სხვანაირი რიცხვები

ერთ-ერთი პირველი რამ, რასაც მათემატიკაში გვასწავლიან, არის ძირითადი მოქმედებები რიცხვებზე: შეკრება, გამოკლება, გამრავლება და გაყოფა. და მაშინვე იჩენს თავს ერთ-ერთი პირველი უცნაურობა, რაც მათემატიკას თან ახლავს: ეს მოქმედებები იმთავითვე უსასრულოდ ბევრ რიცხვებს წარმოქმნის, რაგინდ დიდებსაც (1, 2=1+1, 3=1+1+1, ...) და რაგინდ მცირეებსაც (1/2, 1/3, 1/4, 1/5, ...). თანაც ყველა ეს უსასრულოდ ბევრი რიცხვი ცალსახად და აუცილებლად გაჩნდება, თუ გვინდა, რომ შეკრებას და გამრავლებას მათი ჩვეული თვისებები ჰქონდეთ (მაგალითად, გადანაცვლებადობა, განრიგებადობა). ამავე ძირითადი მოქმედებებით განისაზღვრება კიდევ უფრო მეტი რიცხვები, რომლებსაც წილადებით ვერ გამოვსახავთ — მაგალითად, $\sqrt{2}$ რიცხვია, რომლის თავის თავზე ნამრავლი არის 2.

სინამდვილეში, კარგადაა ცნობილი, თუ როგორ შეიძლება აიგოს „სხვანაირი“ რიცხვები, რომელთა რაოდენობა სასრულია, თუმცა მათზე ძირითადი მოქმედებები თითქმის ისევე მუშაობს, როგორც „ჩვეულებრივ“ რიცხვებზე. უფრო მეტიც, ასეთი აგება ბევრნაირი არსებობს — სულ მცირე, იმდენნაირი, რამდენი მარტივი რიცხვიც გვაქვს, სინამდვილეში კი გაცილებით მეტი. ალბათ მიხვდით, მხედველობაში გვაქვს რომელიმე p მარტივ რიცხვზე გაყოფის ნაშთები, ანუ ნაშთები <u>მოდულით</u> p. მაგალითად, თუ $p = 7$, გვექნება სულ შვიდი „რიცხვი“, 0-დან 6-ის ჩათვლით. მათზე მოქმედებები მიიღება „ჩვეულებრივი“ მოქმედებებისგან მოდულით 7 ნაშთზე გადასვლით. ვთქვათ, $5 + 6 = 4$, რადგან 11-ის ნაშთი 7-ზე გაყოფისას არის 4. გვიჩნდება წილადები, მაგალითად, $1/4 = 2$, ვინაიდან $4 \cdot 2 = 8$-ის ნაშთი 7-ზე გაყოფისას არის 1, ასე რომ 2 „იძენს“ 1/4-ის თვისებებს. მართალია, ამ რიცხვებს შორის არ გვექნება 1/7, მაგრამ „ჩვეულებრივი“ აზრითაც ხომ არ შეგვიძლია 0-ზე გაყოფა, აქ ჩვენთან კი $7 = 0$. ამ რიცხვებს შორის $\sqrt{2}$-იც მოგვეპოვება: მის როლს თამაშობს 3, რადგან $3 \cdot 3 = 9$-ის ნაშთი მოდულით 7 არის 2. აი მაგალითად $\sqrt{5}$-ს კი ვერ ვიპოვით, იმიტომ რომ 0-დან 6-მდე რაც არ უნდა გავამრავლოთ თავის თავზე, ნაშთი მოდულით 7 გამოგვივა მხოლოდ 1, 2 ან 4. რომ აგვეღო $p = 11$, მაშინ $\sqrt{5}$ გვექნებოდა, რადგან $4 \cdot 4 = 16$-ს ნაშთი 11-ზე გაყოფისას არის 5, მაგრამ აღარ გვექნებოდა $\sqrt{2}$.

სინამდვილეში შესაძლებელია p-ს შეუცვლელად ვაფართოვოთ ნაშთების ერთობლიობა ისე, რომ მას სულ უფრო მეტი განტოლების ამონახსნი დაემატოს, უკვე არსებული ამონახსნები კი არ დაიკარგოს. ასეთნაირად ვღებულობთ <u>სასრულ ველებს</u> — რიცხვით სისტემებს, რომლებიც ემსგავსებიან „ჩვეულებრივ“ რიცხვებს, თუმცა ნაშთებზე ყოველთვის აღარ დაიყვანებიან. ასეთი ზოგადი სასრული ველები პირველად განიხილა ევარისტ გალუამ 1830 წელს, და მათ გალუას ველებსაც უწოდებენ ხოლმე. გასაგებია, რომ სასრული ველები მნიშვნელოვან როლს თამაშობენ მათემატიკის მრავალ დარგში, პირველ რიგში რიცხვთა თეორიაში. შესაძლოა უფრო მოულოდნელად მოგეჩვენოთ, რომ გალუას ველებს აქვთ სერიოზული გამოყენებები ისეთ სრულიად პრაქტიკულ საკითხებში, როგორებიცაა კომპიუტერული უსაფრთხოება, შეტყობინებათა გადაცემა ან მონაცემების კოდირება. მაგალითად, შესაძლოა შეგხვედრიათ QR-კოდები

ისინიც სასრულ ველებთან დაკავშირებულ ალგორითმებზეა დაფუძნებული. ჩვენ განვიხილავთ რამდენიმე შედარებით მარტივ საკითხს, რომელთა შესწავლას აადვილებს სასრული ველების მოშველიება. მოვნიშნავთ გზადაგზა გაჩენილ კითხვებს, რომლებზეც შეგიძლიათ იფიქროთ.

ტესტები, კოდები და ვექტორული სივრცეები

დავიწყოთ ორი ერთმანეთისგან სრულიად განსხვავებული ამოცანით. ერთი რეალურად შეგვხვდა ტესტების შედგენისას, მეორეს ხანგრძლივი ისტორია აქვს და შეტყობინებათა გადაცემას უკავშირდება.

ტესტის ვარიანტები

აი გამოგონებული, ძალიან გამარტივებული ვერსია იმისა, რაც რეალურად გვჭირდებოდა:

უნდა შევადგინოთ ტესტის 6 ვარიანტი. თითოეულ ვარიანტში უნდა იყოს 4 დავალება -- ერთი ბიოლოგიაში, ერთი გეოგრაფიაში, ერთი ფიზიკაში, და ერთი ქიმიაში. თითოეულ საგანში გვაქვს სამ-სამი დავალება, ყოველი მათგანი ორ-ორ ვარიანტში უნდა გამეორდეს. ვარიანტები ისე უნდა შევადგინოთ, რომ მათში ერთნაირი დავალებები რაც შეიძლება ცოტა იყოს. უფრო ზუსტად, თუ n_{ij} აღნიშნავს i-ურ და j-ურ ვარიანტში ერთნაირ დავალებათა რაოდენობას, გვინდა რომ რაც შეიძლება მცირე იყოს ყველა $i \neq j$-სათვის n_{ij}-ებს შორის უდიდესი.

აი ერთ-ერთი მცდელობა. ვთქვათ, ბიოლოგიის დავალებებია $ბ_1$, $ბ_2$, $ბ_3$, გეოგრაფიისა $გ_1$, $გ_2$, $გ_3$ და ასე შემდეგ. გასაგებია, რომ პირველი სამი ვარიანტი შეგვიძლია შევადგინოთ ისე, რომ მათში ერთნაირი დავალებები საერთოდ არ მეორდებოდეს: პირველ ვარიანტში შევიტანთ დავალებებს $ბ_1$, $გ_1$, $ფ_1$, $ქ_1$, მეორეში დავალებებს $ბ_2$, $გ_2$, $ფ_2$, $ქ_2$, და მესამეში $ბ_3$, $გ_3$, $ფ_3$, $ქ_3$. დარჩენილ სამ ვარიანტში დავალებები უკვე აუცილებლად უნდა გამეორდეს, რადგან ყველა დავალება რაც გვაქვს უკვე დავხარჯეთ. შეგვიძლია ისინი, მაგალითად, ასე გავანაწილოთ:

		ვარიანტი					
		I	II	III	IV	V	VI
დავალება	ბიოლოგია	$ბ_1$	$ბ_2$	$ბ_3$	$ბ_1$	$ბ_2$	$ბ_3$
	გეოგრაფია	$გ_1$	$გ_2$	$გ_3$	$გ_2$	$გ_3$	$გ_1$
	ფიზიკა	$ფ_1$	$ფ_2$	$ფ_3$	$ფ_3$	$ფ_1$	$ფ_2$
	ქიმია	$ქ_1$	$ქ_2$	$ქ_3$	$ქ_1$	$ქ_3$	$ქ_2$

მაშინ, მაგალითად, პირველ და მეოთხე ვარიანტში იქნება ორი ერთნაირი დავალება ($ბ_1$ და $ქ_1$)

საერთოდაც ამ განლაგებისას ვარიანტებში ერთნაირი დავალებების რაოდენობები ასეთნაირია:

	I	II	III	IV	V	VI
I						
II	0					
III	0	0				
IV	2	1	1			
V	1	1	2	0		
VI	1	2	1	0	0	

ასე რომ ვარიანტების წყვილებში ერთნაირ დავალებათა რაოდენობა არ აღემატება 2-ს.

