წმიდა ტბელ აბუსერიძის სახელობის სასწავლო უნივერსიტეტი

ჰუმანიტარულ მეცნიერებათა და განათლების ფაკულტეტი

სამაგისტრო პროგრამა განათლება

ცივაძე ქეთი

მოდულური არითმეტიკა და რიცხვითი შედარებები

ნაშრომი შესრულებულია განათლების მაგისტრის ხარისხის მოსაპოვებლად

ხელმძღვანელი: ასოცირებული პროფესორი ჭუმბურიძე გივი

ხიჭაური

2017

ანოტაცია

ქეთი ცივაძის სამაგისტრო ნაშრომი - სტუდენტის პედაგოგიური პრაქტიკისადმი ახალი მიდგომები. ნაშრომში განხილულია ნაშთთა (მოდულური) არითმეტიკისა და რიცხვითი შედარებების სწავლების საკითხები დაწყებით, საბაზო და საშუალო საფეხურზე.

თემის აქტუალობა: არის მათემატიკის საკითხები, რომლებიც უშუალოდ უკავშირდება სასკოლო მათემატიკის შინაარს, მაგრამ მათ სათანადო ყურადღება არ ექცეოდა მათემატიკურ სპეციალობებზე სწავლების დროს, სასწავლო მიზნის მიღწევაში ბაშთთა არითმეტიკას მნიშვნელოვანი როლი აქვს. ნაშთიანი გაყოფის შესახებ არსებობს თეორემა: თუ a და b მთელი რიცხვებია , $b>0$ მაშინ ისეთი მთელი q და r, რომ $a=bq+r$ და $0\leq r<b$.

კვლევის მიზანი. კვლევა ეხება მოდულური არითმეტიკის სწავლებას საშუალო საფეხურზე კვლევის მიზანია გაირკვეს ნაშთთა არითმეტიკის სწავლების რა ხარისხი და მდგომარეობაა სკოლებში.

კვლევის ამოცანა. გამოიკითხოს კერძო და საჯარო სკოლის მასწავლებლები, რადგან გავარკვიოთ მათი დამოკიდებულება ნაშთთა არითმეტიკის და რიცხვითი შედარებების საკითხთან დაკავშირებით , რამდენად კარგად შეისწავლება ეს საკითხები სკოლებში და რა პრობლემის წინაშე დგანან მასწავლებლები.

კვლევის საგანი. საგანს წარმოადგენს რიცხვითი შედარებების და ნაშთთა არითმეტიკის საკითხის სწავლება.

ობიექტი.კვლევის ობიექტია აღნიშნული საკითხის სწავლების პროცესი .

სიახლე. ეროვნული სასწავლო გეგმაში, პროგრამის შინაარსი შეივსო ახალი ნაშთთა არითმეტიკის საკითხით. კვლევის სიახლე გახლავთ ის, რომ ამ საკითხების სწავლების პრობლემებს მეთოდურ ლიტერატურაში სათანადო ყურადღება არ ეთმობოდა , საჭიროა დავადგინოთ როგორ ისწავლება ნაშთთა არითმეტიკის საკითხი სკოლებში.

ძირითადი შედგები.კვლევის ჩატარებამ და შეჯამებმა საშუალება მოგვცა გარკვეული დასკვნები გამოგვეტანა და შესაბამისი რეკომენდაციები გაგვეკეთებინა პრობლემის გადასაჭრელად, რაგდან შედეგებიდან გამომდინარე ჩანს, რომ მეტი ყურადღება უნდა დაეთმოს არითმეტიკის და რიცხვითი შედარებების საკითხის სწავლებას.

Abstract

Keti Tsivadze Master Degree - New approaches to student pedagogical practice. The paper discusses the issues of teaching and analyzing the numerical (numerical) arithmetic and numerical comparisons in the initial, basic and secondary stages.

Subject actuality: There are mathematical issues that are directly related to school mathematics content but they were not sufficiently integrated and taught within the programs of mathematical specialties, as a result to which most teachers do not know discrete mathematics, including the scientific basis of the arithmetic balance, thus they have difficulties with explaining and teaching the material appropriately. By omitting and neglecting these issues during the teaching they violate Education Law, Article 5. (Article 5. (5) The implementation of the National Curriculum is mandatory for all general educational institutions).

The aim of the study. The study refers to the teaching of the arithmetic balance for the secondary level students. The aim of the study is to find out the quality and efficiency of teaching the arithmetic balance in schools.

The research task. Conduct a survey of private and public school teachers in order to find out what's their attitude towards teaching the arithmetic balances and numerical comparisons, how well these issues are taught in schools and what are the challenges they face.

The research subject. The subject is the study of the numerical comparisons and the arithmetic balance.

Object. Process of teaching the above mentioned issue.

Novelty. New issues of arithmetic balances are already integrated in the content of the National Curriculum program. The novelty of the study is addressing the problem of methodological literature, not adequately emphasizing the teaching of the above mentioned issue , it is necessary to study how the matter of arithmetic issues are taught in schools.

Basic results. As a result of conducted research, we came to some conclusions and made relevant recommendations for solving the existing problem, as it is evident for the study that teachers frequently ignore teaching the concept of arithmetic balance and numerical comparisons.

შინაარსი

შესავალი

დიდია მათემატიკის მნიშვნელობა ყოველდღიურ ცხოვრებაში. წარმოუდგენელია საზოგადოების განვითარება ანგარიშისა და მათემატიკური მოქმედებების ცოდნის გარეშე. არითმეტიკა სწორედ ადამინთა შრომით საქმიანობაში სხვადასხვა ცხოვრებისეული გამოთვლებისთვის აღმოცენდა. იგი ძალიან ნელა და დიდხანს ვითარდებოდა.

არითმეტიკა შეისწავლის რიცხვთა უმარტივეს თვისებებს და მოქმედებებს მათზე. თავიდან არითმეტიკა მხოლოდ ნატურალურ რიცხვებს განიხილავდა. მათემატიკა ერთ–ერთი უძველესი მეცნიერებაა. იგი არის მეცნიერება რეალური სამყაროს რაოდენობრივი მიმართებებისა და სივრცითი ფორმების შესახებ. ეს მიმართებები კი უწყვეტად ფართოვდება. თვით ტერმინი მათემატიკა ბერძნული წარმოშობისაა, μάθημα (máthema) „მეცნიერებას, ცოდნას, სწავლას“ ნიშნავს, ხოლო μαθηματικός (mathematikós) – „სწავლის მოყვარულს“.

თანამედროვე ეპოქაში მათემატიკა ცხოვრების განუყრელი ნაწილია. იგი გამოიყენება ადამიანის საქმიანობის ყველა სფეროში: მეცნიერებასა და ტექნოლოგიებში, მედიცინაში, ეკონომიკაში, გარემოს დაცვასა და აღდგენა-კეთილმოწყობაში, სოციალურ გადაწყვეტილებათა მიღებაში. საინფორმაციო და გამოთვლითი ტექნოლოგიების განვითარება, სივრცე-დროის სტრუქტურის უკეთ გააზრება, ბუნებაში არსებული მრავალი კანონზომიერების აღმოჩენა და აღწერა, ნათლად წარმოაჩენს მათემატიკის სამეცნიერო და კულტურულ ღირებულებას. მათემატიკა ხელს უწყობს ადამიანის გონებრივი შესაძლებლობების განვითარებას. იგი იძლევა ეფექტიანი, ლაკონური და არაორაზროვანი კომუნიკაციის საშუალებას. მათემატიკის გამოყენებით შესაძლებელია რთული სიტუაციის თვალსაჩინო წარმოჩენა, მოვლენების ახსნა და მათი შედეგების განჭვრეტა. მათემატიკაში შექმნილი აბსტრაქტული სისტემები და თეორიული მოდელები გამოიყენება კანონზომიერებების შესასწავლად, სიტუაციის გასაანალიზებლად და პრობლემების გადასაჭრელად.მათემატიკის სწავლებისას, ძირითადი ფოკუსის გადატანა

როგორც პრაქტიკული ასევე მეცნიერული ხასიათის პრობლემების გადაჭრაზე, აძლიერებს მოსწავლეთა მოტივაციას და აღძრავს მათემატიკისადმი ინტერესს. მათემატიკის სტანდარტის ერთერთი მნიშვნელოვანი სიახლე არის, დისკრეტული მათემატიკის ელემენტების შეტანა საშუალო სკოლაში. დაემატა ნაშთთა არითმეტიკის სწავლების საკითხი. სამაგისტრო თემა სწორედ ეხება ნაშთთა არითმეტიკის სწავლების პრობლემატიკას საშუალო საფეხურზე.(http://mes.gov.ge/content.php?id=3929&lang=geo)

თემის აქტუალობა: ნაშთთა არითმეტიკის სწავლების სკითხი, ერთერთი აქტუალური თემაა, რადგან ის ახალი შეტანილია ეროვნულ სასწავლო გეგმაში/. ამ საკითხის სავლებას სათანადო ყურადღება არ ექცეოდა მათემატიკურ სპეციალობებზე , ამიტომ მასწავლებლების უმრავლესობა კარგად არ იცნობს ნაშთთა არითმეტიკის მეცნიერულ საფუძვლებს , ამიტომ მისი გადაცემა მოსწავლეებისთვის თითქმის არ ხდება , ტოვებენ აღნიშნულ საკითხს ან მხოლოდ ელემენტარული ნაშთიანი გაყოფის სწავლებით შემოიფარგლებიან. ეროვნულ გამოცდებზე ხშირად იყენებენ ამოცანებს ნაშთთა არითმეტიკიდან.

კვლევის ამოცანები: პრობლემის გადაჭრის გზები, მასწავლებელთა პრაქტიკული გამოცდილების შესწავლა და სათანადო რეკომენდაციენის შემუშავება.

კვლევის მეთოდი: სწავლების პროცესზე დაკვირვება ინტერნეტ–რესურსის მოძიება, დახარისხება, გამოყენება, გამოკითხვა, გამოცდილების შესწავლა და ანალიზი.

თავი №1

§1. საშუალო სკოლაში ნაშთთა არითმეტიკის სწავლება ეროვნული სასწავლო გეგმის მიხედვით

განათლების ისტორიის შესწავლა გვიჩვენებს, რომ ცალკეულ საგანთა სწავლების მეთოდიკას დიდი ყურადღება ექცეოდა ძველთაგან. სწავლების მეთოდები და ფორმები თანდათან დაიხვეწა და სრულყოფილი გახდა. ეს პროცესი დღესაც მიმდინარეობს და გაგრძელდება. ის მდიდარი პედაგოგიური მემკვიდრეობა, რომელიც წინაპრებისაგან მემკვიდრეობით გადმოგვეცა , სწავლების პროცესში გათვალისწინებული უნდა იქნეს და გამოყენებადი პედაგოგიური და მეთოდიკური თვალსაზრისით. საგნის სწავლების ეფექტურობის მაღალი დონე მიიღწევა მაშინ, როცა სწავლება იქნება მიზანდასახული, ბუნებრივი და შეესაბამება მოსწავლის განვითარების ასაკობრივ და ინდივიდუალურ თავისებურებებს. ყველა სასწავლო საგანს დიდი მნიშვნელობა აქვს მოსწავლეთა გონებრივ განვითარებასა და მთელი რიგი უნარ-ჩვევების ფორმირებაში, მაგრამ ლოგიკური აზროვნების განვითარებაში ერთ-ერთ მთავარი ადგილი მათემატიკას ეკუთვნის. მათემატიკა მოსწავლეთა შემეცნების ყველა საფუძველთა საფუძველს წარმოადგენს, იგი გვეხმარება ბუნებაში არსებული მრავალფეროვნების შინაგანი კავშირების შეცნობაში. (თ.დოგრაშვილი.2010წ გვ.6).

განათლებისა და მეცნიერების სამინისტრომ, შეიმუშავა ზოგადი განათლების ეროვნული მიზნების დოკუმენტი, რომელიც ზოგადსაგანმანათლებლო სისტემის სასურველ შედეგს აღწერს (დოკუმენტი დამტკიცებულია საქართველოს მთავრობის მიერ. განკარგულება №84, 2004 წლის 14 ოქტომბერი).

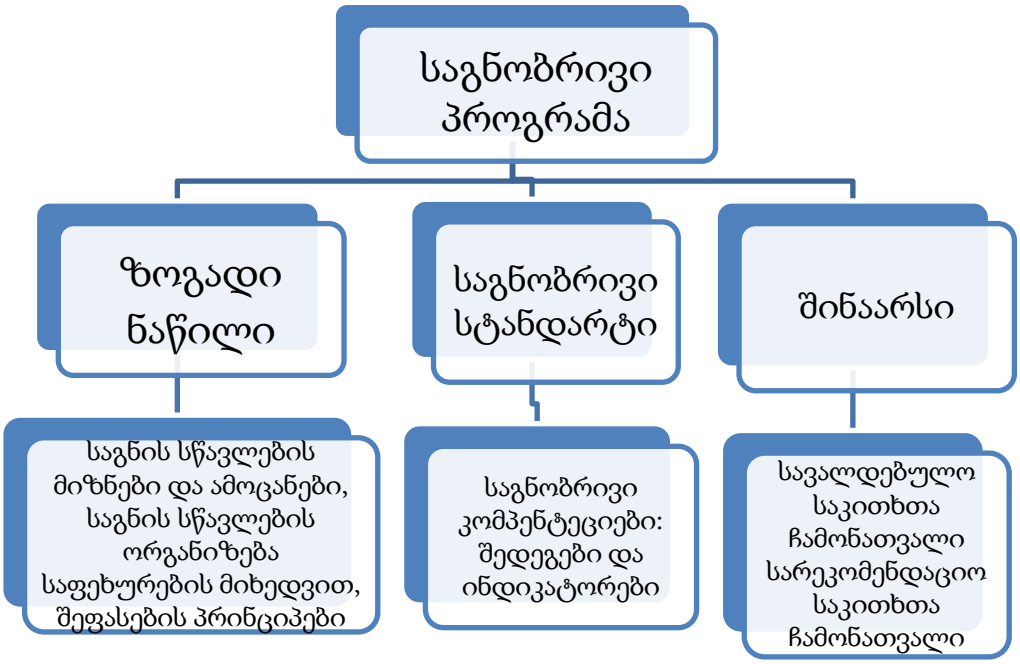
ზოგადსაგანმანათლებლო სკოლა დაყოფილია სამ საფეხურად: დაწყებითი (I – VI კლასები), საბაზო (VII – IX კლასები) და საშუალო (X – XII კლასები). მათემატიკის სასწავლო კურსის აგების პრინციპი ითვალისწინებს ამ დაყოფას

და თითოეულ საფეხურზე მათემატიკის სწავლებას აქვს მკაფიოდ ჩამოყალიბებული მიზნები.

ეროვნული სასწავლო გეგმა არის ერთ-ერთი მთავარი დოკუმენტი, რომელიც განსაზღვრავს , თუ როგორი თაობების აღზრდას უნდა შეუწყოს ხელი საქართველოს ზოგადი განათლების სისტემამ. ეროვნული სასწავლო გეგმის მთავარი ამოცანაა, შექმნას ეროვნული მიზნების მისაღწევი საგანმანათლებლო გარემო და რესურსები. ამ მიზნიდან გამომდინარე, შემუშავებულია პიროვნების განვითარებაზე ორიენტირებულ საგანმანათლებლო კონცეფცია. პიროვნებაზე ორიენტირებული საგანმანათლებლო პროცესის ცენტრში დგას მოსწავლე, მისი განვითარების პროცესი და მის მიერ მიღწეული შედეგი. შედეგზე ორიენტირებაში იგულისხმება არა მხოლოდ მოსწავლისათვის მიწოდებული ინფორმაციის დამახსოვრება, არამედ ამ ინფორმაციის მყარ,ფუნქციურ და დინამიურ ცოდნად გარდაქმნა.

აქედან გამომდინარე, ეროვნული სასწავლო გეგმის პრინციპია შედეგზე ორიენტირება, რაც გულისხმობს მოსწავლეთა აღჭურვას ქმედითი ცოდნით. საგნობრივი პროგრამების სამნაწილიან სტრუქტურაში ასახულია არსებული მოთხოვნები:

საგნობრივი პროგრამების სტრუქტურა



„საგნობრივი პროგრამების ზოგადი ნაწილი განსაზღვრავს საგნის სწავლების ამოცანებს და იმ ძირითად ორიენტირებს, რომლებიც ზოგადი განათლების ეროვნული მიზნებიდან გამომდინარეობს.“ (11.10.2011 N224/ნ 1.1 ოვნული სასწავლო გეგმა 2011:3].

საგნობრივი სტანდარტში ასახულია ის არსებითი , საგნობრივი კომპეტენციები , რომლითაც მოსწავლეები უნდა დაეუფლონ დასახული მიზნების მისაღწევად. საგნობრივ სტანდარტში მოცემული და აღწერილი კომპეტენციები მოიცავს ცოდნის სამ კატეგორიას : ა) დეკლარატული ანუ სტატიკური ხასიათის ცოდნას, რომელიც ვერ უზრუნველყოფს ცოდნის პროცედურულად გამოყენებას. სტატიკურია მოსწავლის ცოდნა, თუ მან იცის კონკრეტული მათემატიკური ოპერაციის წარმოების წესი, თუმცა ვერ იყენებს მას; ბ) პროცედურულს ანუ დინამიურ ცოდნას, რომელიც ცოდნის გამოყენების და ამ ცოდნის რეალიზების საშუალებას იძლევა; პროცედურულია მოსწავლის ცოდნა, თუ ის ასრულებს მათემატიკურ ოპერაციას. მისი ათვისება შესაძლებელია მრავალჯერადი გავარჯიშების გზით და გ) პირობისეულ ცოდნას, ანუ ფუნქციურ ცოდნას, ეს კატეგორია უზრუნველყოფს ცოდნის ადეკვატურად გამოყენებას.

