კოდები, ტესტები, განლაგებები... - გაგრძელება

გვაქვს ასეთი გეგმა: ჯერ გვინდა ავაგოთ რიცხვების მაგვარი სისტემა, რომელშიც გვექნება ყველა ჩვეულებრივი მოქმედება -- შეკრება, გამოკლება, გამრავლება, გაყოფა, რომლებსაც ყველა ჩვეულებრივი თვისება ექნება. შემდეგ ამ რიცხვების საშუალებით ავაგებთ სივრცეებს, რომლებშიც გვექნება მანძილის მაგვარი რამ. ბოლოს, ამ სივრცეებში ავაგებთ კარგ კოდებს -- წერტილების ისეთ განლაგებებს, რომ ამ მანძილის აზრით სივრცის მოცემულ „ყუთში“ რაც შეიძლება მეტი წერტილი ჩაეტიოს და თან ამ წერტილებს შორის მანძილები რაც შეიძლება დიდი იყოს.

ველები

ჩვენი „ახალი“ რიცხვების მთავარი თავისებურება იქნება ის, რომ მათი რაოდენობა იქნება სასრული. ეს პირველი შეხედვით შეუძლებელია: როგორც კი გვაქვს რიცხვი 1 და შეკრება, ეგრევე რიცხვების უსასრულო რაოდენობა გვიჩნდება -- $1+1$, $1+1+1$, $1+1+1+1$, ...

ასე რომ თუ გვინდა, რომ რიცხვების რაოდენობა სასრული იყოს, აუცილებლად უნდა მოხდეს შემდეგი რამ: რომ დავიწყოთ ერთიანით, დავუმატოთ მას ერთიანი, შემდეგ ნაბიჯზე კვლავ დავუმატოთ ერთიანი, და ასე ყოველ ჯერზე რასაც მივიღებთ იმას კვლავ ვუმატოთ ერთიანი, ადრე თუ გვიან უნდა გამოგვივიდეს იგივე, რაც უკვე გვქონდა. სხვანაირად რომ ვთქვათ, გვექნება რომელიღაც m და n ნატურალური რიცხვებისთვის

$$\underbrace{1+1+\cdots+1}_{m} = \underbrace{1+1+\cdots+1}_{m+n}$$

(ერთიანს რომ თავის თავთან m-ჯერ შევკრებთ, იგივე უნდა გამოგვივიდეს, რაც მაგ ჯამს რომ კიდევ n-ჯერ დავუმატოთ ერთიანი).

გასაგებია, რომ თუ მიღებული ტოლობის ორივე მხარეს m-ჯერ გამოვაკლებთ ერთიანს, დავასკვნით, რომ სინამდვილეში n-ურ ნაბიჯზე მიგვიღია ნოლი:

$$0 = \underbrace{1+1+\cdots+1}_{n}$$

(ოღონდ გასაგებია, რომ ამისთვის შეკრების გარკვეული თვისებები გვჭირდება; ამ თვისებებს სულ მალე ჩამოვწერთ). ასე რომ, თუ ერთიანების მიმატებას გავაგრძელებთ, წრეზე წავალთ, აქამდე რაც გვქონდა, თავიდან გამეორდება. მაგალითად, თუ ყველაზე პატარა n, რომლისთვისაც ნოლი მივიღეთ, არის 6, გამოგვივა მიმდევრობა 0,1,2,3,4,5,0,1,2,3,4,5,0,1,2,3,...

ეს ერთი შეხედვით უცნაური ვითარება სინამდვილეში ძალიან ადვილი „მოსაწყობია“: სწორედ ასეთი რამ მოხდება, თუ ყველა რიცხვს შევცვლით n-ზე მისი გაყოფის ნაშთით. ნაშთები შეკრებისა და გამრავლების მიმართ მშვენივრად იქცევიან. მაგალითად, 6-ზე გაყოფისას ნაშთების შეკრების ცხრილი ასეთია:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

ხოლო გამრავლების ცხრილი ასეთი:

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

მიაქციეთ ყურადღება ერთ რამეს: „უფასოდ“ მივიღეთ უარყოფითი რიცხვები, იმიტომ რომ, მაგალითად, ჩვენი ახალი შეკრების აზრით $2+4=0$, ასე რომ 4 იგივეა, რაც -2.

აქვე მიაქციეთ ყურადღება კიდევ ერთ რამეს: წილადები ასე უფასოდ მაინც და მაინც ვერ მივიღეთ. მაგალითად, 1/5 კი გვაქვს, იმიტომ რომ გამოგვივიდა $5 \times 5 = 1$, რაც ნიშნავს, რომ 1/5=5. მაგრამ 1/2 არ გვაქვს, იმიტომ რომ 1/2-ს უნდა ჰქონდეს თვისება $(1/2) \times 2 = 1$, ჩვენთან კი 2-ზე რაც არ უნდა ვამრავლოთ, ვღებულობთ ან 0-ს, ან 2-ს ან 4-ს, ხოლო 1-ს ვერანაირად ვერ ვღებულობთ. არადა ნებისმიერ არანულოვან რიცხვზე გაყოფა დაგვჭირდება. თურმე ამის მიღწევაც შეიძლება, თუ აი იმ n-ს ჭკვიანურად შევარჩევთ.

დავუკვირდეთ, რამ გაგვიჩინა პრობლემა. რამ და გამრავლების ცხრილში „ზედმეტმა“ ნოლებმა. გასაგებია, რომ პირველ სტრიქონსა და პირველ სვეტში ნოლები უნდა ეწეროს, იმიტომ რომ ყოველი a რიცხვისთვის $a \times 0 = 0 \times a = 0$. მაგრამ ჩვენს გამრავლების ცხრილში სხვაგანაც ნოლები დგას. გასაგებია, რატომაც: 6-ს ხომ გამყოფები აქვს, მაგალითად, $2 \times 3 = 6$, რაც ნიშნავს, რომ ჩვენს გამრავლების ცხრილში $2 \times 3 = 0$.

ეხლა ნახეთ, ვთქვათ, რომელიმე a-სთვის $1/a$ მოიძებნება, ე. ი. რომელიღაც b-სთვის $a \times b = 1$. მაშინ როგორც კი რომელიმე c-სათვის $a \times c = 0$, ამ ტოლობის ორივე მხარე რომ გავამრავლოთ b-ზე, მივიღებთ, რომ $(a \times c) \times b = 0 \times b = 0$, არა და ამავე დროს

$$(a \times c) \times b = (c \times a) \times b = c \times (a \times b) = c \times 1 = c$$

ასე რომ გამოგვივიდა ასეთი რამ -- თუ $a \times b = 1$, მაშინ $a \times c = 0$ შეიძლება მოხდეს მხოლოდ იმ შემთხვევაში, თუ $c = 0$. დასკვნა: თუ გვინდა, რომ ყველა არანულოვანი a ნაშთისთვის მისი შებრუნებული $1/a$ არსებობდეს, ჩვენს n-ს გამყოფები არ უნდა გააჩნდეს.