კითხვა: ხომ არ არსებობს უკეთესი განლაგება? სახელდობრ, ისეთი, რომ ვარიანტების ნებისმიერ წყვილს ჰქონდეს არაუმეტეს ერთი საერთო დავალება?

შეცდომებიანი შეტყობინებები

ეხლა მეორე, ერთი შეხედვით სულ სხვა ამოცანა.

გვინდა რაიმე შეტყობინების გადაცემა, მაგალითად, ინტერნეტით. წარმოვიდგინოთ, რომ ჩვენს განკარგულებაშია მინიმალური შესაძლებლობის მქონე მოწყობილობა: დროის ყოველ ერთეულში (მაგალითად, წამის მეათასედში) მას შეუძლია გააგზავნოს იმპულსი ან არ გააგზავნოს. პირველი შემთხვევა აღვნიშნოთ სიმბოლოთი „+“, ხოლო მეორე სიმბოლოთი „−“. ჩვენ შეგვიძლია თითოეულ გადასაცემ ასოს შევუსაბამოთ ამ სიმბოლოების ესა თუ ის მიმდევრობა, კოდური სიტყვა. მაგალითად, „ა“-ს შეგვიძლია შევუსაბამოთ (−,−,−,−,−,−), „ბ“-ს (−,−,−,−,−,+), „გ“-ს (−,−,−,−,+,−), „დ“-ს (−,−,−,−,+,+) და ასე შემდეგ. მივიღებთ გარკვეულ კოდს.

მაგალითად, ასეთი კოდით სიტყვა „დაბა“ გადაიცემა როგორც −−−−++−−−−−−−−−−+−−−−−−−

მაგრამ გადაცემისას შეიძლება მოხდეს შეცდომები. მაგალითად, რომელიმე დროის ერთეულში გადამცემმა სიგნალი გამოუშვა, მიმღებამდე კი ამ სიგნალმა ვერ მიაღწია. მაშინ მიმღები ჩათვლის, რომ შეტყობინების შესაბამის ადგილას დგას „−“, სინამდვილეში კი უნდა ყოფილიყო „+“. შედეგად, თუ კოდური სიტყვით −−−−++ გადაცემული იყო ასო „დ“, და ეს შეცდომა მოხდა ბოლო სიგნალის გადაცემისას, მიმღები ჩათვლის, რომ კოდური სიტყვით −−−−+− გამოგზავნილია ასო „ბ“. შეტყობინება

−	−	−	−	+	+	−	−	−	−	−	−	−	−	−	−	−	+	−	−	−	−	−	−
დ						ა						ბ						ა					

მიმღებამდე მიაღწევს ასეთი სახით

–	–	–	–	+	–	–	–	–	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–
ბ						ა						ბ						ა					

ასეთი შეცდომები ხშირი იქნება, რადგან კოდური სიტყვები თითქმის ერთნაირია. „ბ“-ს და „დ“-ს შესაბამისი კოდური სიტყვები −−−−+− და −−−−++ ერთმანეთს ემთხვევა ყველა პოზიციაში, გარდა უკანასკნელისა. პოზიციების რაოდენობები, რომლებშიც კოდური სიტყვები ერთმანეთს ემთხვევა, ამ მაგალითში ასეთია:

	ა	ბ	გ	დ
ა				
ბ	5			
გ	5	4		
დ	4	5	5	

ამიტომ ჯობია შეძლებისდაგვარად კოდური სიტყვები ისე შევარჩიოთ, რომ შემთხვევით გაპარული შეცდომა იოლად აღმოვაჩინოთ - ან იქნებ სწორი კოდური სიტყვის აღდგენაც შეგვეძლოს.

ამისათვის საჭიროა, რომ სიტყვები რაც შეიძლება ნაკლებ პოზიციაში ემთხვეოდეს ერთმანეთს.

მაგალითად, ასეთი კოდური სიტყვები რომ შეგვერჩია:

„ა“: −−−−−−

„ბ“: ++++++

„გ“: +−+−+−

„დ“: −+−+−+

მაშინ დამთხვევების რაოდენობები სიტყვებს შორის ნაკლები იქნება:

	ა	ბ	გ	დ
ა				
ბ	0			
გ	3	3		
დ	3	3	0	

ასეთი კოდისთვის, თუ, ვთქვათ, მივიღებთ სიტყვას „−−+−−−“, გვეცოდინება, რომ შეცდომა მოხდა. უფრო მეტიც, თუ ვიცით, რომ ერთ შეცდომაზე მეტი არ მომხდარა, სწორ კოდურ სიტყვას ცალსახად აღვადგენთ.

კითხვა: ვთქვათ, ვიცით, რომ შეიძლებოდა ორი შეცდომა მომხდარიყო. მაშინ თუ შევძლებთ ყოველთვის მივხვდეთ, შეცდომა მოხდა თუ არა? და თუ შევძლებთ სწორი კოდური სიტყვის აღდგენას? და სამი შეცდომის შემთხვევაში თუ შევძლებთ?

სინამდვილეში ჩვენ მხოლოდ ოთხი ასოთი შემოვიფარგლეთ, არადა მთელი ანბანი უნდა იყოს კოდირებული. თუ ჩვენ გვინდა შეცდომების გასწორება შევძლოთ, კოდური სიტყვები უფრო გრძელი უნდა იყოს. უფრო გრძელი კოდური სიტყვების გადაცემას კი მეტი დრო დაჭირდება. ამიტომ გვინდა ჩვენს მიზანს მივაღწიოთ რაც შეიძლება მოკლე კოდური სიტყვების გამოყენებით.

რა კავშირშია ეს ყველაფერი იმასთან, რითაც დავიწყეთ – ტესტების შედგენასთან ვარიანტებს შორის დავალებების რაც შეიძლება ნაკლები გამეორებებით?

ჩვენთან კოდური სიტყვების როლს თამაშობენ ვარიანტები, პოზიციების როლს კი – დავალებების თემები. მაგალითად, IV ვარიანტში ჩვენ მოვათავსეთ დავალებები ($ბ_1$, $გ_2$, $ფ_3$, $ქ_1$); ამ ვარიანტს შეგვიძლია შევუსაბამოთ კოდური სიტყვა „1231“. ან, ვთქვათ, III ვარიანტისთვის გვქონდა დავალებები ($ბ_3$, $გ_3$, $ფ_3$, $ქ_3$), რასაც შეესაბამება კოდური სიტყვა „3333“. განსხვავება ისაა, რომ „+“ და „−“ სიმბოლოების მაგიერ კოდური სიტყვები შედგენილი იქნება სიმბოლოებით „1“, „2“ და „3“ – იმდენით, რამდენი დავალებაც გვაქვს თითოეული საგნისათვის.

ჩვენთან გადამწყვეტი იყო იმის ცოდნა, თუ რამდენი დავალება მეორდება რომელიმე ორ ვარიანტში. ზოგადი კოდისათვის გადამწყვეტია იმის ცოდნა, თუ რამდენ პოზიციაში ემთხვევა ერთმანეთს რომელიმე ორი კოდური სიტყვა.

ორ x, y კოდურ სიტყვას შორის მანძილი $d(x, y)$ ბუნებრივია დავარქვათ იმ პოზიციათა რაოდენობას, რომლებშიც ეს კოდური სიტყვები ერთმანეთისგან განსხვავდებიან.

C კოდის დაშორება $d(C)$ ვუწოდოთ განსხვავებულ კოდურ სიტყვებს შორის უმცირეს მანძილს.

ამრიგად, ჩვენ გვაინტერესებს კოდები, რომელთა დაშორებაც რაც შეიძლება დიდია, ე. ი. რომლებისთვისაც განსხვავებულ კოდურ სიტყვებს შორის უმცირესი მანძილი რაც შეიძლება დიდია.

თუ C კოდის დაშორება მეტია მოცემულ k რიცხვზე, $d(C) > k$, მაშინ თითოეულ სიტყვაში k-მდე შეცდომის მიხვედრას შევძლებთ.

კითხვა: როგორ მივაღწევთ ამას?