პირობისეულია მოსწავლის ცოდნა, თუ მას შეუძლია დასმული ამოცანის ამოსახსნელად შეარჩიოს სათანადო მათემატიკური ოპერაცია. (11.10.2011 N224/ნ)

ცოდნის სამი კატეგორია (11.10.2011 N224/ნ)

1.2

საგნობრივი პროგრამების ძირითადი ნაწილში სწავლების მიზნები ჩამოყალიბებულია კონკრეტული შედეგების სახით, ანუ იმ ცოდნისა და უნარ-ჩვევების სახით, რომლებიც უნდა წარმოაჩინოს მოსწავლემ სასწავლო პროცესის დასრულების შემდეგ. სტანდარტში მოცემულია შედეგები და ინდიკატორები , რომლის საშუალებითაც მასწავლებელს ეძლევა კონკრეტული მითითება იმის შესახებ, თუ როგორ და რა კუთხით უნდა დაამუშავებინოს მოსწავლეებს მოცემული შინაარსობრივი საკითხები. იმისთვის რომ მოსწავლეებმა საფუძვლიანი და გააზრებული ცოდნა მიიღონ , საგნობრივი პროგრამა საშუალებას გვაძლევს და მიუთითებს , თუ როგორ უნდა წარიმართოს სასწავლო პროცესი .(11.10.2011 N224/ნ)

ეროვნულის სასწავლო გეგმაში მოცემული პროგრამის შინაარსში წარმოადგენილია სავალდებულო და სარეკომენდაციო სასწავლო საკითხები (11.10.2011 N224/ნ);

ეროვნული სასწავლო გეგმას შეიმუშავებს საქართველოს განათლებისა და მეცნიერების სამინისტრო და ზოგადი განათლების განვითარების

დეპარტამენტი. იგი განკუთვნილია ზოგადი განათლების სფეროში მონაწილე ყველა სუბიექტისთვის (11.10.2011 N224/ნ).

მათემატიკის სწავლების მიზნები და ამოცანები ეროვნული სასწავლო გეგმით შემდეგია:

ზოგადსაგანმანათლებლო სკოლაში მათემატიკის სწავლების ძირითადი მიზნებია:

- მოსწავლეებისათვის აზროვნების უნარის განვითარება;
- დედუქციური და ინდუქციური მსჯელობის, შეხედულებათა დასაბუთების მოვლენებისა და ფაქტების ანალიზის უნარის განვითარება;
- მათემატიკის, როგორც სამყაროს აღწერისა და მეცნიერების უნივერსალური ენის ათვისება;
- მათემატიკის, როგორც ზოგადსაკაცობრიო კულტურის შემადგენელი ნაწილის გაცნობიერება;
- სწავლის შემდგომი ეტაპისათვის ან პროფესიული საქმიანობისათვის მომზადება;

მათემატიკის ცოდნა ნიშნავს მათემატიკური ცნებებისა და პროცედურების ფლობას, მათი გამოყენების უნარს რეალური პრობლემების გადაჭრისას; აგრეთვე კომუნიკაციის იმ საშუალებების ფლობას, რომლებიც საჭიროა ინფორმაციის მისაღებად და გადასაცემად მათემატიკური ენისა და საშუალებების გამოყენებით. [ეროვნული სასწავლო გეგმა 2011:373-374].

მათემატიკური განათლება ხელს უწყობს : პრობლემის გადაჭრის, მოდელირების, დამოუკიდებლობის, მსჯელობა-დასაბუთების და კომუნიკაციის უნარ-ჩვევების ჩამოყალიბებას:

ცხოვრებისეული ამოცანების გადასაწყვეტად აუცილებელია მოხდეს ცოდნის გადაცემა და შესაბამისად ამ ცოდნის გამოყენების უნარის განვითარება.

ეროვნული სასწავლო გეგმის მიხედვით, მათემატიკის საგნობრივ პროგრამაში გამოყოფილია ოთხი მიმართულება: რიცხვები და მოქმედებები; გეომეტრია და სივრცის აღქმა; მონაცემთა ანალიზი, სტატისტიკა და ალბათობა; კანონზომიერებები და ალგებრა.ეს მიმართულებები ერთმანეთთან მჭირო

კავშირშია და მოიცავს იმ ცოდნას და უნარ-ჩვევებს, რომელსაც მოსწავლე უნდა დაეუფლოს ზოგადსაგანმანათლებლო სკოლაში. მიმართულებებად დაყოფა საშუალებას იძლევა მიეთითოს, სწავლების ამა თუ იმ საფეხურზე, თუ რაზე უნდა გამახვილდეს მეტი ყურადღება.

რიცხვები და მოქმედებები:

- რიცხვები, მათი გამოყენებები და რიცხვის წარმოდგენის საშუალებები;
- მოქმედებები რიცხვებზე და რიცხვითი თანაფარდობები;
- რაოდენობათა შეფასება და მიახლოება;
- სიდიდეები, ზომის ერთეულები და რიცხვების სხვა გამოყენებები.

გეომეტრია და სივრცის აღქმა:

- გეომეტრიული ობიექტები: მათი თვისებები, ურთიერთმიმართება და კონსტრუირება;
- ზომა და გაზომვის საშუალებები;
- გარდაქმნები და ფიგურათა სიმეტრიულობა;
- კოორდინატები და მათი გამოყენება გეომეტრიაში.

მონაცემთა ანალიზი, ალბათობა და სტატისტიკა:

- მონაცემთა წყაროები და მონაცემთა მოპოვების საშუალებები;
- მონაცემთა მოწესრიგების ხერხები და მონაცემთა წარმოდგენის საშუალებები;
- მონაცემთა შემაჯამებელი რიცხვითი მახასიათებლები;
- ალბათური მოდელები;
- შერჩევითი მეთოდი და შერჩევის რიცხვითი მახასიათებლები.

კანონზომიერებები და ალგებრა:

- სიმრავლეები, ასახვები, ფუნქციები და მათი გამოყენება;
- დისკრეტული მათემატიკის ელემენტები და მათი გამოყენება;
- ალგორითმები და მათი გამოყენება;

ალგებრული ოპერაციები და მათი თვისებები; [ეროვნული სასწავლო გეგმა 2011:375-376].

კანონზომიერებები და ალგებრა

ამ მიმართულების მიზანია, მოსწავლეს ჩამოუყალიბდეს კანონზომიერებების, ალგებრული მიმართებებისა და ფუნქციური დამოკიდებულებების ამოცნობის და აღწერის, აგრეთვე მათი საშუალებით მოვლენების მოდელირებისა და პრობლემების გადაჭრის უნარები.

დაწყებითი საფეხურზე ამ მიმართულების მიზანია მარტივი კანონზომიერებებისა და სიდიდეებს შორის დამოკიდებულების ამოცნობის უნარის განვითარება, ასოთი აღნიშნვნის გამოყენების და არითმეტიკული ოპერაციების შესწავლა.

საბაზო საფეხურზე მიმართულების მიზანია სიდიდეებს შორის დამოკიდებულებებთან დაკავშირებული ცნებებისა და პროცედურების შესწავლა. პრობლემის გადაჭრისას ასოითი გამოსახულების გამოყენების, განტოლების შედგენისა და ამოხსნის უნარის განვითარება; გარკვეული წარმოდგენების შექმნა სიმრავლურ ცნებებსა და ოპერაციებზე.

საშუალო საფეხურის მიზანია ფუნქციათა ოჯახების, მათი შედარებისა კვლევის მეთოდების შესწავლა; სტრუქტურის აღწერისა და შესწავლისას დისკრეტული მათემატიკის აპარატის გამოყენების უნარის განვითარება.

საშუალო სკოლაში მათემატიკის სწავლების შინაარსს შემდეგ მოთხოვნებს უყენებენ: 1) საგანმანათლებლო ღირებულებები. 2) გამოყენებებზე ორიენტაცია. 3) მათემატიკის გამოყენებების ჩვევების დაუფლება. 4) საშუალო სკოლის დამთავერბისა და უმაღლეს სკოლაში სწავლის გაგრძელების საშუალებების შექმნა. მათემატიკის განვითარებას ცვლილებები შეჰქონდა სასკოლო მათემატიკის შინაარსში – იცვლებოდა აქცენტები, რომლებიც საგანმანათლებლო ღირებულებებსა და გამოყენებებს უკავშირდება; ძველ საბერძნეთში მთელ რიცხვთა თვისებების შესწავლის დროს ვერავინ წარმოიდგენდა ამ თვისებების გამოყენებებს (კრიპტოგრაფიაში). (http://mes.gov.ge/content.php?id=3929&lang=geo)

მათემატიკის განვითარების მესამე პერიოდის – მე-19 საუკუნის მიწურულს უკავშირდება დისკრეტული მათემატიკის ისეთი დარგების განვითარება, როგორიცაა სიმრავლეთა თეორია და მათემატიკური ლოგიკა,

კომბინატორული ალბათობის თეორია, კომბინატორული ანალიზი, გრაფთა თეორია, ალგორითმების თეორია, ავტომატთა თეორია, თამაშთა თეორია. დისკრეტული მათემატიკის დახასიათება და ანალიზი გადმოცემულია ალექსანდრე ხარაზიშვილის წიგნში ([1]): "ჩვენი აზრით, საჭიროა ამ ფაქტორის (ოცდამეერთე საუკუნეში დისკრეტული მათემტიკის მნიშვნელობა და მისდამი ინტერესი კიდევ უფრო გაიზრდება) გათვალისწინება საშუალო სკოლებისა და უმაღლესი სასწავლებლების პროგრამაში. კერძოდ, აუცილებელია, რომ ამ სასწავლო პროგრამებში დისკრეტული მათემატიკის ხვედრითი წილი ცოტათი მაინც შეესაბამებოდეს იმ პროპორციას, რაც დღეს რეალურად არსებობს დისკრეტულ და დანარჩენ მათემატიკას შორის. ეს მეთოდოლოგიურადაც გამართლებული იქნება, რადგან ჩვენი ალფაბეტი, სასაუბრო ენა, მსჯელობის ფორმები და სხვადასხვა ტიპის გამოთვლითი პროცესები დისკრეტული ფენომენის ფორმებია. ამიტომ დისკრეტული მათემატიკის მეთოდები და ამოცანები ფსიქოლოგიურადაც შედარებით ადვილად მისაღებია მოსწავლეებისა და სტუდენტებისათვის, თუკი მათ შესაბამის მასალას სათანადო თანამიმდევრობით მივაწვდით. შემთხვევითი არაა, რომ სახალისო მათემატიკის ამოცანები, რომლებიც ზეპირსიტყვიერებით ვრცელდება, როგორც წესი, დისკრეტული (კომბინატორული) მათემატიკის სფეროდანაა აღებული . კარგი იქნება, თუკი ახალგაზრდა ადრეულ ასაკშივე მიეჩვევა იმ კატეგორიებით აზროვნებას, რომელიც მას მომავალში უფრო გამოადგება. რასაკვირველია, ცუდი არ არის ის გარემოება, როცა მოსწავლე გაწაფულია სხვადასხვა ტიპის განტოლებების ამოხსნასა და ათასგვარი მათემატიკური გამოსახულებების გამარტივებაში, მაგრამ საჭიროა არსებითად გავითვალისწინოთ ის ფაქტიც, რომ თანამედროვე კომპიუტერები მსგავს საქმიანობას ადამიანზე გაცილებით უფრო, კარგად, სწრაფად და ზუსტად ასრულებენ. ამიტომ ზოგ შემთხვევაში უპრიანი იქნება აქცენტები განტოლების ამოხსნის ტექნიკური დეტალებიდან იმავე განტოლების შედგენის პროცესზე გადავიტანოთ. უფრო ზუსტად, ბევრად მეტი ყურადღება უნდა მივაქციოთ მათემატიკური მოდელირების შემოქმედებით პროცესს, ვიდრე გამოთვლითი

ხასიათის ტექნიკურ პრობლემებს. აქვე შეგვიძლია აღვნიშნოთ, რომ ბოლო დროს ამ მხრივ საშუალო სკოლების ზოგიერთი სახელმძღვანელოში უკვე შეიმჩნევა დადებითი ტენდენციები . იმედია, რომ მომავალში ეს ტენდენციები უფრო გაღრმავდება და ანალოგიური ცვლილებები, შესაბამისად უფრო მკაფიოდ აისახება მათემატიკის პროგრამებში". აქ მითითებული სახელმძღვანელოს წერის პროცესში არ იყო ჯერ კიდევ შექმნილი მათემატიკის სასკოლო კურსის სტანდარტი. მაშინ ჩატარებული კონკურსების დებულების შესაბამისად პროგრამების შედ გენაც სახელმძღვანელოების ავტორებს ევალებოდა.

2007 წლიდან იწყება ახალ ეროვნულ სასწავლო გეგმის შედგენა. ამჟამად სკოლებში 2017-2021 წლების ეროვნული სასწავლო გეგმის მიხედვით შედგენილი სახელმძღვანელოებია მოქმედებაში.

ეროვნული სასწავლო გეგმის მიხედვით , როგორც ვიცით გამოყოფილია ოთხი მიმართულება: რიცხვები და რიცხვებზე მოქმედებები; გეომეტრია და სივრცის აღქმა; სტატისტიკა და ალბათობა; კანონზომიერებები და ალგებრა. აღსანიშნავია, რომ მიმართულებების მიხედვით დიდი ადგილი აქვს დათმობილი დისკრეტული მათემატიკისა და მისი გამოყენებითი ასპექტების სწავლებას: ნაშთთა არითმეტიკა, კომბინატორიკა, კომბინატორული ალბათობა, ლოგიკა და დასაბუთების ხერხები, ალგორითმები, სიმრავლეთა თეორია; ისწავლება მათემატიკის სხვადასხვა მეთოდი – კოორდინატთა მეთოდი, ვექტორული ანალიზის მეთოდი.

მნიშვნელოვანი ადგილი აქვს დათმობილი ნაშთთა არითმეტიკისა და მისი გამოყენებების სწავლებას. ამ თეორიის საფუძველი ნაშთიანი გაყოფის შესახებ თეორემაა: თუ a და b მთელი რიცხვებია, $b>0$, მაშინ არსებობს ისეთი მთელი q და r, რომ $a=bq+r$ და $0\le r<b$. ამ თეორემას ზოგიერთი ავტორი გაყოფის ალგორითმს უწოდებს . მისი დამტკიცება იმ უდიდესი q რიცხვის არსებობის ინტუიციურ გააზრებას უკავშირდება, როცა bq არის b-ს ისეთი უდიდესი ჯერადი, რომელიც a-ს არ აღემატება, ანუ $r=a-bq$ არაუარყოფითია და $b(q+1)>a$. ამ ფაქტის ინტერპრეტაცია გასაგები ხდება რიცხვითი წრფის მოშველიებით;

თუ a>b, მაშინ რიცხვით წრფეზე გადავდებთ b-ს ჯერადის ტოლ მონაკვეთებს 1·b; 2·b, ... – მანამ, სანამ a არ იქნება b-ს ამ ჯერადებზე ნაკლები.

დაწყებით საფეხურზე გეომეტრიული წარმოდგენების გამოყენება აადვილებს ნაშთის გააზრებას. უკვე მე-4 კლასში მოსწავლეს მოეთხოვება გამოთვლებზე ამოცანების ამოხსნისას, ნაშთით გაყოფის შემთხვევაში, ამოცანის კონტექსის გათვალისწინებით ნაშთის ინტერპრეტაცია; მონაცემის ზომის ერთი ერთეულიდან მეორე ერთეულში გადაყვანის პროცესში ნაშთით გაყოფის გამოყენება.

საბაზო სკოლის საფეხურზე იწყება ნაშთით გაყოფის გამოყენება გაყოფადობის ნიშნების წარმოდგენისას, კონკრეტულ შემთხვევებში დასაბუთების ელემენტების შემოღებისა და გააზრების პროცესში.

მე-9 კლასის სახელმძღვანელოში აღნიშნულ თემას სპეციალური პარაგრაფიც აქვს დათმობილი , ნაშთთა არითმეტიკა სახელწოდებით. უცხოურ ლიტერატურაში ეს თემა მოდულარული არითმეტიკის სახელწოდებითაა ცნობილი. ამ საკითხის სრულყოფილი გადაცემისთვის მასწავლებელი კარგად უნდა იცნობდეს აბსტრაქციის ერთ-ერთ ფორმას – გაიგივებას, რომელიც ხშირად გამოიყენება მათემატიკაში – ექვივალენტობის ყოველი კლასი (ჩვენს შემთხვევაში – ნაშთთა კლასი) აღიწერება და "წარმოიდგინება" მისი ერთი წარმომადგენლით (ამ შემთხვევაში – ნაშთით); კლასებზე "მოქმედებებს" ცვლის ნაშთებზე მოქმედებები, ნაშთთა კლასების სიმრავლე სასრული რგოლის მაგალითია; როცა მოდული მარტივი რიცხვია, მაშინ ეს რგოლი ველია. ძალიან მნიშვნელოვანია ჯგუფური მუშაობის შესრულება, როცა ვიხილავთ სხვადასხვა მოდულის შემთხვევებს, აქ ყურადღებას ვამახვილებთ ამ "არაჩვეულებრივი არითმეტიკის" ერთ უცნაურ თვისებაზეც – შეიძლება არანულოვანი ნაშთების ნამრავლი ნულის ტოლი იყოს.