გასაგებია, რომ თვითონ n და 1 კი ყოველთვის იქნებიან n-ის გამყოფები, იგულისხმება საკუთრივი გამყოფები, ე. ი. n-ისგან და 1-ისგან განსხვავებული გამყოფები. ანუ, n მარტივი რიცხვი უნდა იყოს.

მოდით მართლაც მოვსინჯოთ 6-ის მაგიერ 7 და ვნახოთ, რა გამოგვივა. შეკრება-გამრავლების ცხრილებს კვლავ იოლად შევადგენთ:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

და

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

წილადების საქმე აშკარად გამოსწორდა: გამრავლების ცხრილში ნოლები გვაქვს მხოლოდ პირველ სვეტსა და პირველ სტრიქონში. და მართლაც, ყველა დანარჩენ სტრიქონსა და სვეტში გაჩნდა თითო ერთიანი, ეს კი ნიშნავს, რომ 1/2, 1/3, 1/4, 1/5, 1/6 ყველა სახეზეა. მაგალითად, 1/4=2, იმიტომ რომ $4 \times 2 = 1$ (რვის ნაშთი 7-ზე გაყოფისას არის 1), ან, 1/3=5.

მოდით შევაჯამოთ რაც აქამდე ფაქტები დაგვიგროვდა. ვაფიქსირებთ რაიმე n ნატურალურ რიცხვს და ვიღებთ ნაშთებს n-ზე გაყოფისას (ამბობენ კიდევ ნაშთებს <u>მოდულით n</u>). მაშინ შეკრების, გამოკლების და გამრავლების საქმე კარგად გვაქვს, ოღონდ გაყოფა შეიძლება გაგვიფუჭდეს. იმისთვის, რომ გაყოფასთანაც არ გვქონდეს პრობლემები, აუცილებელია, რომ გამრავლების ცხრილში ნოლები შეგვხვდეს მხოლოდ პირველ სტრიქონსა და პირველ სვეტში, ანუ $a \times b = 0$ ხდებოდეს მხოლოდ იმ შემთხვევაში, თუ ან $a = 0$ ან $b = 0$ (ამბობენ კიდევ, რომ არ გვაქვს <u>ნულის გამყოფები</u>). ეს ნიშნავს ზუსტად იმას, რომ n იყოს მარტივი რიცხვი, ე. ი. თუ ab იყოფა n-ზე, ერთ-ერთი მათგანი უნდა იყოფოდეს n-ზე.

დავალება 1

მარტივ რიცხვებს უფრო ხშირად განსაზღვრავენ, როგორც ისეთ მთელ რიცხვებს, რომლებსაც არ გააჩნიათ სხვა გამყოფები თავისი თავისა და 1-ის გარდა. ჩვენ გამოგვადგა ასეთი განსაზღვრება: „რიცხვი p მარტივია“ ნიშნავს, რომ თუ ორი მთელი რიცხვის ნამრავლი ab იყოფა p-ზე, მაშინ ან a ან b უნდა გაიყოს p-ზე. აჩვენეთ, რომ მარტივი რიცხვის ეს ორი განსაზღვრება მართლაც ტოლფასია.

ბოლოს დავრწმუნდით, ოღონდ მხოლოდ ერთ მაგალითზე, როცა $n = 7$, რომ ეს აუცილებელი პირობა საკმარისიცაა. სახელდობრ, დავინახეთ, რომ 7-ზე გაყოფის ყოველ არანულოვან ნაშთს გააჩნია შებრუნებული გამრავლების მიმართ, ასე რომ გაყოფა მართლაც შესაძლებელია.

ჩვენ გვინდა იგივეში დავრწმუნდეთ ზოგადად, ნებისმიერი n-ისათვისაც, ოღონდ ამისთვის ზუსტად უნდა ჩამოვაყალიბოთ, რას ვგულისხმობთ. თქვენ ალბათ შეამჩნიეთ, რომ გზადაგზა შეკრებისა და გამრავლების რამდენიმე თვისება გამოვიყენეთ. სანამ გავაგრძელებთ, ყველა ეს თვისება უნდა ჩამოვწეროთ. საკმაოდ მოზრდილი სია გამოგვივა, მაგრამ რომ წაიკითხავთ, იმედია დამეთანხმებით, რომ ყველა ეს თვისება თქვენთვის კარგად ცნობილი და გასაგებია.

მაშ ასე, გვაქვს რაიმე ერთობლიობა A, რომლის ელემენტებსაც აღვნიშნავთ ლათინური ასოებით $a, b, c, \ldots$ და რომელზეც შეგიძლიათ იგულისხმოთ, რომ ის შედგება ყველა ნაშთებისაგან რაიმე ფიქსირებული მოდულით n, მაგრამ სინამდვილეში ბევრი სხვა მაგალითებიც გვექნება.

ვიტყვით, რომ A ქმნის რგოლს, თუ A-ს ელემენტებზე განსაზღვრული გვაქვს შეკრება და გამრავლება: ყოველი a-სა და b-სათვის A-დან განსაზღვრულია $a + b$ და $a \times b$, რომლებიც ასევე A-ს ეკუთვნიან, და კიდევ A-ში გვაქვს ორი გამორჩეული ელემენტი 0 და 1. ამასთან ყველა a, b, c-სათვის A-ში უნდა სრულდებოდეს ასეთი ტოლობები:

$$a + b = b + a$$
$$(a + b) + c = a + (b + c)$$
$$a + 0 = a$$
$$a \times b = b \times a$$
$$(a \times b) \times c = a \times (b \times c)$$
$$a \times 1 = a$$
$$a \times (b + c) = (a \times b) + (a \times c)$$

და კიდევ, ყოველი a-სათვის A-დან, A-შივე უნდა არსებობდეს ისეთი $-a$, რომ

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

ამ ბოლო პირობის წყალობით A-ში გვექნება გამოკლებაც: უბრალოდ ვწეროთ ხოლმე $a + (-b)$-ს ნაცვლად $a - b$.

დავალება 2

გამოკლების გამოყენებით ბოლო მოთხოვნილი ტოლობა $a + (-a) = 0$ იგივეა, რაც $a - a = 0$.

აჩვენეთ, რომ პირიქითაც, თუ A რგოლში $a - b = 0$, მაშინ $a = b$.

