \notin \mathcal{C}$$

$A \subseteq B$  označen „kάπερι μεμένη ορ Α μάκρε σύμμετρη ορ Β“

- $A \times B = \{(a, b) \mid a \in A, b \in B\}$  დეკარტის ნიმუში

Ex. A {1,2}, B {3,4}

$$A \times B = \{(1,3), (1,4), (2,3), (2,4)\}$$

$$|A \times B| = |A| \cdot |B|$$

შოთა  
რევული  
კომისია  
სამართლებრივი

# 1. ფუნქცია \*

•  $f: A \rightarrow B$

$$\begin{array}{ccc} & \uparrow & \uparrow \\ \text{ფორმი} & & \text{კოდორმენი} \end{array}$$

/\* ფორმი  $\neq$  განსაზღვრის შე

но სიმარტინი განიხილება ცვლადი

მაგ. შეიძლება ფორმი  $R$  იყოს,  $\leftarrow f(x) = \frac{1}{x}$

მაგრამ განსაზღვრის შე -  $R \setminus 0$

ანალოგიურად კოდორმენი  $\neq$  მნიშვნელობათა სიმარტი

\*/

• ფუნქცია  $shs: \{T, F\} \rightarrow \{T, F\}$

$x$	$shs x$
T	F
F	T

/\* ძელი ცენტრი  $\longrightarrow$  ახალი ცენტრი

\* ნაწილობრივი ფუნქცია  $\longrightarrow$  ფუნქცია

\* ფუნქცია  $\longrightarrow$  ცოცალები ფუნქცია

\*/

• জ্ঞানজ্ঞো  $f(x) = e^x$

$$f: \mathbb{R} \rightarrow \mathbb{R}$$

• জ্ঞানজ্ঞো  $f \{1, 2, 5, 7, 8\} \rightarrow \{1, 2, 3\}$

$x$	$f(x)$
1	2
2	1
5	3
7	—
8	1

• যোগসম্বূহো

$$g \circ f : A \rightarrow C$$

$$f: A \rightarrow B$$

$$g \circ f(x) = g(f(x))$$

$$g: B \rightarrow C$$

অংগ.  $f: \mathbb{R} \rightarrow \mathbb{R}$

$$f(x) = e^x$$

$$g: \mathbb{R} \rightarrow \mathbb{R}$$

$$g(x) = x^2$$

$$f \circ g(x) = f(g(x)) = e^{x^2}$$

$$g \circ f(x) = g(f(x)) = e^{2x}$$

## • $R$ - მიმართება

$$R: A \rightarrow B$$

$$f(x) = y \quad \text{ფუნქცია}$$

$$x R y \quad \text{მიმართება}$$

$$\text{ა. 2. } x < y$$

$$\begin{array}{c} \uparrow \\ R \text{ მიმართება} \end{array}$$

$$R: A \rightarrow B$$

$$\text{ფუნქცია: } \begin{array}{c} \text{ყოველ ელემენტს } A\text{-დან} \\ \text{გვა 1 ელემენტი } B\text{-დან} \end{array} \quad \begin{array}{c} \text{თუ } x R x \text{ ას } x R y, \\ \text{მაშინ } x = y \end{array}$$

$$\text{ცოცალები: } \begin{array}{c} \text{ყოველ ელემენტს } A\text{-დან} \\ \text{გან 1 ელემენტი } B\text{-დან} \end{array} \quad \begin{array}{c} \leftarrow \forall x \exists y : x R y \end{array}$$

$$\text{სუბსტიტუცია: } \begin{array}{c} \text{ყოველ ელემენტს } B\text{-დან} \\ \text{გან 1 ელემენტი } A\text{-დან} \end{array} \quad \begin{array}{c} \leftarrow \forall y \exists x : x R y \end{array}$$

ARB

$$\text{ინექსიონი: } \begin{array}{c} \text{ყოველ ელემენტს } B\text{-დან} \\ \text{გან 1 ელემენტი } A\text{-დან} \end{array} \quad \begin{array}{c} \rightarrow \text{თუ } x R z \text{ ას } y R z, \\ \text{მაშინ } x = y \end{array}$$

$$\begin{array}{c} \downarrow \\ \text{თუ } f(x) = f(y), \text{ მაშინ} \\ x = y \end{array}$$

$$\text{შიგწილები: } \text{ოთხივე თვისება}$$

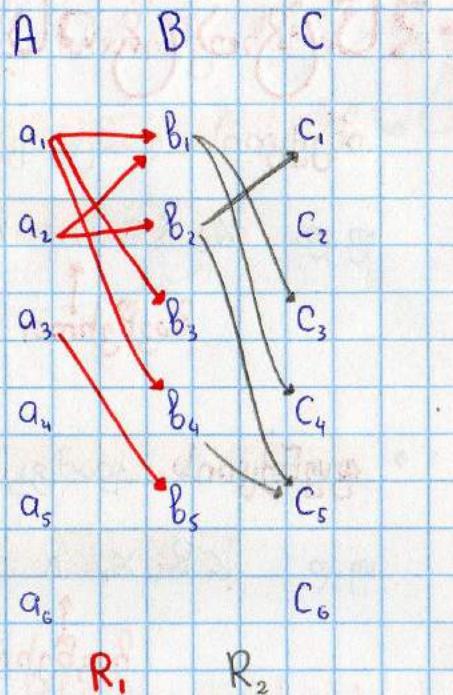
(უხოლუესაობის შესტანისას)

def.  $R_1: A \rightarrow B$   $R_2: B \rightarrow C$

$(R_2 \circ R_1): A \rightarrow C$

★  $\times (R_2 \circ R_1) y =$

★  $\exists z \in B: (x R_1 z) \wedge (z R_2 y)$



•  $R_1 = R_2 \quad \forall x, y: x R_1 y \Leftrightarrow x R_2 y$

•  $x R y$  անձնութեան

$R^{-1}: B \rightarrow A \longrightarrow R: A \rightarrow B$

$\begin{cases} x R^{-1} y \text{ այն ըստ ու մերժութեան} \\ y R x \end{cases}$

$x = f^{-1}(y) \Leftrightarrow y = f(x)$



## R մուծահուցման ըամբայացման գոյնո

- **Ինյեկտուս** ըամբայացման ուժը զանելաւ R-ու ոնցվածությունը

սյ.թ.  $x_1 R z \wedge x_2 R z \Rightarrow x_1 = x_2$  բամբայացման մեջ  
 հաշնելու մեջ  
 սյ.թ.  $x R z$   
 ոնցվածություն

- **Գոյնելյուս** ըամբայացման

սյ.թ.  $z R_1 x_1 \wedge z R_2 x_2 \Rightarrow x_1 = x_2$   
 հաշնելու մեջ  
 սյ.թ.

- **Խորհրդական** ըամբայացման

սյ.թ.  $\forall y \exists x : x R y$

- **Կորպարական** ըամբայացման

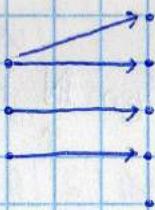
սյ.թ.  $\forall x \exists y : x R y$

# უნისასასო უნი სისტემის სისტემის

- $\exists$  სუბექტის ფუნქცია :  $A \rightarrow B \Leftrightarrow |A| \geq |B|$



- $\exists$  ცოცალების ინკავში :  $A \rightarrow B \Leftrightarrow |A| \leq |B|$



•  $P(N)$  იგნა გოძისა, ხელ  
 $\mathbb{R} [0;1] - \text{ში}$

- $\exists$  შექმნა :  $A \rightarrow B \Leftrightarrow |A| = |B|$

1 თუ  $|A| \geq |B|$ , ვამს  $|B| \leq |A|$

2 თუ  $|A| \leq |B| \wedge |B| \leq |C|$ , ვამს  $|A| \leq |C|$  ეხანდიდებოდა  
 $\geq \qquad \geq \qquad \geq$

3 თუ  $|A| \leq |B| \wedge |A| \geq |B|$ , ვამს  $|A| = |B|$

- |                     |        |
|---------------------|--------|
| • სუბექტის ფუნქცია  | $\geq$ |
| • ცოცალების ინკავში | $\leq$ |
| • შექმნა            | $=$    |

$$\{0, 1, 2, 3, \dots\}$$

$$\{1, 2, 3, \dots\}$$

$$f: \{0, 1, 2, 3, \dots\} \rightarrow \{1, 2, 3, \dots\}$$

$$f(x) = x + 1$$

$$|\{0, 1, 2, 3, \dots\}| = |\{1, 2, 3, \dots\}|$$

↓

$$\bullet |\infty \text{ undezemj} + 1 \text{ jomjbgol}| = |\infty \text{ undezemj}|$$

↓

$$\bullet |\mathbb{N}| = |\text{mengen } N \text{ hofb338ol}| = |\text{mengen } N \text{ hofb338ol}|$$

$$\boxed{f(x) = 2x} \quad \boxed{f(x) = x + 1} \quad \boxed{f(x) = 2x - 1}$$

$$\bullet \text{mengen } |\mathbb{N}| = |\mathbb{Z}|$$

$$0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6$$

$$0 \ -1 \ 1 \ -2 \ 2 \ -3 \ 3$$

$$f(x) = \begin{cases} \text{mengen } x \text{ mengen } f(x) = \frac{x}{2} \\ \text{mengen } x \text{ mengen } f(x) = -\frac{x-1}{2} - 1 \end{cases}$$

თეორემი - თვლიანია ესასწევობა თუ მისი  
სის სისი ჩამნებუ შედეგის

• თუ  $A \{a_0, a_1, a_2, a_3 \dots\}$   $\leftarrow$  თვლიანია

$B \{b_0, b_1, b_2, b_3 \dots\}$   $\leftarrow$  თვლიანია

კანის  $A \cup B \{a_0, B_0, B_1, B_2, \dots\}$   $\leftarrow$  ესას თვლიანია

•  $A \subseteq B \wedge B$ -თვლიანია

$$|B| \leq |N| \quad |A| \leq |B|$$

ესას გადამდებობა

$$|A| \leq |N| \Rightarrow A$$
-ს თვლიანია

// გამოვლენა

$$A_1 \cup A_2 \cup A_3 = (A_1 \cup A_2) \cup A_3 \leftarrow \text{თვლიანია}$$

↓

$$A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n \leftarrow \text{თვლიანია}$$

II პირის სავა თუ ას ესისხიერი სურველის სიმარტვისავის?

$$\begin{aligned}
 A_1 - \text{თვლარი} &= \{ a_{00}, a_{01}, a_{02} \dots \} & \text{ისნა!} \\
 A_2 &= \{ a_{10}, a_{11}, a_{12} \dots \} \\
 A_3 &= \{ a_{20}, a_{21}, a_{22} \dots \} \\
 \vdots & \\
 & a_{30}
 \end{aligned}$$

\* შესრომა იწერს თუ ას პოვინრობები დართვების:

$$\{ \underbrace{a_{00}, a_{01}, a_{02} \dots}_{a_{10}, a_{11}, a_{12} \dots} \}$$

ჩარგან  $\mathbb{N}$  სიძრივლიდან ამოვვენებენ პოვინრები

ლა  $\Rightarrow$  შემდეგ პოვინრები  $(a_{10}, \dots)$  ვერა კარავნომაზო

\* იმავე შესრომა ჩვეულები თუ ვერცხლისა  
ჩვინების კარანტინი.

- სწორი გზი დაგვასრულებით კარანტინი იწერს

- შათვლადობის დაძლევისა  $\rightarrow$  საწ. დაშვებით

$$\exists f: \mathbb{N} \rightarrow K \quad (\text{სუბჟექტები})$$

↑  
სუბჟექტი სიძრივე

- ឧ.ប.  $[0, 1]$  ជាពួរាយនៃ ឲ្យតាមករណី

пог. 6.6.  $|\{0,1\}| = |\mathbb{N}| \rightarrow \exists f: \mathbb{N} \rightarrow \{0,1\}$   $f$  - фнк. фнкцнс.

$$f(0) = x_0 = 0, x_{00}, x_{01}, x_{02}, \dots$$

$y \neq x_0, y \neq x_1, \dots$

三

$$f(1) = x_1 = 0, x_{10} \text{ (circled)} x_{11} x_{12} \dots$$

yz in Singhra and Sengar

$$f(2) = x_2 = 0, x_{20} x_{21} x_{22} \dots$$

## • f the brightness

10

f  $\downarrow$  shows Nottingham

ახლა უნდა დავძლევით, ხოდ ჩამონავალში

sh shob homog y

$$y = 0, y_3 y_2 y_3 \dots$$

5)  $y_1 = 3x_0$   $x_{00} \leftarrow (\text{hadj bb3}) \text{ objen hajgb3o obj, hmd}$

$$\hat{y} \neq x_0$$

$$|y_i - x_0| \geq 2$$

$$2) \quad y_2 = \sin x_1$$

1

$$y \neq x,$$

$$\text{högejöd } \text{välj } |y_1 - x_0| = 1$$

ոժելի թշնամունք, իմաց կամ  $y = x$ .

