ა. რაზმაძე

რიცხვთა თეორია

თბილისის უნივერსიტეტის გამომცემლობა
თბილისი 1992

22.13
511
რ 177

მკითხველს ვთავაზობთ სრულიად ახალგაზრდა ანდრია რაზმაძის სადიპლომო ნაშრომს, რომელიც მოსკოვის უნივერსიტეტის არქივში იქნა მიკვლეული. მასში ჩანს ახალგაზრდა მეცნიერის ერუდიცია, სამეცნიერო ლიტერატურის ღრმა ცოდნა და ანალიტიკური აზროვნება.

იგი დიდ დახმარებას გაუწევს მათემატიკოს სტუდენტებს, ასპირანტებსა და მეცნიერებს.

მთარგმნელი დოც. რ. ბერიძე

რედაქტორი დოც. ნ. ქალდანი

რეცენზენტი დოც. ა. თავაძე

1602030000

P ———

608(06)—92

წ ი ნ ა თ ქ მ ა

წიგნი სრულიად ახალგაზრდა ანდრია რაზმაძის სადიპლომო ნაშრომია, დათარიღებული 1910 წლით. იგი მოწონებულია მოსკოვის უნივერსიტეტის პროფესორის, ცნობილი მათემატიკოსის დ. ეგოროვის მიერ (წარწერა შრომის თავფურცელზე „Одобряю О. П. Д. Егоров, 11, IV. 10). ნაშრომს მოსკოვის უნივერსიტეტის არქივში მუშაობის დროს მიაკვლია ქუთაისის პედაგოგიური ინსტიტუტის დოცენტმა ბატონმა იროდიონ ერემეიშვილმა. იგი სჩვა ანალოგიური ნაშრომებისაგან გამოირჩევა ფუნდამენტურობით, არსებული ლიტერატურის ღრმა და საფუძვლიანი ცოდნით. ი. ერემეიშვილმა გადაიღო ფოტოპირი, ჩამოიტანა საქართველოში და გადასცა ანდრია რაზმაძის საიუბილეო კომისიას.

ქართული მათემატიკური საზოგადოება და სტუდენტი ახალგაზრდობა სიამოვნებით გაეცნობა ქართული მათემატიკური სკოლის ისტორიის ამ საინტერესო დოკუმენტს.

მთარგმნელი

ბა იყოს სრული ან არასრული, იმის მიხედვით, არის თუ არა ერთი სიმრავლის ყველა ელემენტი მეორე სიმრავლის ყველა ელემენტთან შესაბამისობაში, ან არსებობს ერთი სიმრავლის ელემენტთა გარკვეული რაოდენობა, რომელსაც არა აქვს შესაბამისი ელემენტები მეორე სიმრავლეში.

§ 2. რიგობრივი რიცხვები

თუ ელემენტთა დალაგებულ სიმრავლეს გამოვაკლებთ ელემენტთა გარკვეულ (სასრულ ან უსასრულო) რაოდენობას, მაშინ დარჩენილ სიმრავლეს მოცემული სიმრავლის ნაწილი ეწოდება. დალაგებულ სიმრავლეს სასრული ეწოდება, თუ იგი აკმაყოფილებს შემდეგ პირობებს:

1. ამ სიმრავლეში არსებობს ერთი ელემენტი, რომლის რანგი ყველა სხვა ელემენტის რანგზე დაბალია.

2. არსებობს ერთი ელემენტი, რომლის რანგი ყველა სხვა ელემენტის რანგზე მაღალია.

3. სიმრავლის ყოველ ნაწილში არის ელემენტი, რომლის რანგი ყველა დანარჩენი ელემენტის რანგზე დაბალია და ელემენტი, რომლის რანგი ყველა სხვა ელემენტის რანგზე მაღალია.

ნათქვამიდან გამომდინარეობს, რომ სასრული დალაგებული სიმრავლის ყოველი ნაწილი აგრეთვე სასრული დალაგებული სიმრავლეა.