ამ თემის შემდგომი განვითარება და გამოყენების ასპექტების წარმოდგენა საშუალო სკოლის მესამე საფეხურზე გრძელდება.

ეს საფეხური უმაღლეს სკოლაში სწავლის გაგრძელებისთვის მომზადებასაც ითვალისწინებს. მთელ რიცხვთა არითმეტიკის საკითხები მსოფლიოს ყველა

უმაღლესი სასწავლებლის ინფორმაციული ტექნოლოგიების შემსწავლელი ფაკულტეტების სასწავლო პროგრამების განუყოფელ ნაწილად იქცა. ეს არც არის გასაკვირი, მათემატიკის შესწავლის საგანი სხვადასხვა მათემატიკური სტრუქტურაა. ამ სტრუქტურათა ყველა მარტივი და გამორჩეული მაგალითი მთელ რიცხვთა სისტემაში შეიძლება ვეძიოთ (მაგალითად, ნაშთთა კლასების რგოლი, დაყვანილ ნაშთთა კლასების ველი). ამასთანავე, მთელ რიცხვთა თეორიას ჩვენ რეალობაში საკმაოდ ფართო გამოყენება მოეძებნება. ამ გამოყენებების წარმოდგენა "საათის არითმეტიკის" განხილვით იწყება. ამ არითმეტიკიდან, რომლის ნულოვანი ელემენტის როლს ასრულებს რიცხვი 12, იწყება გადასვლა ნაშთთა არითმეტიკაზე, რომლის ნულოვავნი ელემენტი ნულით იქნება წარმოდგენილი.

გ.გოგიშვილი, თ.ვეფხვაძე, ი.მებონია, ლ.ქურჩიშვილის სახელმძღვანელოში, დაშიფრვის პირველი მაგალითების განხილვა იწყება მე-11 კლასში – ანბანის წანაცვლების ოპერაციით, რომელიც ანბანში ასოების რაოდენობის მიხედვით განსაზღრული მოდულის არითმეტიკაზე გადასვლით ხასიათდება. შედარების მიმართების განხილვა და უფრო არსებითი შესწავლა მე-11 კლასში უნდა დავიწყოთ. აქცენტი უნდა გაკეთდეს მთელ რიცხვთა იმ გამოყენებებზე (ინფორმაციის საიდუმლო გადაცემის ამოცანები – შიფრის შედგენის წესები), რომელმაც მთელი რიცხვის თვისებებისადმი ინტერესი თანამედროვე "კომპიუტერული რევოლუციის" შემადგენელ ნაწილად გახადა. ამ მიმართულებით კვლევა უკვე მე-20 საუკუნეში დაიწყო: "კომპიუტერულმა რევოლუციამ, რომელმაც დიდი რიცხვების გამოყენების საშუალება მისცა ადამიანს, კვლავ მიაპყრო მეცნიერთა ყურადღება იმ კანონზომიერებებზე, რომლებიც ნატურალური რიცხვებით აღიწერება, კვლავ ააღორძინა და ახალი იმპულსი მისცა პითაგორელთა ინტერესს მთელი რიხვებისა და მათი უდიდეს მნიშვნელობისადმი".

მე-11 კლასში შეიძლება დავიწყოთ ნაშთთა არითმეტიკის გამოყენების მაგალითების განხილვა (შეჯიბრების განრიგის შედგენა, წრფივი შედარების ამოხსნასთან დაკავშირებული შიფრის შედგენა). მოსწავლეთა ძირითადი

აქტივობა ამ დროს უკავშირდება ორი ხსვადასხვა ტიპის შიფრის გამოყენებას – პირველი შიფრი დაკავშირებულია k რიცხვის შემოტანასა და m რიცხვით გამოსახული შეტყობინების რაიმე დიდი მარტივი p მოდულით mk რიცხვის p-ზე გაყოფისას მიღებული ნაშთით ჩანაცვლებაზე.

შემდგომი აქტივობები გაშიფვრის განხორციელებისათვის საჭირო ჩვევების დაუფლებას ეძღვნება – განვიხილავთ მაგალითებს, როცა საჭიროა $ax \equiv b (mod p)$ შედარების ამონახსნის პოვნა. აქ, ცხადია, შესაძლებელია ფერმას მცირე თეორემის გამოყენება, რომელიც კლასგარეშე მუშაობის დროს შეიძლება გაკეთდეს. ამ შედარებების ამონახსნების პოვნა კი შესაძლებელია სინჯვის მეთოდით, ან ევკლიდეს ალგორითმის გამოყენებით. ეს უკანასკნელი, თავის მხრივ, ორუცნობიანი განტოლების მთელ რიცხვებში ამოხსნების პოვნას უკავშირდება.

ნაშთთა არითმეტიკის ელემენტების სწავლება სკოლაში მათემატიკის სწავლების სხვადასხვა მიზნების განხორციელების ერთ-ერთი საშუალებაა: გარემომცველი სამყაროს შემეცნებისას მათემატიკური მეთოდების გამოყენება, ძირითადი ფოკუსის გადატანა, როგორც პრაქტიკული, ასევე, მეცნიერული ხასიათის პრობლემების გადაჭრაზე; მოსწავლეთა მოტივაციის გაზრდა; შემოქმედებითი უნარის განვითარება; სწავლის შემდგომი ეტაპისათვის ან პროფესიული საქმიანობისათვის მომზადება; ცხოვრებისეული ამოცანების გადასაწყვეტად საჭირო ცოდნის გადაცემა და ამ ცოდნის გამოყენების უნარის განვითარება.

ნაშთთა არითმეტიკის ელემენტების სწავლების ეფექტურობა უკავშირდება სწავლების პროცესში მათემტიკური კვლევის ისეთი მეთოდების გამოყენებას, როგორიცაა დაკვირვება, შედარება ,განზოგადება და სპეციალიზაცია, აბსტრაქცია და კონკრეტიზაცია (კლასის "გაიგივება" კონკრეტულ ნაშთთან), ინდუქცია და დედუქცია.(თ.ვეფხვაძე .2013წ)

„მათემატიკის სტანდარტი:

მე-4 კლასი

მათ. IV.3. მოსწავლეს შეუძლია გამრავლება-გაყოფის მოქმედებების შესრულების რომელიმე ხერხის გამოყენება.

• გამოთვლებზე ამოცანების ამოხსნისას, ნაშთით გაყოფის შემთხვევაში, ახდენს ნაშთის ინტერპრეტაციას ამოცანის კონტექსტის გათვალისწინებით.

პროგრამის შინაარსი

1.ნაშთით გაყოფა

მე-5 კლასი

მათ. V.4. მოსწავლეს შეუძლია ზომის სხვადასხვა ერთეულების ერთმანეთთან დაკავშირება და გამოყენება.

• იყენებს ნაშთით გაყოფას ზომის მოცემულ ერთეულებში მონაცემის სხვა ერთეულით გამოსახვისას (მაგალითად, რამდენი საათია 50000 წამი).

მე-6 კლასი

მათ.VI.4. მოსწავლეს შეუძლია პრობლემების გადაჭრა გამოთვლების, ვარიანტების დათვლის და მიმართებების გამოყენებით.

• იყენებს პოზიციური სისტემის შესახებ ცოდნას, ამოწურვის და გამორიცხვის ხერხებს და ნაშთით გაყოფას ამოცანების ამოხსნისას (მაგალითად, ამოცანები ვარიანტების დათვლაზე; წერითი ალგორითმის გამოყენებით შესრულებული გამრავლების ნიმუშში გამოტოვებული ციფრების ჩასმა და პასუხის დასაბუთება; დადგენა, თუ რამდენი წელია მაგალითად 1200 დღე ნაკიანი წლების გათვალისწინებით);

მე-7 კლასი

<u>პროგრამის შინაარსი</u>

1.ნაშთით გაყოფა, ნაშთი და გაყოფადობის ნიშნებიდან ზოგიერთი.

მე-8 კლასი

<u>პროგრამის შინაარსი</u>

1.ნაშთი.

მე-9 კლასი

მათ. IX.1. აღნიშნავს ნაშთის პერიოდულობას ერთნიშნა რიცხვზე ნატურალური რიცხვების თანმიმდევრულად გაყოფისას; განმარტავს შემჩნეულ კანონზომიერებას;

მათ. IX.2. იყენებს გაყოფადობის ნიშნებს და ნაშთის თვისებებს რიცხვებისა და არითმეტიკული მოქმედებების შედეგის თვისებებზე მსჯელობისას (მაგალითად, "რას მივიღებთ ნაშთში თუ 2345 გავყოფთ 3-ზე?");

მათ. IX.3. მოსწავლეს შეუძლია მსჯელობა-დასაბუთების ზოგიერთი ხერხის გამოყენება.

- ასაბუთებს ნაშთთა არითმეტიკის დებულებებს და იყენებს ნაშთთა არითმეტიკის ელემენტებს ამოცანების ამოხსნისას (მაგალითად, რიცხვების შეკრება/გამოკლება მოდულით 12, 60 ან 360; ისეთი ამოცანების ამოხსნისას, რომლებიც დაკავშირებულია საათთან ან კუთხით მობრუნებასთან).

<u>პროგრამის შინაარსი</u>

- ნაშთთა არითმეტიკის ელემენტები.

მე-11 კლასი

მათ. XI.3. გაძ. მოსწავლეს შეუძლია პრაქტიკული საქმიანობიდან მომდინარე პრობლემების გადაწყვეტა

- ასრულებს ინფორმაციის დაშიფვრასთან დაკავშირებულ გამოთვლებს და ახდენს ინფორმაციის გაშიფვრა-წაკითხვას რომელიმე მისთვის ცნობილი ალგორითმის გამოყენებით (მაგალითად, $f(x) = ax + b \mod n$ გარდაქმნის შებრუნებული გარდაქმნის, ანუ გაშიფვრის "გასაღების" მოსაძებნად იყენებს ევკლიდეს ალგორითმს; ახდენს ამ პროცედურის დემონსტრირებას კალკულატორის ან კომპიუტერის გამოყენებით).

<u>პროგრამის შინაარსი</u>

- ნაშთების არითმეტიკის ელემენტები."

[http://mes.gov.ge/content.php?id=3929&lang=geo 2011]

§2. რიცხვითი შედარებები და ნაშთთა სისტემები

ახლა რაც შეეხება რიცხვთა თეორიის და კერძოდ მოდულური არითმეტიკის წარმოშობაზე.

1801 წელს გერმანიაში ლათინურ ენაზე გამოქვეყნდა კარლ ფრიდრიხ გაუსის (1777-1855) 600-გვერდიანი წიგნი სახელწოდებით "არითმეტიკული გამოკვლევები",.ამ შრომაში გაუსმა საფუძვლიანად დაამუშავა შედარებითი თეორია, დაამტკიცა რიცხვთა თეორიის ერთ-ერთი ცენტრალური თეორემა - კვადრატულ ნაშთთა შექცევადობის კანონი, რომლის დამტკიცებას დიდხანს ცდილობდნენ იმ დროის უდიდესი მათემატიკოსები. ამ შედევრით, ფელიქს კლაინის სიტყვით, გაუსმა შექმნა თანამედროვე რიცხვთა თეორია და წინასწარ განსაზღვრა მთელი მისი შემდგომი განვითარება დღევანდლამდე.

ამ წიგნში გაუსის მიერ პირველად არის შემოღებული მათემატიკისათვის მეტად მნიშვნელოვანი ცნება _ "შედარება" და გადმოცემულია შედარებათა ზოგადი თეორია.

განსაზღვრება 1. ვთქვათ, m ნატურალური რიცხვია, ხოლო a და b მთელი რიცხვები. თუ a- b სხვაობა უნაშთოდ იყოფა m -ზე, მაშინ ამბობენ, a სადარია b -სი მოდულით m და ამ ფაქტს ეგრეთ წოდებული შედარების სახით ჩაწერენ:

$a \equiv b \pmod m \iff m|(a - b) \iff a - b = km,\ k \in Z.$

მაშასადამე $a \equiv b \pmod m$ ნიშნავს :

$a = b + km$, k მთელი რიცხვია.

ამასთანავე , ცხადია, ყოველი a და b მთელი რიცხვებისთვის $a \equiv a \pmod m$;

თუ $a \equiv b \pmod m$, მაშინ $b \equiv a \pmod m$.

მაგალითად, $67 \equiv -3 \pmod 7$, რადგან $7|[67-(-3)]=70$ და ა.შ.

თუ $m \nmid (a-b)$, მაშინ ამბობენ, რომ a არასადარია b-სი მოდულით m და წერენ: $a \not\equiv b \pmod m$. მაგალითად, $53 \not\equiv 5 \pmod 7$, რადგან $7 \nmid (53-5)=48$; ასევე, $13 \not\equiv -4 \pmod{15}$, რადგან $15 \nmid [13-(-4)]=17$ და ა.შ.

განსაზღვრებიდან უშუალოდ გამომდინარეობს, რომ $a \equiv 0 \pmod m$, მაშინ $a|m$ და პირიქით $a|m$, მაშინ $a \equiv m \pmod m$.

აღსანიშნავია აგრეთვე, რომ შედარების ნიშანიც (“ ≡ ”) გაუსის შემოღებულია. იგი უნებლიედ ტოლობის ნიშანს მოგვაგონებს. საქმე ის არის, რომ შედარებას ბევრი ისეთი თვისება აქვს, რომელიც აქვს აგრეთვე ტოლობას და ეს ნიშანიც გარკვეულწილად ხაზს უსვამს ერთგვარ ანალოგიას ამ ორ მიმართებას შორის.

შედარების ცნებას, როგორც ეს განმარტებიდან გამომდინარეობს, ახასიათებს შემდეგი სამი ძირითადი თვისება;

(1) $a\equiv a(\mathrm{mod}\ m)$ $a\in Z$, $m\in N$ (რეფლექსურობის თვისება);

(2) თუ $a\equiv b(\mathrm{mod}\ m)$, maSin $b\equiv a(\mathrm{mod}\ m)$ $a\in Z$, $m\in N$ (სიმეტრიულობის თვისება);

(3) თუ $a\equiv b(\mathrm{mod}\ m)$ და $b\equiv c(\mathrm{mod}\ m)$, მაშინ $a\equiv c(\mathrm{mod}\ m)$ $a,b,c\in Z$, $m\in N$ (ტრანზიტულობსი თვისება);

ვაჩვენოთ რომ ეს მართლაც ასეა;

(1) განმარტების თანახმად, $a\equiv a(\mathrm{mod}\ m) <=> m|(a\_a)=0$;

(2) განმარტების თანახმად, $a\equiv b(\mathrm{mod}\ m) <=> m|(a\_b) => m|(b\_a) <=> b\equiv a(\mathrm{mod}\ m)$;

(3) განმარტების თანახმად, $a\equiv b(\mathrm{mod}\ m) <=> m|(a\_b)$ da $b\equiv c(\mathrm{mod}\ m) <=> m|(b\_c) => m|[(a\_b)+(b\_c)]=a\_b$;

გარდა აღნიშნული თვისებებისა, შედარებებს აქვთ ბევრი სხვა თვისებაც, რომლებსაც ჩამოვაყალიბებთ თეორემების სახით და დავამტკიცებთ.

შედარებები შეიძლება შევკრიბოთ, გამოვაკლოთ, გავამრავლოთ; შედარება შეიძლება ავახარისხოთ კიდეც:

თუ $a\equiv b(\mathrm{mod}\ m)$ და $c\equiv d(\mathrm{mod}\ m)$, მაშინ

$a+c\equiv b+d(\mathrm{mod}\ m)$; $a-c\equiv b-d(\mathrm{mod}\ m)$;

$ac\equiv bd(\mathrm{mod}\ m)$; $a^k\equiv b^k(\mathrm{mod}\ m)$, $k\in N$;

თეორემა 1. თუ $a\equiv b(\mathrm{mod}\ m)$ და $c\equiv d(\mathrm{mod}\ m)$, მაშინ $a+c\equiv b+d(\mathrm{mod}\ m)$ და $a\_c\equiv b\_d(\mathrm{mod}\ m)$.

დამტკიცება. პირობის თანახმად $m|(a\_b)$ და $m|(c\_d)$, ამიტომ $m|[(a\_b)+(c\_d)]=(a+c)\_(b+d)$ და $m|[(a\_b)\_(c\_d)]=(a\_c)\_(b\_d)$, ე.ი. $a+c\equiv b+d(\mathrm{mod}\ m)$ და $a\_c\equiv b\_d(\mathrm{mod}\ m)$.□

ამ თეორემიდან გამომდინარეობს ორი მნიშვნელოვანი შედეგი.

შედეგი 1.1. შედარების ნებისმიერი შესაკრები მოპირდაპირე ნიშნით შეიძლება გადატანილ იქნეს შედარების მეორე ნაწილში.