მინიშნება: ეს ერთი შეხედვით თავისთავად ცხადია, მაგრამ მსჯელობაში თქვენ შეგიძლიათ გამოიყენოთ მხოლოდ ის ტოლობები, რომლებიც აქამდე ჩამოვთვალეთ. რეალურად დაგჭირდებათ ამ ტოლობებიდან პირველი სამი ($a + b = b + a$, $(a + b) + c = a + (b + c)$ და $a + 0 = a$), თან რამდენიმეჯერ. მე გამომივიდა 6-ჯერ, საინტერესოა თქვენ რამდენჯერ დაგჭირდებათ ამ ტოლობების გამოყენება.

დავალება 3

აჩვენეთ, რომ A რგოლის ყოველი a ელემენტისათვის $-(-a) = a$.

დავალება 4

აჩვენეთ, რომ A რგოლის ნებისმიერი a, b, c ელემენტებისათვის $a \times (b - c) = a \times b - a \times c$.

დავალება 5 (ძალიან ადვილი)

ვთქვათ, A არის ყველა ნაშთები რაიმე n მოდულით. რატომ შესრულდება A-ში ბოლო პირობა $a + (-a) = 0$? რაიმე a ნაშთისათვის როგორ გამოვთვალოთ $-a$?

ვიტყვით, რომ A არის ველი, თუ ის არის რგოლი და კიდევ დამატებით 0-ის გარდა ყველა დანარჩენი a-სათვის A-დან A-შივე არსებობს ისეთი a^{-1}, რომ

$$a \times a^{-1} = 1$$

თუ ეს პირობაც სრულდება, გვექნება გაყოფაც: უბრალოდ გამოსახულებას $a \times b^{-1}$ დავარქვათ a/b.

დავალება 6 (ზომიერად ადვილი)

რატომ ვითხოვთ a^{-1}-ის არსებობას მხოლოდ არანულოვანი a-სათვის? რა მოხდება, დამატებით რომ მოვითხოვოთ ისეთი 0^{-1}-ის არსებობაც, რომ $0 \times 0^{-1} = 1$?

ჩვენ ვნახეთ, რომ როდესაც $n = 7$, ნაშთები მოდულით n მართლაც ქმნიან ველს: უბრალოდ შევხედეთ გამრავლების ცხრილს და დავრწმუნდით, რომ ყველა სტრიქონსა და სვეტში პირველების გარდა სადღაც გვიზის 1. ვნახოთ ახლა, რომ საზოგადოდ თუ $n = p$ ნებისმიერი მარტივი რიცხვია, მაშინაც ველს მივიღებთ. ეს ნიშნავს ასეთ რამეს: მოგვცეს რაიმე არანულოვანი ნაშთი a მოდულით p, ე. ი. უბრალოდ რაიმე მთელი რიცხვი, რომელსაც ვიხილავთ p-ს მიმატებამდე სიზუსტით. უნდა ვიპოვოთ მისთვის ისეთი a^{-1}, რომ $a \times a^{-1} = 1$.

ავიღოთ და უბრალოდ გადავსინჯოთ ყველა არანულოვანი ნაშთი 1,2,..., $p - 1$ რაც კი გვაქვს. ანუ, შევხედოთ a-ზე ყველა ნამრავლის ჩამონათვალს $a \times 1$, $a \times 2$, ..., $a \times (p - 1)$ იმ იმედით, ხომ არ არის მათ შორის 1. საკვანძო კითხვა აქ ასეთია: შეიძლება თუ არა ამ ჩამონათვალში რომელიმე ორი ნაშთი გამეორდეს? შეიძლება მოხდეს, რომ $a \times i = a \times j$?

თუ ასეთი რამ შეგვხვდა, მაშინ გვექნება $a \times i - a \times j = 0$, და თუ დავალება 4 გააკეთეთ, აქედან დაასკვნით, რომ $a \times (i - j) = 0$. მაგრამ ჩვენი p მარტივია, ასე რომ, რადგან ნაშთი a არანულოვანია, ნულოვანი უნდა იყოს ნაშთი $i - j$. ახლა თუ დავალება 2-შიც გაერკვიეთ, მიიღებთ, რომ $i = j$.

ამრიგად გამოგვივიდა, რომ ნაშთთა ჩამონათვალში $a \times 1$, $a \times 2$, ..., $a \times (p - 1)$ გამეორებები არა გვაქვს. თან არც 0 შეგვხვდება, ვინაიდან ყოველ ადგილას არანულოვანი ნაშთების ნამრავლი დგას და p მარტივია. ასე რომ ეს ჩამონათვალი შედგება ისევ ყველა არანულოვანი ნაშთისაგან 1,2,...,$p - 1$ (ოღონდ, შესაძლოა, რაღაც სხვა თანმიმდევრობით). კერძოდ, ამ ჩამონათვალში სადღაც უნდა შეგვხვდეს ნაშთი 1, ასე რომ მოიძებნება ისეთი ნაშთი x, რომ $a \times x = 1$. სწორედ ეს x იქნება ჩვენთვის a^{-1}, ასე რომ ნაშთები მარტივი p მოდულით მართლაც ველს ქმნიან. ეს ველი აღინიშნება $\mathbb{F}_p$-თი, მას p-ური მარტივი ველი ეწოდება.

მარტივი ველების გარდა კიდევ ბევრი სასრული ველი არსებობს. ყველა მათგანი მიიღება უფრო პატარა ველებიდან განტოლებათა ამონახსნების დამატებით. აი მაგალითი. დავიწყოთ სასრული ველით $\mathbb{F}_3$, რომელშიც სულ სამი ელემენტია, 0, 1 და 2. შევნიშნოთ, რომ ეს 2 იგივეა, რაც -1, იმიტომ რომ 3-ის მოდულით 2+1=0. შეკრებისა და გამრავლების ცხრილებიც სულ პატარებია, გარდა ტოლობებისა, რომლებსაც აქვთ სახე $0 + a = a$, $a + (-a) = 0$, $1 \times a = a$, კიდევ $(-1) + (-1) = 1$ და $(-1) \times (-1) = 1$. სინამდვილეში ეს უკანასკნელი ტოლობაც გამომდინარეობს მხოლოდ იქედან, რომ $\mathbb{F}_3$ რგოლია:

დავალება 7

აჩვენეთ, რომ ნებისმიერ რგოლში სრულდება ტოლობები $-a = (-1) \times a$ და (მინიშნება: დავალება 3-ის გამოყენებით) $(-1) \times (-1) = 1$. უფრო ზოგადად, დაამტკიცეთ ტოლობები $(-a) \times b = -(a \times b)$ და $(-a) \times (-b) = a \times b$.