ორ სასრულ დალაგებულ სიმრავლეს მსგავსი ეწოდება, თუ მათ ელემენტებს შორის არსებობს ურთიერთცალსახა შესაბამისობა, თანაც ისეთი, რომ ელემენტთა დალაგება ამ შესაბამისობის დროს შენარჩუნებულია. ეს იმას ნიშნავს, რომ თუ a და b ერთი სიმრავლის ორი ელემენტია, a' და b' მათი შესაბამისი ელემენტებია მეორე სიმრავლეში, ამასთან, $a<b$, მაშინ $a'<b'$.

თუ სასრული დალაგებული სიმრავლეები მსგავსია, მაშინ ამბობენ, რომ მათ ერთი და იგივე რიგობრივი რიცხვი აქვთ. ვთქვათ, A, B და C სამი ისეთი დალაგებული სიმრავლეა, რომ A და B სიმრავლეები C სიმრავლის მსგავსია, მაშინ, ცხადია, A და B სიმრავლეები მსგავსია.

შაშასადამე, ამ სამ დალაგებულ სიმრავლეს აქვს ერთი და იგივე რიგობრივი რიცხვი.

მივედით ასეთ დასკვნამდე: რიგობრივი რიცხვი ახასიათებს დალაგებული მსგავსი სიმრავლეების კლასს.

თუ A სიმრავლე შეიცავს ერთ ელემენტს, მაშინ ამბობენ, რომ მისი რიგობრივი რიცხვი არის ერთი და აღნიშნავენ სიმბოლოთი 1. რიგობრივი რიცხვი 1 ახასიათებს ყველა ერთელემენტიან სიმრავლეს. თუ A სიმრავლეს, რომელიც ერთ a ელემენტს შეიცავს, მივუერთებთ ახალ b ელემენტს, მივიღებთ $(a; b)$ სიმრავლეს, რომლის რიგობრივი რიცხვი არის 2. a-ს ეწოდება პირველი ელემენტი, b-ს მეორე ელემენტი. თუ $(a; b)$ სიმრავლეს მივუერთებთ კიდევ ერთ c ელემენტს, მივიღებთ $(a; b; c)$ სიმრავლეს, რომლის რიგობრივი რიცხვი არის 3. ასე დახასიათდება ამ წესით აგებული ყველა დალაგებული სიმრავლე. ამავე გზით ავაგებთ $(a; b; c; \ldots, h)$ სიმრავლეს, რომლის რიგობრივი რიცხვი არის n. თუ ამ სიმრავლეს მივუერთებთ k ელემენტს, მივიღებთ $(a; b; c; \ldots, h; k)$ სიმრავლეს, რომლის რიგობრივი რიცხვი იქნება n-ისაგან განსხვავებული n' რიცხვი.

თ ე ო რ ე მ ა 1. ყოველი დალაგებული სიმრავლე, რომლის აგება შეიძლება მითითებული გზით, არის სასრული და, პირიქით, ყოველი სასრული დალაგებული სიმრავლე შეიძლება აიგოს მითითებული გზით.

თ ე ო რ ე მ ა II. სასრული დალაგებული სიმრავლე არ შეიძლება იყოს თავისი ნაწილის მსგავსი.

ამ თეორემებიდან ჩვენ შეიძლება გავაკეთოთ ასეთი დასკვნა:

რიცხვები 1, 2, 3,..., რომლებიც განისაზღვრა როგორც (a), $(a; b)$, $(a; b; c)$,... სიმრავლეების რიგობრივი რიცხვები, ყველა ერთმანეთისაგან განსხვავებულია, რადგან, თუ რომელიმე რიგობრივი n რიცხვი მეორე n' რიგობრივი რიცხვის ტოლია, მაშინ შესაბამისი სიმრავლეები მსგავსი აღმოჩნდება და წინააღმდეგობას მივიღებთ.

თ ე ო რ ე მ ა III. ყოველი რიგობრივი რიცხვი განიხილება როგორც ერთადერთი იდეალური ობიექტი, რადგან ის წარმოადგენს რაღაცას მუდმივს, რომელიც ჩვენთვის სავსებით განსაზღვრულია.