დამტკიცება. ვთქვათ, მოცემულია a+b≡c(mod m) შედარება. რეფლექსურობის თანახმად, b≡b(mod m). ამ შედარებათა წევრ-წევრად გამოკლებით მივიღებთ, რომ a≡b_c(mod m).□

შედეგი 1.2. შედარებაში შეიძლება ჩამოცილება და დამატება შესაკრებებისა, რომლებიც უნაშთოდ იყოფიან მოდულზე. ე.ი. თუ b|m, მაშინ a+b≡c(mod m) => a≡c (mod m) და a ≡c(mod m) => a+b≡c(mod m).

დამტკიცება. ვთქვათ, a+b≡c(mod m). რადგან b|m <=> b≡0(mod m). ამ ორი შედარებიდან, თუ პირველს გამოვაკლებთ მეორეს, მივიღებთ a≡c(mod m).□

შედეგი 1.3. თუ $a_1 \equiv b_1$, $a_2 \equiv b_2, \ldots, a_n \equiv b_n \pmod m$, მაშინ

$a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \pmod m$.(პირდაპირ გამომდინარეობს თეორემა 1-დან).

თეორემა 2. თუ a≡b(mod m), მაშინ ∀ k∈Z_ ak≡bk(mod m).

დამტკიცება. პირობის თანახმად, m| (a _ b) => m| k(a _ b)=ak_ bk <=> ak≡bk(mod m).□

თეორემა 3. თუ a≡b(mod m) და c≡d(mod m), მაშინ ac≡bd(mod m).

დამტკიცება. თეორემა 2-ის ძალით, a≡b(mod m) => ac≡bc(mod m) და c≡d(mod m) => bc≡bd(mod m), საიდანაც შედარების ტრაზიტულობის გამო, ac≡bd(mod m).□

შედეგი 3.1. თუ $a_1 \equiv b_1$, $a_2 \equiv b_2, \ldots, a_n \equiv b_n \pmod m$, მაშინ

$a_1 a_2 \ldots a_{n-1} a_n \equiv b_1 b_2 \ldots b_{n-1} b_n \pmod m$.(პირდაპირ გამომდინარეობს თეორემა 1-დან).

შედეგი 3.2. თუ a≡b(mod m) da k∈N∪{0}, მაშინ $a^k \equiv b^k \pmod m$.

დამტკიცება. თუ k=0, დასამტკიცებელი შედარების ჭეშმარიტება ცხადია, რადგან m|(a^0_b^0)=1_1=0. თუ k>0, საკმარისია a≡b(mod m)

შედარება გადავწეროთ k-ჯერ და ვისარგებლოთ თეორემა 3-ით.

რაიმე მთელი რიცხვების შეკრებით, გამოკლებით ან გამრვალებით მიღებული ნებისმიერი გამოსახულების მნიშვნელობის m მოდულზე გაყოფით მიღებული ნაშთი არ შეიცვლება, თუ ამ გამოსახულებაში შემავალ რიცხვებს შევცვლით მათი m-ზე გაყოფისას მიღებული ნაშთებით.

თეორემა 4. თუ na≡nb(mod m), n≠0, მაშინ a≡b(mod $\frac{m}{(m,n)}$).

დამტკიცება. პირობის თანახმად, m|(na_nb)=n(a_b). შემოვიღოთ აღნიშვნები: (m,n)=d, n=dN, m=dM. მაშინ, dM|dN(a_b) => M|N(a_b).

რადაგან (M,N)=1, ამიტომ M|(a_b). m=dM => M = $\frac{m}{d}$= $\frac{\text{m}}{(\text{m, n})}$, e.i. $\frac{\text{m}}{(\text{m, n})}$|(a_b)

<=> a≡b(mod $\frac{m}{(m,n)}$).□

შედეგი 4,1. შედარება შეიძლება შევკვეცოთ მოდულთან ურთიერთმარტივ რიცხვზე, ე.ი. თუ na≡nb(mod m) da (m,n)=1, მაშინ

a≡b(mod m) .

შედეგი 4.1 წარმოადგენს თეორემა 4-ის კერძო შემთხვევას, როცა (m,n)=1.

მაშასადამე,მთელ რიცხვთა სიმრავლე m მდოულით m კლასად იყოფა. ქვემოთ წარმოგენილია m=5-ის შემთხვევაა.

კლასი	ნაშთი
...; -5; 0; 5; ...	0
...; -4; 1; 6; ...	1
...; -3; 2; 7; ...	2
...; -2; 3; 8; ...	3
...; -1; 4; 9; ...	4

2.1

სულ 5 კლასი გვაქვს; ყოველ კლასში ის რიცხვებია, რომელთა 5-ზე გაყოფისას მიიღება ერთი და იგივე ნაშთი - 0; 1; 2; 3 ან 4.

ამ თვალსაზრისით, ერთი და იმავე კლასის რიცხვები , შეიძლება არც განვასხვავოთ და ისინი ამ კლასის მხოლოდ უმცირესი არაუარყოფითი რიცხვით (ნაშთით) წარმოვადგინოთ; ნაშთებისთვის კი შემდეგი წესით შემოვიღოთ შეკრებისა და გამრავლების ოპერაციები: თუ r_1 და r_2 ორი ნაშთია, მათი „ჯამი“ ვუწოდოთ ნაშთს, რომელიც მიიღება (r_1+ r_2)-ის გაყოფით 5-ზე; შესაბამისად ვწერთ, მაგალითად „ტოლობებს“ მოდულით 5;

2+3=0; 3+3=1; 2+1=3; 4+4=3.

გამრავლების ცხრილი

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2.2

შეკრების ცხრილი

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

2.3

$r_1 \cdot r_2$ ნამრავლი ვუწოდოთ ნაშთს, რომელიც მიიღება $r_1 \cdot r_2$-ის 5-ზე გაყოფისას; შესაბამისად , მაგალითად გვაქვს ტოლობები:

$2 \cdot 3 = 1$; $3 \cdot 3 = 4$; $2 \cdot 1 = 2$; $4 \cdot 4 = 1$.

მივიღებთ შეკრების და გამრავლების ცხრილებს - „5 მოდულის არითმეტიკის“: ანალოგიურად შეიძლება ნებისმიერი m ნატურალური რიცხვისთვის „m მოდულის არითმეტიკის: განსაზღვრა. ამ არითმეტიკაში ნებისმიერი a, b და c ნაშთებისთვის გვაქვს

$a+b= b+ a$ - ჯამის გადანაცვლებადობის თვისება,

$(a+b)+ c= a+(b+ c)$ - ჯამის ჯგუფთებადობის თვისება,

$(ab)\ c= a(bc)$ - გამრავლების ჯგუფთებადობის თვისება,

$a(b+ c)= ab+ ac$ - გამრავლების განროგებადობის თვისება შეკრების მიმართ;

ასე არითმეტიკაში , მაგალითად, გვაქვს:

$(a+b)^2= a^2+ 2ab+ b^2$

$(a+b)(c+d)= ac+ ad+ bc+ bd$;

გვაქვს შეკრების მიმართ „ნეიტრალური“ ელემენტი - ნაშთი 0, ანუ ნებისმიერი a-სთვის, $a+0= a$; გამრავლების მიმართ „ ნეიტრალური“ ელემენტი - ნაშთი 1; ანუ ნებისმიერი a-სთვის: $a \cdot 1= a$

ახლა განვიხილოთ ნაშთთა სისტემები

დასახელებული $m \in N$ რიცხვისათვის და $\forall\ a \in Z$ რიცხვისათვის $\exists$ ერთადერთი წყვილი $k,r \in Z$ რიცხვებისა, რომლებიც ასეთ დამოკიდებულებაშია a-თან

$$a=mk+r,\ 0 \le r \le m\_1.$$

გადავწერით ეს ტოლობა შედარების სახით

$$a \equiv r \pmod m. \qquad (1)$$

განსაზღვრება 5. ყველა იმ მთელ რიცხვთა სიმრავლეს, რომლის ყოველი წევრი სადარია მოცემული r რიცხვისა m მოდულით, ეწოდება ნაშთთა კლასი m მოდულით, რომელსაც ასე აღნიშნავენ c_r.

რადგან (1) შედარებაში r რიცხვი ღებულობს m სხვადასხვა მნიშვნელობას, ამიტომ m მოდულით განსაზღვრული ნაშთთა კლასების რაოდენობა არის m. ეს კლასებია: $c_0, c_1, \ldots, c_{m\_1}$.

ცხადია, რომ m მოდულით აღებული ნებისმიერი კლასის ყოველი ორი რიცხვი ურთიერთსადარია m მოდულით. მართლაც, $\forall\ a,b \in c_r$ რიცხვებისთვის c_r კლასის განმარტების თანახმად

$a \equiv r \pmod m$ da $b \equiv r \pmod m$, => $a \equiv b \pmod m$.

ადვილი საჩვენებელია, რომ $c_0, c_1, \ldots, c_{m\_1}$ კლასებიდან ნებისმიერ ორ მათგანს არ აქვს საერთო წერტილი. მართლაც ვთწვათ, c_i და c_j არიან ორი ნებისმიერი სახვასხვა კლასი, $i \neq j$, $0 \le i < j \le m\_1$ da დავუშვათ, რომ მათ აქვთ ერთი საერთო ელემენტი, ვთქვათ, c. მაშინ c_r კლასის განმარტების თანახმად

$i \equiv c \pmod m$ და $j \equiv c \pmod m$, => $i \equiv j \pmod m$, რაც შეუძლებელია, რადგან

$$0 < i\_j < m.$$

მიღებული წინააღმდეგობიდან გამომდინარეობს, რომ ყოველი კლასი სრულიად ცალსახად განისაზღვრება მისი ნებისმიერი ერთი ელემენტით, რომელსაც ამ კლასის ნაშთი ჰქვია.

განსაზღვრება 6. m მოდულით აღებული ყოველი კლასიდან სათითაოდ აღებულ რიცხვთა ნებისმიერ სისტემას ეწოდება ნაშთთა სრული სისტემა მ მოდულით.

ამ განსაზღვრებიდან გამომდინარეობს, რომ m მოდულით განსაზღვრული ნაშთთა სრული სისტემა შედგება ისეთი m რიცხვისაგან, რომლებიც წყვილ-წყვილად არასადარია m მოდულით.

მაგალითად: 0, 1, 2, . . . , m_1 და 1, 2, . . . , m წარმოადგენენ ნაშთთა სრულ სისტემებს m მოდულით.

განსაზღვრება 7. კლასს, რომელიც შედგება მოდულთან თანამარტივი რიცხვებისაგან, ეწოდება ნაშთთა დაყვანილი სისტემა ამ მოდულით.

თეორემა 5*. თუ a≡b(mod m), მაშინ (a,m)=(b, m) a,b∈Z, m∈N.

დამტკიცება. a≡b(mod m) შედარებიან გვაქვს

$$m|(a\_b), \Rightarrow a\_b=mk, \quad k\in Z$$

საიდანაც მივიღებთ , რომ

$$a=mk+b. \qquad (2)$$

(2) ტოლობიდან გამომდინარებოს, რომ a და m რიცხვების ყოველი საერთო გამყოფი იქნება b რიცხვის გამყოფიც. მართლაც, ვთქვათ, d არის a და m რიცხვების რომელიმე საერთო გამყოფი, მაშინ

$$d|a, d|m \Rightarrow d|b=a\_mk.$$

ე.ი. a და m რიცხვების ყოველი საერთო გამყოფი წარმოადგენს ამავე დროს b და m რიცხვების საერთო გამყოფს და პირიქით. ეს კი იმას ნიშნავს, რომ ამ რიცხვების საერთო უდიდესი გამყოფებიც ერთმანეთს დაემთხვევა (a,m)=(b, m).□

თუ დავუბრუნდებით ნაშთთა კლასებს, ამ თეორემის თანახმად, თუ კლასის ერთი რომელიმე რიცხვი თანამარტივია m მოდულთან, მაშინ ამ კლასის ყველა რიცხვი აგრეთვე თანამარტივი იქნება m მოდულთან.

თეორემა 6. m მოდულით განსაზღვრული დაყვანილ კლასთა რიცხვი არის φ(m), სადაც φ(m) ეილერის ფუნქციაა.

დამტკიცება. თეორემა 5-ის ძალით, m მოდულით განსაზღვრულ დაყვანილ კლასთა რაოდენობა უდრის ნაშთთა სრულ 1, 2, . . . , m სისტემაში m-თან თანამარტივ რიცხვთა რაოდენობას, რომელიც განმარტების თანახმად ემთხვევა φ(m)-ს.□

თეორემა 7.(ეილერი) თუ m ნატურალური რიცხვია და (a,m)=1, მაშინ

$$a\varphi^{(m)}\equiv 1(\text{mod } m).$$

დამტკიცება. განვიხილოთ m მოდულით მიღებული ნაშთთა დაყვანილი სისტემა

$$r_1,r_2,\ldots,r\varphi_{(m)}. \qquad (1)$$

პირობის თანახამად (a,m)=1, ამიტომ ნაშთთა დაყვანილი სისტემა იქნება აგრეთვე

$$ar_1,ar_2,\ldots,ar\varphi_{(m)}. \qquad (2)$$

radgan (1) და (2) წარმოადგენენ ნაშთთა დაყვანილ სისტემებს, ამიტომ ყოველი რიცხვი (1) სისტემიდან სადარია მხოლოდ ართი რიცხვისა (2) სისტემიდან და პირიქით. ამიტომ შეგვიძლია დავწეროთ შემდეგი შედარებები:

$$\begin{aligned} &ar_1\equiv r_{i(1)}(\text{mod } m)\\ &ar_2\equiv r_{i(2)}(\text{mod } m)\\ &\ldots\ldots\ldots\ldots\\ &ar\varphi_{(m)}\equiv r_{i(\varphi_{(m)})}(\text{mod } m) \end{aligned} \qquad (3)$$

სადაც $r_{i(1)}, r_{i(2)},\ldots, r_{i(\varphi_{(m)})}$ წარმოადგენენ (1) სისტემის რიცხვებს, აღებულს რაღაც სხვა მიმდევრობით.

თუ (3) შედარებებს გადავამრავლებთ, მივიღებთ

$$a\varphi^{(m)}R=R(\text{mod } m), \qquad (4)$$

სადაც $R= r_{i(1)}\, r_{i(2)}\ldots r_{i(\varphi_{(m)})}$. (1) სისტემის ყოველი რიცხვი ურთიერთმარტივია m-თან. ამიტომ, მათი ნამრავლიც ურთიერთმატივი იქნება m -თან, ე.ი. (R,m)=1. ახლა თუ გამოვიყენებთ შედეგ 4.1-ს, მაშინ (4) შედარების შეკვეცით R-ზე მივიღებთ დასამტკიცებელს.

§3. ნაშთთა (მოდულური) არითმეტიკის პრაქტიკული გამოყენება

მოვიყვანოთ რამდენიმე პრაქტიკული მაგალითი. რა ციფრით მთავრდება 2^{999}? ამოვიწეროთ მიმდევრობით 2-ს ხარისხები:

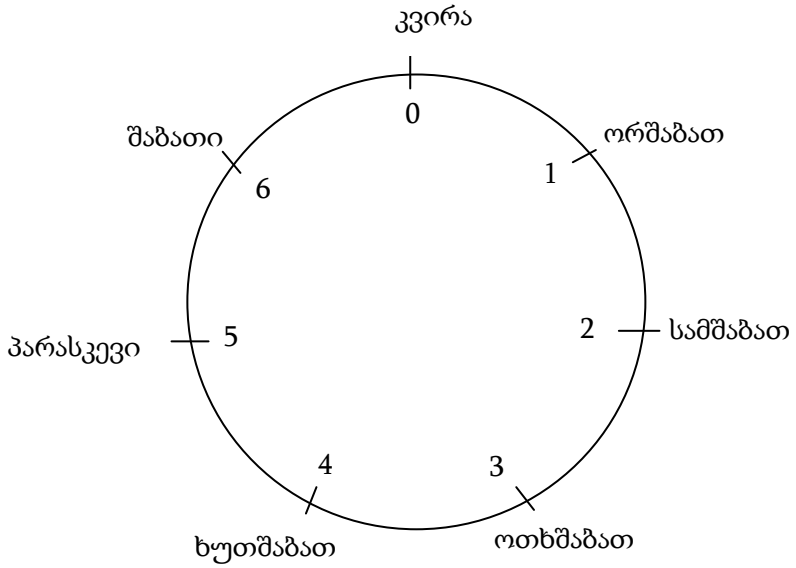
2,4,8,16,32,64...

როგორც ჩანს ყოველი 4 რიცხვის შემდეგ ბოლო ციფრი მეორდება, 2^n _ის ბოლო ციფრი მხოლოდ იმაზეა დამოკიდებული, რა ნაშთი მიიღება n-ის 4-ზე გაყოფისას. რადგან 999=996+3=4 · 249+3,ამიტომ ჩვენი ამოცანის პასუხი არის 8.

ამ მაგალითში ხარისხის მაჩვენებლებისსიმრავლე 4კლასად დაიყო ... 4k, 4k+1, 4k+2, 4k+3.

განვიხილოთ კიდევ ერთი მაგალითი „არაჩვეულებრივი არითმეტიკის“ შესახებ.