ვინაიდან $(-1) \times (-1) = 1 \times 1 = 1$, $\mathbb{F}_3$-ს არ გააჩნია „წარმოსახვითი ერთეული“ -- ისეთი ელემენტი i, რომლისთვისაც $i \times i = -1$. ავიღოთ და „ძალით“ დავუმატოთ $\mathbb{F}_3$-ს ასეთი i. ეს გამოიწვევს კიდევ სხვა ელემენტების დამატების აუცილებლობას, მაგალითად, $-i$, $1 + i$-ც დაგვჭირდება, მაგრამ არც მაინცდამაინც ბევრი სხვა რამ. შეკრება „მოითხოვს“ ყველანაირ ელემენტებს $a + bi$, სადაც a და b შეიძლება იყოს 0, 1 ან -1, სულ 9 ცალი

გვექნება. და კარგი ისაა, რომ მეტი არც არაფერი დაგვჭირდება. სხვანაირად რომ ვთქვათ, გამრავლების ცხრილი თავისით „შეიკვრება“. მაგალითად, $(i-1)\times(-i) = i\times(-i) - 1\times(-i) = -(i\times i) - (-i) = -(-1) + i = 1 + i$ (აქ თითქმის ყველა წინა დავალება გამოვიყენეთ). მივიღებთ ველს $\mathbb{F}_9$ ასეთი შეკრებისა და გამრავლების ცხრილებით:

+	0	1	-1	i	$-i$	$i+1$	$i-1$	$1-i$	$-1-i$
0	0	1	-1	i	$-i$	$i+1$	$i-1$	$1-i$	$-1-i$
1	1	-1	0	$i+1$	$1-i$	$i-1$	i	$-1-i$	$-i$
-1	-1	0	1	$i-1$	$-1-i$	i	$i+1$	$-i$	$1-i$
i	i	$i+1$	$i-1$	$-i$	0	$1-i$	$-1-i$	1	-1
$-i$	$-i$	$1-i$	$-1-i$	0	i	1	-1	$i+1$	$i-1$
$i+1$	$i+1$	$i-1$	i	$1-i$	1	$-1-i$	$-i$	-1	0
$i-1$	$i-1$	i	$i+1$	$-1-i$	-1	$-i$	$1-i$	0	1
$1-i$	$1-i$	$-1-i$	1	1	$i+1$	-1	0	$i-1$	i
$-1-i$	$-1-i$	$-i$	$1-i$	-1	$i-1$	0	1	i	$i+1$

და

×	0	1	-1	i	$-i$	$i+1$	$i-1$	$1-i$	$-1-i$
0	0	0	0	0	0	0	0	0	0
1	0	1	-1	i	$-i$	$i+1$	$i-1$	$1-i$	$-1-i$
-1	0	-1	1	$-i$	i	$-1-i$	$1-i$	$i-1$	$i+1$
i	0	i	$-i$	-1	1	$i-1$	$-1-i$	$i+1$	$1-i$
$-i$	0	$-i$	i	1	-1	$1-i$	$i+1$	$-1-i$	$i-1$
$i+1$	0	$i+1$	$-1-i$	$i-1$	$1-i$	$-i$	1	-1	i
$i-1$	0	$i-1$	$1-i$	$-1-i$	$i+1$	1	i	$-i$	-1
$1-i$	0	$1-i$	$i-1$	$i+1$	$-1-i$	-1	$-i$	i	1
$-1-i$	0	$-1-i$	$i+1$	$1-i$	$i-1$	i	-1	1	$-i$

ერთი შეხედვით გაუგებარია, ასეთი რამ როგორ მოვუხერხოთ ყველაზე პატარა ველს, რომელიც ჯერ არც გვიხსენებია. ეს არის სულ ორელემენტიანი ველი $\mathbb{F}_2$, რომელშიც არაფერია 0-ისა და 1-ის გარდა, და რომელშიც $1+1=0$. ამ ველში წარმოსახვითი ერთეული გვაქვს იმ მარტივი მიზეზის გამო, რომ $-1=1$ (სწორედაც იმიტომ, რომ $1+1=0$). მერე რა? კიდევ ძალიან ბევრი განტოლებაა, რომელთა ამონახსნები ამ ველს არ გააჩნია. ავიღოთ რაიმე ახალი ელემენტი x, რომელზეც ჯერ არაფერი ვიცით. რა შეიძლება იყოს ჩვენს ველში ამ x-ის თავის თავზე ნამრავლი $x^2 = x\times x$? უკვე რაც გვაქვს $\mathbb{F}_2$-ში, შეიძლება გვქონდეს $x^2=1$ ან $x^2=0$. ამ განტოლებების ამონახსნები $\mathbb{F}_2$-ში უკვე გვაქვს. იქნებ $x^2=x$? ამ განტოლების ამონახსნებიც გვაქვს $\mathbb{F}_2$-ში. გვრჩება კიდევ ასეთი შესაძლებლობა: განტოლება $x^2=x+1$. აი ამ განტოლებას უკვე არც 0 არც 1 არ აკმაყოფილებს. ეს გვაძლევს ოთხელემენტიან ველს $\mathbb{F}_4$ ელემენტებით 0, 1, x და $x+1$ ასეთი შეკრებითა და გამრავლებით:

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	4	1	0

×	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

დავალება 8

$\mathbb{F}_2$-ს რომ მივუერთოთ ისეთი ახალი ელემენტი y, რომ $y^3 = y + 1$, მაშინ რამდენელემენტიან ველს მივიღებთ? შეადგინეთ ამ ველის შეკრებისა და გამრავლების ცხრილები.

სინამდვილეში საქმე ცოტა უფრო რთულადაა, ველისთვის ზოგიერთი განტოლების ამონახსნების დამატებამ შეიძლება ველი აღარ მოგვცეს.

დავალება 9 (შედარებით რთული)

$\mathbb{F}_2$-ს რომ მივუერთოთ ისეთი ახალი ელემენტი z, რომ $z^5 = z + 1$, ველი აღარ გამოგვივა: გვექნება ორი ისეთი არანულოვანი ელემენტი a და b, რომ $a \times b = 0$. შეგიძლიათ მოძებნოთ ეს ელემენტები?

იმის გარკვევაში, თუ რომელი განტოლებები „ვარგა“ ველების გასაფართოებლად და რომლები არა, გვეხმარება ერთი სასიამოვნო გარემოება. თურმე სასრული ველების გამრავლების ცხრილები საკმაოდ მარტივადაა მოწყობილი, და სირთულე მხოლოდ შეკრებასა და გამრავლებას შორის ურთიერთკავშირის გარკვევაშია (როგორც ეს „ჩვეულებრივ“ რიცხვებშიც ხდება).