ზემოთ ჩვენ განვიხილეთ სასრული დალაგებული სიმრავლის ცნება. ახლა განვსაზღვროთ უსასრულო დალაგებული სიმრავლე. მარ-

ტივი უსასრულო დალაგებული სიმრავლე გვესმის ასე: ეს არის სიმრავლე, რომელიც არ შეიცავს უმაღლესი რანგის ელემენტს, მაგრამ მის ყოველ ნაწილს გააჩნია უმაღლესი რანგის ელემენტი. მარტივი უსასრულო სიმრავლე სასრული დალაგებული სიმრავლისაგან იმით განსხვავდება, რომ არ შეიცავს უმაღლესი რანგის მქონე ელემენტს.

რიგობრივი რიცხვების სიმრავლე შეადგენს მარტივ უსასრულო დალაგებულ სიმრავლეს. ეს ობიექტები შეიძლება გამოვსახოთ სიმბოლოებით α, β, γ,..., ან 1, 2, 3,... .

რაიმე სახის ობიექტთა სასრული სიმრავლის თვლის ოპერაცია შეიძლება გავიგოთ, როგორც ამ ობიექტების რიგობრივ რიცხვთა სიმრავლის ელემენტებთან შესაბამისობაში მოყვანა, ისე რომ, როცა რიგობრივ რიცხვს აქვს შესაბამისი ელემენტი, მაშინ ნებისმიერ სხვა რიგობრივ რიცხვსაც აქვს შესაბამისი ელემენტი. თვლის პროცესით ელემენტთა ყოველი სასრული სიმრავლე შეიძლება დავალაგოთ. ამიტომ ყოველი სასრული სიმრავლე აუცილებლად დალაგებული სიმრავლეა.

რიგობრივი რიცხვების სიმრავლე, რომელიც მოცემული სიმრავლის თვლის დროს გამოიყენება, ცხადია, მოცემული სიმრავლის მსგავსი სიმრავლეა. უკანასკნელი რიგობრივი რიცხვი, რომელიც სასრული სიმრავლის თვლის დროს გამოიყენება, არის ამ სასრული სიმრავლის რიგობრივი რიცხვი ან, უბრალოდ, სასრული სიმრავლის რიცხვი (Anzahl, the Number).

§3. ოპერაციები მთელ რიცხვებზე

ვთქვათ, ორ სასრულ დალაგებულ A და B სიმრავლეებს აქვს m და n რიგობრივი რიცხვები. A და B გავაერთიანოთ ერთ C დალაგებულ სიმრავლეში, რომელშიც A-ს ნებისმიერი ელემენტის რანგი B-ს ნებისმიერი ელემენტის რანგზე დაბალია და A-ს ნებისმიერ ორ ელემენტს ისეთივე შედარებითი რიგი აქვს C-ში, როგორც საწყის სიმრავლეებში. მაშინ ამბობენ, რომ C რთული სიმრავლის რიგობრივი რიცხვი p არის m და n რიგობრივი რიცხვების ჯამი და აღნიშნავენ ასე: $p=m+n$.

ახლა შეიძლება ვაჩვენოთ, რომ ახალი სიმრავლე სასრულია

და მისი რიგობრივი რიცხვი არ შეიცვლება, თუ A და B სიმრავლეებს მსგავსი სიმრავლეებით შევცვლით. ეს ნიშნავს, რომ p ჯამი არის რაღაც სასრული რიცხვი, რომელიც დამოკიდებულია მხოლოდ m და n რიცხვებზე, რადგან (A, B) და (B, A)-ს აქვს ერთი და იგივე რიგობრივი რიცხვი, ამიტომ, ცხადია, $m+n=n+m$. უკანასკნელი ტოლობა არის შეკრების კომუტაციურობის კანონი. ორი m და n რიცხვების ჯამის პოვნის ოპერაციას შეკრების ოპერაცია ეწოდება. უნდა შევნიშნოთ, რომ m და n ორი რიცხვის ჯამის პოვნა არ შეიძლება იმ დაშვებით, რომ ეს უბრალოდ აბსოლუტური რიცხვებია. ამ ჯამის პოვნა მხოლოდ მას შემდეგ შეიძლება, როცა ისინი განიხილება, როგორც A და B სიმრავლეების რიგობრივი რიცხვები და მაშინ $m+n$ წარმოადგენს A და B სიმრავლეებისაგან შედგენილი C რთული სიმრავლის რიგობრივ რიცხვს. შეკრების ოპერაციის გავრცელება შეიძლება სიმრავლეთა უფრო დიდ რაოდენობაზე. მაგალითად, თუ $A, B, C, \ldots, L$ მოცემული სიმრავლეებია, ხოლო $m, n, p, \ldots, z$ მათი რიგობრივი რიცხვებია, S არის ამ სიმრავლეებისაგან მითითებული გზით აგებული რთული სიმრავლე, რომლის რიგობრივი რიცხვი არის S, მაშინ S არის $m, n, p, \ldots, z$ რიგობრივი რიცხვების ჯამი და აღინიშნება ასე:

$$S=m+n+p+\ldots+z.$$

აქედან ადვილად ჩანს, რომ

$$(m+n)+p=m+(n+p).$$

ეს ტოლობა გამოხატავს შეკრების ჯუფთებადობის კანონს.

თუ სასრულ A სიმრავლეში, რომლის რიგობრივი რიცხვია m, ყოველ ელემენტს შევცვლით სასრული B სიმრავლით, რომლის რიგობრივი რიცხვია n, მაშინ ამბობენ, რომ ასეთი გზით მიღებული C რთული სიმრავლის რიგობრივი p რიცხვი არის m და n რიგობრივი რიცხვების mn ნამრავლი. ცხადია, თუ A და B სიმრავლეებს შევცვლით მათი მსგავსი A' და B' სიმრავლეებით, მაშინ აგებული რთული სიმრავლის რიგობრივი რიცხვი იგივე იქნება: $p=mn$. აქედან ცხადია, რომ p დამოკიდებულია მხოლოდ m და n რიცხვებზე.

ახლა ძნელი არ არის ვაჩვენოთ შემდეგი ტოლობები:

1. $mn = \underbrace{m+m+\cdots+m}_{n\text{-ჯერ}}$.

2. $mn = nm$.

ეს არის გამრავლების კომუტაციურობის კანონი.

3. $m(n+q) = mn+nq$.

ეს ტოლობა წარმოადგენს გამრავლების დისტრიბუციულობის კანონს.

რიცხვის თავის თავზე გამრავლების შედეგი აღინიშნება a^n სიმბოლოთი, სადაც n მიუთითებს, რამდენჯერ გვხვდება a ნამრავლში. ასე რომ,

$$a^n = \underbrace{a \cdot a \cdot a \ldots a}_{n\text{-ჯერ}}.$$

ამ განმარტებიდან უშუალოდ გამომდინარეობს ტოლობა $a^m \cdot a^n = a^{m+n}$. თუ გვაქვს ტოლობა $m+n=p$, სადაც p და n მოცემულია, მაშინ m ცალსახად განისაზღვრება. m რიცხვის პოვნის ოპერაციას გამოკლება ეწოდება და $m=p-n$. აქედან გამომდინარეობს, რომ $(p-n)+n=p$.

ჩვენ განვიხილეთ შემდეგი ოპერაციები: შეკრება, გამოკლება და გამრავლება. ეს არის ძირითადი ოპერაციები რიცხვთა თეორიაში.

II თ ა ვ ი

§1. მთელ რიცხვთა გაყოფადობის შესახებ

ჩვენ გვაქვს რიცხვითი (Z) მწკრივი

..., —3, —2, —1, 0; 1, 2, 3,... .

ამ რიცხვით მწკრივს აქვს შემდეგი თვისება: ამ მწკრივის რომელიმე ორი რიცხვის ჯამი, სხვაობა და ნამრავლი ისევ ამ მწკრივის რიცხვია. (Z) რიცხვთა ასეთი მწკრივი ქმნის რიცხვთა სისტემას (Zahlensistem).

ვთქვათ, n არის (Z) სისტემის რაიმე რიცხვი. (Z) მწკრივის რიცხვები გავამრავლოთ n-ზე. მივიღებთ ახალ მწკრივს, რომლის რიცხვები (Z) მწკრივის რიცხვებია. ეს იქნება მწკრივი

..., —3n, —2n, —1.n, 0, 1$\cdot n$, 2$\cdot n$, 3$\cdot n$... .