სურათზე (3.1) კვირის დღეები რიცხვებით არის გადანომრილი - რიცხვები



წრეწირზეა განლაგებული. კვირას მივანიჭეთ ნომერი - 0, ორშაბათს -1; სამშაბათს - 2, ოთხშაბათს - 3, ხუთშაბათს - 4, პარასკევს -5, შაბათს -6.

ვთქვათ, დღეს სამშაბათია, რა დღე იქნება 4 დღის შემდეგ? წრეწირზე მონიშნული 2-დან გადავთვლით 4 დანაყოფს; 4დღის შემდეგ შაბათია, 2+4=6; 6 - შაბათის ნომერია.რა დღე იქნება 27 დღის შემდეგ? რა დღე იყო 20 დღის წინ? ამ

კითხვებზე პასუხის გასაცემად მოგვიწევს „2“ წერტილიდან, შესაბამისად 27 დანაყოფის გადათვლა რიცხვების ზრდის მიმართულებით და 20 დანაყოფის გადათვლა კლების მიმართულებით.

პირველ შემთხვევაში მოგვიწევს წრეწირზე 29_ის შესაბამისი წერტილის პოვნა (2+27=29), მეორე შემთხვევაში - (-18)-ის (2-20=-18). ამისთვის საკმარისია მე-7 დღე (კვირაა) კვლავ 0-ით წარმოვადგინოთ, მე-8 – 1-ით, მე-9 – 2-ით და ა. შ. მე-14 კვლავ 0-ით, მე-15 – 1-ით და ა.შ. კვირის წინა დღეს(რომლის ნომერია 6) შეიძლება მივანიჭოთ ნომერი -1, ამ უკანასკნელის წინა დღეს - (-2).

შეიძლება ითქვას, გვაქვს მთელ რიცხვთა სიმრავლის ასახვა კვირის დღეებზე.

...; -14; -7; 0; 7; 14;… (7n სახის რიცხვები, nZ)	კვირა
...; -6; 1; 8;... (7n+1 სახის რიცხვები, nZ)	ორშაბათი
...; -5; 2; 9;... (7n+2 სახის რიცხვები, nZ)	სამშაბათი
...; -4; 3; 10;... (7n+3 სახის რიცხვები, nZ)	ოთხშაბათი
...; -3; 4; 11;... (7n+4 სახის რიცხვები, nZ)	ხუთშაბათი
...; -2; 5; 12;... (7n+5 სახის რიცხვები, nZ)	პარასკევი
...; -1; 6; 13;... (7n+6 სახის რიცხვები, nZ)	შაბათი

3.2

მაშასადამე, მთელ რიცხვთა სიმრავლე 7 ნაწილად - 7კლასად დაიყო.ყოველი მთელი რიცხვი ერთ-ერთ კლასში ხვდება; მაგალითად, რიცხვები: 29, 50, 64

მოხვდება იმავე კლასში, რომელშიცაა რიცხვი1 - თითოეული მათგანი 7n+1 სახისაა.

დღეს თუ სამშაბათია (მე-2 დღე), 27 ღის შემდეგ იქნება ორშაბათი; 20 დღის წინ იყო ოთხშაბათი: 2- 20=-18 ; -18=7(-3)+3

ზემოთ წარმოდგენილ კლასებს ეწოდება კლასები მოდულით 7.

მოდულურ არითმეტიკას დღესაც საკმაოდ დიდი წარმატებით იყენებენ სხადასხვა სფეროში პრაქტიკული ამოცანების გადასაწყვეტად. მოდულური არითმეტიკის გამოყენების ერთ-ერთ მარტივ მაგალითად შეიძლება განვიხილოთ შეჯიბრების განრიგის შედგენის ამოცანა.

ვთქვათ, შეჯიბრება n გუნდს შორის ტარდება. თუ n კენტია, ცხადია შეჯიბრების ყოველ ტურში ყველა მონაწილე დაკავებული ვერ იქნება _ ერთ-ერთს მეტოქე არ ეყოლება. შეგვიძლია ვიგულისხმოთ, რომ შეჯიბრებაში ერთით მეტი მონაწილეა და მასთან "შეხვედრის" დროს მოწინააღმდეგე თავისუფალია. მაშასადამე, შეიძლება ჩავთვალოთ, რომ n ლუწია. ამ თვალსაზრისით თითოეულ გუნდს n-1 თამაშის ჩატარება მოუწევს და შესაბამისად შეჯიბრება n-1 ტურად მოეწყობა.

მოვახდინოთ გუნდების გადანომვრა. ყოველ გუნდს მივანიჭოთ ერთ-ერთი ნომერი რიცხვებიდან 1, 2, . . . , n-1, n დაშემდგომ ეს გუნდი ამ ნომრით მოვიხსენიოთ. მაგალითად, გუნდი x.

ყოველი ტურის ნომერიც ერთ-ერთი რიცხვია {1, 2, . . . , n-1} სიმრავლიდან.

გუნდ x -ს k-ურ ტურში (k=1, 2, . . . , n-1) შევახვედროთ ის გუნდი y_k, რომლისთვისაც

$$x+y_k\equiv k(\mathrm{mod}\ (n\_1)). \qquad (1)$$

თუ x≤n_1, მაშინ სხვადასხვა გუნდებს, ამ წესის მიხედვით, ყოველ ტურში სხვადასხვა მეტოქე ეყოლებათ. მართლაც, თუ ვიგულისხმებთ, რომ რომელიმე k ტურში

$$x+y_k\equiv k(\mathrm{mod}\ (n\_1))$$

და

$$x'+y_k\equiv k(\mathrm{mod}\ (n\_1))$$

მაშინ

$$x \equiv x'(\mathrm{mod}\ (n\_1)). \qquad (2)$$

ამრიგად, x =x′.

თუმცა, თავიდან უნდა ავიცილოთ ერთი შემთხვევა _ ყოველი k-თვის იარსებებს ისეთი x,რომ $x=y_k$. ანუ ყოველ ტურში (1) წესი ერთ-ერთ x-ს მეტოქედ ამავე გუნდს დაუნიშნავს. ვიპოვოთ ამ გუნდის ნომერი. (1)-დან გვ

$$2x \equiv k(\mathrm{mod}\ (n\_1)) \qquad (3)$$

ადვილია იმის შემოწმება, რომ ის ერთადერთი $x \in \{1,2,...,n\_1\}$ რიცხვი, რომელიც (3)-ს აკმაყოფილებს არის $\frac{k}{2}$, თუ k ლუწია; ხოლო თუ k კენტია, მაშინ არის $\frac{k+n-1}{2}$. k-ურ ტურში ამ x ნომრიან გუნდს თუ შვახვედრებთ გუნდ n -ს (რომელიც აქამდე განხილვაში არ მონაწილეობდა), ხოლო ყველა დანარჩენს, რომელთა ნომრები არ აღემატება (n_1)-ს, მეტოქეს შევურჩევთ (1) ფორმულის მხედვით, შეჯიბრების განრიგი უნაკლო გახდება.

ახლა რაიმე კონკრეტულ შემთხვევაში შევამოწმოთ, როგორ "მუშაობს" შემოთავაზებული განრიგი.

მაგალითისათვის შევადგინოთ შეჯიბრების განრიგი 8 გუნდისათვის. ე.ი. n=8; ტურების რაოდენობაა 8_1=7.

<u>I ტური</u>

k=1. მაშინ ცალკეა განსახილველი $\frac{k+n-1}{2}$_ნომრიანი გუნდი, ანუ $\frac{1+8-1}{2}=4$_ ნომრიანი გუნდი. მისი მეტოქე დადგენილი წესის თანახმად არის გუნდი 8. დანარჩენი გუნდები $x+y_1 \equiv 1(\mathrm{mod}\ 7)$ ტოლობის მიხედვით შეირჩევა.

1) x=1
   $1+y_1 \equiv 1(\mathrm{mod}\ 7)$
   $y_1 \equiv 0(\mathrm{mod}\ 7)$
   $y_1=7$

5) x=5
   $5+y_1 \equiv 1(\mathrm{mod}\ 7)$
   $y_1 \equiv -4(\mathrm{mod}\ 7)$
   $y_1=3$

2)	x=2 $2+y_1\equiv1(\text{mod } 7)$ $y_1\equiv\_1(\text{mod } 7)$ $y_1=6$	6)	x=6 $6+y_1\equiv1(\text{mod } 7)$ $y_1\equiv-5(\text{mod } 7)$ $y_1=2$
3)	x=3 $3+y_1\equiv1(\text{mod } 7)$ $y_1\equiv-2(\text{mod } 7)$ $y_1=5$	7)	x=7 $7+y_1\equiv1(\text{mod } 7)$ $y_1\equiv-6(\text{mod } 7)$ $y_1=1$
4)	$y_1=8$ შეთანხმების თანახმად x=4	8)	x=8 $y_1=4$

II ტური

k=2, ცალკეა განსახილველი $\frac{2}{2}=1\_$ ნომრიანი გუნდი. მისი მეტოქე წესის მიხედვით არის გუნდი 8.

1)	x=1 $y_2=8$	5)	x=5 $5+y_2\equiv2(\text{mod } 7)$ $y_2\equiv-3(\text{mod } 7)$ $y_2=4$
2)	x=2 $2+y_2\equiv2(\text{mod } 7)$ $y_2\equiv0(\text{mod } 7)$ $y_2=7$	6)	x=6 $6+y_2\equiv2(\text{mod } 7)$ $y_2\equiv-4(\text{mod } 7)$ $y_2=3$
3)	x=3 $3+y_2\equiv2(\text{mod } 7)$ $y_2\equiv-1(\text{mod } 7)$ $y_2=6$	7)	x=7 $7+y_2\equiv2(\text{mod } 7)$ $y_2\equiv-5(\text{mod } 7)$ $y_2=2$
4)	x=4 $4+y_2\equiv2(\text{mod } 7)$ $y_2\equiv-2(\text{mod } 7)$ $y_2=5$	8)	x=8 $y_2=1$

III ტური

k=3, ცალკეა განსახილველი $\frac{3+8-1}{2}=5-$ _ ნომრიანი გუნდი. მისი მეტოქე წესის მიხედვით არის გუნდი 8.

1)	x=1 $1+y_3\equiv 3 \pmod 7$ $y_3\equiv 2 \pmod 7$ $y_3=2$	5) x=5 $y_3=8$
2)	x=2 $2+y_3\equiv 3 \pmod 7$ $y_3\equiv 1 \pmod 7$ $y_3=1$	6) x=6 $6+y_3\equiv 3 \pmod 7$ $y_3\equiv -3 \pmod 7$ $y_3=4$
3)	x=3 $3+y_3\equiv 3 \pmod 7$ $y_3\equiv \pmod 7$ $y_3=7$	7) x=7 $7+y_3\equiv 3 \pmod 7$ $y_3\equiv -4 \pmod 7$ $y_3=3$
4)	x=4 $4+y_3\equiv 3 \pmod 7$ $y_3\equiv -1 \pmod 7$ $y_3=6$	8) x=8 $y_3=5$

IV ტური

k=4, ცალკეა განსახილველი $\frac{4}{2}=2-$ ნომრიანი გუნდი. მისი მეტოქე წესის მიხედვით არის გუნდი 8.

1)	x=1 $1+y_4\equiv 4 \pmod 7$ $y_4\equiv 3 \pmod 7$ $y_4=3$	5) x=5 $5+y_4\equiv 4 \pmod 7$ $y_4\equiv -1 \pmod 7$ $y_4=6$
2)	x=2 $y_4=8$	6) x=6 $6+y_4\equiv \pmod 7$

			$y_4 \equiv -2 \pmod 7$ $y_4 = 5$
3)	$x=3$ $3+y_4 \equiv 4 \pmod 7$ $y_4 \equiv 1 \pmod 7$ $y_4 = 1$	7)	$x=7$ $7+y_4 \equiv 4 \pmod 7$ $y_4 \equiv -3 \pmod 7$ $y_4 = 4$
4)	$x=4$ $4+y_4 \equiv 4 \pmod 7$ $y_4 \equiv 0 \pmod 7$ $y_4 = 7$	8)	$x=8$ $y_4 = 2$

V ტური

k=5, ცალკეა განსახილველი $\frac{5+8-1}{2} = 6 -$ ნომრიანი გუნდი. მისი მეტოქე წესის მიხედვით არის გუნდი 8.

1)	$x=1$ $1+y_5 \equiv 5 \pmod 7$ $y_5 \equiv 4 \pmod 7$ $y_5 = 4$	5)	$x=5$ $5+y_5 \equiv 5 \pmod 7$ $y_5 \equiv 0 \pmod 7$ $y_5 = 7$
2)	$x=2$ $2+y_5 \equiv 5 \pmod 7$ $y_5 \equiv 3 \pmod 7$ $y_5 = 3$	6)	$x=6$ $y_5 = 8$
3)	$x=3$ $3+y_5 \equiv 5 \pmod 7$ $y_5 \equiv 2 \pmod 7$ $y_5 = 2$	7)	$x=7$ $7+y_5 \equiv 5 \pmod 7$ $y_5 \equiv -2 \pmod 7$ $y_5 = 5$
4)	$x=4$ $4+y_5 \equiv 5 \pmod 7$ $y_5 \equiv 1 \pmod 7$ $y_5 = 1$	8)	$x=8$ $y_5 = 6$

VI ტური

k=6, ცალკეა განსახილველი $\frac{6}{2}=3-$ ნომრიანი გუნდი. მისი მეტოქე წესის მიხედვით არის გუნდი 8.

1)	x=1 $1+y_6\equiv 6(\text{mod } 7)$ $y_6\equiv 5(\text{mod } 7)$ $y_6=5$	6)	x=5 $5+y_6\equiv 6(\text{mod } 7)$ $y_6\equiv 1(\text{mod } 7)$ $y_6=1$
2)	x=2 $2+y_6\equiv 6(\text{mod } 7)$ $y_6\equiv 4(\text{mod } 7)$ $y_6= 4$	7)	x=6 $6+ y_6\equiv 6(\text{mod } 7)$ $y_6\equiv 0(\text{mod } 7)$ $y_6=7$
3)	x=3 $y_6=8$	8)	x=7 $7+y_6\equiv 6(\text{mod } 7)$ $y_6\equiv -1(\text{mod } 7)$ $y_6=6$
4)	x=4 $4+y_6\equiv 6(\text{mod } 7)$ $y_6\equiv 2(\text{mod } 7)$ $y_6=2$	9)	x=8 $y_6=3$

VII ტური

ამ ტურში მეტოქეების შერჩევა უფრო მარტივად მოხდება. თითოეულ x გუნდს შეხვდება ის y_7 გუნდი, რომელსაც ჯერ არ შეხვედრია. გვექნება

1) x=1, $y_7=6$;
2) x=2, $y_7=5$;
3) x=3, $y_7=4$;
4) x=4, $y_7=3$;
5) x=5, $y_7=2$;
6) x=6, $y_7=1$;
7) x=7, $y_7=8$;
8) x=8, $y_7=7$;

ამგავარად, შევადგინეთ შეჯიბრების ცხრილი 8 გუნდისათვის, რომელიც უნაკლოა იმ თვალსაზრისით, რომ 8-ვე გუნდისთვის სამართლიანადაა შედგენილი.

x / **k**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	7	6	5	8	3	2	1	4
2	8	7	6	5	4	3	2	1
3	2	1	7	6	8	4	3	5
4	3	8	1	7	6	5	4	2
5	4	3	2	1	7	8	5	6
6	5	4	8	2	1	7	6	3
7	6	5	4	3	2	1	8	7

3.3 რაღა თქმა უნდა ეჭვგარეშეა, რომ ასეთი ცხრილის შედგენა შესაძლებელია ნებისმიერი n გუნდისათვის.

მოდულურ არითმეტიკას დიდი გამოყენება აქვს აგრეთვე კოდირების სისტემაში. უძველესი დროიდან გაჩნდა რაიმე ჩანაწერის ან ინფორმაციის გასაიდუმლოების (დაშიფრვის) საჭიროება, რათა გარეშე პირთათვის მის შინაარსში გარკვევა შეუძლებელი ყოფილიყო, როცა გადაცემული ინფორმაცია მათ ხელთ ჩაუვარდებოდა. ამ მიზნით ადამიანები მიმართავენ ინფორმაციის დაშიფვრას _ შიფრის გამოყენებას. შიფრი ინფორმაციის გარდაქმნის ხერხია. შიფრის შედგენის წესებს და მისი არაკანონიერი გამოყენებისაგან დაცვის მეთოდებს რიცხვთა თეორიის ერთ-ერთი ნაწილი კრიპტოგრაფია შეისწავლის.

აღსანიშნავია, რომ კრიპტოგრაფიას ადამიანი უძველესი დროიდან იყენებს. ერთ-ერთი უძველესი მაგალითი იულიუს კეისრის (100-44 ძვ.წ.აღ.) შიფრია. იგი მოცემული ტექტის ისეთი გარდაქმნაა, როცა ანბანის ყოველი ასო ამ ასოს

შემდეგ რიგით მესამე ასოთი იცვლება. ე.ი. ისევე, როგორც მოდულურ არითმეტიკაში შეკრების პროცესის განსაზღვრისას ანბანის ასოებს წრეწირზე განვალაგებთ; მაშინ ცხადია, მაგალითად, ბოლო ასო კეისრის ხერხის მიხედვით მესამე ასოთი შეიცვლება.