თეორემა. სასრულ ველში, რომლის ელემენტების რაოდენობაა q, მოიძებნება ისეთი ელემენტი a, რომ ელემენტები $1 = a^0$, $a = a^1$, $a \times a = a^2$, $a \times a \times a = a^3$, …, a^{q-2} ყველა ერთმანეთისგან განსხვავებულია.

ასეთ ელემენტს პირველადი ელემენტი ეწოდება. მაგალითად, ჩვენს მიერ აგებულ ოთხელემენტიან ველში $\mathbb{F}_4$ ელემენტებით 0,1, x და $x + 1$ პირველადი ელემენტებია x-იც და $x + 1$-იც, რადგან $x^2 = x + 1$ და $(x + 1)^2 = x$. ან, ვთქვათ, სულ დასაწყისში რომ ავაგეთ შვიდელემენტიანი ველი, რომელიც შედგებოდა ნაშთებისაგან მოდულით 7, მანდ პირველადი ელემენტია ნაშთი 3. მართლაც, 7-ზე ნაშთებზე გადასვლით ვპოულობთ

$$3^2 = 9 = 2$$
$$3^3 = 3^2 \times 3 = 2 \times 3 = 6$$
$$3^4 = 3^2 \times 3^2 = 2 \times 2 = 4$$
$$3^5 = 3 \times 3^4 = 3 \times 4 = 12 = 5$$

q-ელემენტიანი ველის რაიმე პირველადი ელემენტი a თუ ხელში გვაქვს, გამრავლების ტაბულა ძალიან მარტივდება: ნულზე გამრავლება ხომ ნულს გვაძლევს, ყველა არანულოვან ელემენტს კი აქვს სახე a^k რომელიღაც k-სათვის, ხოლო $a^k a^l = a^{k+l}$.

ისღა გვრჩება გავარკვიოთ, თუ რა უნდა ვქნათ, თუ $k + l$ აღემატება $q - 2$-ს, მაგრამ ეს იოლია. ვნახოთ ჯერ, რას შეიძლება უდრიდეს a^{q-1}. ნული ვერ იქნება: რადგან ველში ვიმყოფებით, არანულოვანი ნაშთების ნამრავლი არანულოვანია, ხოლო $a^{q-1} = a \times a^{q-2}$. მაშასადამე a^{q-1} უნდა დაემთხვეს 1, a, a^2, …, a^{q-2}-დან ერთ-ერთს. ვთქვათ, $a^{q-1} = a^k$. მაშინ $a^{q-1} - a^k = 0$, და თუ a^k-ს ფრჩხილებს გარეთ გავიტანთ, მივიღებთ, რომ უნდა გვქონდეს $a^k \times \left(a^{q-1-k} - 1\right) = 0$. რადგან ველში ვართ, მაშინ ან a^k ან $a^{q-1-k} - 1$ ნული უნდა იყოს. მაგრამ a^k ხომ ერთ-ერთი არანულოვანი ნაშთი იყო, ასე რომ $a^{q-1-k} - 1 = 0$, ანუ $a^{q-1-k} = 1$. არა და a ხომ პირველადი ფესვია, ასე რომ a^{q-1-k} ვერ იქნება a, a^2, …, a^{q-2}-დან ვერცერთი, ანუ k ვერ იქნება $1, 2, \ldots, q - 2$-დან ვერცერთი. გვრჩება ერთადერთი შესაძლებლობა $k = 0$, ანუ $a^{q-1} = 1$.

აქედან იოლად ვღებულობთ, რომ $a^j = a^{j+q-1}$ ყოველი j-სათვის, ასე რომ გამრავლების ცხრილის ამბავი გარკვეულია: $a^k a^l = a^m$, სადაც m არის $k + l$-ის $q - 1$-ზე გაყოფის ნაშთი.

აქედანვე ირკვევა, თუ რატომ შეგვხვდა $\mathbb{F}_4$-ში ორი სხვადასხვა პირველადი ელემენტი.

დავალება 10 (ზომიერად რთული)

აჩვენეთ, რომ თუ a არის q-ელემენტიანი ველის პირველადი ელემენტი, მაშინ ამ ველის პირველადი ელემენტები არიან ზუსტად ყველა ის ხარისხები a^j, რომელთათვისაც j-სა და $q-1$-ს არ გააჩნიათ 1-ისგან განსხვავებული საერთო გამყოფები.

დავალება 11 (მარტივი)

3-ის გარდა კიდევ რომლებია შვიდზე გაყოფის ნაშთების ველში პირველადი ელემენტები?

დავალება 12 (წინაზე ცოტათი უფრო რთული)

იპოვეთ პირველადი ელემენტები ჩვენს მიერ აგებულ ცხრაელემენტიან ველში $\mathbb{F}_9$.

ვექტორული სივრცეები

შეიძლება ითქვას, დავაგროვეთ ის სულ უმცირესი ცოდნა სასრული რიცხვითი სისტემების შესახებ, რომელიც შეგვაძლებინებს ვიმსჯელოთ ამ რიცხვებისგან გაკეთებულ სივრცეებზე. კიდევ ერთხელ შეგახსენებთ ჩვენს სულ პირველ ამოცანას, ყუთში ბურთების ჩაწყობის შესახებ. იქ ჩვენ სივრცეები „ავაწყვეთ“ „ჩვეულებრივი“ რიცხვებისგან, ჩვენი სივრცეების წერტილებს ჰქონდათ სახე $(x_1, \dots, x_d)$, სადაც ეს x-ები რაიმე რიცხვები იყო. ახლა იმავენაირად მოვიქცევით: ავიღებთ რაიმე სასრულ ველს F, და ჩვენი x-ები იქნებიან ამ ველის ელემენტები. პირველად გაგვიჩნდება რაღაც, რაც მოგვაგონებს იმ ცხრილებს, რომლებზეც ადრე ვლაპარაკობდით.