ეს არის (Z) მწკრივის წესიერი ნაწილი, რადგან qn რიცხვიდან $n(q+1)$ რიცხვზე გადასასვლელად qn-ს უნდა მივუმატოთ შემდეგი რიცხვები:

1, 2, 3,..., n—1.

აქედან ვღებულობთ: ვთქვათ, m და n არის (Z) მწკრივის რაიმე ორი რიცხვი. მაშინ m გამოისახება n-ის საშუალებით შემდეგი ფორმულით:

$$m=qn+R, \tag{1}$$

სადაც q არის (Z) მწკრივის რაიმე რიცხვი, ხოლო r არის 0, 1, 2,... n—1 რიცხვებიდან ერთ-ერთი. თუ $r=0$, მაშინ გვაქვს $m=qn$ და ამ-

ბობენ, რომ m არის n-ის ჯერადი. n-ის ყოველ ჯერადს აქვს qn სახე, ამიტომ q რიცხვიც m რიცხვის გამყოფია. q რიცხვს n რიცხვის მიმართ დამატებითი გამყოფი ეწოდება. თუ n რიცხვს განვიხილავთ m რიცხვის გამყოფად, მაშინ q არის m რიცხვის n რიცხვთან შეფარდება და ეს აღინიშნება ასე:

$$q=\frac{m}{n}. \tag{2}$$

იმ შემთხვევაში, როცა m რიცხვი არ არის n რიცხვის ჯერადი, წინა აღნიშვნას აზრი არა აქვს. თუ ჩვენ შევინარჩუნებთ ამ აღნიშვნას მაშინ,როცა m არ არის n-ის ჯერადი, $\frac{m}{n}$ გამოსახულებას ეწოდება წილადი. ვნახოთ, როგორ უნდა გავიგოთ წილადების შეკრება, გამოკლება და გამრავლება. ვთქვათ, გვაქვს ორი წილადი $\frac{m}{n}$ და $\frac{m'}{n'}$, $m=nq+r$ (3), $m'=q'n'+r'$(4), q', q, n, n' (Z) მწკრივის რიცხვებია, $r=0, 1, \ldots, n-1$, $r'=0, 1, \ldots, n'-1$, მაშინ

$$mn'\pm m'n=q''nn'+\omega \tag{5}$$

$$rn'\pm r'n=knn'+\omega, \quad q''=q\pm q'+k, \quad \omega=0, 1, 2,\ldots, nn'-1.$$

რადგან (3) და (4) შეესაბამება $\frac{m}{n}$ და $\frac{m'}{n'}$, ხოლო (5) შეესაბამება $\frac{mn'\pm m'n}{nn'}$ წილადს.

თუ $r=r'=0$, მაშინ $\frac{m}{n}=q$, $\frac{m'}{n'}=q'$, $k=0$ და ე. ი. $\omega=0$. მივიღებთ $\frac{mn'\pm m'n}{nn'}=q''=q\pm q'$. მაშასადამე,

$$\frac{mn'\pm m'n}{nn'}=\frac{m}{n}\pm\frac{m'}{n'} \tag{6}$$

(6) ტოლობა განსაზღვრავს $\frac{m}{n}$ და $\frac{m'}{n'}$ წილადების ჯამს და სხვაობას.

ორი $\frac{m}{n}$ და $\frac{m'}{n'}$ წილადების ნამრავლი განვსაზღვროთ ტოლობიდან

$$\frac{mm'}{nn'}=\frac{m}{n}\cdot\frac{m'}{n'}.$$

ავიღოთ $m=nq+r$ ტოლობა. თუ $r\neq 0$, მაშინ q არის უდიდესი მთელი რიცხვი, რომელიც მოთავსდება $\frac{m}{n}$ წილადში. r რიცხვს ნაშთი ეწოდება. $\frac{m}{n}$ წილადში მოთავსებული უდიდესი მთელი რიცხვი Legendre-მა აღნიშნა $E\left(\frac{m}{n}\right)$ (Entier). აქედან