333.

$$3) \quad y_3 = 5h_5 \quad x_{22}$$

$$x_0 = 0,38999\dots$$

11

$$y \neq x_2$$

$$x_0 = y$$

ԽԱՏԱԿԻԽՐԱՄ ԽՈԺԱՅՐԱՐԱՐՈՒՅՆ 2

Խճիչը ու դժվաճիչը պահպանում են առաջարկերը և առաջարկերը պահպանում են խճիչը և դժվաճիչը:

$$\text{Ex. } P(\mathbb{N}) = \{ \emptyset, \{1, 2, 3\}, \dots, \text{empty set}, \text{big empty set}, \dots \}$$

ગુણ. •  $|N| \geq |P(N)|$  સભ્ય

ဗု.ပု. ၁၇ အဲလွှာလွှာများ  $f: \mathbb{N} \rightarrow P(\mathbb{N})$  :  $f$  လွှာလွှာများကို အကြောင်းပြု

~~пог. вв.~~  $f: \mathbb{N} \rightarrow P(\mathbb{N}) \leftarrow \text{bigbigfizognomus}$

$$* S = \{0, 3, 4\} \rightarrow T \quad F \quad F \quad T \quad T \quad F \dots$$

$S \in P(\mathbb{N})$        $S \in 0$      $S \in 1$      $S \in 2$      $S \in 3$      $S \in 4$      $S \in 5$

$$f(0) = \{0, 3, 4\} \rightarrow \text{TTFTTF...}$$

$$f(1) = \{0, 2, 4, 6, \dots\} \rightarrow \text{TF}\textcircled{T}\text{FTF\dots}$$

$$f(2) = \{1, 3, 5, 7, \dots\} \rightarrow \text{FTFTFT\dots}$$

Եղ. լո., հմձ սձ ենածո տի Եղիսո յ

$y \leftrightarrow FTT \dots$  ლიაკონსლენგის შეინტენით  $T$ -ს ნაცვლად  
ანგეთ  $F$ -ს და შინიდნით

$$y \neq f(0), f(1) \dots$$

Կ-Ն Բանվայ Շյուդրոյն վայ և անուն անուն

$y \in P(\mathbb{N})$  թա տան Յի բյուրու ու Նորման

$\Rightarrow$  f shoo lighfigemn ~~\*~~  $y = \{x \in \mathbb{N} \mid x \notin f(x)\}$

სტრუქტურული განვითარების სამსახური

თუ  $S \leftarrow$  სიმულირე

$$P(S) = \{x \mid x \subseteq S\}$$

მაგ.  $\{1, 2, 3\} = S$   $|S| = 3$

$$P(S) = \{ \{1\}, \{2\}, \{3\},$$

$$\{1, 2\}, \{1, 3\}, \{2, 3\}$$

$$\{1, 2, 3\}, \emptyset \}$$

$$|P(S)| = 8$$

$|S| < |P(S)|$

მაგ.  $S = \emptyset$  0 კონკრეტული

$$P(S) = \{\emptyset\}$$
 1 კონკრეტული

მაგ.  $\{1\} = S$  1 კონკრეტული

$$\{\emptyset, \{1\}\} = P(S)$$
 2 კონკრეტული

ახლა დავამტკიცოთ, რომ ეს სისტემა  $S$  სიმულირე ბინარულ სისტემაზე მომდევნობს

სისტემაზე მომდევნობს

მეცნ.  $|S| < |P(S)|$  (ესახ.)

ამისთვის გვაძლევთ 2. ჩადას დამტკიცება

①  $|S| \leq |P(S)|$

②  $|S| \geq |P(S)|$

მეცნ. 1.  $f: S \rightarrow P(S)$  ცოდნალური რელაცია

$x$ -ს შემსახუმო  $\{x\}$  ✓

★ սյ. լո. 2

լուզ. և բ.  $f: S \rightarrow P(S)$

աշումուն ույտու յ, հոգյունոյն

$y \in P(S)$  (անյ  $y \subseteq S$ )

\* լու յի յ ժողու ույտու  $x$  յին երջաշրջոյն

հոգյունոյն ժու լիցունուան  $f(x)$ -ի (այս  $f(2) = \{1, 3, 5, 7, \dots\}$ )

$$y = \{x \in S \mid x \notin f(x)\}$$

$$\forall x \in S : y \neq f(x)$$

աշխանուան

- $y$  ժու լուրջիւ ժիյ 1  $x$ -ու  $f$ -ին իւնան
- (անյ  $f$  ժոց լիցիւյսոյ)

լուզ. և բ.  $\exists x_0 : f(x_0) = y$

$$x_0 \in f(x_0) ?$$

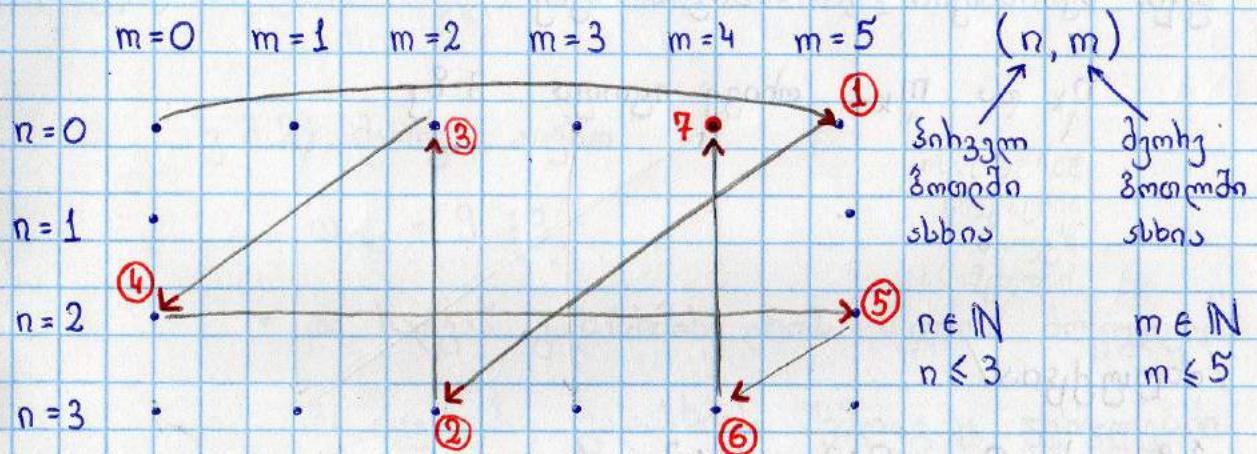
$$3_1) x_0 \in f(x_0) \rightarrow x_0 \notin y \rightarrow x_0 \notin f(x_0) \times$$

$$3_2) x_0 \notin f(x_0) \rightarrow x_0 \in y \rightarrow x_0 \in f(x_0) \times$$

- $|N| < |P(N)| < |P(P(N))| < \dots$

# ინდუსტრიალური

უ. 3ლ-იანი და 5ლ-იანი ფერებით 4 ლ-ის მიღება



- მაგ წერეთ მა განვითარებული, ხადან ვართხა/უვერა/რაოგა

ორგანიზით ენა-ენა შორის არც არ ხდეთ სავა ან  
უარესი უნდა იყოს, ან ამ წერეთ მასვერა მეტადონია

- ამასთან შევიძლოა ...

- ლიკონალბერ კარასხა ერთანაგეთში
- ვესტიკალბერ უაღუშეს წერეთში
- შოტლანდიალბერ უაღუშეს წერეთში

- შეიძლება თუ ას ნე-იანი და გე-იანი ჯერებით  
4 ლიტრის მიღება ?

უ.ლ. ნებისმიერი  $k$  ნაზისტის შეხე (გარამება / ივნება / დაღვეული)

$n_k$  და  $m_k$  მნიშვნელოვანი სამართლის  
შეხების  
ასეულობის  
მიღების  
სიმრავლის

/ინდუქცია/

შეზღუდვა:  $k=0$   $0:3$   $0:3$  ✓

ნაზისტი: დამკვება  $n_k:3$   $m_k:3$

უ.ლ.  $n_{k+1}:3$   $m_{k+1}:3$

3.1) ავსება  $\rightarrow$  გ.პ. ვაკუუმი აქტივული  $n_{k+1} = n_k:3$

$$m_{k+1} = 9:3$$

3.2) დაცვა  $\rightarrow$  გ.პ. ვაკუუმი აქტივული  $n_{k+1} = n_k:3$

$$m_{k+1} = 0:3$$

### 3.3) გარასება

გ.გ. პირველი გარასები

3.3.1) პირველი დაივალი:  $n_{k+1} = 0 : 3$

$$m_{k+1} = n_k + m_k : 3$$

3.3.2) მეორე აუცხმა

$$m_{k+1} = 9 : 3$$

- და ხარგან გარასების ქმნას წყლის მოსახლეობა  
ან იცვლება გარასების შემდეგაც ჯეხფლება  
ისევ  $n_k + m_k$  ლიტრი იტენის

↓

$$n_{k+1} = n_k + m_k - 9 : 3$$

$\Rightarrow$  4 სტ იყოფა 3-ზე ან 6 და 9 ლ-იანი ჯეხფლებით  
მეეძღვებელის 4-ის მიღება ✓

გაუნდებულება 7 ფლეხლით იქნა

# ნაბილობის ლალაგება

იტვე

- პინაჩული მიმსახურის

მიმსახურების ხასიათების შემდეგი თვისებებით:

/\*  $R: A \rightarrow A$  (domain = codomain) \*/

ჩატარებულობა:  $\forall a : aRa$

კი:  $=$ ;  $\leq$ ;  $\subseteq$

შა:  $<$ ;  $f(x) = x^2$   $f: \mathbb{R} \rightarrow \mathbb{R}$   $\forall a : a (f(a) = a^2) a^2$

$a \neq a^2$  ✗

გრანგიცულობა:  $\forall a, b, c : aRb \wedge bRc \Rightarrow aRc$

კი:  $\leq$ ;  $<$

შა:  $\neq$

სიძეგების ლალაგება:  $\forall a, b : aRb \Rightarrow bRa$

კი:  $=$ ;  $a, b$ -ს 2-ე გაყოფის ნაშთი ეხონას.

შა:  $\leq$ ;  $<$

ანგუსტეგების ლალაგება:  $\forall a, b (სადაც a \neq b) : aRb \Rightarrow \neg(bRa)$

კი:  $<$ ;  $\leq$  (იმისადაც  $=$  ვერ სიძეგების ვრცელობს, სადაც  $a \neq b$ )

შა:  $a, b$ -ს 2-ე გაყოფის ნაშთი ეხონას.

ასიძეგების ლალაგება:  $\forall a, b : aRb \Rightarrow \neg(bRa)$

კი:  $<$

შა:  $\leq$ ,  $a, b$  2-ე გაყოფის ნაშთი ეხონას.

- $R$  - ასიმეტრიული  $\Rightarrow R$  - ანტისიმეტრიული
- ↑  
უფრო ძლიერი

$R$  - ნაწილობრივი დალაგება (სუსკია/ძრუება/სიგრძეა თუ ...)

- **სუსკია:** თუ  $a \leq b$ ,  $a = b$ ,  $a > b$
  - **ძლიერი:** თუ  $a < b$ ,  $a = b$ ,  $a > b$
- $\rightarrow ( <, \leq, \geq, \geq, a:b )$

$\mathbb{N}$ -ზე

მიმართება

- ნაწილობრივი დალაგება, ხოდელსაც მხო განსხვავებული  
ელემენტის ერთანანერთან შედგება შესაბამის კრიტერიუმები

$\forall a, b (a \neq b) : aRb \vee bRa$

**ყო:**  $\leq, \geq, <, >$

**ახა:**  $a \neq b : R$ -ზე

- ექვივილინგუსტის პირადება: თუ  $aRb$ ,  $bRa$

დაგ. ( $=$ ,  $R : \mathbb{Z} \rightarrow \mathbb{Z}$  ( $a$ -ს და  $b$ -ს ერთნაირი მხები გაყოფის ნაშთი აქვა))

ზოგადობა

ექვივილინგუსტის კრიტერიუმი

- $aRb \Leftrightarrow$  თუ  $a-b$  და  $b-a$  ერთნაირი [ჩატარებული] აქვა

- სუსტი ნაწილობრივი დალაგვების შეზენებულები ს.ნ.გ.
- ძალი ნაწილობრივი დალაგვების შეზენებულები გ.ნ.გ.

### • ექვივალენტობის ცოდნა

თუ გვაქვს სარაც ექვივალენტობის მიმართება. მასთან  
ეს სიტყვა, ხომალი განსაზღვრულია ექვივალენტობის  
მიმართება შევიძლის ნაჩროვილით ხოვთხა ჩვეფება. (ცოდნებად)  
დაყოფილია.