ამ კითხვაზე პასუხის გასაადვილებლად ვნახოთ ერთი მსგავსი დებულება.

თუ $d(C) > 2k$, მაშინ თითოეულ სიტყვაში k-მდე შეცდომის გასწორებაა შესაძლებელი.

მართლაც, ვთქვათ მივიღეთ სიტყვა x. თუ ამ სიტყვის მიღებისას მოხდა არა უმეტეს k შეცდომისა, მოიძებნება კოდური სიტყვა c, რომლისგანაც x განსხვავდება არა უმეტეს k პოზიციაში. ნებისმიერი სხვა c' კოდური სიტყვისათვის, c და c' ერთმანეთისგან განსხვავდება $2k$-ზე მეტ პოზიციაში, რადგან $d(C) > 2k$. ამიტომ x და c' ერთმანეთისგან k-ზე მეტ პოზიციაში უნდა განსხვავდებოდნენ. მართლაც, წინააღმდეგ შემთხვევაში, მაშინაც კი, თუ პოზიციები, სადაც x განსხვავდება c-სგან და პოზიციები, სადაც x განსხვავდება c'-სგან, ყველა სხვადასხვაა, ეს მოგვცემდა c-სა და c'-ს შორის არა უმეტეს $2k$ განსხვავებას, მაშინ როცა ამ განსხვავებათა რაოდენობა $2k$-ზე მეტია. ამრიგად, თუ ვიცით, რომ შეცდომების რაოდენობა არ აღემატებოდა k-ს, გვეცოდინება, რომ x-ის მიღებას შევძლებდით მხოლოდ იმ შემთხვევაში, თუ გამოგზავნილი იქნებოდა c.

კოდური სიტყვების გამოკლება და რიცხვზე გამრავლება

სიტყვებს შორის მანძილებისა და კოდის დაშორების შესწავლა გაგვიადვილდებოდა, თუ შევძლებდით სიტყვები გამოგვეკლო ერთმანეთისათვის და დაგვეთვალა ნულების რაოდენობა. ორ სიტყვას ზუსტად იმდენი დამთხვევა ექნებოდა, რამდენი ნულიცაა მათ სხვაობაში, ამიტომ მანძილი ტოლი იქნებოდა სხვაობაში არანულოვანი პოზიციებისა.

მანძილი ორ კოდურ სიტყვას შორის უდრის მანძილს მათ სხვაობასა და ნულოვან სიტყვას შორის. თანაც თუ ეს სხვაობაც კოდური სიტყვაა, და მისი გამრავლება შეგვიძლია არანულოვან რიცხვზე, ნულების რაოდენობა არ შეიცვლება. ასეთნაირად შევძლებდით ერთი „კარგი“ კოდური სიტყვიდან ახალი, ასევე „კარგი“ კოდური სიტყვების მიღებას.

მაგალითად, ჩვენს ერთ-ერთ კოდში „ბ“-ს შეესაბამებოდა −−−−−+, ხოლო „გ“-ს −−−−+−. წარმოვადგინოთ სიმბოლო „−“ 0-ის მეშვეობით, „+“ კი 1-ის მეშვეობით, ისე რომ „ბ“-ს შესაბამისი კოდური სიტყვა იყოს 000001, ხოლო „გ“-სი 000010

გამოკლების ერთ-ერთი შესაძლებლობაა

(0,0,0,0,0,1) – (0,0,0,0,1,0) = (0–0,0–0,0–0,0–0,0–1,1–0) = (0,0,0,0,–1,1)

მივიღეთ ოთხი ცალი 0, იმიტომ რომ გვქონდა ოთხი დამთხვევა.

ეს (0,0,0,0,–1,1) რომ გავამრავლოთ, მაგალითად, 3-ზე, მივიღებთ 3(0,0,0,0,–1,1) = (3×0,3×0,3×0,3×0,3×(–1),3×1) = (0,0,0,0,–3,3), ნულების იმავე რაოდენობით.

ცუდი ისაა, რომ გაგვიჩნდა ახალი სიმბოლოები, რომლებიც ჩვენს კოდებში საერთოდ არ მონაწილეობდა: –1, –3 და 3

ან, ვთქვათ, ჩვენს ვარიანტს III შეესაბამებოდა სიტყვა 3333, ხოლო ვარიანტს IV კი 1231. გამოკლება მოგვცემს

(3,3,3,3) – (1,2,3,1) = (3–1,3–2,3–3,3–1) = (2,1,0,2)

მივიღეთ ერთი ცალი 0, რადგან გვქონდა ერთი დამთხვევა.

ეს (2,1,0,2) რომ გავამრავლოთ, მაგალითად, 4-ზე, მივიღებთ

4×(2,1,0,2) = (4×2,4×1,4×0,4×2) = (8,4,0,8).

აქაც გაგვიჩნდა „ზედმეტი“ რიცხვები: ჩვენს კოდებში მონაწილეობდა მხოლოდ 1, 2 და 3, ჩვენ კი კიდევ დაგვემატა 0, 4 და 8.

შეგვიძლია მოვიცილოთ ეს „ზედმეტი“ რიცხვები? პირველ შემთხვევაში ეს ნიშნავს ვისწავლოთ ისეთი შეკრება, გამოკლება და გამრავლება, რომ 0 და 1-ის გარდა სხვა არაფერი მიიღებოდეს. მეორე შემთხვევაში უნდა მიიღებოდეს მხოლოდ 1, 2 ან 3.

ამის მიღწევა ძალიან მარტივია: პირველ შემთხვევაში ყველა ლუწ რიცხვს, რომლებსაც მივიღებთ, შევხედოთ როგორც 0-ს, ხოლო ყველა კენტს, როგორც 1-ს.

მეორე შემთხვევაში, რიცხვებს ..., -6, -3, 0, 3, 6, ... შევხედოთ როგორც 0-ს, რიცხვებს ..., -5, -2, 1, 4, 7, ... როგორც 1-ს, და რიცხვებს ..., -4, -1, 2, 5, 8, ... როგორც 2-ს.

სხვანაირად რომ ვთქვათ, პირველ შემთხვევაში გადავდივართ 2-ზე გაყოფისას ნაშთზე, მეორე შემთხვევაში კი 3-ზე გაყოფისას ნაშთზე.

ნებისმიერ p მარტივ რიცხვზე (5-ზე, 7-ზე, 11-ზე,...) გაყოფის ნაშთებიც გამოგვადგებოდა.

რატომ მაინც და მაინც მარტივზე?

ჩვენ გვინდა, რომ ორი კოდური სიტყვის რაიმე ერთსა და იმავე არანულოვანზე გამრავლებისას პოზიციათა დამთხვევების რაოდენობა არ გაიზარდოს. ან, რაც იგივეა, ერთი კოდური სიტყვის რაიმე არანულოვანზე გამრავლებისას მასში ნულების რაოდენობა არ გაიზარდოს. ეს ხდება ზუსტად მაშინ, როცა ნაშთებს მარტივ რიცხვზე გაყოფისას ვიღებთ.

კითხვა: ვთქვათ და ავიღეთ არამარტივი p, მაგალითად 343. რომელ არანულოვან ნაშთებზე გამრავლებისას შეიძლება კოდურ სიტყვაში ნულების რაოდენობა გაიზარდოს და რატომ?

p მარტივ რიცხვზე გაყოფის ნაშთები ქმნიან ველს: განსაზღვრულია მათი შეკრება, გამოკლება, გამრავლება, და თანაც ყოველ არანულოვან ნაშთზე გაყოფა შეგვიძლია.

კითხვები: მოცემული $n > 0$ ნატურალური რიცხვისთვის აღვნიშნოთ Z_n-ით რიცხვთა სისტემა, რომელშიც შედის n ცალი რიცხვი $\{0,1,\dots,n-1\}$ და შეკრება და გამრავლება განსაზღვრულია n-ზე გაყოფისას მიღებული ნაშთის საშუალებით.

როგორი უნდა იყოს n, რომ განტოლებას $a + x = b$ ყოველთვის ჰქონდეს ერთადერთი ამონახსნი Z_n-ში, როცა a, b ასევე Z_n-იდანაა?

როგორი უნდა იყოს n, რომ განტოლებას $ax = b$ ყოველთვის ჰქონდეს ერთადერთი ამონახსნი Z_n-ში, როცა a, b ასევე Z_n-იდანაა და $a \neq 0$? რა ხდება, როცა $a = 0$?

რომელი n-ისათვის აქვს Z_n-ში განტოლებას $xx = 2$ ერთადერთი ამონახსნი? ზუსტად ორი ამონახსნი? ორზე მეტი ამონახსნი? არც ერთი ამონახსნი?