$$E\left(\frac{m}{n}\right)=q.$$

ფუნქციონალური თანაფარდობა $E\left(\frac{m}{n}\right)=q$ გულისხმობს, რომ არგუმენტი არის დადებითი რიცხვი. Ganss-მა განავრცო ეს აღნიშვნა უარყოფითი არგუმენტისათვის. მან აღნიშნა X-ის შესაბამისი სიდიდე $[x]$—ით. სამართლიანია უტოლობა

$$[x]\leqslant x\leqslant[x]+1.$$

2. რაიმე რიცხვის გამყოფების განხილვის დროს საკმარისია განვიხილოთ დადებითი გამყოფები. თუ გვაქვს ორი m და m' რიცხვი, $m=qn$, $m'=q'n$. მაშინ n არის m და m' რიცხვების საერთო გამყოფი. თუ ორი რიცხვის საერთო გამყოფი მხოლოდ 1-ია, მაშინ ამ რიცხვებს თანამარტივი ეწოდება. m რიცხვის m-ისაგან განსხვავებული ნებისმიერი გამყოფი m-ზე ნაკლებია.

ვთქვათ, m და m' ორი რიცხვია და $m<m'$. ამ რიცხვთა საერთო გამყოფები აუცილებლად $[1, 2, 3,\ldots, m]$ მონაკვეთზე არის მოთავსებული. რადგან m სასრული რიცხვია, ამიტომ m და m' რიცხვების

საერთო გამყოფებს შორის მოიძებნება უდიდესი,; ვთქვათ, ეს არის δ. მაშინ $m=\delta\mu$, $m'=\delta\mu'$.

δ რიცხვს ეწოდება m და m' რიცხვების უდიდესი საერთო გამყოფი. ცხადია, μ და μ' რიცხვები თანამარტივი იქნება.

ვთქვათ, მოცემულია (Z) სისტემა

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

გავამრავლოთ ეს რიცხვები n-ზე, მივიღებთ ახალ მწკრივს:

$$\ldots, -3n, -2n, -1\cdot n, 0, 1\cdot n, 2-n, 3\cdot n, \ldots$$

უკანასკნელი მწკრივი მიიღება (Z) მწკრივისგან და აქვს შემდეგი შესანიშნავი თვისება: ამ მწკრივის ორი რომელიმე რიცხვის ჯამი და სხვაობა არის ისევ ამ წკრივის რიცხვი. ასეთ შემთხვევაში ამბობენ, რომ ასეთი რიცხვები ეკუთვნის გარკვეულ მოდულს ან ეს რიცხვები თვითონ ქმნიან მოდულს.

ავიღოთ (Z) მწკრივი. ვთქვათ m არის (Z) მწკრივის რიცხვი, რომელიც გარკვეულ M მოდულს ეკუთვნის. თუ m არ არის უმცირესი იმ რიცხვთა შორის, რომლებიც M მოდულს ეკუთვნის, მაშინ $[1, 2, 3, \ldots, m]$ მონაკვეთზე აუცილებლად იარსებებს უმცირესი რიცხვი, რომელიც m-ზე ნაკლებია და M მოდულს ეკუთვნის. ვთქვათ, ეს რიცხვი არის n. მაშინ M მოდულის ყველა რიცხვი ჩაიწერება zn ფორმით, სადაც z არის (Z) მწკრივის რაიმე რიცხვი.

თ ე ო რ ე მ ა I. ყველა რიცხვი, რომელიც ერთსა და იმავე მოდულს ეკუთვნის, ჩაიწერება nz ფორმულით, სადაც z არის (Z) მწკრივის რაიმე რიცხვი, ხოლო n ამ მოდულის კუთვნილი უმცირესი დადებითი რიცხვია.

თ ე ო რ ე მ ა II. $ax+by$ სახის რიცხვების სიმრავლე (x და y (Z) მწკრივის რიცხვებია) ეკუთვნის δz მოდულს, სადაც δ არის a და b რიცხვების უდიდესი საერთო გამყოფი. δz მოდულის რიცხვები ax და by მოდულების უდიდესი საერთო გამყოფებია.