**ექვივალენტობის მიმართება** გვევმოწვევ ეს მთელი ელემენტი  
(ხომალი მონისაც ასეს მიმართება) ასეს ასე ასე  
ესი და იგივე ჩვეფში

a-ს ექვივალენტობის ჯგუფი (ცოდნა) ([a])

შეს ყველა ის ელემენტი, ხომალისაც ერთადა ეს

a ელემენტი ან ყველა ის ელემენტი ხომალის a-სთან

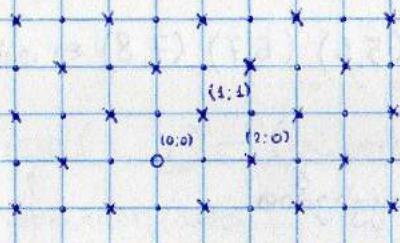
R მიმართებაში ასეს განსაზღვრული

$$[a] = \{x \mid xRa\}$$

ინგლისის მიერ გაგებულია

შევვიდლის 4 ნაზი მძღვანელი:

- 1) 
  - 2) 
  - 3) 
  - 4) 



$$\text{კონტროლის მიზანი: } x+y:2$$

$$\text{点 } B_0 : \quad x = 0 \quad y = 0$$

$$0+0=0:2$$

ນົບແລ້ວ ດີວ່າວ່າ  $x_k + y_k = 2$

$k+1 - j$  گویان:

$$3_s) (+2; +0) = x_{k+1} + y_{k+1} = \underbrace{x_k + y_k}_{:2} + 2 \Rightarrow :2$$

$$3_2) (-2; +0) = x_{k+1} + y_{k+1} = \overbrace{x_k + y_k} - 2 \Rightarrow :2$$

$$3) \quad (+1; +1) = x_{k+1} + y_{k+1} = x_k + y_k + 2 : 2$$

$$3_4) (-1; -1) = x_{k+1} + y_{k+1} = x_k + y_k - 2 : 2$$

1	2	3
4	5	6
7	8	

შესაძლებელია თუ ან ამ მხს აღიღონ გავისვალოთ

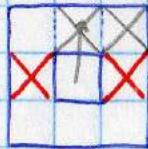
$(1,2) (2,3) (3,4) (4,5) (5,6) (6,7) (7,8) \leftarrow$  თანმიმდევრული წყვილები

3<sub>1</sub>) ჰონიგონფარების გაფარებით

წყვილები ას დასრულება

3<sub>2</sub>) ვაჩვილების გაფარებით

2 ასანის წყვილი წერძობება



⇓

შეძლებელის ძხოვი 7-ს და 8-ს გავისვალოთ აღიღები

# ԵՅԼՈՐԵՐ ԱՐՅՈՒՆՈՒԹՅՈՒՆ ՈՆՉՈՒՅՆԱԿԱՐԱ Մ.Լ.Յ.

ԱՅԱԼՈՐԵՐ ԱՐՅՈՒՆՈՒԹՅՈՒՆ ՄԱՏԱԲԱՐ

$a \in \mathbb{N}$   $b \in \mathbb{N}$  (e.g.  $a \geq b$ )

$$x_0 = a \quad y_0 = b$$

$$x_1 = y_0 \quad y_1 = \text{rem}(x_0, y_0) \rightarrow (x_0 \bmod y_0)$$

↑  
remainder (հանուն)

$x_0 - ab$   $y_0$ -ից ջայուղուն համեմ

$$x_2 = y_1 \quad y_2 = \text{rem}(x_1, y_1)$$

⋮

$$x_n = y_{n-1} \quad y_n = \text{rem}(x_{n-1}, y_{n-1})$$

⋮

$$x_k = y_{k-1} \quad y_k = 0 \quad \text{rem}(x_{k-1}, y_{k-1})$$

մ.լ.յ. (a, b)

$$y_n = x_{n-1} - q_{n-1} y_{n-1} \quad q_{n-1} \in \mathbb{N}$$

• ՈՆՉՈՒՅՆԱԿԱՐԱ:  $\text{մ.լ.յ.}(x_0, y_0) = \text{մ.լ.յ.}(a, b)$

մեջյան

• ՀԱՅՈՒ:  $n=0 \quad x_0 = a \quad y_0 = b$

$\text{մ.լ.յ.}(x_0, y_0) = \text{մ.լ.յ.}(a, b) \checkmark$

- ## • សោរោចោះ

podzjazd: g.b.z.  $(x_m, y_m)$  = g.b.z.  $(a, b)$

$$\text{vgl. } \text{P.} : \text{vgl. b. g. } (x_{m+1}, y_{m+1}) = \text{g. b. g. } (a, b)$$

აპის დასამცემებლად ვაძლევებ

$$\text{vgl. b. z. } (x_{m+1}, y_{m+1}) = \text{vgl. b. z. } (x_m, y_m)$$

$$1) \text{ wj. po. } x_m : g \wedge y_m : g \Rightarrow x_{m+1} : g \wedge y_{m+1} : g$$

$$1. \quad x_{m+1} = y_m \quad (\text{yebuqnu} : g) \quad \checkmark$$

$$2. y_{m+1} = \text{rem}(x_m, y_m) = \underbrace{x_m - q_{m+1} y_m}_{\substack{\vdots g \\ \hline}} \quad (q_{m+1} \in \mathbb{N})$$

$$2) \text{ vgl. } X_{m+1} : g \wedge y_{m+1} : g \Rightarrow X_m : g \wedge y_m : g$$

$$1. y_m = x_{m+1} : g \quad \checkmark$$

$$2. \quad x_m = q_m \cdot \underbrace{y_m}_{\stackrel{\div g}{\downarrow}} + \underbrace{y_{m+1}}_{\stackrel{\div g}{\downarrow}}$$

$$x_m = 9 \quad \checkmark$$

- 1) ပုံ 2) ပုံပါ ပုံပါနေရာတွေဟာ ပုံပါ  $(x_m, y_m)$ -၏ ပို့မှတ်များ

Ճշհաշընյան =  $(x_{m+1}, y_{m+1})$ -ներ եղիում ճշհաշընյան  $\Rightarrow$

$$\text{w.l.o.g. } (x_m, y_m) = \text{g.l.g. } (x_{m+s}, y_{m+s})$$

- Ծավալքային, իմաց լամազման համար (հայ 0-ը թի)

Ճ. 1783 314

← մասնաւոր կողմանը (rem (1783, 314))

- Մ. Ծավալքային

$$\text{յ. լ. զ. } (x_k, 0) = \text{յ. լ. զ. } (a, b)$$

համայնքում 0-ներ յ. լ. զ. տարածություն ու առաջանակ 0 կազմություն ունեցած

$$\text{յ. լ. զ. } (x_k, 0) = x_k$$

$$x_k = \text{յ. լ. զ. } (a, b)$$

# სცაბილური ლანგვილება

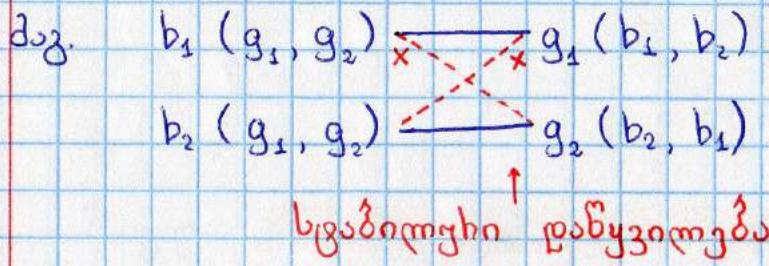
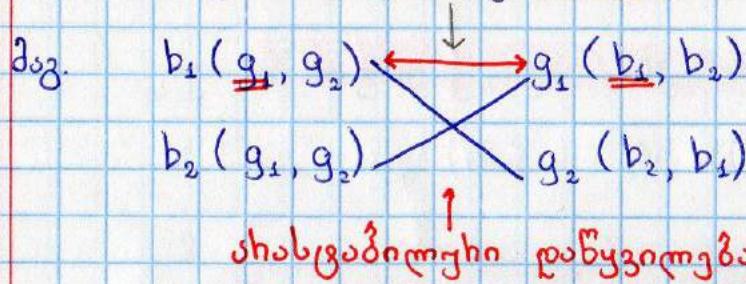
სცაბილურის ლანგვილება თუ ას გავვაჩნია

- ახასცაბილური ნუკლი

თუ ავილებთ 2 ახადაქონინებელ ადამიანს და

მათ ონიველს თავის სახეცნომს ესჩვენის ესაძანევი

მაშინ ეს ახასცაბილური ნუკლია.



- სცაბილური ლანგვილების ესო-ესო აღვარითი

- სცაბილური
- 1. შეთავაზებები
  - 2. ფასები
  - 3. დამთავრების მემორიები

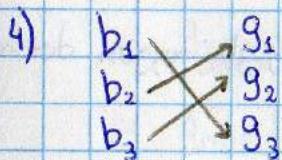
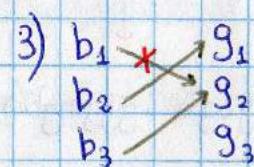
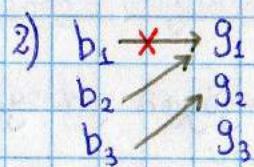
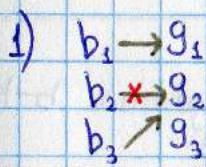
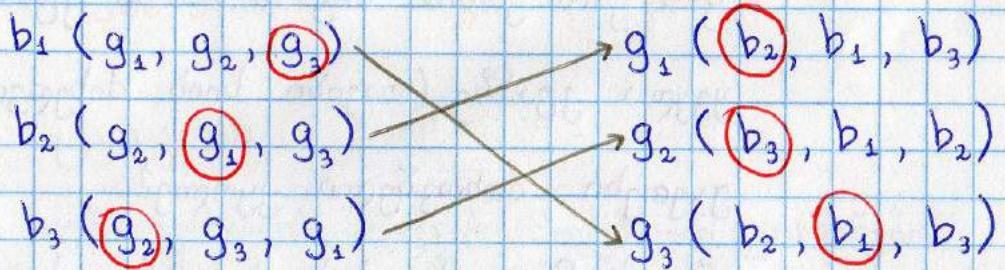
1) შეთავაზებული - ყველა შიფრი სთავაზობს მის სიაში ყველაზე მაღლა მყოფ გოგოს.

2) ფუქული - სიაში ყველაზე მაღლა მყოფი შიფრის გახდა თითო გოგო ყველა სხვა მოხოვნელს ეფუძნება კაშს.

ფუქულის შემდეგ შიფრი ამ გოგოს შემს სიირან.

3) ღამთავაზული - თუ ყველა გოგოსთან ამ ეფაზზე გაფართოება 1 მოხოვნელი მივიღა

ასკ.



დავაძლევილოთ, რომ ის ალგორითმი გავალებს  
სიგანგილეების დაწყვილებას  
ანუ

უ.დ. ჩოდ ან ასებობს ასასერილებელი წყვილი

უ.დ.  $b \geq g$  ან იქნება ასასერილებელი

თუ 1)  $b$  ან ძისლია  $g$ -სთან  $\rightarrow g$  უფრო დაბროა

$b$ -ს სიამი ვიზუალური  $g$  (ვისთანაც დაწყვილდა)

ანუ  $b \geq g$  ან ასე ასასერილებელი წყვილი.

თუ 2)  $b$  ძივიდა  $g$ -სთან და გილო ექი  $\rightarrow$  თუ გოგო

$g$ -მ ექი ერთხა გადა  $b$ -ს. ამ კვანძის აქტი

ყველა კვანძზე (თავისი სის მიხედვით)

ექი ერთხა მოხვენელი კუოლება.

ანუ  $b \geq g$  ან ასე ასასერილებელი წყვილი

↓

საბაზო : შეავს კუთხის მოხვენელი და ექი ერთხა  $b$ -ს

ინდ.ნაზ : დამკვება -  $k$  ნაბიჯის აქტ შეავს  $b_k \geq b$  მოხვენელი

$b_{k+1} \geq b_k > b \Rightarrow k+1$ -ი. ნაბიჯის შეავს კუთხის მოხვენელი

1) და 2) დან გამომდინარე დაწყვილებას სიგანგილეს

ალგორითმის მიხედვით ქონინება  
ონცდალურია იძისთვის ვინე სოავაზობს  
ად შემთხვევაში ბიუტისთვის

რას ნიშნავს ონცდალური ?

ავილოთ ვინდე  $b_i$ , რომლის სია შემდეგნაირია

$b_i (g_1, \textcircled{g_2}, g_3, \textcircled{g_4}, g_5, \textcircled{g_6}, \textcircled{g_7}, g_8, g_9)$

○ ← დანცვილების ვარიაციები სცადილება დანცვილებები  
ჩვენი ალგორითმით თუ შეკარგვაზ სცადილება

დანცვილების  $b_i$  დანცვილდება ○ ვარიაციებს  
შორის ხდება თავსთან ანუ -  $\textcircled{g_2}$  - თან

დავაძლვა იმისთვის

უკა რომ ალგორითმის შედეგად მოღებული ქონინების  
სიმაღლე ონცდალურის ბიუტისთვის, ანუ

• თუ (რომ ალგორითმი სცადილება ფონინებით საშავლე M-ში)

ბიუტ B-ს შედეგი შეულებელი A, მაშინ ჩვეულოს

შედეგად მოღებულ ფონინებით სიმაღლეში

გასი შეულებელი A ან უკავშირი.