კოდს ეწოდება წრფივი, თუ ის შედგენილია რაიმე $\mathbb{F}$ ველის ელემენტებისაგან ისეთნაირად, რომ რომელიმე ორი კოდური სიტყვის სხვაობა ან კოდური სიტყვის გამრავლება ველის ელემენტზე კვლავ კოდური სიტყვაა.

ასეთ შემთხვევაში ვიტყვით, რომ კოდური სიტყვები ქმნიან ვექტორულ სივრცეს $\mathbb{F}$ ველზე.

წრფივ კოდებთან მუშაობა უფრო იოლია, ვიდრე ნებისმიერ ზოგად კოდებთან. „კარგი“ წრფივი კოდი შედგება ისეთი სიტყვებისაგან, რომლებშიც 0 იშვიათად გვხვდება.

ამ თემის მომდევნო ნაწილში უფრო ზუსტად განვმარტავთ (სასრული) **ველის** ცნებას, ამ ველზე განსაზღვრული **ვექტორული სივრცის** ცნებას და ვნახავთ, თუ როგორ შეიძლება ამ ცნებების გამოყენებით აქ განხილული ამოცანების ერთ მათემატიკურ ენაზე თარგმნა და დასმულ შეკითხვებზე პასუხის სისტემატური ძიება.

წინა მასალის შეხსენება

ჩვენ განვიხილეთ ორი სხვადასხვა ამოცანა, რომელთა შესასწავლად სასარგებლო იყო დაშორების, ან მანძილის შემოღება: ერთ შემთხვევაში ტესტის ორი ვარიანტის ერთმანეთისგან დაშორება იყო იმ პოზიციების რაოდენობა, რომლებზეც ამ ვარიანტებში განსხვავებული ამოცანები იყო. მეორე შემთხვევაში ორ კოდურ სიტყვას შორის დაშორება იყო იმ პოზიციების რაოდენობა, რომლებშიც ამ სიტყვებში განსხვავებული სიმბოლოები იყო.

შემდეგ ჩვენ შევნიშნეთ, რომ ასეთ დაშორებებთან, ანუ მანძილებთან მუშაობა ადვილდება, თუ რამენაირად განსაზღვრულია ვარიანტების ან კოდური სიტყვების გამოკლება: მაშინ ეს მანძილი იქნება იგივე, რაც სხვაობაში არანულოვან სიმბოლოთა რაოდენობა. ეს იგივეა, რაც მანძილი სხვაობიდან ისეთ სიტყვამდე, რომელიც სულ ნულებისგან შედგება.

ამრიგად, ჩვენ გვაინტერესებს კოდური სიტყვები, რომლებშიც რაც შეიძლება მეტი არანულოვანი სიმბოლოა. და ასეთი სიტყვების მოძიება გაადვილდება, თუ სხვაობის გარდა კიდევ განსაზღვრულია კოდური სიტყვის გამრავლება სიმბოლოთი წარმოდგენილ რიცხვზე. მართლაც, სიტყვის არანულოვან სიმბოლოზე გამრავლებისას ამ სიტყვაში არანულოვან სიმბოლოთა რაოდენობა არ მცირდება, თუ ორი არანულოვანი სიმბოლოს ნამრავლი არ უდრის ნულოვან სიმბოლოს.

როგორც ხედავთ, ჩვენ გვჭირდება სხვაობისა და სიმბოლოზე გამრავლების ოპერაციების გარკვეული თვისებები, რომელთა მოკლედ გამოთქმა ასე შეგვიძლია: სიმბოლოები უნდა ქმნიდნენ **ველს**, ხოლო კოდური სიტყვები უნდა ქმნიდნენ **ვექტორულ სივრცეს** ამ ველზე.

ველები

ამრიგად, წრფივი კოდისათვის ანბანი, ესე იგი სიმბოლოები, რომლებითაც შედგენილია კოდური სიტყვები, უნდა ქმნიდნენ ველს $\mathbb{F}$. უფრო ზუსტად, ეს ნიშნავს შემდეგს.

- ანბანში უნდა გვქონდეს სიმბოლოები 0 და 1
- ანბანის ყოველი ორი a და b სიმბოლოსათვის განსაზღვრული უნდა იყოს მათი ჯამი $a + b$, სხვაობა $a - b$ და ნამრავლი $a \cdot b$, რომლებიც აგრეთვე ანბანის სიმბოლოებია.
- მათთვის უნდა კმაყოფილდებოდეს არითმეტიკის „ჩვეულებრივი“ ტოლობები

$$\begin{gathered} a + 0 = a \\ a + b = b + a \\ (a + b) + c = a + (b + c) \\ (a - b) + b = a \\ a \cdot 1 = a \\ a \cdot b = b \cdot a \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ a \cdot (b + c) = a \cdot b + a \cdot c \end{gathered}$$

თუ ეს ყველაფერი სრულდება, ვიტყვით, რომ სიმბოლოები ქმნიან **რგოლს**.

- თუ გარდა ამისა, როდესაც $b \neq 0$ (ე. ი. b არ არის სიმბოლო 0), განსაზღვრულია განაყოფიც a/b, და

$$(a/b) \cdot b = a \quad (\text{როცა } b \neq 0)$$

მაშინ ვიტყვით, რომ სიმბოლოები ქმნიან **ველს**.

საკმარისია მოვითხოვოთ მხოლოდ $a^{-1} = 1/a$ განაყოფების არსებობა, დანარჩენი განაყოფები მათი საშუალებით განისაზღვრება (კითხვა: თუ ხვდებით, როგორ?)

როგორც ვთქვით, ველის მაგალითებს იძლევიან ნაშთები რომელიმე p მარტივ რიცხვზე გაყოფისას. ეს არის **მარტივი ველი** $\mathbb{F}_p$. ყველაზე პატარა მაგალითს იძლევა $p = 2$: ველში $\mathbb{F}_2$ გვაქვს სულ ორი ნაშთი, 0 და 1. ან, რაც იგივეა, ვაწარმოებთ „ჩვეულებრივ“ შეკრებას, გამოკლებას, გამრავლებას და გაყოფას, ოღონდ ვღებულობთ რამდენიმე „უჩვეულო“ შედეგს. მაგალითად, $1 + 1 = 0$ (რადგან ორი კენტი რიცხვის ჯამი ლუწია), $0 - 1 = 1$ (ლუწს გამოკლებული კენტი კენტია).

კითხვა 1.1: როდესაც $p = 23$ გვჭირდება ყველანაირი წილადები (განაყოფები) a/b სადაც b არ იყოფა 23-ზე. კერძოდ, 2/3 რისი ტოლი იქნება ამ შემთხვევაში?

მარტივი ველების გარდა ველების სხვა მაგალითებიც არსებობს.

მაგალითად, ყველა რაციონალური რიცხვის (წილადების) ერთობლიობა ველია, წილადების შეკრება-გამოკლებისა და გამრავლება-გაყოფის მიმართ. მაგრამ მარტივი ველებისგან განსხვავებით ეს ველი უსასრულოა.

არსებობს სასრული ველებიც, რომლებიც განსხვავებულია ყოველი $\mathbb{F}_p$ მარტივი ველისაგან. მაგალითად, ველში $\mathbb{F}_2$ არ არსებობს ისეთი ელემენტი a, რომ $a \cdot a = a + 1$. $\mathbb{F}_2$-ში სულ ორი ელემენტია, 0 და 1, და მარტივი შესამოწმებელია, რომ $0 = 0 \cdot 0 \neq 0 + 1 = 1$, ისევე როგორც $1 = 1 \cdot 1 \neq 1 + 1 = 0$. მაგრამ $\mathbb{F}_2$-ს შეგვიძლია დავუმატოთ ასეთი ახალი ელემენტი a. მივიღებთ ველს $\mathbb{F}_4$, რომელშიც 0-ისა და 1-ის გარდა გვექნება კიდევ a და $a + 1$. შევნიშნოთ, რომ ეს ველი შეიცავს $\mathbb{F}_2$-ს. ვინაიდან $\mathbb{F}_2$-ში სრულდება $1 + 1 = 0$, $\mathbb{F}_2$-ის შემცველ ნებისმიერ ველში ნებისმიერი a-სათვის გვექნება

$$a + a = a \cdot 1 + a \cdot 1 = a \cdot (1 + 1) = a \cdot 0 = 0$$

კითხვა 1.2: საიდან ვიცით, რომ $a \cdot 0 = 0$? ეს ტოლობა სინამდვილეში ნებისმიერ ველში სრულდება, შეგიძლიათ ახსნათ, რატომ?