ამ მაგალითიდან ჩანს, რომ ამ ტიპის შიფრის შედგენისას შეიძლება გამოვიყენით მოდულური არითმეტიკა.

მეორე მსოფლიო ომის (1939-1945 წ.წ.) პირველ ნახევარში ფაშისტური გერმანიის სამხედრო გემების მოულოდნელი თავდასხმები დიდ ზიანს აყენებდა ინგლისის, აშშ-ს და საბჭოთა კავშირის სამხედრო და სავაჭრო გემებს. გერმანელთა გემების საბრძოლო მოქმედებას დიდ დახმარებას უწევდა ინფორმაციის გადაცემის გასაიდუმლოებული სისტემა, რომელიც სპეციალურ კოდს _ "ენიგმას" იყენებდა. ამ კოდის გახსნა ინგლისელმა ალან ტიურინგმა შეძლო, რითაც დიდი წვლილი შეიტანა საკუთარი ქვეყნისა და მის მოკავშირეთა თავდაცვის გაძლიერებაში.

ვისაუბროთ ინფორმაციის გარდაქმნის სხადასხვა ხერხების _ სხვადასხვა შიფრის შესახებ. განვიხილოთ კოდირების კეისრისეული სისტემა. ამ დროს ცხადია, ასოების გადათვლა იმ მოდულურ არითმეტიკაში ხდება, რომელშიც მოდული ანბანში შემავალი ასოების ოდენობის ტოლია. მაშასდამე, ასოების გადანომრვის შემდეგ გვაქვს ასახვა:

$$x \to x+k;$$

მაგალითად, 26 მოდულის არითმეტიკაში (რაც ლათინური ანბანისთვისაც გამოდგება), თუ k=7, მაშინ 23→4, ანუ W→D (W ასო იცვლება D ასოთი). გაშიფრვის პროცესი ცხადია ამ ასახვის შექცეული ასახვის პოვნაა.

დაშიფრვის კიდევ ერთი სქემა გამარტივებული სახით შეიძლება ასე წარმოვადგინოთ: თუ ყოველ ასოს ორნიშნა რიცხვით წარმოვადგენთ (მაგალითად, A-01, B-02,…, Z-26), მაშინ რაიმე ფრაზის გადაცემა ფაქტობრივად დიდი რიცხვის გადაცემაა.

ინფორმაციის გადამცემი და მიმღები პირების შეთანხმებით შეირჩევა რაიმე დიდი მარტივი p რიცხვი, მოდულური არითმეტიკის მოდული, რომელიც

შეიძლება არ იყოს გასაიდუმლოებული. შეთანხმება ხდება ე. წ. შიფრის საკვანძო k რიცხვის შესახებაც, k∈{1, 2, . . . , p_1}.

თუ ინფორმაცია გამოსახულია რაიმე m რიცხვით (m შეიძლება მარტივი არ იყოს, p კი იმდენად დიდია, რომ m<p), მის ნაცვლად იგზავნება m* რიცხვი (m* არის ნაშთი, რომელიც მიიღება mk-ს p-ზე გაყოფისას) _ ფრაზა, რომელიც m*-ით გამოისახება; იგი შეიძლება განისაზღვროს პირობით:

$$mk \equiv m^* \pmod{p}. \qquad (1)$$

გაშიფრვა _ m-ის პოვნაა _ (1) შედარების ამოხსნა, ანუ p მოდულის არითმეტიკაში m- ის მიმართ წრფივი განტოლების ამოხსნა: mk=m*.

მაგალითად, დავშიფროთ ამ წესის გამოყენებით ასო L (L_12). ვთქვათ, p=23, k=10; დასაშიფრი გვაქვს m=12 რიცხვი.

$$12 \bullet 10 \equiv m^* \pmod{23}$$

$$120 \equiv m^* \pmod{23}$$

$$m^* \equiv 5 \pmod{23}.$$

ე.ი. L→5. მოცემული ასოს გასაშიფრად საჭიროა ამოვხსნათ შემდეგი შედარება $10m \equiv 5 \pmod{23}$ $2m \equiv 1 \pmod{23}$

$$2m = 1 + 23 \quad m = 12 \ (12\_ L).$$

თუმცა დაშიფრვის ამ ხერხს გარკვეული უსიამოვნო თავისებურება ახასიათებს; როცა მოდული დიდი რიცხვია, ამ წესით ფესვის სწრაფად მოძებნა არ ხერხდება. რეალურ ყოფით საკითხებში კი, ხშირად, გარკვეული დროის შემდეგ გაშიფრული ინფორმაციის მნიშვნელობა მცირეა, ან სრულიად უსარგებლოა.

ახლა დაშიფრვის კიდევ ერთ ხერხს შემოგთავაზებთ. ქართული ანბანის 33 ასო 33 რიცხვით წარმოვადგინოთ: ა _ 1, ბ _ 2, . . . , ჳ _ 33. სიტყვების ჩაწერისას კიდევ ერთი ნიშანი გამოვიყენოთ _ 0 იყოს ნიშნაკი სიტყვების გაცალკავებისთვის; მაშასადამე, ყოველი ასო A={0, 1, 2, . . . , 33} სიმრავლის ერთ-ერთ ელემენტს შეესაბამება. დაშიფრვა მოვახდინოთ A სიმრავლეზე განსაზღვრული რაიმე წრფივი x→ax+b ფუნქციის მნიშვნელობების სადარი რიცხვებით A სიმრავლიდან. ამ ფუნქციის შექცევადობის პირობა შესრულდება, თუ a თანამარტივი იქნება 34-თან.

დაშიფრვის ამ ხერხის გამოყენებით განვიხილოთ ასეთი სახალისო მათემატიკური თამაში; თამაში განვიხილოთ ორი დაპირისპირებული გუნდისათვის; თითოეულ გუნდში ორი მონაწილეა, ანუ სულ თამაშში მონაწილეობს ოთხი ადამიანი, რომელთაგან თითოეულს ჰყავს თავის მეწყვილე. მოთამაშეები განლაგდებიან წრეზე ისე, რომ მეწყვილეები ერთმანეთის მოპირდაპირე მხარეს აღმოჩნდნენ (ანუ მეწყვილეები გვერდი-გვერდ არ უნდა მოხვდნენ). მეწყვილეები წინასწარ შეიმუშავებენ საკუთარ შიფრს, ანუ დაასახელებენ ფუნქციას $x \to ax+b$. ორივე გუნდს საკუთარი შიფრი ექნება (ცხადია, მოწინააღმდეგე გუნდებმა ერთმანეთის შიფრები არ უნდა იცოდნენ). თამაშის წესები ასეთია: ერთ-ერთი რომელიმე მოთამაშე თავის გვერდით მჯდომ მოწინააღმდეგეს ეუბნება თავის სურვილით რაიმე სიტყვას ისე, რომ დანარჩენმა ორმა ეს საიდუმლო სიტყვა არ იცოდეს. საიდუმლო სიტყვის მიმღები მოთამაშე დაშიფრავს მიღებულ სიტყვას და დაშიფრულს გადასცემს თავის მეწყვილეს, რომესაც ევალება ამ დაშიფრული სიტყვის აღდგენა (გაშიფრვა) და გამოცხადება. თუ ამ უკანასკნელმა სიტყვა სწორად აღადგინა, მოგებული ქულა ჩაეთვლება მის გუნდს, წინააღმდეგ შემთხვევაში _ მის მოწინააღმდეგეს.

განვიხილოთ კონკრეტული მაგალითი: ვთქვათ, დასაშიფრი გვაქვს სიტყვა

ასო	a	b	g	d	e	v	z	T	i	k	l	m	n	o	p	J	r
რიცხვი	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ასო	s	t	u	f	q	R	y	S	C	c	Z	w	W	x	j	h	
რიცხვი	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

3.4

აიღოთ ასახვა x→19x+11. ჩვენს მიერ შემოღებული აღნიშვნების თანახმად, მოცემული სიტყვის ასოებს შევუსაბამოთ ცხრილში მოცემული შესაბამისი რიცხვითი ეკვივალენტები.

გვაქვს

მ: 19•12+11=239≡1(mod 34), მ→ა;

ა: 19•1+11=30≡30(mod 34), ა→ჭ;

თ: 19•8+11=163≡27(mod 34), თ→ც;

ე: 19•5+11=106≡4(mod 34), ა→დ;

ტ: 19•19+11=372≡32(mod 34), ტ→ჯ;

ი: 19•9+11=182≡12(mod 34), ი→მ;

კ: 19•10+11=201≡31(mod 34), კ→ხ;

ამრიგად, დასაშიფრი სიტყვა ,,მათემატიკა“ (→,,აჭცდაჭჯმხჭ“).

იმისათვის, რომ სიტყვა აღვადგინოთ (ანუ გავშიფროთ), მოგვიწევს x→19x+11 ასახვის შექცეული ასახვის პოვნა, ანუ მოცემული y-თვის

$$19x+11 \equiv y \pmod{34} \qquad (3)$$

შედარების ამოხსნა y-ის მიმართ.

საკმარისია 19-ის შებრუნებული ვიპოვოთ 34-ის არითმეტიკაში. ეს შეიძლება გაკეთდეს სხვადასხვა ხერხით.

მაგალითად, ევკლიდეს ალგორითმის მიხედვით,

$34=19 \bullet 1+15 \quad 19 =15 \bullet 1 +4$

$15 =4 \bullet 3+3 \quad 4 = 3 \bullet 1 + 1$

$3 = 1 \bullet 3$

(34-ისა 19-ის საერთო უდიდესი გამყოფის პოვნის ხერხი).

ამ ტოლობებიდან: 1 უნდა გამოვსახოთ 34 და 19-ით.

$1 = 4 – 3 \bullet 1 = 4 – (15 – 4 \bullet 3) = 4 \bullet 4 – 15 = 4 \bullet (19 – 15 \bullet 1) - 15 = 4 \bullet 19 – 15 \bullet 5 =$

$= 4 \bullet 19 – (34 – 19) \bullet 5 = 4 \bullet 19 – 5 \bullet 34 + 5 \bullet 19 = 9 \bullet 19 – 5 \bullet 34$

ე.ი. $9 \bullet 19 \equiv 1 \pmod{34}$

მაშასადამე, 9 არის 19-ის შებრუნებული 34-ის არითმეტიკაში. (3)-ის 9-ზე გავამრავლებით მივიღებთ:

$9 \bullet 19 x + 9 \bullet 11 \equiv 9y \quad 9 \cdot 19 x + 9 \cdot 11 \equiv 9 y$

$x \equiv 9y - 99 \; x \equiv 9y - 31 \pmod{34}$

მაშასადამე, $x \to 19x+11$ ასახვის შექცეული ასახვაა $x \to 9x\_31$.

მაგალითად, თუ გავშიფრავთ ასო “ჯ”-ს, მივიღებთ ასო “ა”-ს.

ჯ: $9 \bullet 30 – 31 = 239 \equiv 1 \pmod{34}$ ჯ→ა.

ახლა შემოგთავაზებთ დაშიფრვის კიდევ ერთ ხერხს, რომელსაც RSA _ შიფრი ეწოდება _ მისი შემდგენლების გვარების პირველი ასოების მიხედვით (R. Rivest, A. Shamir, L. Adleman). RSA სისტემის გამოყენებისას მთვარი სიძნელე დიდი ნატურალური რიცხვის მარტივ მამრავლებად დაშლას უკავშირდება (იგულისხმება რაიმე დიდი რიცხვის ორი მარტივი რიცხვის ნამრავლად დაშლა).

RSA სისტემის დაშიფრვის ხერხი და აგებულება ასეთია. გვაქვს ე. წ. საჯარო გასაღები (e, n) წყვილის სახით, რომლის საშუალებითაც ხდება დაშიფრვა. აქ n=pq, სადაც p და q დიდი მარტივი რიცხვებია, ხოლო (e,φ(n))=1.

შეტყობინების დასაშიფრად, სიმარტივის მიზნით, ტექსტს ვყოფთ ბლოკებად. ვთქვათ, დასაშიფრი ტექსტი დავყავით k ბლოკად. გადავიყვანთ მათ შესაბამის რიცხვით ეკვივალენტში (A_0, B_1, C_2,…, Z_25) და ღია ტექსტის ყოველი P_i-ur ბლოკს (i=1,...,k) შეუსაბამებთ C_i ბლოკს შემეგნაირად: $C_i \equiv P_i^e \pmod n$,

სადაც (e, n) დაშიფრვის გასაღებია.

დაშიფრული ტექსტის გასაშიფრად საჭიროა გაშიფრვის საიდუმლო გასაღები (d, n), ისეთი, რომ

$P_i \equiv C_i^d \pmod n$.

ასეთი d კი არსებობს, რადგან (e,φ(n))=1. ე.ი. არსებობს d რიცხვი ისეთი, რომ $ed \equiv 1 \pmod{\varphi(n)} \Rightarrow ed = 1+\varphi(n)k,\ k \in Z$

და ეილერის თეორემის თანახმად ადგილი აქვს შემდეგ შედარებას

$$C_i^d \equiv P_i^{ed} \pmod n \equiv P_i^{1+\varphi^{(n)k}} \equiv P_i \pmod n.$$

მაგრამ d-ს მოსაძებნად საჭიროა φ(n)-ის ცოდნა.თუ n=pq რიცხვი დიდი მარტივი რიცხვების ნამრავლია, მაშინ φ(n)- ის მულტიპლიკაციურობის გამო გვექნება

- $\varphi(n)=\varphi(pq)=\varphi(p)\ \varphi(q)=(p\_1)(q\_1)$

და თუ არ ვიცით p და q, მაშინ φ(n)-ის პოვნაც შეუძლებელია.

ღია გასაღებით დაშიფრვა-გაშიფრვა განვიხილოთ შემდეგ მაგალითზე: ვთქვათ, RSA სისტემის ღია გასაღებია (e, n)=(7, 4087). ე.ი. e=7 მაჩვენებელია, ხოლო n=4087 _ მოდული. როცა დაშიფრვის გასაღებს ვირჩევდით, გავითვალისწინეთ, რომ n=61•67=4087 ორი მარტივი რიცხვის ნამრავლია (p=61, q=67), ხოლო (e,φ(n))=1. მართლაც, φ(4087)= φ(61) φ(67)=60•66=3960, ხოლო (7, 3960)=1.

დავშიფროთ ამ გასაღებით შემდეგი ტექსტი (შეტყობინება)

NUMBER THEORY

გადავიყვანოთ რიცხვით ეკვივალენტში და მოვახდინოთ მისი ბლოკებად დაყოფა (დაბლოკვა).

ასო	A	B	C	D	E	F	G	H	I	J	K	L	M
რიცხვითი ეკვივალენტი	0	1	2	3	4	5	6	7	8	9	10	11	12
ასო	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
რიცხვითი ეკვივალენტი	13	14	15	16	17	18	19	20	21	22	23	24	25

3.5

გვაქვს 1320 1214 1719 7414 1724 (1)

მოვახდინოთ გარდაქმნა ანუ დაშიფრვა ფორმულით

$$C_i \equiv P_i^7 \pmod n \quad (i=1,\ldots, 5),$$

$C_1 \equiv 1320^{7} \pmod{4087}$; $C_2 \equiv 1214^{7} \pmod{4087}$; $C_3 \equiv 1719^{7} \pmod{4087}$;

$C_1=1835$; $C_2=2799$; $C_3=50$;

$C_4 \equiv 7414^{7} \pmod{4087}$; $C_5 \equiv 1724^{7} \pmod{4087}$;

$C_4=4003$; $C_5=3858$;

მივიღებ 1835 2799 0050 4003 3858 (2)ასე დაიშიფრება მოცემული ტექტი. ამის გაკეთება შეუძლია ყველას,ვინც იცის დაშიფრვის ღია გასაღები ანუ (e, n). რაც შეეხება გაშიფრვას, მისი გაკეთება შეუძლია მხოლოდ იმას, ვისიც არის ეს შიფრი, ანუ ვინც შეადგინა $n=61\bullet 67$ ორი მარტივი რიცხვის ნამრავლი. მას შეუძლია გამოთვალოს $\varphi(4087)=3960$ და იპოვის e=7_ის შებრუნებული 4087 მოდულის არითმეტიკაში. მართლაც, d-ს საპოვნელად საჭიროა ამოვხსნათ წრფივი შედარ $7d \equiv 1 \pmod{4087}$ $7d=1+4087$ $d=584$

მივიღეთ, რომ 7-ის შებრუნებული 4087 მოდულის არითმეტიკაში არის 584, რადგან $7\bullet 584 \equiv 1 \pmod{4087}$. ე.ი. გაშიფრვის გასაღებია (d, n)=(584, 4087) წყვილი. მართლაც, თუ (2) დაშიფრული ტექსტისათვის გამოვიყენებთ გარდაქმნას

$$P_i \equiv C_i^{584} \pmod{4087}, \quad (i=1,\ldots, 5),$$

მივიღებთ (1)-ს, რომლის შესაბამისი ასოითი ეკვივალენტი მოგვცემს თავდაპირველ ტექსტს.