უ. ლ. თუ მ-ში  $B \xrightarrow{\text{სიგამ.}} A$   
 გამო აღვ. ში  $B \xrightarrow{\text{სიგამ.}} A' \mid A' \geq A$

მაგ. სასწავლა

↓

B აოგოსთან შედეგი დაწყვილია ციტუაცია

A გრჩების

$B(A' < A) \xrightarrow{g'} A'$

$b \quad g' < g$

$\xrightarrow{g}$

$\xrightarrow{h}$

$B'(A' < A) \xrightarrow{g} A(B' > B)$

$b' > b \quad g' > g$

$\xrightarrow{h}$

$\xrightarrow{g}$

A-ს უნდა ექვემდებარდეს ეს გადასახადის მიზანით  
 ამავე გადასახადის მიზანით გადასახადის მიზანით  
 A-ს უნდა ექვემდებარდეს ეს გადასახადის მიზანით  
 ამავე გადასახადის მიზანით გადასახადის მიზანით  
 A(B' > B)-ს უნდა ექვემდებარდეს ეს გადასახადის მიზანით  
 B'(A > A'), რომ B' და B-ს  
 გრჩების მიზანით გადასახადის მიზანით გადასახადის მიზანით  
 გრჩების მიზანით გადასახადის მიზანით გრჩების მიზანით

M-ში სა გადასახადი არ იმართდა

$B(A > A') \xrightarrow{+} A(B' > B)$   
 $B'(A > A') \xrightarrow{g} A'$

შესრულებული ნიუკო ≠

ବନ୍ଦାପ୍ରଦୀପ

## მიმართული გრაფები

Հոմանական  $R: A \rightarrow A$ -ին պահանջվում է այսպիսի շատություն, որը պահպան է առանձին աշխատանքների համար:

$$V = A \quad \text{Външната обхватът}$$

$$E = \{ (a, b) \mid aRb \} \quad \text{Enðumjölni} \quad \text{Viðhægumjölni}$$

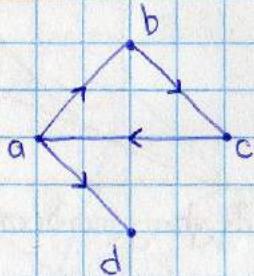
285

$a_0 a_1 a_2 \dots a_{k-1}$  shub 260 only

or any  $(a_0, a_1) \in E \wedge (a_1, a_2) \in E \wedge \dots \wedge (a_{k-2}, a_{k-1}) \in E$

զօնել Եղիշեցի = Բանյօնել հորթ. = Եցյեռյօնել հորթ. - 1

Ճիշտություն չէ: Եզրակացնելու առաջնային նպատակը



abcd sh shh shhgozo gzo

յուն: ցնու ա<sub>0</sub>, ա<sub>1</sub>, ..., ա<sub>k-1</sub> եւըցի ա<sub>0</sub> = ա<sub>k-1</sub>

Առյուծ Տօղիդյ: Թոթոցներ հարցվենք

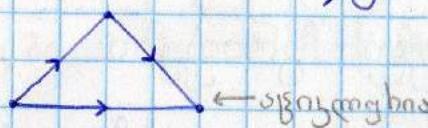
ასტროგრაფიული ფორმი:  $(a_0 \equiv a_{k-1}) - \text{ის კართველობის მინიმუმი}$

## ગુરુજીની પ્રેરણો

- 0 სუბჰანს გზა თავის თავის
  - 1 სუბჰანს გზა თავის თავის
  - b 0 სუბჰანს გზა
  - b b 1 სუბჰანს გზა
  - b b b ... (ცეკვისას)

**აციკლური:** ძიდშითული გხაფი, ხოდელის ან 83 ქვე

$\rightarrow 0$  სიგრძის ძალით ციკლები



• თუ  $R$  აზის მუცელი ნაწილობრივი დარაგება, მაშინ

$R$ -ის შესაბამისი გხაფი აზის აციკლური  
დაგამცემით.

სამ. გვიძლე პირველი ციკლი  $a_0, a_1, \dots, a_{k-1}, a_0$   
 $\text{სიგრძე} > 0$

$$E = \{(a, b) \mid a R b\}$$

$$(a_0, a_1) \in E \rightarrow a_0 R a_1$$

$$(a_1, a_2) \in E \rightarrow a_1 R a_2$$

$$(a_2, a_3) \in E \rightarrow a_2 R a_3$$

⋮

$$(a_{k-1}, a_0) \in E \rightarrow a_{k-1} R a_0$$

გრაფიკი.

$a_0 R a_1$

$a_1 R a_2$

$a_2 R a_3$

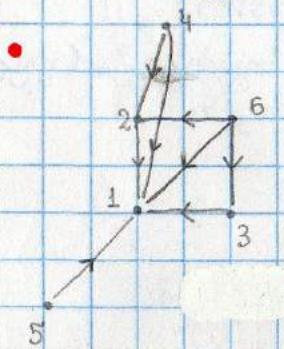
$a_{k-1} R a_0$

ანგილიური გრაფიკი არ არის.

$a_{k-1} \neq a_0$

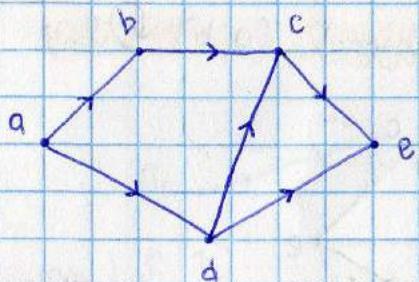
პ. 3.  $\{1, 2, 3, 4, 5, 6\}$  - ში გაყოფილი (R)

$aRb$  ან  $a:b \wedge a \neq b$



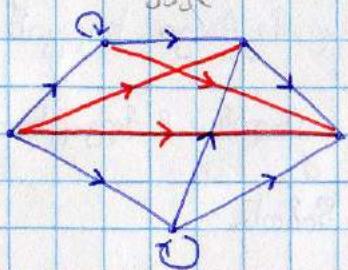
კვლების ნიშნული

- D - პირისაული გრაფი



პ. 5. ღ.

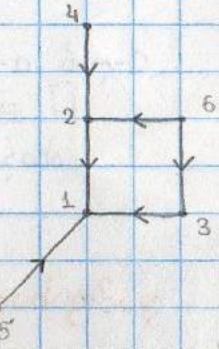
- $D^*$  - ერთეული გრაფის პირისაული  
კვლები, ნიშნ D-დან +



- $aD^*b$  ან  $D$ -ში  $a$ -დან  $b$ -მდე კვლები  $> 0$  საგრძლეო გრაფი

$b$  0 საგრძლეო გრაფი

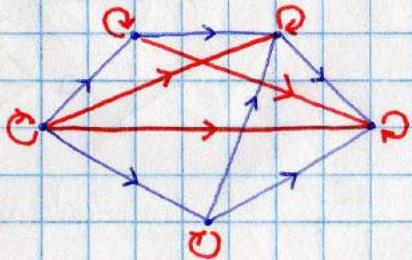
$b$  1 საგრძლეო გრაფი



6. 5. ღ.

- $D^*$  - გრაფის პირისაული

- $aD^*b$  ან  $D$ -ში  $a$ -დან  $b$ -მდე კვლები, ნიშნ D-დან +



$D^*$  - ხელოვანები

$D^*$  - გრაფის პირისაული

$D^*$  - გრაფის პირისაული

თუ  $D$  უკლესია, მაშინ  $D^*$  ასიმეტრიულია

დამცველი ტერმინი კვლები

დამტკიცება: დავ. სამ. •  $D$ - აქილეგისა და  $D^+$  შეა ასიმულებოთ

$$aD^+b \downarrow \quad \uparrow bD^+a$$

ა-დან  $a$ -მდე კვადრატული დარებითი სიტყვის გვა (ყვიცო)

შეა აქილეგი \*

/\* cover( $D$ ) დამტახვი გხაფი \*/

დამტახვი ნიში - ნიში, ხომლის გვილავ აუკირდებელია

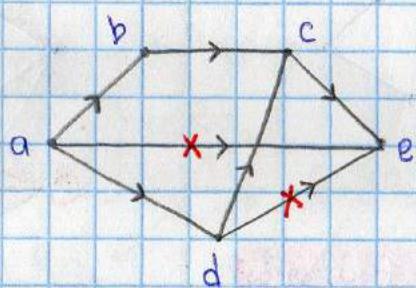
ასეთ /\* \*/

( $a, b$ ) შის დამტახვი თუ  $a$ -დან  $b$ -მდე

კვერაზე გრძელია

ყველა გვა გაიკვით (ა, ბ) ნიშის

გნეში დავცოდოთ



მაგ. (ა, ე) მა შის დამტახვი ჩარგან

შესაბამის ისეთი გვა ა-დან ე-მდე, ხომლის

მა გაიკვით (ა, ე) ნიშის.

•  $D$ -ს დამტახვი გხაფი შის დამტახვი ნიშიერისგან

მეტადან გხაფი.

սահմանա այլ. (cover(D))<sup>+</sup> = D<sup>+</sup> այս է պայմանական

$$1) (\text{cover}(D))^+ \subseteq D^+$$

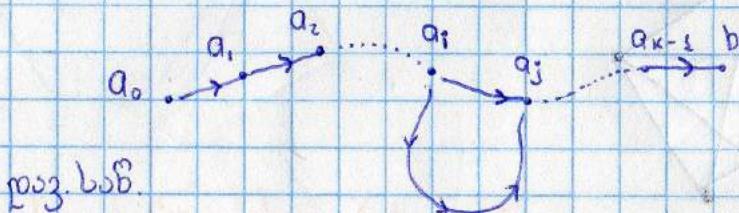
ուղարկած համ:  $\text{cover}(D) \subseteq D$

$$2) \text{այլ. } D^+ \subseteq (\text{cover}(D))^+$$

այս յ.թ. ուղ ա-բան բ-ձբյ ժիշտ չեն զիս Ռ-ին

Ճշնո՞ւ ॥————॥ ժիշտ չեն զիս cover(D)-ինց

- աշուրու պայմանա չհայտն չեն ա-բան բ-ձբյ



(a<sub>i</sub>; a<sub>j</sub>) նինմ ժիշտ ուժգուշացն

այս ժիշգոմն յային չհայտն չեն a<sub>i</sub> սան a<sub>j</sub> թեյ

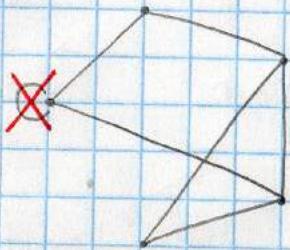
॥

a<sub>0</sub>...b ժիշտ պայմանա պայմանա չհայտն չեն \*

• \*

aR<sup>+</sup>b  $\Leftrightarrow$  R-ին  $\exists$  n ենթակա չեն ա-բան բ-ձբյ

ଅନୁମିତିମାନତତ୍ତ୍ଵବ୍ଦୀ ପାଠ୍ୟକ୍ରମିକ



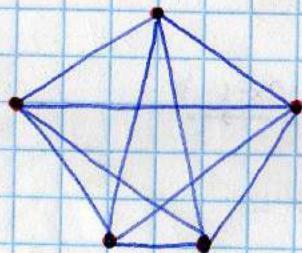
## V - Ծայրագծը եղիքը

$E = \{ \{a, b\} - \text{მა კლემნტების სიმსაცვევები } V-\text{ის } \}$

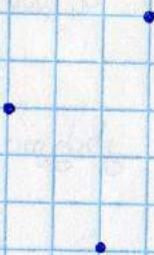
Համակարգը շեղացնեն նույզիններ  
Ցնուցնելու համար տեղ (a, b) (b, a)  
Անշարժական, անմասնական յու հույներուն  
Տեղական առաջնահանձնութեան  $\{a, b\} = \{b, a\}$

- $\{a, a\} = \{a\} \Rightarrow$   
 $\Rightarrow$  1 յայդյանան ենթազույց  $\Rightarrow$   
 $\Rightarrow$  տ ժառ ենթազույց

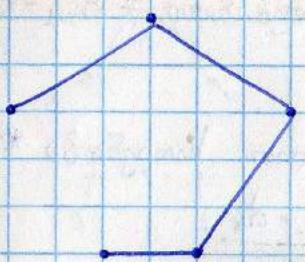
- $K_n$  完全圖 (complete graph)



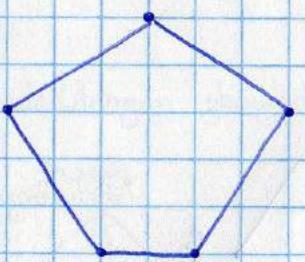
- $E_n$  յշեցըն զիւց (empty graph)



- $L_n$  ხაზოვანი გხაფი

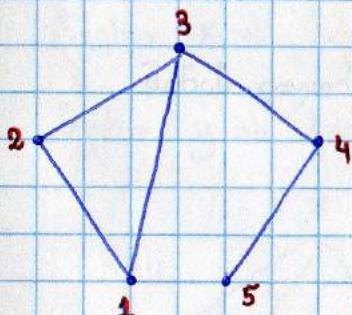


- $C_n$  წხიული გხაფი (ყიული გხაფი)



ნუკუნოს ხარისხი (degree)

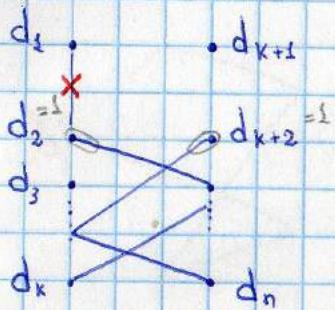
- $d$  = ნუკუნოს გუბობლების საორენობა



$$d_1 = 2 \quad d_2 = 2 \quad d_3 = 3 \quad d_4 = 2 \quad d_5 = 1$$

$$* d_1 + d_2 + d_3 + \dots + d_n = 2 \cdot \text{ნუკუნოს ხარი}$$

## bipartite graph



$$d_1 + d_2 + \dots + d_k = \text{ნიმუშის ხარჯი} = d_{k+1} + d_{k+2} + \dots + d_n$$

/\* აქობრების საშუალო ხარჯის გადასახვა \*/

$$\text{გადასახვა} = \frac{d_1 + d_2 + \dots + d_k}{k}$$

$$\text{გადასახვა} = \frac{d_{k+1} + d_{k+2} + \dots + d_n}{n-k}$$

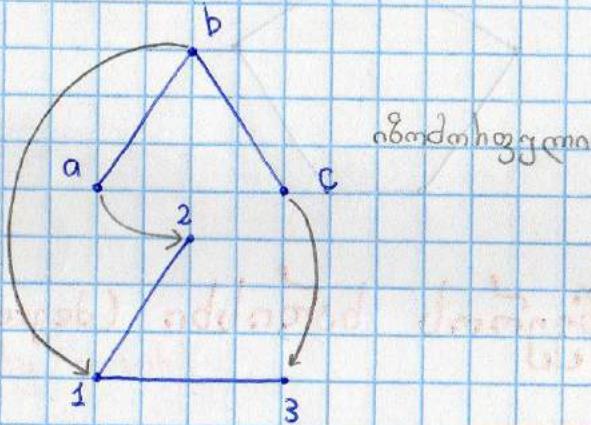
## იზომობრიგი

$$V_1 = \{a, b, c\}$$

$$E_1 = \{\{a, b\}, \{b, c\}\}$$

$$V_2 = \{1, 2, 3\}$$

$$E_2 = \{\{1, 2\}, \{1, 3\}\}$$



იზომობრიგი:  $f: V_1 \rightarrow V_2$  (ზოგჯერ)