$\mathbb{F}_4$-ში გამრავლების ბოლომდე გასარკვევად დაგვრჩა დავთვალოთ

$$a \cdot (a + 1) \text{ და } (a + 1) \cdot (a + 1),$$

რისთვისაც გამოვიყენებთ განრიგებადობის წესს $a \cdot (b + c) = a \cdot b + a \cdot c$ და მივიღებთ

$$a \cdot (a + 1) = a \cdot a + a \cdot 1 = (a + 1) + a = (1 + a) + a = 1 + (a + a) = 1 + 0 = 1$$

და

$$(a+1)\cdot(a+1) = a\cdot(a+1) + 1\cdot(a+1) = 1 + (a+1) = 1 + (1+a) = (1+1) + a = 0 + a = a$$

დაგვრჩა გაყოფა. 1-ზე გაყოფა ისევე ხდება, როგორც $\mathbb{F}_2$-ში. ხოლო ვინაიდან $a\cdot(a+1) = 1$, a-ზე გაყოფა იგივეა, რაც $(a+1)$-ზე გამრავლება, ხოლო $(a+1)$-ზე გაყოფა იგივე, რაც a-ზე გამრავლება.

კითხვა 1.3: გამოკლება რატომ გამოვტოვეთ?

კითხვა 1.4: რატომ არაა $\mathbb{F}_4$ მარტივი?

შეგახსენებთ, რომ ელემენტი a **ნულის გამყოფია**, თუ არსებობს არანულოვანი ელემენტი b, ისეთი რომ $a\cdot b = 0$. მოდით დავამტკიცოთ, რომ ველში ვერ იქნება ნულის გამყოფები. მართლაც დავუშვათ $a\cdot b = 0$ და $a \neq 0$. მაშინ $b = a^{-1}\cdot a\cdot b = a^{-1}\cdot 0 = 0$. რაც გვაჩვენებს, რომ მაშინ b ვერ იქნება არანულოვანი.

კითხვა 1.5: სწორია თუ არა, რომ პირიქითაც, თუ რგოლში არაა ნულის გამყოფები, მაშინ ის ველია? თურმე ეს მართლაც ასეა სასრული რგოლებისთვის, მაგრამ აღარაა სწორი უსასრულოებისთვის. შეგიძლიათ ახსნათ, რატომ?

ჩვენ უკვე ვნახეთ მარტივი სასრული ველები $\mathbb{F}_p$ და ერთი არამარტივი სასრული ველი $\mathbb{F}_4$. ზოგადად რამდენი ელემენტი შეიძლება იყოს სასრულ ველში? ამ შეკითხვაზე პასუხს ცოტა მოგვიანებით გავიგებთ.

თუ $\mathbb{F}_q$ არის q -ელემენტიანი სასრული ველი, მაშინ ელემენტები $0, 1, (1+1), (1+1+1)$, და ასე შემდეგ ყველა ეკუთვნის $\mathbb{F}_q$-ს. ასევე შევნიშნოთ, რომ რადგან $\mathbb{F}_q$ სასრულია, ამ მიმდევრობაში უნდა შეგვხვდეს ორი ერთნაირი ელემენტი. რადგან მათი სხვაობა ნული იქნება, მივიღებთ, რომ რაღაც ნატურალური რიცხვისთვის $p \in \mathbb{N}$ უნდა შესრულდეს $\underbrace{1+\cdots+1}_{p-ჯერ} = 0$.

ვთქვათ $\mathbb{F}$ რამე ველია. ისეთ უმცირეს რიცხვს $p \in \mathbb{N}$ რომლისთვისაც სრულდება $\underbrace{1+\cdots+1}_{p-ჯერ} = 0$ ეწოდება $\mathbb{F}$ **ველის მახასიათებელი**.

როგორი შეიძლება იყოს სასრული ველის მახასიათებელი? თურმე ნებისმიერი სასრული ველის მახასიათებელი p არის მარტივი რიცხვი. მართლაც, ვთქვათ არსებობს სასრული ველი $\mathbb{F}_q$ მახასიათებლით $p = p_1\cdot p_2$, მაშინ

$$\underbrace{1+\cdots+1}_{p-ჯერ} = 0 = (\underbrace{1+\cdots+1}_{p_1-ჯერ})(\underbrace{1+\cdots+1}_{p_2-ჯერ})$$

რადგან ველში არ გვაქვს ნულის გამყოფები და p უმცირესია ისეთ k-ებს შორის, რომლებისთვისაც $\underbrace{1+\cdots+1}_{k-ჯერ} = 0$ ამიტომ $p = p_1$ ან $p = p_2$.

გამოდის, რომ რა სასრული ველი $\mathbb{F}_q$-ც არ უნდა ავიღოთ რომელშიც q ცალი ელემენტია და რომლის მახასიათებელია p შესრულდება შემდეგი:

$$\{0,1,\dots,\underbrace{1+\cdots+1}_{(p-1)-\text{ჯერ}}\}=\mathbb{F}_p\subseteq\mathbb{F}_q$$

ზემოთ უკვე მოვიყვანეთ 4-ელემენტიანი ველის, $\mathbb{F}_4$-ს მაგალითი; მოდით კიდევ ავაგოთ სასრული ველები, რომლებიც არ იქნებიან ჩვენს მიერ აქამდე ნანახი სასრული ველების, $\mathbb{F}_p$-ების ტიპის, სადაც p მარტივი რიცხვია.

განვიხილოთ ჩვენი კარგი ნაცნობი, სამელემენტიანი სასრული ველი.

$$\mathbb{F}_3=\{0,1,2\}.$$

დავთვალოთ მისი ელემენტების კვადრატები;

$$0\cdot 0=0(\mathbf{mod}\ 3),\qquad 1\cdot 1=1(\mathbf{mod}\ 3),\qquad 2\cdot 2=1(\mathbf{mod}\ 3).$$

აღმოჩნდა, რომ $\mathbb{F}_3$-ში არ არსებობს $\sqrt{2}$ (არცერთი ელემენტის კვადრატი არ უდრის 2-ს).

უფრო ზოგადად, განვიხილოთ რამე მარტივი რიცხვი p და შესაბამისი ველი $\mathbb{F}_p$. ავირჩიოთ რამე ელემენტი $a\in\mathbb{F}_p$ რომელიც არ არის არცერთი ელემენტის კვადრატი, სხვა სიტყვებით, ისეთი, რომ $\mathbb{F}_p$-ში არ არსებობს $\sqrt{a}$. განვმარტოთ ახალი სიმრავლე, $\mathbb{F}_p(\sqrt{a})$, რომლის ელემენტებია $x+y\sqrt{a}$ სახის გამოსახულებები, სადაც x და y არიან $\mathbb{F}_p$-ს ნებისმიერი ელემენტები.

შეკრება და გამრავლება განვმარტოთ შემდეგნაირად:

$$(x_1+y_1\sqrt{a})+(x_2+y_2\sqrt{a})=(x_1+x_2)+(y_1+y_2)\sqrt{a}$$

$$(x_1+y_1\sqrt{a})\cdot(x_2+y_2\sqrt{a})=(x_1x_2+ay_1y_2)+(x_1y_2+x_2y_1)\sqrt{a}$$

სადაც x_1,x_2,y_1,y_2 კოეფიციენტების შეკრებასა და გამრავლებას ვასრულებთ მოდულით p.

<u>კითხვა 1.6:</u> როგორ დავრწმუნდეთ, რომ ასეთნაირად მიიღება ველი, და რომ მისი ელემენტების რაოდენობა უდრის p^2-ს?

ველებში $\mathbb{F}_7$ და $\mathbb{F}_{11}$ არ არსებობს $\sqrt{-1}$ (რომელიც პირველ შემთხვევაში იგივეა რაც $\sqrt{6}$ და მეორე შემთხვევაში იგივეა რაც $\sqrt{10}$), <u>დარწმუნდით ამაში</u> შემოწმების გზით ან გამოიყენეთ ამოცანა 6. შესაბამისად ველებს $\mathbb{F}_7(\sqrt{-1})$ და $\mathbb{F}_{11}(\sqrt{-1})$ აქვთ $7^2=49$ და $11^2=121$ ელემენტი. თუმცა მაგალითად $\mathbb{F}_5$-თვის $\sqrt{-1}$-ის დამატებით ვერ მივიღებთ $5^2=25$ ელემენტიან ველს, რადგან $\sqrt{-1}\in\mathbb{F}_5$.

<u>კითხვა 1.7:</u> მაინც რომ ჩავატაროთ აღწერილი აგება $x+y\sqrt{-1}$ სახის გამოსახულებებით, რაღაცას კი მივიღებთ, და რატომ არ გამოდგება?

ველებში $\mathbb{F}_5$ და $\mathbb{F}_{13}$ არ არის $\sqrt{2}$ – ეს ჩვენ ერთ-ერთ წინა კითხვაზე პასუხში დავადგინეთ. შესაბამისად ველებს $\mathbb{F}_5(\sqrt{2})$ და $\mathbb{F}_{13}(\sqrt{2})$ აქვთ $5^2=25$ და $13^2=169$ ელემენტი.