კვლევითი ნაწილი

კვლევის პირველი ეტაპი -ეროვნულ სასწავლო გეგმაში ახალი საკითხის, ნაშთთა არითმეტიკის, შეტანასთან დაკავშირებული სირთულეებისა და პრობლემების გასარკვევად ჩავატარე კვლევა.გამოვიყენე როგორც რაოდენობრივი (კითხვარი), ასევე თვისობრივი კვლევა (მეორეული ინფორმაციის ანალიზი).<u>მასწავლებლის კითხვარის მიზანი იყო:</u>

- გაგვერკვია, რამდენად მნიშველოვნად თვლიდნენ მასწავლებლები ნაშთთა არითმეტიკის სწავლებას საშუალო საფეხურზე;

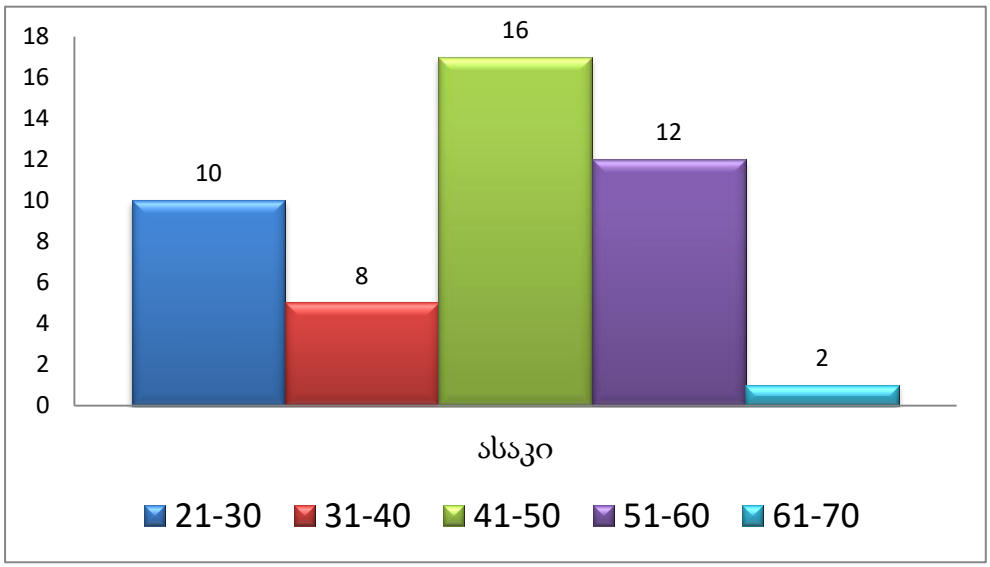
- რა მეთოდებს იყნებენ ისინი მასალის ასათვისებლად;
- საკმარის დროს უთმობენ თუ არა ნაშთთა არითმეტიკის (მოდულური არითმეტიკის) სწავლებას.

კვლევის მეორე ეტაპი -კვლევის ამ ეტაპზე მოხდა სამიზნე ჯგუფის განსაზღვრა, შევარჩიე საჯარო და კერძო სკოლის მათემატიკის მასწავლებლები, რის შემდეგადაც შევადგინე მათთვის კითხვარი, რომელიც საშუალებას მომცემდა ჰიპოთეზის წამოსაყენებლად.

კვლევის მესამე ეტაპი -ამ ეტაპზე მოხდა მასწავლებელთა გამოკითხვა, შემდეგ მონაცემების დამუშავება და ანალიზი. კითხვარის მიზანი იყო, მივეყვანეთ ჰიპოტეზის განამტკიცებამდე ან უარყოფამდე. კვლევის ამ ეტაპის ჩატარების დროს შეგვხვდა სირთულეები, რადგან მასწავლებელთა გარკვეულმა ნაწილმა უარი განაცხადა ჩვენთან თანამშრომლობაზე და კითხვარის შევსებაზე.

გამოკითხვა ჩავატარე 7 სკოლაში , ასევე შედეგები მივიღე ინტერნეტის საშუალებითაც. სულ გამოვკითხე 48 მასწავლებელი, აქედან 30 მასწავლებელი სკოლაში გამოვკითხე, დანარჩენ 18 კითხვარზე პასუხი ინტერნეტის მეშვეობით მივიღე. ჩემი კითხვარი იწყებოდა ზოგადი ინფორმაციის შევსებით, რომლის მიხედვით, გამოკითხულთაგან 39 მდედრობითი სქესის წარმომადგენელი იყო, 9 - მამრობითი სქესის.

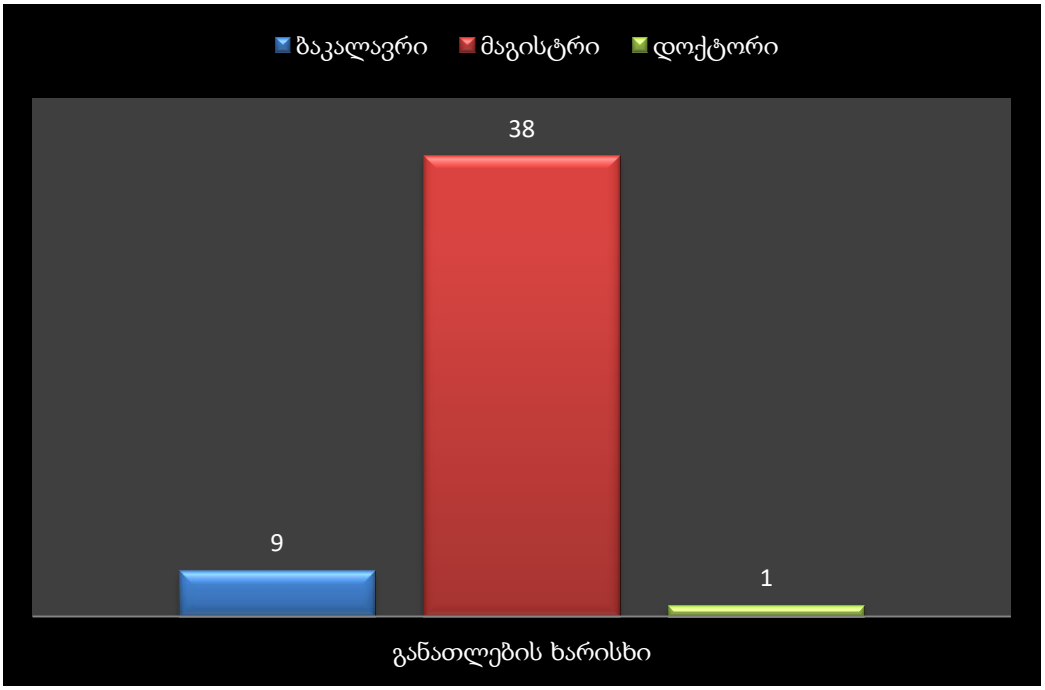
რაც შეეხება მათ ასაკობრივ ზღვარს, დიაგრამაზე ის ასე გამოიყრება:



დიაგარამა #1

სკოლაში მომუშავე მასწავლებლების თითქმის 34%-ის ასაკი 41-დან 51წლამდე მერყეობს. იყო პერიოდი, როცა ახალგაზრდებს არ სურდათ სკოლაში მასწავლებად მუშაობა,თუმცა ამ თვალსაზრისით შეინიშნება დადებითი ტენდეციები, 21-31 წლამდე გამოკითხული მასწავლებლის პროცენტული წილი 21%_ს შეადგენს.

ახლა ვნახოთ, თუ როგორია მასწავლებელთა განათლების ხარისხი:

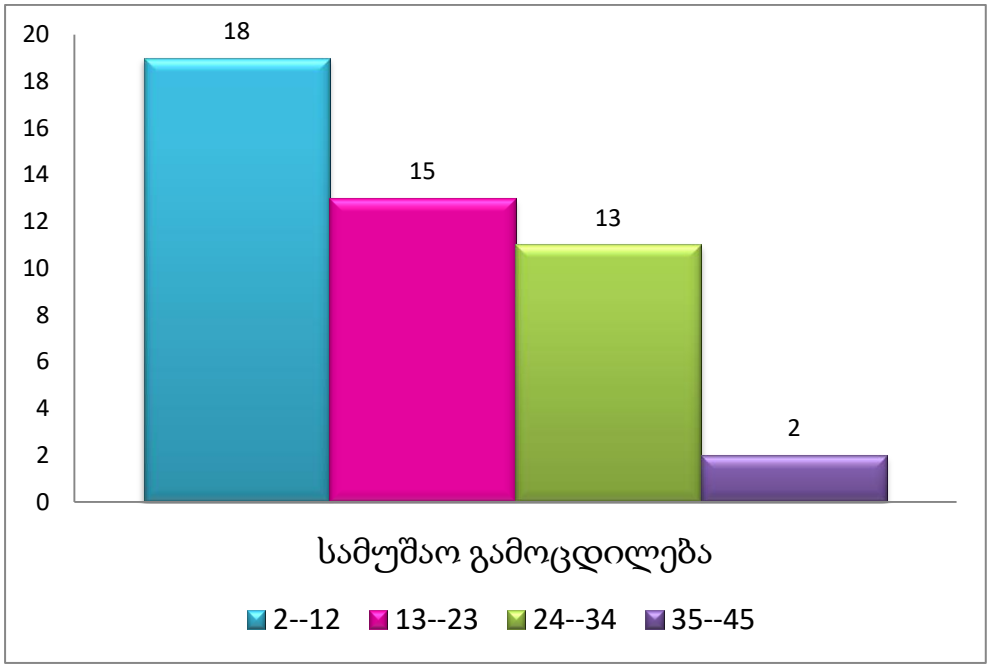


დიაგარამა #2

გამოკითხულთა 80% მაგისტრის ხარისხისაა, აქ შედიან ის მასწავლებლები , რომლებმაც 5 წელი ისწავლეს უნივერსიტეტში და მათი განათლება უტოლდება დღევანდელი მაგისტრატურის ხარისხს.

გამოკითხული მასწავლებლებიდან 38 არის სერტიფიცირებული (80%) , ხოლო არასერტიფიცირებული 10 (20%)პედაგოგი.მასწავლებელთა საკმაოდ დიდი რაოდენობა არის სერტიფიცირებული, ეს ჩემი აზრით, მიუთითებს პედაგოგთა მაღალ კვალიფიკაციაზე.

მასწავლებლების სამუშაო გამოცდილება ასე გადანაწილდა:

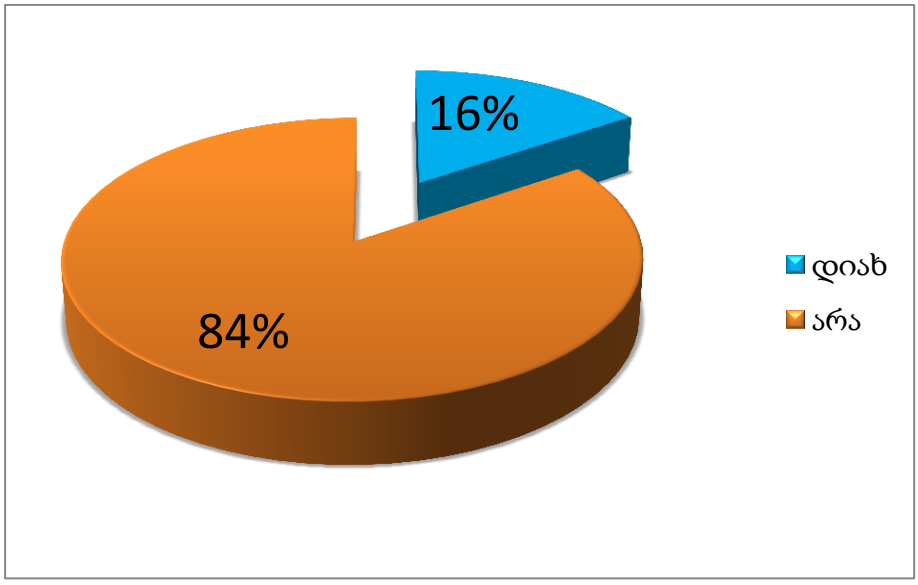


დიაგარამა #3

ახლა რაც შეეხება უშუალოდ კითხვარს, კითხვარი შედგება 10 შეკითხვისგან, აქედან 8 დახურულია ,ხოლო 2 ღია ტიპის კითხვას მოიცავს.სამწუხაროდ პედაგოგთა უმრავლესობამ ღია ტიპის შეკითხვისთვის გამოყოფილი ადგილი ცარიელიდატოვა.

გავეცნოთ კითხვარს:

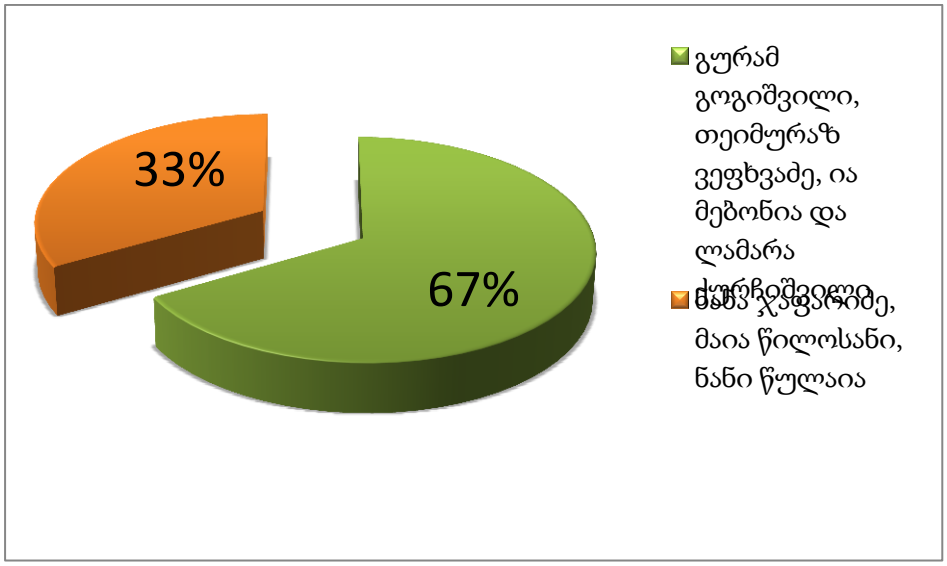
1) **მიგაჩნიათ თუ არა, რომ ნაშთთა არითმეტიკის ჩართვა ეროვნულ სასწავლო გეგმაში ზედმეტია?**



დიაგარამა #4

უმრავლესობის აზრით, ნაშთა არითმეტიკის სწავლება აუცილებლია, შესაბამისად, მისი შეტანა ეროვნულ სასწავლო გეგმაში მართებულია, თუმცა გამოკითხულთა გარკვეული ნაწილი თვლის, რომ სრულებით ზედმეტია და არაა საჭირო მისი სწავლება. ნაშთით გაყოფის სწავლება მე-4 კლასიდან იწყება და გრძელდება მე-12 კლასმადე ნაშთთა არითმეტიკის საკითხით. მისი ამოღება, დაუშვებელია, ეროვნულ სასწავლო გეგმაში შეტანილია მე-4 -- მე-9 კლასებში და მე-11 კლასში, მე-10 კლასში არ ხდება ნაშთთა არითმეტიკის ელემენტების სწავლება, ჩემი აზრით, აქაც უნდა შეიტანონ აღნიშნული საკითხი.

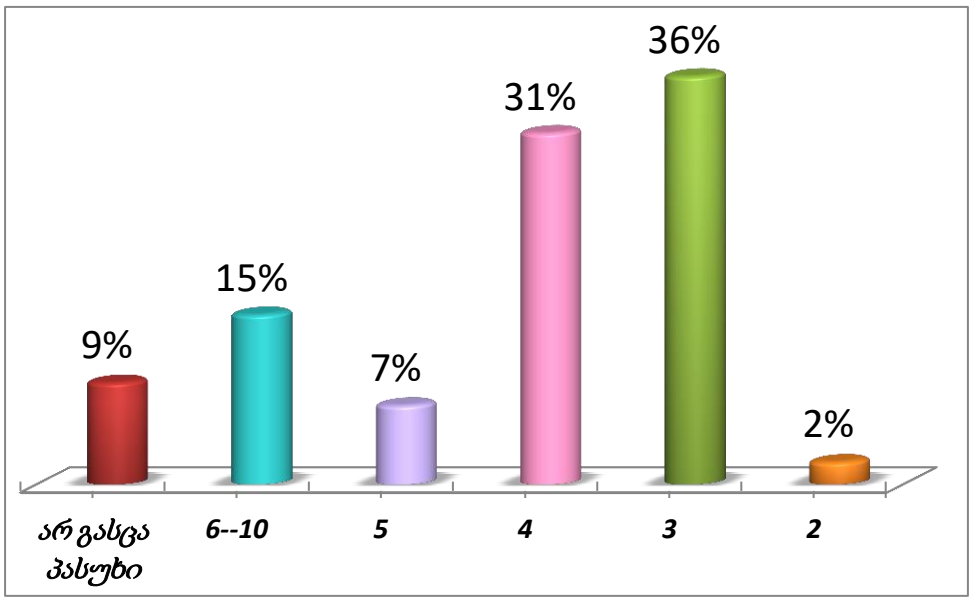
2) **რომელი ავტორის სახელმძღვანელოს იყენებთ მათემატიკის სწავლებისას საშუალო საფეხურზე?**



დიაგარამა #5

გამოკითხულთა თითქმის 67% იყენებს გურამ გოგიშვილის, თეიმურაზ ვეფხვაძის, ია მებონიას და ლამარა ქურჩიშვილის სახელმძღვანელოს. 33%- ნანა ჯაფარიძის, მაია წილოსანის, ნანი წულაიას წიგნს. ამ ავტორის სახელმძღვანელოში, მე-11 კლასში არაა შეტანილი ნაშთთა არითმეტიკის საკითხი, (http://eqe.ge/geo/textbook_approval/) მიუხედავად იმისა რომ ეროვნულ სასწავლო გეგმაში, მათემატიკის სტანდარტში, მე-11 კლასის პროგრამის შინაარსში შედის საკითხი ნაშთების არითმეტიკის ელემენტები და როგორც ვიცით პროგრამის შინაარსში შესული საკითხების სწავლება სავალდებულოა.