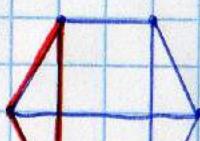
სარაფ  $(a, b) \in E_1$  განსაზღვრული მარჩენი

ორი  $(f(a), f(b)) \in E_2$

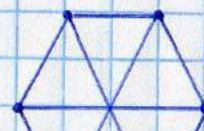
როგორ გვაძლევთ  $\forall$  იზომობრიგის

1. მეცნიერებლის წვერის ხარისხი  $= d$  (ორ მატებვების შესახვა)

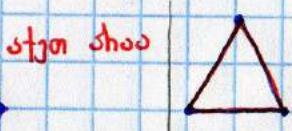
2. ციფრების



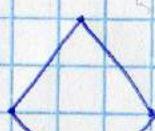
ორგება



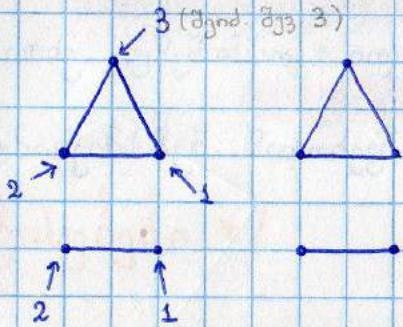
ხარისხი ცოდნის



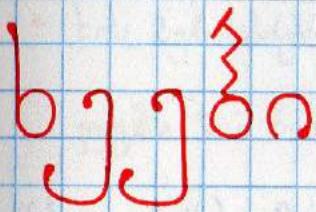
1  
1  
1



- გხაფების ძრის შეიძლება ჩატრენირებაზე იზომონიზმი დამყარება

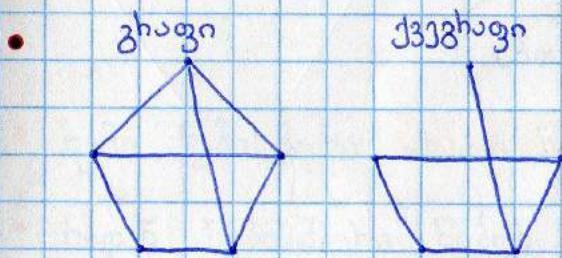


$$2 \cdot 3 \cdot 1 \cdot 2 \cdot 1 = 12 \text{ ნური იზომონიზმი}$$

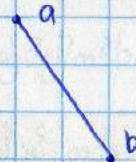


- მასივი გზა - თუ წვერები არ მეტყველება
- მასივის ყველი თუ
- დაღვენითი სიგრძესა
- არ ყველებს ასეთი წვერის ან წიბოს მასში ან მკლება

- ახალი გრაფი მასივი ყველი მინიჭებ 3 სიგრძის ცვლის.



•

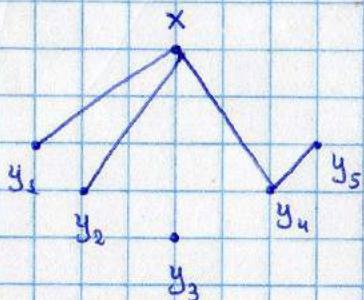


aba არ შეს მასივი ყველი, ჩატრენიზმის წიბოს იდენტური

### გრაფობი

წვერი  $x$ -ის გრაფი ყომანები  $C(x)$  არის ყველი ისეთი

წვერი  $y$ -ის სიტყვის ჩოტლადოვა  $x$ -ის შემთხვევაში გზა.



$$C(x) = \{y_1, y_2, y_4, y_5\}$$

- გხაფს ენორება **გმელი** თუ ის გთი გმელი კომპონენტის გადასაცემა. [ანუ ყველა წვერის გმელი კომპონენტი გთი და იგივეა.] [**გმელ გხაფებში ნებისმიერი წვერისან ნებისმიერი არის ასევე გმელის გზა.**]
- გხაფს ენორება **K-მაგარ გმელი** თუ ის ნებისმიერი  $K-1$  წილის ნაძლის შემთხვევა გმელი არის.   
  $\Downarrow$    
 ▶ ნებისმიერ 2 წერილს შორის ასევე გმელის  $K$  გზა ( $K$ -მაგარ გმელი)

**K** - გმელი კომპონენტის სიტოვნობა

$n = |V|$  - წვერის სიოდენობა

$m = |E|$  - წილის სიოდენობა

**C** - ყიკლების სიოდენობა

- |          |  |
|----------|--|
| <b>★</b> | <b>①</b> $K \geq n-m \Rightarrow m \geq n-K$ |
| <b>★</b> | <b>②</b> $C \geq K - (n-m)$                  |

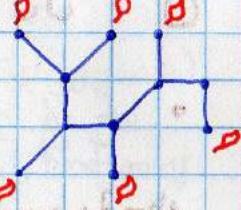
2.5. ინუქცია გხაფები 1.

bj

- ბერები აქცენტის გადაფი

ან აქვს ძირი კონკრეტი

ფოთონები

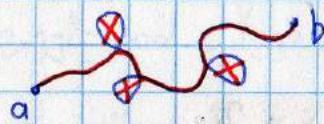


## /\* თქისებები \*/

- ნოს ნებისმიერი მა ნუსაყიდვს შესაბამის ქართული ძირის გან

ლემა 1: ნებისმიერი გხაფში იყ მა განსხვავებელ ნუსაყიდვს შესაბამის

შესაბამის სიტყვა, მარინ მათ შესაბამის ისტისებებს პატივი განსაზღვრავთ



- ბერი ნებისმიერი ახალი ნიზას ჩამატებით გაჩნდება ყური

- ხორან ნებისმიერი ნიზას აძლებით დაირკვევა გამოიყოფა

$$|E| = |V| - 1 \quad e = v - 1$$

edge      vertex

- ნოს ნებისმიერი გამო ფაქტის საკვანვე არის

# /\* \* გრაფების გაფერადება \*/

- თუ  $K$  ფენითა გაფერადება  $\Rightarrow k+1$  ფენითა გაფერადება

ერთაც ხელი  $X(G)$

მინიმუმუნი ხურდების ფენების, ხომლითაც გაფენილი გაფერადება

- $X(K_n) = n$
- $X(\text{კვანძი}) \leq X(\text{მოერთული გაფენი})$  \*
- $X(C_5) = 3$
- $X(C_4) = 2$
- $X(\text{ხაზუანი გაფენი}) = 2$
- $X(b_3) = 2$

## /\* \* თეორემა \*/

თუ  $\forall i : d_i \leq k \leftarrow \max K$

მაშინ  $X(G) \leq k+1$

բազմագույնություն ~~համարակալու համար համար համար համար~~

1 լոզ.  $G_{k+1}$  չափահանդիպություն  $K+1$  ցվիուս (ծավալի սբթցցվածություն)

2. օրյ ամոցողյթու 1 նցիմն նույղյթու  $G_k$  շացել, եռայրով

3. 33 զագյարշմարու կ+1 զվիտ (եթզան զայտի ոճքուցուի)

გამკვების თანხმად ის გაფეხადებულია ( კ ეჭით ) და

3. հոգ Քոշածացու 1 թշհմ. յև նշիմ քայլածները ձեմոց

$k$  Ցշիմ (d<sub>i</sub> ≤ k) ու ոյ ա կը ըստ ըստից ծավալու

Ծցիմս ցիս շանեցացըլու իցի մյածությունը

$k+1-j$  զյիս ու մը ցիս զարգյալութ սահմանները նշված

11

Geometriko  $K+1$  օջիուն

Ճշգիտ ճյածքում ճիշցութ Խ-1 և Տօնական քարցեն

- ქვედა ზოგის დასავალისათვის კარგი საშუალებაა **კლიფის** ძობვა

Յորդո - նիւթո յըցչեցո. ըս հարցս նիւթո շեցու  $X =$

Եզրակացնեալ եալոցիմոծն լա Ա (լոցիմոց)  $\leq$  Ա (այլու լոցոց)

$\Rightarrow X(\text{symm}_n)$  shub  $X(G)$ -l t3jpos 8m3shn ( $X(G) \geq X(\text{symm}_n)$ )

- $\chi(G)$ -ს გერა გრაფის დასაფუძვლად ის უნდა ვინოვოთ **პასუხისმგებელი**

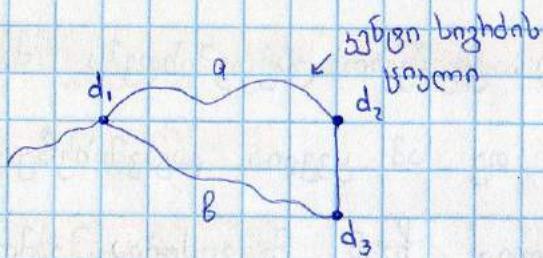
Ետք այս պահին  $\chi(G) \leq k+1$

## აძლიერება (გაფართო გაფეხსარება)

სუ. ასე თუ გაფეხი გაფეხის აქციის სიგრძის მატები უკიდო

მისი 2 ფარ გაფეხსარება შეუძლებელია

დავ. საშ.



ეს სიუკიდო აქციის არ

1) a-ს სიგრძე აქციისა და b-ს სიგრძე აქციისა

მატება  $d_1 - n_b$  ფეხი =  $d_2 - n_b$  ფეხი =  $d_3 - n_b$  ფეხი  $\times$

2) a-ს სიგრძე სამეტოა და b-ს სიგრძე სამეტოა

მატება  $d_1$  ფეხი  $n_b$  მოსახურება სისივრცის ფეხი

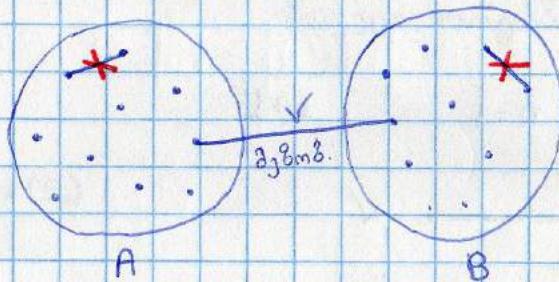
$d_2$  და  $d_3$  მოსახურება მეტი ფეხის გრძელები  $\times$

# ლანგუილების bipartite graphs

ლანგუილების განხილება მემკვევ გაუფეხი:

$$V = A \cup B$$

$$A \cap B = \emptyset$$



- $N(i)$  - ნერმ  $i$ -ს მეზობლების სიმარტი

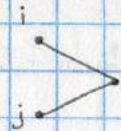
დაგ. ლანგუილების ფორმა

$$(|N(i)| \geq 1)$$



$$\forall i : d_i \geq 1$$

$$\forall i, j : |N(i) \cup N(j)| \geq 2$$



$|N(i) \cup N(j)| = 1$  ლანგუილების ვერ დაგენერირება

$$\forall i, j, k : |N(i) \cup N(j) \cup N(k)| \geq 3$$



$|N(i) \cup N(j) \cup N(k)| = 2$   
\* ლანგუილების ვერ დაგენერირება

⋮

\*  $S$  - სიმარტი

$$N(S) = N(x_1) \cup N(x_2) \cup \dots \cup N(x_k) \text{ სიმარტი}$$

$$\{x_1, x_2, \dots, x_k\} = S$$

>All სიმარტი  $S$ -ს სიმარტი

$$|N(S)| \geq |S|$$

## ကျော်ကျော်မာ

თუ  $\forall S$  -სთვის  $|N(S)| \geq |S|$  ( და პირებითაც )  
მაშინ ლანგვილება აჩვებობს

ମୁଦ୍ରାମୟକଣତ :

$$\text{解法: } n=1 \quad 1 \geq 1$$



ନିର୍ମାଣ.