მაგალითად, ავიღოთ ის სამელემენტიანი ველი $\mathbb{F}_3$, რომელზეც წეხან ვლაპარაკობდით, და ავირჩიოთ $d=3$. მივიღებთ “სივრცეს“ $\mathbb{F}_3^3$, რომელშიც გვექნება სულ $27 (= 3\times 3\times 3)$ „წერტილი”. აი ამ წერტილების სრული ჩამონათვალი:

0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	-1
0	0	0	1	1	1	-1	-1	-1	0	0	0	1	1	1	-1	-1	-1	0	0	0	1	1	1	-1	-1	-1
0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1

ასეთ „სივრცეებთან“ მუშაობისას, როგორც მენტორის საათში გითხარით, ცოტათი გვეხმარება „ჩვეულებრივი“ სივრცული ინტუიცია. თითქოსდა ამ ცხრილის თითოეული სვეტი იყოს რომელიღაც სამგანზომილებიანი სივრცის წერტილი. ამ „სივრცეში“ რაიმე ქვესივრცის, მაგალითად სიბრტყის გამოსაყოფად შეგვიძლია გამოვიყენოთ მარტივი პირობები, წრფივი განტოლებები, მაგალითად ასეთი: ამოვკრიფოთ მხოლოდ ისეთი (x_1, x_2, x_3) სამეულები, რომლებიც აკმაყოფილებენ ტოლობას $x_1 - x_2 - x_3 = 0$. ამ პირობას 27 წერტილიდან აკმაყოფილებს მხოლოდ 9, სახელდობრ,

0	0	0	1	1	1	-1	-1	-1
0	1	-1	0	1	-1	0	1	-1
0	-1	1	1	0	-1	-1	1	0

თუ ეს ინტუიცია დაგვეხმარება, ამ ცხრილს შეგვიძლია მოვექცეთ, თითქოს ის ყოფილიყოს ცხრა წერტილისგან შემდგარი სიბრტყე P ჩვენს სამგანზომილებიან ოცდაშვიდწერტილიან სივრცეში $\mathbb{F}_3^3$.

ეხლა კიდევ გავიხსენოთ ის უცნაური „მანძილები“, რომლებზეც ადრე ვლაპარაკობდით. მანძილი $\mathbb{F}_3^3$-ის ორ (x_1, x_2, x_3) და (y_1, y_2, y_3) წერტილს შორის შეიძლება იყოს 0,1, 2 ან 3. ეს მანძილი არის იმ ადგილების რაოდენობა, რომლებშიც განლაგებული რიცხვები ამ წერტილებს განსხვავებული აქვთ. მაგალითად, თუ $x_1 \neq y_1$, $x_2 = y_2$ და $x_3 \neq y_3$, მანძილი უდრის 2-ს. ჩვენ ვილაპარაკეთ იმის შესახებ, რომ მანძილთან მუშაობა გაადვილდება, თუ შევძლებთ განვსაზღვროთ წერტილების გამოკლება. და ჩვენს მიერ ეხლა აგებულ სივრცეში ეს ზუსტადაც რომ შეგვიძლია: უბრალოდ განვსაზღვროთ $(x_1, x_2, x_3) - (y_1, y_2, y_3) = (x_1 - y_1, x_2 - y_2, x_3 - y_3)$. მაშინ მანძილი ამ წერტილებს შორის იგივეა, რაც მათ სხვაობაში არანულოვანი კოორდინატების რაოდენობა. აქ ჩვენ სხვათა შორის გამოვიყენეთ ერთ-ერთი წინა დავალება.

დავალება 13 (სულ იოლი)

რომელი წინა დავალებიდან გამომდინარეობს, რომ მანძილი მართლაც უდრის სხვაობაში არანულოვანი რიცხვების რაოდენობას?

ახლა შევნიშნოთ, რომ $\mathbb{F}_3^3$-ის ნებისმიერი წერტილებისთვის მათი სხვაობა კვლავ $\mathbb{F}_3^3$-ს ეკუთვნის. ამიტომ, თუ გვაინტერესებს, რამდენნაირი მანძილები გვხვდება $\mathbb{F}_3^3$-ში, უნდა ვნახოთ, რამდენნულიანი წერტილები გვხვდება. კაცმა რომ თქვას, რამდენნულიანი და ყველანაირნულიანები შეგვხვდება, იმიტომ რომ ჩვენ $\mathbb{F}_3^3$-ში რიცხვების საერთოდ ნებისმიერი სამეულები ჩავყარეთ. თითქოს რაღაც უშინაარსო გამოგვივიდა. მაგრამ ახლა შევხედოთ იმავე თვალსაზრისით P სიბრტყეს, რომელიც ჩვენ $\mathbb{F}_3^3$-ის შემდეგ განვიხილეთ. შეგახსენეთ, P შედგება ყველა ისეთი (x_1, x_2, x_3) სამეულებისგან, რომლებიც აკმაყოფილებენ ტოლობას $x_1 - x_2 - x_3 = 0$. საქმე იმაშია, რომ ამ P-საც აქვს ის თვისება, რომ მისი ნებისმიერი ორი წერტილის სხვაობა კვლავ მას ეკუთვნის. ამიტომ მისთვისაც შეგვიძლია წყვილ-წყვილად მანძილების შესწავლა მის წერტილებში ნულების რაოდენობაზე დაკვირვებით. და აქ უკვე რაღაც შინაარსიანი ხდება: შეხედეთ P-ს წერტილთა ჩამონათვალს. მის წერტილებს შორის არის $(0,0,0)$, რომელშიც, გასაგებია, საერთოდ არაა არანულოვანი რიცხვები. მაგრამ აი მის ყველა დანარჩენ წერტილში არანაკლებ ორი არანულოვანი რიცხვია. ეს კი ნიშნავს, რომ P-ში წერტილებს შორის უმცირესი მანძილი არის 2. ასე რომ P უმცირესი მანძილების თვალსაზრისით $\mathbb{F}_3^3$-ს ჯობნის.

მოდით ახლა, სანამ გავაგრძელებდეთ, ჯერ ზუსტად ჩამოვაყალიბოთ ჩვენი სივრცეების ის თვისებები, რომლებიც დაგვჭირდება, როგორც ეს ველებისათვის გავაკეთეთ.

ამჯერად გვაქვს რაიმე ერთობლიობა V, რომლის ელემენტებს აღვნიშნავთ ასოებით v, w, …

ვიტყვით, რომ V არის ვექტორული სივრცე $\mathbb{F}$ ველზე, თუ ყოველი v-სა და w-სათვის V-დან განსაზღვრულია $v + w$, რომელიც V-ს ეკუთვნის, და გარდა ამისა ყოველი v-სათვის V-დან და ყოველი a-სათვის $\mathbb{F}$-იდან განსაზღვრულია av, რომელიც აგრეთვე V-ს ეკუთვნის. კიდევ V-ში უნდა გვქონდეს გამორჩეული ელემენტი 0. ამასთან ყველა u, v, w-სათვის V-დან და ყველა a, b-სათვის F-დან უნდა სრულდებოდეს ასეთი ტოლობები:

$$
\begin{aligned}
&v + w = w + v \\
&(u + v) + w = u + (v + w) \\
&0 + v = v \\
&a(v + w) = av + aw \\
&(a + b)v = av + bv \\
&1v = v \\
&a(bv) = (a \times b)v
\end{aligned}
$$

თქვენ ალბათ ელოდებით კიდევ ერთ პირობას, ისეთივეს, როგორიც ველებისთვის გვქონდა: რომ V-ს ყოველი v ელემენტისათვის გვქონდეს ისეთი $-v$, რომ $v + (-v) = 0$. მაგრამ საქმე იმაშია, რომ ასეთი ელემენტი უკვე გვაქვს: $-v$ არის $(-1)v$.