ვთქვათ, ველში $\mathbb{F}$ არ არსებობს არც $\sqrt{a}$ და არც $\sqrt{b}$, მისი რომელიღაც ორი a და b ელემენტებისათვის. მაშინ მივიღებთ ორ სხვადასხვა ველს $\mathbb{F}(\sqrt{a})$ და $\mathbb{F}(\sqrt{b})$. თურმე ეს ველები „მართლა სხვადასხვა“ შეიძლება იყოს მხოლოდ თუ $\mathbb{F}$ უსასრულოა. უფრო ზუსტად ეს ნიშნავს იმას, რომ თუ $\mathbb{F}$ სასრულია, მაშინ $\mathbb{F}(\sqrt{a})$-ში ყოველთვის გვექნება $x^2 = b$ განტოლების ამონახსნი, ხოლო $\mathbb{F}(\sqrt{b})$-ში კი $x^2 = a$ განტოლების ამონახსნი.

<u>კითხვა 1.8:</u> მაგალითად, $\mathbb{F}_{11}$-ში არ არსებობს $\sqrt{n}$, თუ $n = 2, 6, 7, 8$ ან 10. მაგრამ თუ $\mathbb{F}_{11}$-ს რომელიმე ამ ფესვს მივუერთებთ, ყველა დანარჩენი ფესვიც გაჩნდება. რას უდრის, მაგალითად, $\mathbb{F}_{11}(\sqrt{6})$-ში $x^2 = n$ განტოლების ამონახსნი, სადაც $n = 2, 7, 8$ ან 10? შეგიძლიათ დაამტკიცოთ, რომ იგივე ხდება ნებისმიერ მარტივ ველში? სხვანაირად რომ ვთქვათ, ავიღოთ რაიმე მარტივი რიცხვი p და ისეთი ნატურალური რიცხვი a, რომ $x^2 = a$ განტოლებას არ გააჩნია ამონახსნი $\mathbb{F}_p$ ველში. მაშინ თითოეული ნატურალური b-სათვის განტოლებას $x^2 = b$ ექნება ამონახსნი ველში $\mathbb{F}_p(\sqrt{a})$.

ამავე დროს, $\mathbb{F}_p(\sqrt{a})$-ში გაჩნდება ახალი ელემენტები, რომლებსაც შეიძლება გააჩნდეთ კვადრატული ფესვები და შეიძლება არა. მაგალითად, შეგიძლიათ დაასახელოთ ელემენტი $\mathbb{F}_{11}(\sqrt{6})$-ში, რომელსაც კვადრატული ფესვი $\mathbb{F}_{11}(\sqrt{6})$-შივე არ გააჩნია?

წრფივი კოდები და ვექტორული სივრცეები

სასრული ველები გამოიყენება განსაკუთრებით მოხერხებული კოდების ასაგებად. ასეთი კოდების ანბანი სასრული ველია, ასე რომ განსაზღვრულია კოდური სიტყვების შეკრება, გამოკლება და ანბანის სიმბოლოზე გამრავლება. ეს გვაძლევს საშუალებას ორი კოდური სიტყვის ერთმანეთთან შედარება გავაადვილოთ, რადგან ის, რაც გვაინტერესებს ამ შედარების შესახებ, შეგვიძლია გავარკვიოთ ამ კოდური სიტყვების სხვაობის შესწავლით. კერძოდ, ჩვენ გვინდა ხოლმე, რომ დაშორება რაც შეიძლება დიდი იყოს, და ეს ნიშნავს, რომ სხვაობაში რაც შეიძლება ცოტა ნულები გვხვდებოდეს.

ანბანის სიმბოლოზე გამრავლებაც ჩვენთვის მსგავსი მიზეზითაა სასარგებლო. ზოგად კოდში ახალი კოდური სიტყვების ჩამატება ისე, რომ დაშორება არ „გავაფუჭოთ“ (ე. ი. არ შევამციროთ) საკმაოდ რთულია. მაგრამ თუ ჩვენი კოდური სიტყვები ველის ელემენტებისგან შედგება, სიტყვის თითოეული სიმბოლოს ველის ერთსა და იმავე არანულოვან ელემენტზე გამრავლება ამ სიტყვაში ნულების რაოდენობას არ გაგვიზრდის, რაც მოგვცემს გარანტიას, რომ ასეთი გამრავლებით მიღებული სიტყვის დამატება კოდს არ გაგვიუარესებს.

<u>კოდი</u> რაიმე $\mathbb{F}$ ველზე შედგება ერთი და იმავე სიგრძის კოდური სიტყვებისაგან, რომლებისთვისაც ანბანია $\mathbb{F}$-ის ელემენტები.

ასეთი კოდი <u>წრფივია</u>, თუ

- ნებისმიერი კოდური სიტყვებისათვის $(a_1, \dots, a_n)$ და $(b_1, \dots, b_n)$ მათი სხვაობა
$$(a_1 - b_1, \dots, a_n - b_n)$$
აგრეთვე კოდური სიტყვაა

და ასევე,

- ნებისმიერი a-სათვის $\mathbb{F}$-იდან და ნებისმიერი კოდური სიტყვისათვის $(a_1, \dots, a_n)$ ამ სიტყვის a-ზე ნამრავლი $(a \cdot a_1, \dots, a \cdot a_n)$ აგრეთვე კოდური სიტყვა უნდა იყოს.

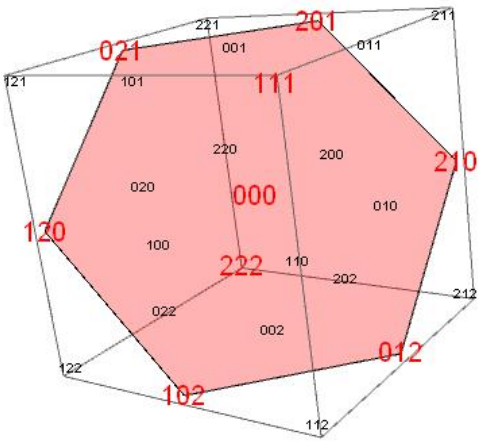
მაგალითად, შეგვიძლია ავიღოთ ერთი და იმავე n სიგრძის ყველა შესაძლო კოდური სიტყვა $(a_1, \dots, a_n)$. გასაგებია, რომ ეს წრფივი კოდია, მაგრამ ჩვენი თვალსაზრისით ის ნაკლებად საინტერესოა, რადგან ამ კოდის დაშორება ძალიან მცირეა, ის უდრის ერთს. მართლაც, გავიხსენოთ, რომ კოდის დაშორება არის განსხვავებულ კოდურ სიტყვათა დაშორებებს შორის უმცირესი. ამ შემთხვევაში კი, თუ ავიღებთ რაიმე კოდურ სიტყვას და მასში მხოლოდ ერთ სიმბოლოს შევცვლით ნებისმიერი სხვა სიმბოლოთი, კვლავ კოდურ სიტყვას მივიღებთ, რომლის თავდაპირველი სიტყვისგან დაშორება ერთის ტოლია (ისინი მხოლოდ ერთ პოზიციაში განსხვავდებიან ერთმანეთისგან).

ჩვენთვის უფრო საინტერესო წრფივი კოდების ძებნა შეიძლება სხვადასხვა, მათ შორის გეომეტრიული მოსაზრებებით.

მაგალითად, სივრცეში კოორდინატთა სათავეზე რომ გავატაროთ სიბრტყე, რომელიც საკოორდინატო ღერძებს მხოლოდ სათავეში კვეთს, მაშინ 3-ზე გაყოფისას ნაშთებზე გადასვლით ეს მოგვაძებნინებს წრფივ კოდს, რომლის არანულოვან სიტყვებშიც 0 გვხვდება არაუმეტეს ერთხელ:

012, 021, 102, 201, 120, 210, 111, 222, 000

აქ ჩვენ ვისარგებლეთ იმით, რომ 3-ზე გაყოფისას ნაშთი 2 იქცევა როგორც -1, რადგან ნაშთი $1 + 2$ არის 0:



ამ კოდში ნებისმიერი ორი სიტყვა არცერთ ან მხოლოდ ერთ პოზიციაში ემთხვევა ერთმანეთს. ასეთნაირად მივიღებთ წრფივ კოდს $\mathbb{F}_3$ ველზე, დაშორებით 2.

წრფივ კოდებში მანძილები და დაშორებები გამოისახება წონებით. $x = (a_1, \dots, a_n)$ კოდური სიტყვის **წონა** $w(x)$ არის მასში არანულოვანი პოზიციების რაოდენობა. C **კოდის წონა** $w(C)$ არის მასში შემავალი არანულოვანი სიტყვების წონებს შორის უმცირესი.