բաժյջներ:  $n = 1 \dots m$  - հաշվառությունների սեղմանը

ગુ.પ્ર. :  $n = m+1$  - લોગલ લિગન્યુઝસ  $|N(S)| \geq |S|$

$$|N(S)| \geq |S| \quad \text{զայտակ} \quad 2 \quad \text{նախորդաբ} \quad \begin{matrix} \nearrow |N(S)| \geq |S| + 1 \\ \searrow |N(S)| = |S| \end{matrix}$$

$$3.1) \quad \forall S \ (1 \leq |S| \leq n-1) \quad |N(S)| \geq |S| + 1$$

ՀՅՈՒՅՆՈՅ ԵԳՅՈՆԵՑՆՈՅԻ ԵԿԱԾՈՂԻ ՀԱՅԱՅՑԿԱԾՈՂՈՅ

Ըստ պահումունքի  $S$ -եւ թվականի  $|N(S)|$  ըստ պահումունքի 1-ու բարձրացնելու

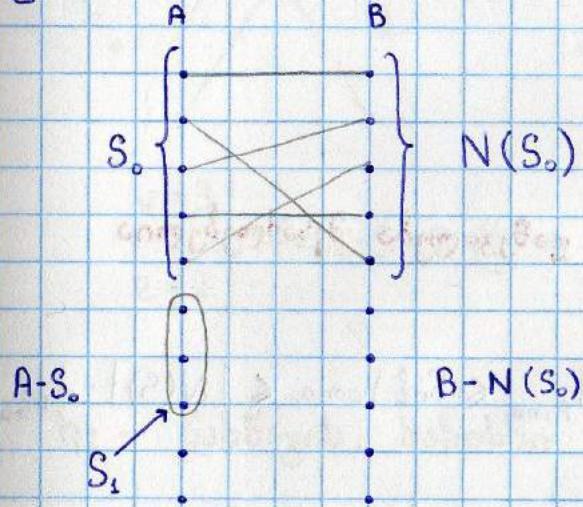
(පිළිබඳ තිය), මෙයින් සාම්ජ්‍යාච්චා තුළුවේ

↳ **Lemma**  $|N(S)| \geq |S| + 1 - 1 \geq |S|$

რაოგორიც  $m + 1 - 1 = m$  ინდ. ფაქ. განახლების საწყისი იან



3.2)  $\exists S_0$  ( $1 \leq |S_0| \leq n-1$ ) :  $|N(S_0)| = |S_0|$



$$1 \leq |S_0| \leq m$$

$S_0$  թափանցողութ է  $N(S_0)$ -ուն  
ուժույթութ թափանցութ

Մ.թ. հմ ա- $S_0$ -ի և  $B-N(S_0)$  թափանցութ պահանջման

$$|N(S_1) - N(S_0) \cap N(S_0)| \geq |S_1|$$

Ճշգրիտութ :  $|N(S_0 \cup S_1)| \geq |S_0| + |S_1|$

$$|N(S_0)| + |N(S_1) - N(S_0) \cap N(S_0)|$$

" օգոզյա եայ թափանցութ  
|N(S\_1) - N(S\_0)|"

$$\cancel{|N(S_0)|} + |N(S_1) - N(S_0) \cap N(S_0)| \geq \cancel{|S_0|} + |S_1|$$

$$|N(S_1) - N(S_0) \cap N(S_0)| \geq |S_1|$$

⇓

Ոճք. թափանցութ ահայտութ թանհիք ենթութու

**թափանցութուն եղիք :**

- Յունակութ  $S_0$ , հմայլութ  $|S_0| = |N(S_0)|$
- թափանցութուն  $S_0$  թափանցութ  $N(S_0)$
- թափանցութուն թափանցութ ենթութու

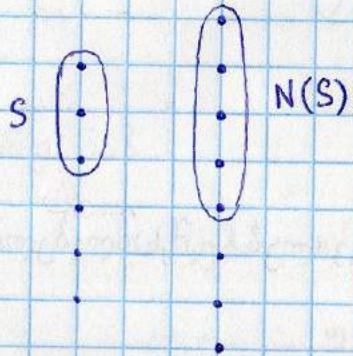
\* შავები. ამონ.

თუ  $|A| \leq |B|$

ეს  $d_{A_{\min}} \geq d_{B_{\max}}$

მაშინ  $\forall S \subseteq A : |N(S)| \geq |S| \Rightarrow$  დაწყვილება შესაძლებელია

დავაძლევოთ:



$$|S| \cdot d_{A_{\min}} \leq \text{ნოზ. ზომა} \leq |N(S)| \cdot d_{B_{\max}}$$

$$|S| \cdot d_{A_{\min}} \leq |N(S)| \cdot d_{B_{\max}}$$

$$|N(S)| \geq |S| \frac{d_{A_{\min}}}{d_{B_{\max}}} \geq |S| \quad \geq 1$$

## ტოტემი გრაფები

V - ნუკრების რაოდენობა

E - ნიბულების რაოდენობა \*

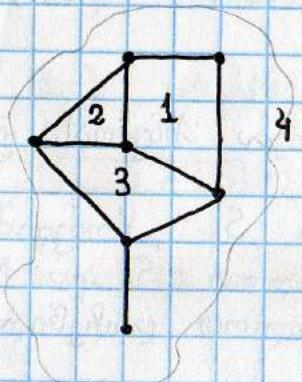
f - ნახევრების რაოდენობა

ელემენტების ფორმები

$$f = e - V + 2$$

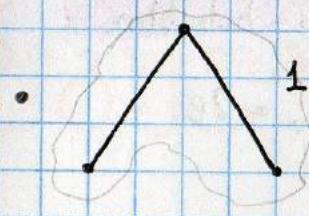
\* გეომეტრიული

\*  $V \geq 3$

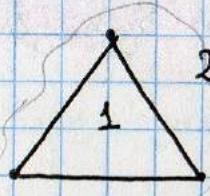


4 ნახევრები

დავ.



$$\left. \begin{array}{l} v=3 \\ e=2 \end{array} \right\} f = 2-3+2 = 1$$

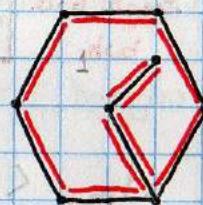


$$\left. \begin{array}{l} v=3 \\ e=3 \end{array} \right\} f = 3-3+2 = 2$$

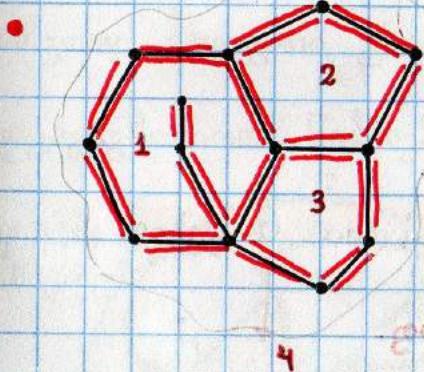
$h_i$  - ნახნავის ხაზები

ნახნავის ძოსაზღვრულ ნიშნების რაოდენობა

2-ჯე ძოსაზღვრულ 2-ჯე იფარება



$h_1 = 10$



$$h_1 + h_2 + \dots + h_f = 2e$$

თუ  $v \geq 3$  ნახნავი ძინიშვნის სამკუთხედის

$$h_i \geq 3$$

$$2e = h_1 + h_2 + \dots + h_f \geq \underbrace{3+3+\dots+3}_f = 3f$$

↓

$$2e \geq 3f$$

$$e \leq \frac{3v-6}{2} *$$

$$2e \geq 3v - 6$$

- შეცველი გრაფის ნუკლეობის სამულო ხახისხი

ხოგონი ყველა გრაფისთვის  $d_1 + d_2 + \dots + d_v = 2e$

$$\star \frac{d_1 + d_2 + \dots + d_v}{v} = \frac{2e}{v} \leq \frac{2(3v-6)}{v} \leq 6 - \frac{12}{v} < 6$$

↓

*Egg. საბ.*  
*bu h.*

$$\frac{d_1 + d_2 + \dots + d_v}{v} \leq 6 - \frac{12}{v} < 6$$

$$\star d_{\min} < 6$$

$$\downarrow \\ d_{\min} \not\geq 6$$

$$\downarrow \\ d_{\min} < 6$$

$$\downarrow \\ d_{\min} \leq 5$$

$$\downarrow$$

- ★ ყველა შეცველი გრაფი გაფეხარებათა 6 ფეხით ინდიკირდება ნუკლეობის მიღებაზე

5 ფეხითაც

4 ფეხითაც (ბეჭი ვა)

- როგორ შევაძლოთ შეცველის ფუნქცია:

- $e \leq 3v - 6 \leftarrow$  ყველა გრაფისთვის

- $e \leq 2v - 4 \leftarrow$  bipartite graphs

- $h_1 + h_2 + \dots + h_f = 2e \geq 3 + 3 + \dots + 3 \quad (h_i \geq 3)$

$$2e \geq 3 \cdot f$$

$$f = e - v + 2$$

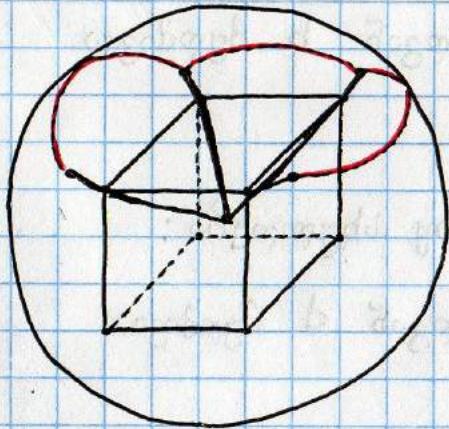
# რეგულარული

# მრავალნახევრი

regular solids

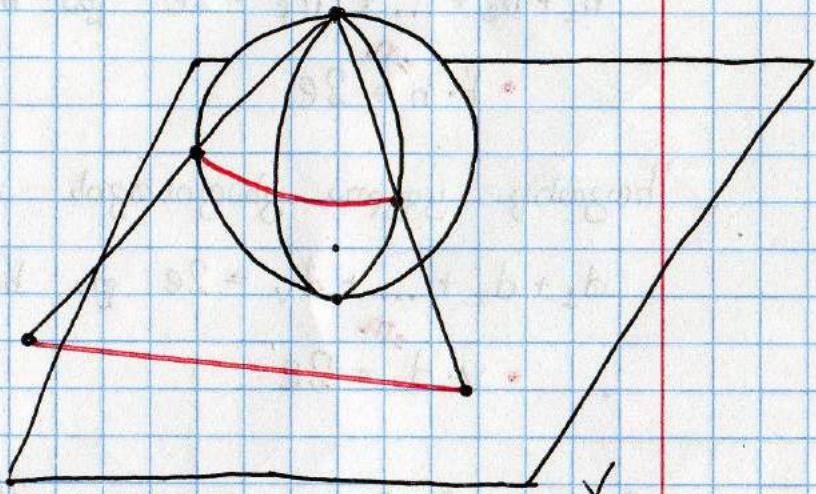
- მრავალნახევრა - სამგანზომილებიანი სასხლნახევრიანი ფიგურა
- თუ მრავალნახევრას არ არის იდენტური ნესიერი მრავალნახევრი და თითოეულ ნერჩომი ცოდი საორგანობის წახევი „ხვიდება უთბონებს“ მრავალნახევრა რეგულარულია.

ეს ხომ ჩვეულები მრავალნახევრა შეგვიძლია წარმოვადგინოთ ხოვთხს მხრივ განვითაროთ. ჩავროთ მრავალნახევრა სფერომი და დაკავევმილოთ წიბოები



ამ გეგმილებისან გარავიდეთ

სიბცყის გეგმილებზე



გარავერით

მხრივ განვითაროთ

- $m$ -ით აღვნიშნოთ წვეროები მემხვერით წახნაგების ხაორენ.
- $n$ -ით აღვნიშნოთ წახნაგის გვერდების ხაორენობა

ჩვეულებით მხავარწახნაგის შესაბამის შეცველ გხაფში

- თითოეული წვერის ხაზის სისისი ( $d$ ) =  $m$ -ს და ყველა

წვერის ფორმის

- თითოეული წახნაგის ხაზის სისისი ( $h$ ) =  $n$ -ს

- $d$  - წვერის ხაზის სისისი - მერმივი ( $=m$ )

- $h$  - წახნაგის ხაზის სისისი - მერმივი ( $=n$ )

ხოგონის ყველა შეცველი გხაფის ფორმის სტანდარტი:

$$h_1 + h_2 + \dots + h_f = 2e \quad \text{და ხადგან } h \text{ მერმივი}$$

$$\bullet f \cdot h = 2e$$

ხოგონის ყველა გხაფის ფორმის სტანდარტი:

$$d_1 + d_2 + \dots + d_v = 2e \quad \text{და ხადგან } d \text{ მერმივი}$$

$$\bullet v \cdot d = 2e$$

$$f = e - v + 2 \quad \text{ჩავსვათ} \quad \bullet$$

$$\bullet v \cdot d = 2e \Rightarrow v = \frac{2e}{d}$$

$$\bullet f \cdot h = 2e \Rightarrow f = \frac{2e}{h}$$

$$\frac{2e}{h} = e - \frac{2e}{d} + 2$$

$$\bullet \quad \frac{1}{d} + \frac{1}{h} = \frac{1}{2} + \frac{1}{e} > \frac{1}{2}$$

ვიწით, ხომ  $h \geq 3$  ყველა შეცველი გხაფისთვის

$d \geq 3$ , ხოგან თუ ას ას არცებუ ფიგურა ას არცებუ 3 განზომელ.

$$\text{თუ } h \geq 3 \rightarrow h \leq \frac{1}{3} \rightarrow \frac{1}{d} \text{ უნდა იყოს} > \frac{1}{6} \rightarrow d < 6$$

$$\text{თუ } d \geq 3 \rightarrow d \leq \frac{1}{3} \rightarrow \frac{1}{h} \text{ უნდა იყოს} > \frac{1}{6} \rightarrow h < 6$$

$$d = 3, 4, 5$$

$$h = 3, 4, 5$$

$$d=3 \quad d=4 \quad d=5$$

$h=3$	$\checkmark_{e=6}$	$\checkmark_{e=12}$	$\checkmark_{e=30}$
$h=4$	$\checkmark_{e=12}$	$\times_{e=0}$	$\times_{e=-20}$
$h=5$	$\checkmark_{e=30}$	$\times_{e=-20}$	$\times_{e=-10}$

$$\frac{1}{e} = \frac{1}{h} + \frac{1}{d} - \frac{1}{2}$$

$$e > 0$$

ასევე სულ 5-ნაირი ჩეგელასულონ მასალაციონელი.

# Conditionals

second - მენება, იხეალები

third - ფასი, შესვლელი

უ.ლ. ყველა შეცველი გხაფი

გაფეხაღებადის 5 ფეხით.