დავალება 14

აჩვენეთ, რომ ყოველი V ვექტორული სივრცის ყოველი v ელემენტისათვის $v + (-1)v = 0$.

მინიშნება: ამის საჩვენებლად ჯერ მოგიწევთ იმის ჩვენება, რომ $0v = 0$. სინამდვილეში ამდაგვარი დავალება ჩვენ უკვე გვქონდა, ერთადერთი განსხვავებაა, რომ აქ მარცხნივ და მარჯვნივ რომ 0 დგას ეგენი სხვადასხვა რამეებია: მარცხენა ნოლი ველს ეკუთვნის, მარჯვენა კი V-ს.

$\mathbb{F}$ ველზე ვექტორული სივრცის მთავარი მაგალითი: ავირჩიოთ რაიმე ნატურალური რიცხვი n და განვიხილოთ $\mathbb{F}^n$, $\mathbb{F}$-ის ელემენტების ყველანაირი n-ეულები $(x_1, \dots, x_n)$. მათი შეკრება ხდება ასეთი წესით: $(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$, გამორჩეული ელემენტია (0,...,0), ხოლო ველის ელემენტებზე ასეთნაირად ვამრავლებთ: $a(x_1, \dots, x_n) = (a \times x_1, \dots, a \times x_n)$. იმის შემოწმება, რომ ყველა საჭირო ტოლობა შესრულდება, იმდენად ადვილია, რომ ამის შესახებ დავალებას არც შემოგკადრებთ.

რაღა თქმა უნდა, ის $\mathbb{F}_3^3$, თავიდან რომ განვიხილეთ, ამ მაგალითის კერძო შემთხვევაა. იქ ჩვენ გვქონდა კიდევ „სიბრტყე“ P. ის არის ვექტორული სივრცის ქვესივრცის მაგალითი. ზოგადად, $\mathbb{F}$ ველზე V ვექტორული სივრცის ქვესივრცე არის მისი ისეთი ქვესიმრავლე $W \subseteq V$, რომ ნებისმიერი w, w'-ისთვის W-დან $w + w'$ ეკუთვნის W-ს, და გარდა ამისა ნებისმიერი a-სთვის $\mathbb{F}$-იდან aw-ც ეკუთვნის W-ს.

დავალება 15

ავირჩიოთ რაიმე $\mathbb{F}$ ველში რაიმე ელემენტები $c_1, \dots, c_n$. აჩვენეთ, რომ $\mathbb{F}^n$-ის ყველა ისეთი ელემენტები $(x_1, \dots, x_n)$, რომლებისთვისაც სრულდება ტოლობა $c_1x_1 + \dots + c_nx_n = 0$, ქმნიან $\mathbb{F}^n$-ის ქვესივრცეს.

დავალება 16 (ძალიან ადვილი)

თუ W_1 და W_2 რაიმე V ვექტორული სივრცის ქვესივრცეებია, მაშინ მათი თანაკვეთა $W_1 \cap W_2$, ე. ი. V-ს ყველა იმ ელემენტთა ერთობლიობა, რომლებიც W_1-საც ეკუთვნიან და W_2-საც, აგრეთვე V-ს ქვესივრცეა.

წრფივი კოდები. რიდ–სოლომონის კოდი

როგორც იქნა მივადექით ჩვენი ინტერესის მთავარ საგანს. წრფივი კოდი ეწოდება რაიმე სასრულ $\mathbb{F}$ ველზე $\mathbb{F}^n$ ვექტორული სივრცის რაიმე W ქვესივრცეს. ამ კოდის წონა არის მასში შემავალ არანულოვან n-ეულებში არანულოვანი რიცხვების უმცირესი რაოდენობა.

სხვანაირად რომ ვთქვათ, W-ს წონა არის d, თუ რა არანულოვანი $(x_1, \dots, x_n)$-იც არ უნდა ავიღოთ W-დან, აღმოჩნდება, რომ $x_1, \dots, x_n$-ს შორის d ცალი მაინც არ არის ნულის ტოლი.

შეგახსენებთ, რომ ჩვენ გვქონდა არა მაინც და მაინც წრფივი კოდის დაშორების ცნება. კოდის დაშორება იყო d, თუ რა ორი განსხვავებული $(x_1, \dots, x_n)$ და $(y_1, \dots, y_n)$-იც არ უნდა აგვეღო, მათ შორის მანძილი იქნებოდა d მაინც. ანუ, ისეთი k-ების რაოდენობა, რომ $x_k \neq y_k$, არ იქნებოდა d-ზე ნაკლები. იმის გათვალისწინებით, რაც აქამდე ვილაპარაკეთ, შემდეგი დავალება თქვენთვის სრულიად ცხადი უნდა იყოს.

დავალება 17 (ძალიან ადვილი)

წრფივი კოდის დაშორება უდრის მის წონას.

ჩვენ ვეძებთ $\mathbb{F}^n$-ში რაც შეიძლება ბევრელემენტიან კოდებს, რომლებსაც რაც შეიძლება დიდი წონა აქვთ. არის ორი უკიდურესობა: ყველაზე მეტი ელემენტი, გასაგებია, მთელს $\mathbb{F}^n$-შია, მაგრამ მას ძალიან პატარა წონა აქვს.

დავალება 18

რას უდრის მთელი $\mathbb{F}^n$-ის წონა?

მეორეს მხრივ, შეგვიძლია ასე მოვიქცეთ. ავიღოთ რომელიმე ერთი ისეთი ვექტორი $(x_1, \dots, x_n)$ (ელემენტი $\mathbb{F}^n$-დან), რომ $x_1, \dots, x_n$-ს შორის საერთოდ არა გვაქვს ნულები, მაგალითად (1,...,1), და განვიხილოთ მისი ყველანაირი ნამრავლები $\mathbb{F}$-ის ელემენტებზე, $(ax_1, \dots, ax_n)$. ეს ნამრავლები ქმნიან წრფივ კოდს, და მისი წონა უდიდესია რაც კი შეიძლება რაიმე კოდს გააჩნდეს, ეს წონა არის n. მაგრამ ამ კოდში სულ ცოტა ელემენტებია, იმდენივე, რამცენიც $\mathbb{F}$-შია, მასზე ცოტა ელემენტები მხოლოდ ნულოვან სივრცეშია, რომელიც შეიცავს მხოლოდ 0-ს.