იმისთვის, რომ დავინახოთ კოდის წონის უპირატესობა კოდის დაშორებასთან მიმართებაში, განვიხილოთ შემდეგი მაგალითი. ავიღოთ შემდეგი კოდი C რომელიც შედგება თექვსმეტი ცალი 7-სიმბოლოიანი კოდური სიტყვისგან

(0000000)	(0001111)	(0010101)	(0011010)
(0100110)	(0101001)	(0110011)	(0111100)
(1000011)	(1001100)	(1010110)	(1011001)
(1100101)	(1101010)	(1110000)	(1111111)

იმის შემოწმება, რომ ეს კოდი წრფივია ორობითი კომპონენტობრივი შეკრების და გამრავლების მიმართ მარტივია, მაგრამ ძალიან მოსაწყენი. ეს კოდი აღმოაჩენს შეცდომის არსებობას და სწორად გაასწორებს მას, თუ შეცდომა მოხდა მხოლოდ ერთ სიმბოლოზე, და ამის დასანახად გამოგვადგებოდა $d(C)$-ს დათვლა. მაგრამ $d(C)$-ის დასადგენად გვჭირდება ყველა შესაძლო მანძილის დათვლა, რაც საკმაოდ შრომატევადი პროცესია (გამოსათვლელია $16 \cdot 15$ შემთხვევა). გაცილებით მარტივია დავრწმუნდეთ, რომ კოდში შემავალი კოდური სიტყვების მინიმალური წონა უდრის 3-ს.

შევნიშნოთ, რომ თუ x და y არიან წრფივი კოდის კოდური სიტყვები მაშინ $w(x-y) = d(x,y)$. მართლაც, სხვაობაში ნულები ზუსტად იმ პოზიციებში დაჯდება, სადაც x-სა და y-ს ერთნაირი სიმბოლოები აქვთ.

თუ კოდი C წრფივია, მაშინ მისი დაშორება უდრის მის წონას, $d(C) = w(C)$.

<u>კითხვა 1.9</u>: რატომ არის სწორი, რომ თუ კოდი C წრფივია, მაშინ მისი დაშორება უდრის მის წონას, $d(C) = w(C)$?

ვექტორული სივრცეები

როგორც ვთქვით, ჩვენთვის საინტერესოა ისეთი კოდები, რომელთა ანბანი ქმნის სასრულ ველს, ხოლო კოდური სიტყვების სხვაობები ან ველის ელემენტზე ნამრავლები კვლავ კოდური სიტყვებია. ამ თვისებების მქონე სიმრავლეებს ამ ველზე ვექტორული სივრცეები ეწოდებათ.

$\mathbb{F}$ ველზე <u>**ვექტორული სივრცე**</u> V შედგება ელემენტებისგან x, y, ... რომელთა შორისაც არის გამოყოფილი ნულოვანი ელემენტი 0 და რომლებისთვისაც განსაზღვრულია შეკრება, გამოკლება და $\mathbb{F}$ ველის ელემენტებზე გამრავლება. ეს ნიშნავს, რომ V-ს ყოველი ორი ელემენტისათვის x, y განსაზღვრულია V-სავე ელემენტები $x+y$ და $x-y$; გარდა ამისა, $\mathbb{F}$-ის ყოველი ელემენტისათვის a და V-ს ყოველი ელემენტისათვის x განსაზღვრულია V-ს ელემენტი ax. ამასთან, უნდა სრულდებოდეს შემდეგი ტოლობები:

$$\begin{aligned} x+0 &= x \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \\ (x-y)+y &= x \\ a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ (a\cdot b)x &= a(bx) \\ 1x &= x \end{aligned}$$

აქ x, y, z არიან ნებისმიერი ელემენტები V ვექტორული სივრციდან, ხოლო a, b არიან ნებისმიერი ელემენტები $\mathbb{F}$ ველიდან. (**შენიშვნა**: არ უნდა დაგაბნიოთ ვექტორული სივრცის ნულოვანი ელემენტის აღნიშვნის, 0-ის და ველის ნულოვანი ელემენტის აღნიშვნის 0-ის ერთნაირობამ).

მაგალითი 1: ვექტორული სივრცის მაგალითს წარმოადგენს სიბრტყე ან სივრცე დეკარტული კოორდინატებით. როგორც გახსოვთ სიბრტყის ყოველ წერტილს x შეესაბამება ნამდვილი რიცხვების წყვილი $\vec{x} = (x_1, x_2)$. ასეთი წყვილების შეკრება ხდება კომპონენტობრივად

$$\vec{x} + \vec{y} = (x_1, x_2) + (y_1, y_2) = (x_1 + x_2, y_1 + y_2).$$

ასევე შეგვიძლია წყვილის რიცხვზე გამრავლება $a\vec{x} = a(x_1, x_2) = (ax_1, ax_2)$.

მაგალითი 2: ვექტორული სივრცის კიდევ ერთი მაგალითია სივრცეში კოორდინატთა სათავეზე გამავალი ნებისმიერი სიბრტყე. მაგალითად, ავიღოთ ყველა ისეთი სამეული (x, y, z), რომ $x + y + z = 0$. გასაგებია, რომ თუ $x + y + z = 0$ და $x' + y' + z' = 0$, მაშინ $(x - x') + (y - y') + (z - z') = 0$, ასე რომ თუ (x, y, z) და (x', y', z') ჩვენს სიბრტყეშია, მაშინ $(x, y, z) - (x', y', z') = (x - x', y - y', z - z')$ აგრეთვე ჩვენს სიბრტყეშია. ასევე, თუ $x + y + z = 0$, მაშინ $tx + ty + tz = 0$, ამიტომ თუ (x, y, z) ჩვენს სიბრტყეშია, მაშინ $t(x, y, z) = (tx, ty, tz)$ აგრეთვე ჩვენს სიბრტყეშია.

ორივე ამ მაგალითში განხილული ვექტორული სივრცეები უსასრულო ვექტორული სივრცეებია. ჩვენ კი დაგვჭირდება მხოლოდ სასრული ვექტორული სივრცეები.

მაგალითი 3: ჩვენ ვნახეთ, რომ ყოველი სასრული ველი $\mathbb{F}_q$ შეიცავს მარტივ ველს $\mathbb{F}_p \subseteq \mathbb{F}_q$, რომელიც შედგება 1-ის ყველანაირი ჯერადებისგან $\{0, 1, 1 + 1, \dots\}$. უფრო მეტიც, $\mathbb{F}_p$ არის ქვეველი $\mathbb{F}_q$-ში, რაც ნიშნავს, რომ $\mathbb{F}_p$-ს ელემენტების შეკრება, გამოკლება, გამრავლება თუ გაყოფა ჩატარებული $\mathbb{F}_q$-ში არ გაგვიყვანს $\mathbb{F}_p$-ს გარეთ. ეს გვაძლევს ვექტორული სივრცის მაგალითს: $\mathbb{F}_q$ თავისი შეკრება-გამოკლებითა და $\mathbb{F}_p$-ს ელემენტებზე გამრავლებით იქცევა ვექტორულ სივრცედ $\mathbb{F}_p$-ზე. ცხადია, უფრო ზოგადად, თუ გვაქვს რაიმე ველი $\mathbb{F}$ და მასში ნებისმიერი ქვეველი $\mathbb{F}' \subseteq \mathbb{F}$, მაშინ $\mathbb{F}$ არის ვექტორული სივრცე $\mathbb{F}'$-ზე.

კითხვა 1.10: მოიყვანეთ მაგალითი ისეთი $\mathbb{F}$ ველისა და ისეთი ქვეველისა $\mathbb{F}' \subseteq \mathbb{F}$, რომ $\mathbb{F}'$ არც მარტივია და არც $\mathbb{F}$ ველს არ ემთხვევა.

ვიტყვით, რომ სასრული რაოდენობის ვექტორების ერთობლიობა $\{x_1, x_2, \dots, x_k\}$, **წრფივად დამოუკიდებელია**, თუ $a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$ სრულდება მხოლოდ იმ შემთხვევაში როდესაც $a_1 = a_2 = \cdots = a_k = 0$.

ვექტორი x **გამოისახება** ვექტორებით $x_1, x_2, \dots x_k$ თუ $x = a_1x_1 + a_2x_2 + \cdots + a_kx_k$ სადაც $a_1, a_2, \dots, a_k$ რამე ელემენტებია ველიდან. ვექტორების წრფივად დამოუკიდებლობა გვაჩვენებს რომ ამ სიმრავლეში შემავალი ვექტორები არ გამოისახებიან ერთმანეთის საშუალებით.