შეზა:  $v \leq 5$  ფეხარება 5-ით

ნაბეჭი: ვიყით, ხომ  $\exists$  ნვებო :  $d \leq 5$  ( $\text{ნვებო} \equiv g$ ) ( $G - v+1$  ნვებოანი)

3.1)  $d_g < 5$

ამოვილებით ამ ნვებოს, ინდუტიუტი დაშვებით გავაფეხაღებით

$v$  ნვებოან გხაფს 5 ფეხით. ჩავაძლებოთ  $g$ -ს და

ხარგან  $d_g < 5$  გავაფეხაღებით მას დაჩჩენილი ფეხით

3.2)  $d_g = 5$

ავილოთ ეს ფეხაფი: ვიყით ხომ ამ ფეხაფიში

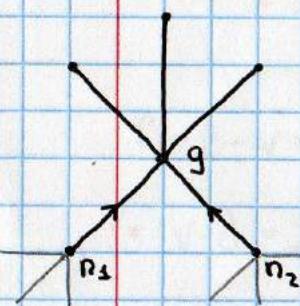
$\exists n_1, n_2$  ხმალის ან ახის ენდანციის მეზობელი.

ნინაალმრეგ შეძოხვევაში მივიღებდით  $K_5$ -ის

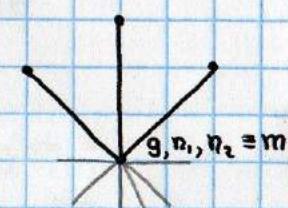
იზომონიფერ გხაფს ხას ან ახის შეცველი

„მევანებოთ“  $n_1, g$  და  $n_2, g$ -სთან

ინდ.დამ.-ით  $v-1$ -იანი 5 ფეხით გად



$v+1$  ნვ.



მივიღეთ  $v-1$

ნვებოანი გხაფი

გავაფეხაროთ და ისევ „გავწეროთ“

გხაფი.  $n_1, n_2$ -ს რაცუცოვით

სს ფეხი, ხას „გარმოშევა“ მ-დან.

ხარგან ისინი ან ახიან მეზობელი

და კი გავაფ. დაჩჩ. მე-5 ფეხით

# ოიცხვთა თეორია

- $a \text{ ლოგიური}$
  - $b \text{ ლოგიური}$
- } ხო ჩაოდენობები მიიღწევა?

- $a : b \Leftrightarrow (a = k \cdot b \quad k \in \mathbb{Z})$

- $c$  გამოისახება  $a$  და  $b$ -ს წილი კომბინაციით

ამ  $\exists k_1, k_2 \in \mathbb{Z} : c = k_1 \cdot a + k_2 \cdot b$

$$0 = 0 \cdot a + 0 \cdot b$$

$$a = 1 \cdot a + 0 \cdot b$$

$$b = 0 \cdot a + 1 \cdot b$$

ინუდიციონ ე.թ. ჩოდ უოველი გარასხმის  
შემდეგ მიიღწევა ჩაოდენობა, ჩოდელის  
ჩაინუხება  $a$  და  $b$ -ს წილი კომბინაციით

დავუძ. 1 გარასხმი ი გარასხმის შემდეგ  $X_n = X_{na} \cdot a + X_{nb} \cdot b$

2 გარასხმი ი გარასხმის შემდეგ  $Y_n = Y_{na} \cdot a + Y_{nb} \cdot b$

$n+1$ -ი გარასხმის შემდეგ:

//

31) ბისექციის დაცვითი გარაისება  $X_n + Y_n = (X_{na} + Y_{na}) \cdot a + (X_{nb} + Y_{nb}) \cdot b$

$(X_n, Y_n) \rightarrow (0, X_n + Y_n) = (X_{n+1}, Y_{n+1}) + (Y_{n+1} + X_{n+1}) \cdot b$

ჩ.ნ.გ. ჩ.ნ.გ.

32) ბერძეს ავსებამდე გარაისება

$(X_n, Y_n) \rightarrow (X_n + Y_n - b, b) = (X_{n+1}, Y_{n+1})$  ✓

ჩ.ნ.გ. ჩ.ნ.გ.

լիեւըն, ձուղձվող հառաջենքներու ոյնքն յ. ա. զ.  $(a, b)$ -ի սպառ  
հարցան  $x = x_a \cdot a + y_a \cdot b$  III  
9  
 $\vdots g$   $\vdots g$

$$g = \text{յ. ա. զ. } (a, b)$$


---

$$\text{այլ. } g = \alpha \cdot a + \beta \cdot b \quad \alpha, \beta \in \mathbb{Z}$$

$m =$  ձուղձվող, հոմանույթ  $\neq 0$  լու շամունեցնա

$$\text{հոգություն } m_a \cdot a + m_b \cdot b$$

$$1) \boxed{m \vdash g}, \text{ հարցան } m = m_a \cdot a + m_b \cdot b \quad \vdots g \quad \vdots g$$

2) շանչություն

$$\begin{aligned} \text{rem}(a, m) &= a - k \cdot m = a - k \cdot m_a \cdot a - k \cdot m_b \cdot b = \\ &= a(1 - k \cdot m_a) - b \cdot (k \cdot m_b) < m = 0 \end{aligned}$$

շամանը, հոման  $\text{rem}(a, m)$  իսկնեցնա, հոգություն  $b$ -ի նիշուզու յունոնայուն, ուն զոյնու, հոման  $\text{rem}(a, m) < m$  լու մ տակ մոնականություն առնելու հոյեցու, հոմանույթ իսկնեցնա, նիշուզու յունոնայուն և սեռու. այ ևսու ուժուան շամանը  $\text{rem}(a, m) = 0$

ნდევე სოფიური

$$\text{rem}(b, m) = \dots = (\dots)a + (\dots)b < m = 0$$

⇓

$$m - a \geq b - b \text{ ს.გ.}$$

$$g - a \geq b - b \text{ გ.ს.გ.}$$

⇓

$$g \geq m$$

$$\left. \begin{array}{l} 3) \quad g \geq m \\ m : g \end{array} \right\} \Rightarrow g = m = m_a \cdot a + m_b \cdot b \quad \checkmark \text{ ჩ.დ.გ.}$$

ხოგონ ვინოვოთ უ.ს.გ.-ს დ და  $\beta$  კოეფიციენტები  
(გამოვვარგვება სხვა გ.ს.გ.-ს ფასითის კოეფიციენტის  
საქმენელით, ხარგუნ  $k \cdot g = k \cdot d \cdot a + k \cdot \beta \cdot b$ )

\* ეცნობოდეს ალგორითმი

$$\begin{array}{cccccc} 187 & 165 & 22 & 11 & 0 \\ a = 187 & 1 & 0 & 1 & -7 \\ b = 165 & 0 & 1 & -1 & 8 \\ r = & - & . & & \end{array}$$

⇓

$$\text{უ.ს.გ.}(a, b) = 11 = -7 \cdot 187 + 8 \cdot 165$$
$$c = 1 - 0 \cdot 1 = 1$$

სუ. 6. გ. - 6 ჯერადი საორგანოს მიერების აღკვლევითი

გ. გ.  $a < b$

გვინდსა მივიღოთ  $c = k \cdot a$   $c \leq b$

$c = \alpha \cdot a + \beta \cdot b$  გ. გ.  $\alpha \geq 0$

31)  $\alpha = 0$   $\beta = 1 \vee \beta = 0$

32)  $\alpha > 0$   $\beta \leq 0$

შევხედოთ ასე, გვატვს დიდი ჩემპიონატი და  
იძისთვის, ხოდ მივიღოთ  $c$  ამ ჩემპიონატი  
 $\alpha$ -სა და  $\beta$ -ს უნდა ჩავასხოთ  $a$  და  $\beta$ -სა და  $\alpha$ -ს აძლიერებით  
იგივე შეგვიძლია გავაკავთოთ მხრივი ამ 2

ფუნქციით:

- ავავსოთ  $a$ , გარივასხათ  $b$ -ში  $(\alpha - \beta)$
- ხოდა  $b$  აივნები დავკავთოთ ის  $(-\beta)$   $(\beta - \beta)$

და  $a$ -ში დაჩინდებოთ ნერლი  $b$ -ში გარივასხათ.

ამით მივიღებთ  $\alpha \cdot a$   
ნერის ხარ.  $= c' = \alpha \cdot a - \beta \cdot b$ , მაგან  $-\beta = \beta$ , ხარგვა

$0 \leq c' \leq b$  და  $0 \leq c \leq b$

- ხილვის ნიფივი კომპინაციით ჩანაწერი ახა  
ერთადებითი

$$c = \alpha \cdot a + \beta \cdot b$$

$$a = a' \cdot g$$

$$b = b' \cdot g$$

ვ. ლ.

$$\bullet c = (\alpha + b')a + (\beta - a')b$$

$$= \alpha \cdot a + b' \cdot a + \beta \cdot b - a' \cdot b =$$

$$= \alpha \cdot a + \beta \cdot b + \cancel{b' \cdot a' \cdot g} - \cancel{a' \cdot b' \cdot g} = \alpha a + \beta b \quad \checkmark$$

$$\bullet c = (\alpha + 2b')a + (\beta - 2a')b \quad \text{ვ. ლ.}$$

# ՃՈՐԾՄԱԿԱՐԾՈՒԹՅՈՒՆ

- $a \equiv b \pmod{n}$  - առ ոչ  $(a-b) : n$  (Ճանձահղողներ) է
- $a \equiv b \pmod{n}$  - առ  $\text{rem}(a, n) = \text{rem}(b, n)$

Քաշամբեալյանություն

$$a = k_1 \cdot n + r_1$$

$$b = k_2 \cdot n + r_2$$

$$a - b = n(k_1 - k_2) + (r_1 - r_2)$$

$\uparrow$   $\uparrow$   
 $[0, n)$   $[0, n)$   
 $\underbrace{\phantom{0}}$   
 $(-n, n)$

$a - b$  համ ուղարքության  $n$ -ից  $r_1 - r_2$  յերս ուղարք

0-ին լցոլու հարցան  $(-n, n)$  մասրություն  $n$ -ից

ճիշտյան ժի ուղարք  $\Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

$$\text{rem}(a, n) = \text{rem}(b, n)$$

հ.թ.ջ.

- $a \equiv \text{rem}(a, n) \pmod{n}$ , հարցան  $a - \text{rem}(a, n) : n$

$$1. a \equiv a \pmod{n}$$

$$2. a \equiv b \pmod{n} \text{ զյառակեմանք, իմա } b \equiv a \pmod{n}$$

$$3. \text{ ոչ } a \equiv b \pmod{n} \text{ յա } b \equiv c \pmod{n}, \text{ մասն } a \equiv c \pmod{n}$$

$$4. a \equiv b \pmod{n} \Rightarrow a+c \equiv b+c \pmod{n}$$

$$5. a \equiv b \pmod{n} \Rightarrow a \cdot c \equiv b \cdot c \pmod{n}$$

$$6. \text{ ոչ } a \equiv b \pmod{n} \text{ յա } c \equiv d \pmod{n}, \text{ մասն } a+c \equiv b+d \pmod{n}$$

$$a \cdot c \equiv b \cdot d \pmod{n}$$

შეტოვნებული რიცხვი და ძის

ნოვნის გრძი

შეტოვნებული რიცხვი

p-ს მოდულით

a ჩივნის შეტოვნებული ისეთი b ჩივნია

რომელისთვისაც სხელდება შემდეგი

$$a \cdot b \equiv 1 \pmod{p}$$

ნოვნის გრძი:

• მაგ.  $10 \cdot x \equiv 1 \pmod{29}$

$$10 \cdot x = 29a + 1 \quad (\text{ჩავსვათ } a \dots)$$

\* თუ  $a \cdot b \equiv 1 \pmod{p}$  ა. ს. გ. თუ  $ab \equiv 1 \pmod{p}$

შეტოვნებული არ ასევებს. გადცეცენა:

$$a \cdot b \equiv 1 \pmod{p} \quad \text{და} \quad \text{ა. ს. გ. } (a, p) = 1 \quad \Rightarrow \quad ab - 1 \equiv 0 \pmod{p}$$

$$\text{ა. ს. გ. } ab - 1 \equiv 0 \pmod{p} \quad \text{გამონ } ab - 1 \equiv 0 \pmod{p} \quad \text{გამონ } n \cdot k - 1 \equiv 0 \pmod{p}$$

$\uparrow$

$$\left\{ \begin{array}{l} n \cdot k - 1 \equiv 0 \pmod{p} \\ k = 1 \end{array} \right. *$$

• յ35 Հունվարի սրբառիութեան մյջինի թյուղու 3-րդ օր

այց.  $12 \cdot x \equiv 1 \pmod{29}$

1) Բյամբոնման 12-եւ ու 29-ու յ. կ. զ. եմ 1-ու

2)

$$1 = \alpha \cdot 12 + \beta \cdot 29$$

$$1 = \alpha \cdot 12 + \beta \cdot 29$$

$$(\alpha \cdot 12) - 1 = -\beta \cdot 29$$

$$\begin{array}{cccccc} 29 & 12_{(2)} & 5_{(2)} & 2_{(2)} & 1_{(2)} & 0 \\ 12 & 0 & 1 & -2 & 5 & \textcircled{-12} \\ 29 & 1 & 0 & 1 & -2 & 5 \end{array}$$

$$\alpha \cdot 12 \equiv 1 \pmod{29}$$

յ. 3.  $\alpha$  \*

3)  $\sim (0, 29)$  Բյառյութու շարժեցու

յ. 3.  $x \equiv -12 \pmod{29}$

յ. 3.  $x \mid x + 12 \pmod{29}$

$x = \textcircled{17}$

$$\begin{aligned} 3) \quad 1 &= \textcircled{-12} \cdot 12 + 5 \cdot 29 = -12 \cdot 12 + 29 \cdot 12 + 5 \cdot 29 - 12 \cdot 29 = \\ &= \textcircled{17} \cdot 12 - 7 \cdot 29 \quad * \end{aligned}$$

• ფერმას მცირე თეორემით შემოწმებულის პოვნა

• ფერმას მცირე თეორემის თანახმარ

$$a^{p-1} - 1 \equiv 0 \pmod{p} \quad \text{თუ } p - \text{პრიმური *$$

⇓

$$a^{p-1} \equiv 1 \pmod{p}$$

⇓

$$a^{p-2} \equiv a^{-1} \pmod{p} \quad (\text{სარაც } p \text{ პრიმური})$$

შემთხვევაში, რომ \* თუ  $a \not\equiv 0 \pmod{p}$  .