დავალება 19 (ადვილი)

აჩვენეთ, რომ q-ელემენტიან ველზე ნებისმიერ არანულოვან ვექტორულ სივრცეს გააჩნია არანაკლებ q ელემენტისა.

აქედან გასაგებია, რომ „კარგი“ კოდები სადღაც შუაშია.

ბოლოს მოვიყვანოთ ასეთი კარგი კოდების ერთ-ერთი ყველაზე სახელგანთქმული მაგალითი, რიდ-სოლომონის კოდი.

ვირჩევთ რაიმე q-ელემენტიან ველს $\mathbb{F}_q$. შეგახსენებთ, რომ მას გააჩნია პირველადი ელემენტები: ისეთი ელემენტები a, რომ ელემენტები $1, a, a^2, \dots, a^{q-2}$ ყველა წყვილ-წყვილად განსხვავებულია. ავირჩიოთ რომელიმე მათგანი, და კიდევ ავირჩიოთ რაიმე ორი ისეთი ნატურალური რიცხვი n და N, რომ $n < N < q$.

რიდ-სოლომონის კოდი $\mathrm{RS}(n, N, q)$ პარამეტრებით n, N, q არის ქვესივრცე $\mathbb{F}_q^N$-ში, რომელიც ასეთნაირად იგება. $\mathbb{F}_q$-ს ნებისმიერ $n+1$ ცალ ელემენტს $c_0, c_1, \dots, c_n$ შევუსაბამოთ $\mathbb{F}_q^N$-ის ელემენტი $(f(1), f(a), f(a^2), \dots, f(a^{N-1}))$, სადაც $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$. კოდი $\mathrm{RS}(n, N, q)$ შედგება $\mathbb{F}_q^N$-ის ყველა ასეთნაირად მიღებული ელემენტისგან.

დავალება 20

აჩვენეთ, რომ $\mathrm{RS}(n, N, q)$ მართლაც წრფივი კოდია, ე. ი. წარმოადგენს $\mathbb{F}_q^N$-ის ქვესივრცეს.

რიდ-სოლომონის კოდი $\mathrm{RS}(n, N, q)$ ცნობილი წრფივი კოდებიდან ერთ-ერთი საუკეთესოა. იგი შედგება q^{n+1} ცალი ელემენტისაგან, ხოლო მისი წონა არის $N - n$.

ვნახოთ, მაგალითად, როგორ გამოიყურება კოდი $\mathrm{RS}(1,4,5)$. რადგან $q = 5$, საქმე გვაქვს 5-ელემენტიან მარტივ ველთან $\mathbb{F}_5$. მასში უნდა ავირჩიოთ პირველადი ელემენტი a. ასეთად გამოდგება, მაგალითად, ნაშთი 2, იმიტომ რომ $\mathbb{F}_5$-ში $2^2 = 4$ და $2^3 = 8 = 3$, და 1,2,4,3 ყველა წყვილ-წყვილად განსხვავებულია. $N = 4$, ასე რომ $\mathrm{RS}(1,4,5)$ არის $\mathbb{F}_5^4$-ის ქვესივრცე, ის შედგება 0,1,2,3,4 ნაშთების ოთხეულებისგან. რადგან $n = 1$, უნდა დავაგროვოთ სულ $q^{n+1} = 5^2 = 25$ ასეთი ოთხეული. ამისათვის ყოველი ორი ნაშთისათვის c_0, c_1 ვიხილავთ ფუნქციას $f(x) = c_0 + c_1 x$ და ამ ფუნქციის მეშვეობით c_0, c_1 წყვილს ვუსაბამებთ ოთხეულს $(f(1), f(a), f(a^2), f(a^3))$, ესე იგი ასეთ ოთხეულს: $(c_0 + c_1, c_0 + 2c_1, c_0 + 4c_1, c_0 + 3c_1)$ (ეს ბოლო სამიანი იმიტომ გაგვიჩნდა, რომ, როგორც ვთქვით, $\mathbb{F}_5$-ში $2^3 = 3$). მაგალითად, წყვილს 3,4 შეესაბამება ოთხეული $(3 + 4, 3 + 2 \times 4, 3 + 4 \times 4, 3 + 3 \times 4) = (2,3,4,0)$. აი სრული ჩამონათვალი, რომელიც ასეთნაირად გამოგვივა:

(0,0)-ს	შეესაბამება	(0,0,0,0)
(0,1)-ს	შეესაბამება	(1,2,4,3)
(0,2)-ს	„----------„	(2,4,3,1)
(0,3)	„----------„	(3,1,2,4)
(0,4)	„----------„	(4,3,1,2)
(1,0)	„----------„	(1,1,1,1)
(1,1)	„----------„	(2,3,0,4)
(1,2)	„----------„	(3,0,4,2)
(1,3)	„----------„	(4,2,3,0)
(1,4)	„----------„	(0,4,2,3)
(2,0)	„----------„	(2,2,2,2)
(2,1)	„----------„	(3,4,1,0)
(2,2)	„----------„	(4,1,0,3)

(2,3)	„----------„	(0,3,4,1)
(2,4)	„----------„	(1,0,3,4)
(3,0)	„----------„	(3,3,3,3)
(3,1)	„----------„	(4,0,2,1)
(3,2)	„----------„	(0,2,1,4)
(3,3)	„----------„	(1,4,0,2)
(3,4)	„----------„	(2,1,4,0)
(4,0)	„----------„	(4,4,4,4)
(4,1)	„----------„	(0,1,3,2)
(4,2)	„----------„	(1,3,2,0)
(4,3)	„----------„	(2,0,1,3)
(4,4)	„----------„	(3,2,0,1)

როგორც ხედავთ, ამ კოდის წონა არის 3, ე. ი. ყოველ ჩამოთვლილ ოთხეულში (0,0,0,0)-ის გარდა სამი ნაშთი მაინც არანულოვანია.

დავალება 21

ასეთივენაირად აღწერეთ კოდი RS$(1,3,4)$. უნდა გამოგივიდეთ 16-ელემენტიანი ქვესივრცე 64-ელემენტიან სივრცეში $\mathbb{F}_4^3$. შეგიძლიათ იპოვით ისეთი c_1, c_2, c_3, რომ ეს ქვესივრცე შედგებოდეს ზუსტად ისეთი სამეულებისაგან (x_1, x_2, x_3), რომელთათვისაც $c_1x_1 + c_2x_2 + c_3x_3 = 0$?