სასრული ვექტორული სივრცის ქვესიმრავლეს B დავუძახოთ **ბაზისი**, თუ ეს ქვესიმრავლე წრფივად დამოუკიდებელია და ნებისმიერი სხვა ვექტორის ამ სიმრავლეში ჩამატებით ერთი მაინც ვექტორი გახდება **წრფივად დამოკიდებული** სხვებზე, ანუ გამოისახება სხვების საშუალებით.

მარტივი დასანახია, რომ სასრულ ვექტორულ სივრცეს გააჩნია ბაზისი. ვიმსჯელოთ შემდეგნაირად: ავიღოთ ნებისმიერი არანულოვანი ვექტორი x_1და შევადგინოთ სიმრავლე $B_1 = \{x_1\}$. განვიხილოთ ყველა ვექტორი რომელიც არ უდრის x_1-ს, ასეთების რაოდენობა სასრულია. თუ რომელიმე ვექტორის x_2-ის ჩამატებით B_1-ში ის დარჩება წრფივად დამოუკიდებელი, ჩავამატოთ ის B_1-ში, ანუ შევადგინოთ ახალი სიმრავლე $B_2 = \{x_1, x_2\}$. ასე გავაგრძელოთ სანამ რომელიღაც სასრულ k-ურ

ნაბიჯზე B_k-ში ახალი ელემენტის დამატება, ისე რომ ახალი სიმრავლე წრფივად დამოუკიდებელი დარჩეს, შეუძლებელი არ გახდება. რადგან ელემენტების რაოდენობა სასრულია, ეს მომენტი რომელიღაც სასრულ ნაბიჯზე დადგება. და მიღებული სიმრავლე იქნება ბაზისი. ასევე გასაგები უნდა იყოს, რომ ბაზისი შეიძლება არ იყოს ერთადერთი.

კითხვა 1.11: შეგიძლიათ მოიფიქროთ სასრული ვექტორული სივრცის მარტივი მაგალითი და აჩვენოთ, რომ მას აქვს ერთზე მეტი ბაზისი?

კითხვა 1.12: დაამტკიცეთ, რომ სასრული ვექტორული სივრცის ნებისმიერ ბაზისში იქნება ელემენტების ერთი და იგივე რაოდენობა.

კითხვა 1.13: დაასახელეთ მაგალით 2-ში მოყვანილი ვექტორული სივრცის რაიმე ბაზისი.

თუ $B = \{v_1, v_2, \dots, v_k\}$ არის V სასრული ვექტორული სივრცის ბაზისი, მაშინ V-ს ნებისმიერი ელემენტი x ერთადერთნაირად ჩაიწერება როგორც $x = a_1v_1 + a_2v_2 + \cdots + a_kv_k$.

კითხვა 1.14: დაამტკიცეთ, რომ ეს მართლაც ასეა.

ასეთ დროს ხანდახან ამბობენ, რომ ამ კერძო ბაზისში x-ის კოორდინატებია კოეფიციენტები $a_1, a_2, \dots, a_k$. გაიხსენეთ, რომ სიბრტყის ან სივრცის წერტილის დეკარტული კოორდინატები ზუსტად ასე განიმარტება. სიბრტყის სტანდარტული ბაზისი შედგება ორი ვექტორისგან ესენია $(1,0)$ და $(0,1)$, შესაბამისად ნებისმიერი ვექტორი $\vec{x} = (x_1, x_2) = x_1(1,0) + x_2(0,1)$.

ამ ნაწილის ბოლოს კი დავამტკიცოთ, რომ სასრულ ველში შეიძლება იყოს მხოლოდ p^k ელემენტი, სადაც p არის ველის მახასიათებელი მარტივი რიცხვი და k რაღაც ნატურალური რიცხვია.

ვთქვათ $\mathbb{F}_q$ არის q ელემენტისგან შედგენილი სასრული ველი რომლის მახასიათებელია p. გაიხსენეთ, რომ ველის მახასიათებელი მარტივი რიცხვია და ისიც, რომ $\mathbb{F}_p \subseteq \mathbb{F}_q$. ერთ-ერთ მაგალითში ჩვენ ვნახეთ, რომ მაშინ $\mathbb{F}_q$ იქნება ვექტორული სივრცე $\mathbb{F}_p$-ზე.

რადგან ახლა $\mathbb{F}_q$ არის სასრული ვექტორული სივრცე, მას გააჩნია ბაზისი. ავიღოთ მისი ნებისმიერი ბაზისი $B = \{v_1, v_2, \dots v_k\}$. $\mathbb{F}_q$-ს ნებისმიერი ელემენტი ერთადერთნაირად ჩაიწერება შემდეგი სახით:

$$x = a_1v_1 + a_2v_2 + \cdots + a_kv_k.$$

შესაბამისად ყველა ვექტორის მიღება შეგვიძლია $a_1, a_2, \dots, a_k$ კოეფიციენტების ცვლის ხარჯზე. გვაქვს a_1-ის არჩევის p ვარიანტი (შეგვიძლია ავირჩიოთ $\mathbb{F}_p$-ს ნებისმიერი ელემენტი); იგივე რაოდენობის არჩევანი გვაქვს სხვა a_i-ებისთვის. კოეფიციენტების როლში $\mathbb{F}_p$ ველის ელემენტების ყველა შესაძლო ჩასმის შედეგად სულ მიიღება ზუსტად p^k ცალი ელემენტი, ამიტომ $q = p^k$.

ამ თემის მომდევნო ნაწილში უფრო აქტიურად შევუდგებით სასრული ველების და სასრულ ველებზე წრფივი სივრცეების გამოყენებას „კარგი“ წრფივი კოდების შესასწავლად.

დამატებითი ამოცანები

გთავაზობთ ამ ნაწილში განხილულ მასალას შეხედოთ, როგორც თავსატეხს, კვესტს. ჩვენი მიზანია ისე გავერკვეთ მასში, რომ შევძლოთ ამოვხსნათ ეს თავსატეხი, დავხუროთ კვესტი. მისი დახურვა არ ნიშნავს ყველაფრის დამთავრებას. ეს მხოლოდ ერთი კვესტია, ასეთი ათასობით ათასია.

ამოცანა 1. მოძებნეთ $4x = 1$ განტოლების ამონახსნი ველში $\mathbb{F}_{101}$.

ამოცანა 2. ჯერ $\mathbb{F}_3$-ში ხოლო შემდეგ $\mathbb{F}_5$-ში ამოხსენით განტოლებათა სისტემა.

$$\begin{cases} x + 2z = 1 \\ y + 2z = 2 \\ 2x + z = 1 \end{cases}$$

ამოცანა 3. ჯერ $\mathbb{F}_5$-ში ხოლო შემდეგ $\mathbb{F}_7$-ში ამოხსენით განტოლებათა სისტემა.

$$\begin{cases} 3x + y + 2z = 1 \\ x + 2y + 3z = 1 \\ 4x + 3y + 2z = 1 \end{cases}$$

ამოცანა 4. ვთქვათ p მარტივი რიცხვია. $\mathbb{F}_p$-ს ელემენტს a დავარქვათ კვადრატული თუ არსებობს $\mathbb{F}_p$-ს ისეთი ელემენტი r რომ სრულდება $r^2 = a$, წინააღმდეგ შემთხვევაში, ე. ი. თუ ასეთი r არ არსებობს, მაშინ a-ს დავუძახოთ არაკვადრატული. რა უფრო მეტია, კვადრატული ელემენტები თუ არაკვადრატული ელემენტები? შეიძლება მოხდეს, რომ ყველა ელემენტი იყოს კვადრატული?

ამოცანა 5. ვთქვათ p მარტივი რიცხვია. დაამტკიცეთ, რომ $(p-1)! \equiv -1 (\mathbf{mod}\ p)$.
აქ $n!$ აღნიშნავს n რიცხვის ფაქტორიალს, ანუ $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$

ამოცანა 6. ვთქვათ p მარტივი რიცხვია. დაამტკიცეთ, რომ $\mathbb{F}_p$-ს ელემენტი a კვადრატულია მაშინ და მხოლოდ მაშინ, როდესაც

$$a^{\frac{p-1}{2}} = 1 \ (\mathbf{mod}\ p).$$

ამოცანა 7. ვთქვათ ველში სრულდება რომ $5 = 21$. სწორია თუ არა, რომ იმავე ველში სრულდება $7 = 15$?

ამოცანა 8. რამდენი ამონახსნი აქვს განტოლებას $x^2 = a$ ველში, სადაც 2^n ელემენტია?

ამოცანა 9. არსებობს თუ არა ველი, რომელშიც არის 2 ელემენტი? 3? 4? 5? 6? 7? 8? 9? 10?