ამა 1,  $a$ -ს შემოწმებული ის ასევე მაგან

ეს ის ნიშნავს იძს, რომ \* თუ  $a \not\equiv 0 \pmod{p}$  .

1-ის,  $a$ -ს შემოწმებული ასევე მაგან. დავაძლოთ:

თუ  $\gcd(a, p) = 1$ , მაშინ  $\exists a^{-1} \pmod{p}$

$$\alpha \cdot a + \beta \cdot p = 1$$

$$\alpha \equiv a^{-1} \pmod{p}$$

$$\alpha \cdot a - 1 = -\beta \cdot p$$

⇓

$$(\alpha \cdot a - 1) \equiv 0 \pmod{p}$$

ხარგან  $\alpha$  ესასხულოდ გვვიჩინოს

$a^{-1}$  გვვიჩინოს.

$$\alpha \cdot a \equiv 1 \pmod{p}$$

$a^{-1}$  ჩ.მ.გ.

# ციფრის განვითარების სისტემის კოდი

Y i C t o r y  
 ↓ ↓ ↓ ↓ ↓ ↓  
 22 09 03 20 15 18 25

$m = 2209032015182513 \leftarrow$  ახელი ეს ხილვის მახასინებელი

$k =$  გასაღები = დიდი მახასინებელი ხილვი

დაშიფრვა:  $m^* = m \cdot k$

გაშიფრვა:  $\frac{m^*}{k} = m$

## ციფრის განვითარების სისტემის კოდი

$$m_1^* = m_1 \cdot k$$

$\uparrow$   
მახასინებელი

$$m_2^* = m_2 \cdot k$$

$\uparrow$   
მახასინებელი

$$\gcd(m_1^*, m_2^*) = k$$

ლილი ხილვების კი ეკვივალენტი ალგორითმი  
არის სწავლად მეტანბეჭდის.

Եղանակները դյուրց յուղ

A

B

A լա B-ի սյն և յահում  
և որոշման K շախալութու

P - լուր, և յահում մահուց հոյեցու

- $0 < k < p$

գալուստանու

$m \rightarrow m_1, m_2, \dots, m_e$  ույ, իմա  $0 \leq m_i < p$ .

Ըստուցված:  $m_i \rightarrow c_i: c_i = \text{rem}(m_i \cdot k, p)$

յանուանու:

Յոյնու, իմա  $c_i = \text{rem}(m_i \cdot k, p)$

⇓

$c_i \equiv m_i \cdot k \pmod{p}$

$c_i \cdot k^{-1} \equiv m_i \pmod{p}$

⇓

$\text{rem}(c_i \cdot k^{-1}, p) = \text{rem}(m_i, p)$

• Յնուանութու  $k^{-1} \pmod{p}$ .

• Յունանութու  $\text{rem}(c_i \cdot k^{-1}, p)$

լա յունանութու  $m_i$ .

հորցան  $0 \leq m_i < p$

լա  $p$  մահուցու

$\text{rem}(m_i, p) = m_i$

## ციურინგის ძერე კოდის გაცემა

- თუ ჩვენ გვაქვს ხოვთხევ ლაშიფრების ისე  
ლაშიფრის მესიკი  $(m_i, c_i)$ ,  $p$  - საჭახო
- ვინოვოთ  $m_i^{-1} \pmod{p}$
- გამოვთვალით  $c_i \cdot m_i^{-1}$ , ჩადგან

$$c_i \cdot m_i^{-1} \equiv m_i^{-1} \cdot k \cdot m_i \equiv k \pmod{p}$$

ჩადგან  $k < p$  და  $p$  ბაზიფიციან

$$\text{rem}(k, p) = k \rightarrow \text{rem}(c_i \cdot m_i, p) = k$$

გეოდასიანი თეორემა

$$a^{p-1} \equiv 1 \pmod{p}$$

სადაც  $p$  პრიმურია და  
ლინგერებია

$a$  ამ მის  $p-1$  ფუნქცია

$$1 \ 2 \ 3 \ \dots \ p-2 \ p-1 \quad (p-8) \text{ გაყოფის ნაშთები}$$

გავაძებავოთ ყველა  $a^{p-1}$

$$a \ 2a \ 3a \ \dots \ a(p-2) \ a(p-1)$$

გავაძლდებოთ, რომ ამ ნიუბების  $p-8$  გაყოფის

სხვადასხვა ნაშთები აქვთ.

ლიკ. სამ.

$$x \cdot a \equiv y \cdot a \pmod{p}$$

$$a(x-y) \equiv 0 \pmod{p}$$

$$a \neq 0 \quad 0 < x < p \quad 0 < y < p$$

$$0 < x-y < p$$

$$-p < x-y < p$$

||

$$x-y \neq p \quad *$$

ესეიგი

$a \ 2a \ 3a \ \dots \ a(p-2) \ a(p-1)$  ხილვავები

გვაძლევენ  $p-8$  გაყოფის კნიხვავებულ ნაშრებს  
სა თან ყველას, ხორგან  $p-1$  ცარი ხილვა გვაძლენ

⇓

$\forall k, n \exists \underset{\wedge}{n, k} k \in \{a, 2a, \dots, a(p-1)\} : k_i \equiv n_i \pmod{p}$   
 $n \in \{1, 2, \dots, p-1\}$

$k_1 \equiv n_1 \pmod{p}$

$k_2 \equiv n_2 \pmod{p}$

↓

$k_1 \cdot k_2 \equiv n_1 \cdot n_2 \pmod{p}$  და ა.შ.

პიკოლები, ხმა

$1 \cdot 2 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot \dots \cdot a(p-1) \pmod{p}$

$(p-1)! \equiv (p-1)! \cdot a^{p-1} \pmod{p}$

$(p-1)! \cdot (a^{p-1} - 1) : p$

ა.შ იყოფა  $p-8$

⇓

$a^{p-1} - 1 : p$

$a^{p-1} \equiv 1 \pmod{p}$  ხ.ღ.გ.

# ეოლეტის თუმცადების

იმისთვის, რომ ლავაშებისთვის ეილეტის ფენცია  
ნიჩველი ჩივი საჭიროა ლავაშებისთვის, რომ

$\text{rem}(k_1 \cdot k, n) \quad \text{rem}(k_2 \cdot k, n) \dots \text{rem}(k_r \cdot k, n)$   
არის

$k_1, k_2, \dots, k_r - n$  გადაწაცვლება

, სარაცის  $k_1, k_2, \dots, k_r$  არის  $n$ -ზე ასევე გლო

$n$ -ის ეთოვების ჩივი ჩივების  $(r = \varphi(n))$  და  
 $k$  ეთოვების ჩივი  $n$ -ის

1) ვაჩვენოთ, რომ  $\text{rem}-ების პირდევების$   
უკალი წევი განსხვავებულია.

დავუძის, რომ

$$\text{rem}(k_i \cdot k, n) = \text{rem}(k_j \cdot k, n)$$

$$k_i \cdot k \equiv k_j \cdot k \pmod{n}$$

ჩადგან  $k$  ეთოვების ჩივი  $n$ -ის

$$k_i \equiv k_j \pmod{n}$$

ჩადგან  $k_i < n \wedge k_j < n$

$$k_i = k_j$$

335 լորյութուն:

$$\gcd(n, \text{rem}(k_i \cdot k, n)) = \gcd(k_i \cdot k, n)$$

$$\begin{cases} \gcd(k_i, n) = 1 \text{ ( յիշուն համար կազմակերպություն )} \\ \gcd(k, n) = 1 \text{ ( յիշուն համար կազմակերպություն )} \end{cases}$$

⇓

$$\gcd(k_i \cdot k, n) = 1 \Rightarrow \gcd(n, \text{rem}(k_i \cdot k, n)) = 1$$

\*  $\text{rem}(k_i \cdot k, n)$

- 0,  $n-1$  մյալություն ( նաև  $n$  )
- $\text{rem}(k_i \cdot k, n)$  յիշուն համար կազմակերպություն  $n$ -ուն

⇓

$$\bullet |\text{rem-յնուն}| = |k_1, k_2, \dots, k_r|$$

- rem-յնուն պարունակությունը ըստ կամաց ազատ պահանջման կազմակերպություն

( համարից  $k_i$ -յնուն )

⇓

...

պահանջման  $k_i$ -ուն պահանջման  $\text{rem}(k_j \cdot k, n)$

պահանջման մուն պահանջման

ნინა დამცავებით დავამცავოთ ესლების ფუნქცია

$$k_1 \cdot k_2 \cdot \dots \cdot k_r = \text{rem}(k_1, k, n) \cdot \text{rem}(k_2, k, n) \cdot \dots$$

$$\cdot \text{rem}(k_r, k, n) \equiv k_1 \cdot k \cdot k_2 \cdot k \dots \cdot k_r \cdot k \pmod{n}$$

$$(k_1 \cdot k_2 \cdot \dots \cdot k_r) \cdot k^r$$

$$k_1 \cdot k_2 \cdot \dots \cdot k_r \equiv (k_1 \cdot k_2 \cdot \dots \cdot k_r) \cdot k^r \pmod{n}$$

ხავან  $\forall k_i$  ესლების  $n$ -ის

$k_1 \cdot k_2 \cdot \dots \cdot k_r - n$  ან  $n$ -ის მიმდევარი ესლები

რაც შევძლოთ  $k_1 \cdot k_2 \cdot \dots \cdot k_r - 1$  შევძლოთ

$$1 \equiv k^r \pmod{n} \quad r = \varphi(n)$$

$$k^{\varphi(n)} \equiv 1 \pmod{n}$$

ესლების ფუნქციის თვისებები

$$\bullet k^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\bullet \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

$$\bullet \varphi(m \cdot n) = \varphi(n) \cdot \varphi(m)$$

$k$  და  $n$  უსლებელი ფუნქციები ენდა იყოს !

$$n \in \mathbb{N}$$

# RSA

- one-way function

- շիշո մեխոց քահանություն պահպան  
մեխոց հայլու

Անյտու աղմանինքա  $c = \text{rem} \left( \frac{m^e}{N} \right)$

1) Յովու տ, և յովու ս

$$c = m^e - k \cdot N \quad k = (\text{int}) \frac{N}{m^e}$$

$k$ -ն էմենք քահանություն ուն  $\Rightarrow c$ -ն էմզն քահանություն

2) Յովու ս, և յովու տ

$$m = \sqrt[e]{c + k \cdot N}$$

յնքա յոնշութ ույտու  $k = (\text{int}) \frac{N}{m^e}$ ,

մաշիս հարցան տ և յովու յամունացնութու

հայենաւու յենոնութու մոնակային

յովու, իու տ  $m^e = k \cdot N + c$  իունաւու

$$k = (\text{int}) \frac{N}{k \cdot N + c}$$

$e, N$  նույնաւու

ახლა მევ დანათ ისეთი „გასაღები“, ხომ ელიტურ „მეორე ძხივობას“ გაგვიძახოვებს.

ან უნდა მევ დანათ ისეთი  $d$ , ხომ

$$m^e \equiv c \pmod{N} \quad \text{დამიუღვის მეჩე}$$

$$c^d \equiv m \pmod{N} \quad \text{აღვარგინოთ წესილი}$$

↓

$$m^{e \cdot d} \equiv m \pmod{N}$$

ამისთვის გვიჩვენება სხვა one-way function

ხომ ელიტურ დაგვიგენერიხებს  $d$ -ს

$N$  მეცნიეროთ შემოგი წესით

$N =$  , სარაფ და 2 რიცხვი განცილებით

ხილვია (გადამხავლება ძიხებია, ძიხები ძაბული დავი)

გასოლების რამაც უნდა იყოს

ახლა კი უნდა ძლივოებით ისეთი ფუნქცია

ხომ ეს სიძახულე დამოკიდებულია  $p_1$  და  $p_2$  - ის კონტაჩი. თუ ვიცით  $p_1$ ,  $p_2$  - განცილებია, თუ ას ვიცით ხილვია.

ამისთვის გამოვიყენოთ ეილენის ფუნქცია

$$\varphi(N) = \varphi(p_1) \cdot \varphi(p_2) = (p_1 - 1)(p_2 - 1)$$

ჩადგან მაჩვივებელია

ზოგადი  $\varphi(N)$ -ის პოვნა ხილოა, ხარგან  $N$   
დიდი ხილვია.  $p_1, p_2$  -ის კუთხით კი დავალო  
2 დიდი ხილვის ნამარტობა, ხოვ ძალივი თქმავით

ვიყით, რამდენიმე

$$m^{\varphi(N) \cdot k} \equiv 1 \pmod{N}$$

ეილენის ფუნქციის თანახმად

$$m^{k \cdot \varphi(N) + 1} \equiv m \pmod{N}$$

(იმის გამო,  $\gcd(m, N) = 1$  !)

ასეთი მიზანის აქვთ განმარტვა

$$k \cdot \varphi(N) + 1 = e \cdot d$$

განმარტვის დანართისას

$$d = \frac{k \cdot \varphi(N) + 1}{e}$$

✓

↓

$$\underline{ed \equiv 1 \pmod{\varphi(N)}}$$