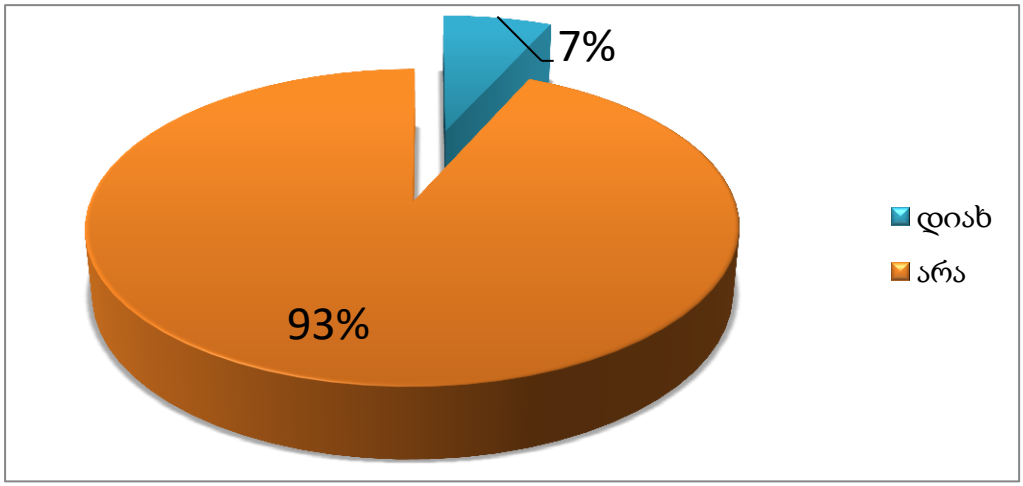
3) **თქვენ მიერ შედგენილ კალენდარულ გეგმაში რამდენ საათს უთმობთ ნაშთთა არითმეტიკის(მოდულური არითმეტიკის) სწავლებას ?**



დიაგარამა #6

ამ კითხვაში იგულისხმება ერთი სასწავლო წლის განმავლობაში გასავლელი ნაშთთა არითმეტიკის სწავლებას რა დროს უთმობს მასწავლებლი მე-11 კლასში. კვლევის დროს დაკვირვებისას დავადგინე, რომ მასწავლბელთა გარკვეულ ნაწილს ჩანიშნული და გაწერილი ჰქონდა კალენდარული გეგმა და ამ კითხვაზე პასუხის გასაცემად დაიხმარეს ჩანაწერი. ასეთი პედაგოგები ძირითადად 3 საათს უთმობდნენ ნაშთთა არითმეტიკის სწავლებას , რაც გამოკითხულთა 36 %_ს შეადგენს. რაც შეეხება იმ მასწავლებელთა ნაწილს, რომელიც 6-10 საათს უთმობს მასალის ათვისებას, ვფიქრობ, გადაჭარბებულია და რეალობას არ შეესაბამება.

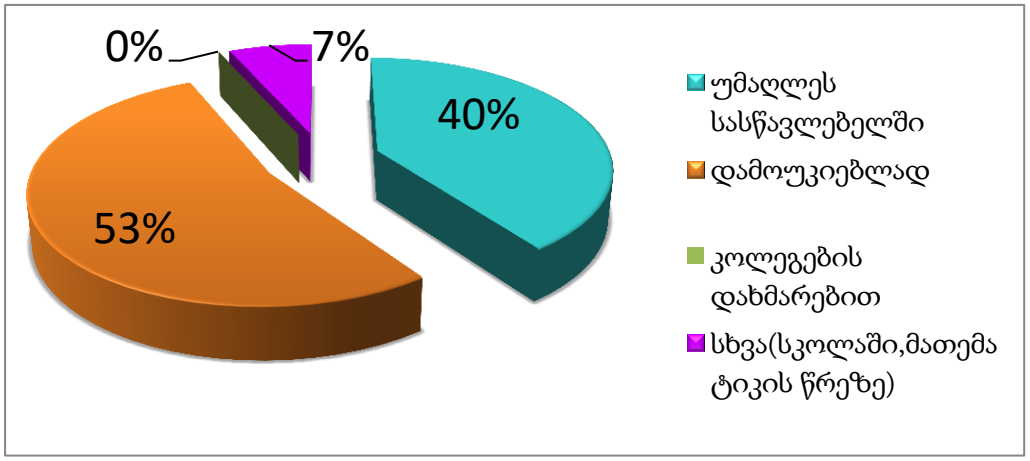
4) გაქვთ თუ არა გავლილი ტრენინგი, რომელიც მოიცავდა ნაშთთა არითმეტიკის სწავლების საკითხს?



დიაგარამა #7

გამოკითხულ მასწავლებელთა 93%_ს არ აქვს გავლილი ტრენინგი , რომელიც ნაშთთა არითმეტიკის სწავლების საკითხს მოიცავდა. სინამდვილეში მასწავლებლთა უმრავლესობას, ჩემი აზრით, უჭირს ნაშთთა არითმეტიკის მასალის კარგად გააზრება და შემდგომ მოსწავლეთათვის ცოდნის გადაცემა. პედაგოგების გადასამზადებლად აუცილებელია ტრენინგები, განსაკუთრებით იმ საკითხებთან დაკავშრებით, რაც ახალი შეტანილია ეროვნულ სასწავლო გეგმაში, ეს საშუალებას მისცემს მათ, საკითხი საფუძვლიანად გაიგონ. დღესდღეობით კი ასეთი გადამზადება როგორც პასუხებიდან ჩანს არ ხდება.

5) **სად შეისწავლეთ საკითხი ნაშთთა არითმეტიკის შესახებ (მოდულურიარითმეტიკა)?**

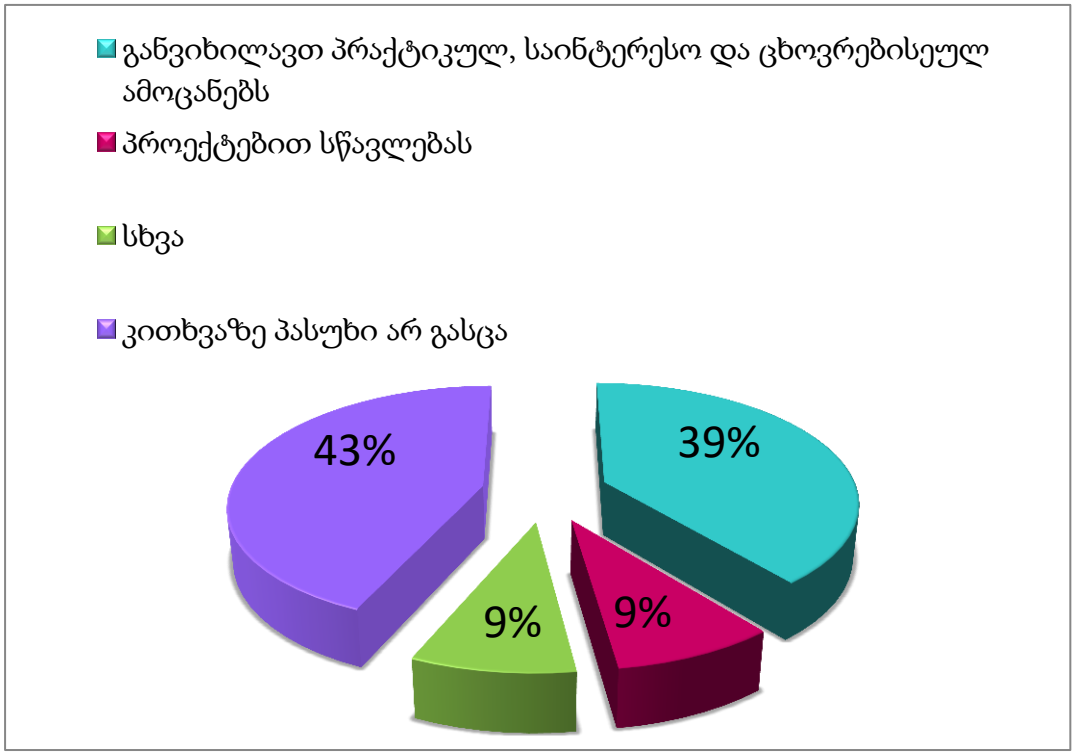


დიაგარამა #8

ნაშთთა არითმეტიკა(მოდულური არითმეტიკა) ჩემი უნივერსიტეტში (ბაკალავრიატის დროს) სწავლების დროს არ ისწავლებოდა, აღნიშნული საკითხი, ვფიქრობ, ჩემთვისაც შეიძლება რთული აღმოჩენილიყო მასალის მოსწავლეთათვის გადასაცემად, რომ არ მესწავლა აღნიშნული საკითხი მაგისტრატურაში. გამოკითხულთა ნახევარზე მეტმა, 53%-მა, დამოუკიდებლად ისწავლა და დაამუშავა საკითხი. 40%-მა განაცხადა, რომ აღნიშნული საკითხი უნივერსიტეტში ისწავლა, ამ 40%-ში შედის ძირითადად 5-წლიანი განათლების მქონე პედაგოგები.

გამოკითხულთა 80% თვლის, რომ დამატებითი სახელმძღვანელო არაა საჭირო. ზოგიერთმა პედაგოგმა საუბარში ისიც აღნიშნა, ნაშთთა არითმეტიკასთან დაკავშირებით სახელმძღვანელოში არსებული მასალაც კი ზედმეტია. მასწავლებლების ასეთი დამოკიდებულება, შესაბამისად, შედეგზეც აისახა.

6) **მოსწავლეების მოტივაციის ასამაღლებლად და ნაშთთა არითმეტიკის საკითხით დასაინტერესებლად რა მეთოდებს, ხერხებს იყენებთ?**

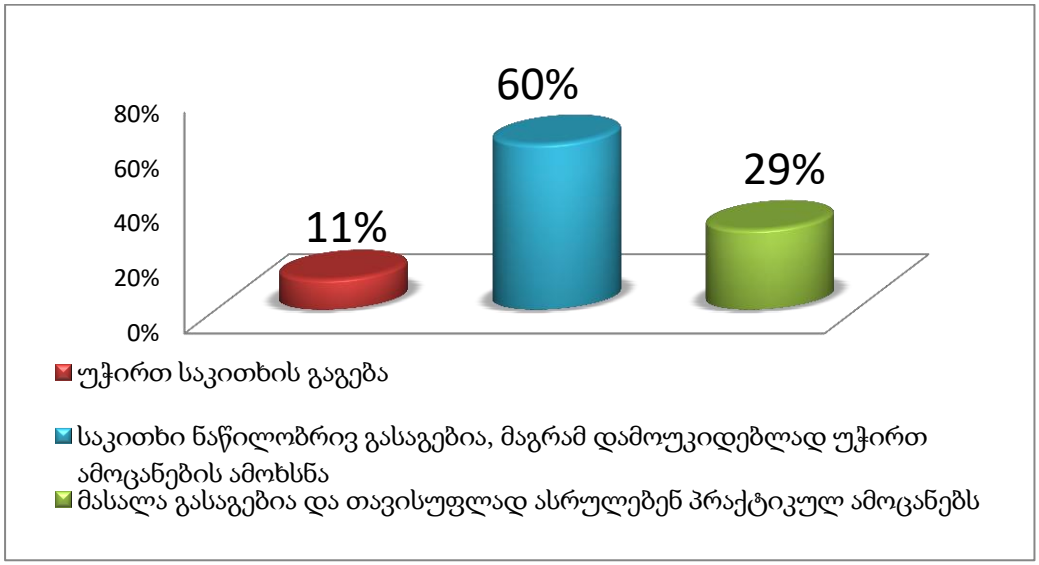


დიაგარამა #9

ეს კითხვაც წარმოადგენდა ღია ტიპს, როგორც აღვნიშნეთ აქაც გამოკითხულთა 43%-მა არ გასცა შეკითხვაზე პასუხი. მიზეზი შეიძლება იყოს ის , რომ მასწავლებლები არ იყენებენ გაკვეთილის დროს არანაირ მოტივაციის ასამაღლებელ საშუალებას.

დიაგრამიდან ჩანს რომ 39% განიხილავს საინტერესო, პრაქტიკულ ამოცანებს , ხოლო პროექტებით სწავლებას 9% იყენებს. დარჩენილმა 9% თქვეს მოსწავლეები წყვილებში და ჯგუფში მუშაობენ,ზოგმა დაწერა ,რომ „საკმარისია სკოლაში მოსწავლემ ისწავლოს გასაყოფი, გამყოფი, არსრული განაყოფი და ნაშთი“.

7) **როგორ ითვისებენ მოსწავლეები მასალას ნაშთთა არითმეტიკაზე?**



დიაგარამა #10

ბოლო კითხვა ეხებოდა იმის დადგენას, თუ როგორ იგებენ მასალას მოსწავლეები. მასწავლებელთა 11%-ის აზრით,მოსწავლეებს უჭირთ საკითხის გაგემა, 60 % თვლის, რომ საკითხი მეტ-ნაკლებად გასაგებია, პრაქტიკული ამოცანების ამოხსნინას სჭირდებათ დახმარება, ხოლო 29%-ს მიაჩნია, რომ საკითხი სავსებით გასაგებია მოსწავლეებისათვის.

რეკომენდაციები

გამოკვლევის შედეგებიდან გამომდინარე, სკოლაში არსებული მდგომარეობა ნაშთთა არითმეტიკის საკითხის სწავლებასთან დაკავშირებით არასახარბიელოა.

ჩვენი რეკომენდაციები ამ საკითხთთან დაკავშირებით შემდეგია:

1.უნდა აღდგეს მასწავლებელთა გადამზადების სისტემა . მაშინ, როცა ახალი საკითხი შედის ეროვნულ სასწავლო გეგმაში, აუცილებელია მასწავლებელთა ინფორმირება და შესაბამისად მომზადება ამ სიახლისათვის. უნდა არსებობდეს გადამზადების ცენტრები, რომლებიც ტრენინგს ჩაუტარებს მოქმედ მასწავლებლებს ახალი საკითხის საფუძვლიანი შესწავლისათვის.

2. საუნივერსიტეტო სწავლების დონის ამაღლება - მომავალი მასწავლებლები უნივერსიტეტში უნდა ეუფლებოდნენ ყველა იმ საკითხს, რომელიც სკოლაში ისწავლება.

გამოყენებული ლიტერატურა

1.ა. ხარაზიშვილი. მათემატიკური ესკიზები, ნაწ. 1. თბილისი, 2007, გვ. 35-37;

2.ა. ბენდუქიძე. მათემატიკა სერიოზული და სახალისო, ნაკადული, 1988.გვ.250;

3.ა. ვალფიში, რიცხვთა თეორიის კურსი. თბილისი სამეცნიერო-მეთოდური კაბინეტის გამომცემლობა, 1947.გვ.310;

4.გ. გოგიშვილი, თ. ვეფხვაძე, ი. მებონია, ლ. ქურჩიშვილი, ალგებრა, მეშვიდე კლასის სახელმძღვანელო, თბილისი,ინტელექტი, 2003. გვ. 231;

5. გ. გოგიშვილი, თ. ვეფხვაძე, ი. მებონია, ლ. ქურჩიშვილი, მათემატიკა მეთერთმეტე კლასის სახელმძღვანელო, თბილისი,გამომცემლობა ინტელექტი,2007. გვ 445;

6.გ. გოგიშვილი, თ. ვეფხვაძე, ი. მებონია, ლ. ქურჩიშვილი, მათემატიკა, სახელმძღვანელოები I-XII კლასის მოსწავლეებისთვის, ინტელექტი, 2011-2012;

7.გ. გოგიშვილი, თ. ვეფხვაძე, ი. მებონია, ლ. ქურჩიშვილი, მათემატიკა,XI კლასი, მასწავლებლის წიგნი, ინტელექტი, 2012. გვ.214

8.გ. ლომაძე, შედარებათა თეორიის ელემენტები, 1979, გვ.24-30;

9.ეროვნული სასწავლო გეგმა 2011-2016 ,საგნობრივი პროგრამა მათემატიკაში გვ.373-478;

10. ე.იმერლიშვილი, მათემატიკის სწავლების ზოგადი მეთოდიკა, თბილისის უნივერსიტეტის გამომცემლობა,2001. გვ. 346;

11. თ.დოგრაშვილი , დისერტაცია, 2010. გვ.171;

12. პ.კოღონია, ა.ლურსმანაშვილი, რიცხვთა თეორიის კურსი, თბილისი, განათლება,1967.გვ.334

13. რ. კურანტი, ჰ. რობინსი. რა არის მათემატიკა, თბილისი, განათლება,1965. გვ.625.

14. www.wikipedia.org

15. www.google.com

16. http://eqe.ge/geo/textbook_approval/

17. http://mes.gov.ge/content.php?id=3929&lang=geo