თ ე ო რ ე მ ა III. თუ δ არის a და b რიცხვების უდიდესი საერთო გამყოფი, მაშინ მოიძებნება ξ და η რიცხვები ისეთი, რომ $a\xi+b\eta=\delta$.

თ ე ო რ ე მ ა IV. a და b რიცხვების ყოველი საერთო გამყოფი ამ რიცხვების უდიდესი საერთო გამყოფის გამყოფს წარმოადგენს.

თ ე ო რ ე მ ა V. თუ a და b თანამარტივი რიცხვებია, მაშინ მოიძებნება რიცხვთა ξ და η წყვილი ისეთი, რომ $a\xi+b\eta=1$.

თ ე ო რ ე მ ა VI. თუ a და b თანამარტივი რიცხვებია და ac ნამრავლი იყოფა b-ზე, მაშინ c გაიყოფა b-ზე.

თუ a და b თანამარტივი რიცხვებია, მაშინ ac ნამრავლს და b რიცხვს ექნება საერთო გამყოფი, (1-სგან განსხვავებული) მხოლოდ მაშინ, როცა c და b რიცხვები თანამარტივი არ არის.

თ ე ო რ ე მ ა VII. თუ a და c რიცხვები თანამარტივია b რიცხვთან, მაშინ ac ნამრავლი და b თანამარტივია.

აქამდე ჩვენ ვპოულობდით ორი რიცხვის უდიდეს საერთო გამყოფს. თურმე, შესაძლებელია მსგავსი მსჯელობით ვიპოვოთ სამი და მეტი რაოდენობის რიცხვთა უდიდესი საერთო გამყოფი. უდიდესი საერთო გამყოფის თვისებები ამ დროს ზუსტად ისეთია, როგორც ორი რიცხვის შემთხვევაში.

ვთქვათ, მაგალითად, m, n, p, q მოცემული რიცხვებია, Δ—მათი უდიდესი საერთო გამყოფი, მაშინ გვექნება:

$$m=m'\Delta, \quad n=n'\Delta \quad p=p'\Delta, \quad q=q'\cdot\Delta$$

m', n', p', q' რიცხვები თანამარტივი იქნება. ე. ი. მათი საერთო გამყოფია მხოლოდ ერთი. თუმცა, ერთმანეთს შორის (წყვილი, სამ-სამად) ისინი შეიძლება არც იყოს თანამარტივი.

§ 3. ვთქვათ, m, n და p სამი რიცხვია, Δ—მათი უდიდესი საერთო გამყოფი. მაშინ

$$m=\Delta m', \quad n=\Delta n', \quad p=\Delta p'.$$

შემდეგ დავუშვათ, რომ m'', n'' და p'' წარმოადგენს (n', p'), (m', p') და (m', n') წყვილების უდიდეს საერთო გამყოფებს შესაბამისად. მაშინ აღმოჩნდება, რომ m, n და p შეიძლება ასე წარმოვადგინოთ:

$$m=\Delta\mu' n'' p''; \quad n=\Delta\nu' m'' p'', \quad p=\Delta\pi' m'' n''.$$

m, n და p სამი რიცხვის ასეთ წარმოდგენას ამ რიცხვების Δ უდიდესი საერთო გამყოფისა და m'', n'', p'', μ', k', π' ნამრავლად ეწოდება (Dedekind) „Die Zerlegung dieselben in ihre Kerne".

§ 4. ვთქვათ, m და m' ორი მოცემული რიცხვია. ყოველ მესამე რიცხვს, რომელიც m და m' რიცხვების ჯერადია, ეწოდება მათი საერთო ჯერადი. m და m' რიცხვების საერთო ჯერადებს შორის უმცირესს მათი უმცირესი საერთო ჯერადი ეწოდება. ცხადია, უმცირესი სა-

ერთო ჯერადი უდრის $\frac{mm'}{\delta}$, სადაც δ არის m და m' რიცხვების უდი-

დესი საერთო გამყოფი. იმ შემთხვევაში, როცა ეს რიცხვები თანამარტივია, მაშინ $\delta=1$-ს და უმცირესი საერთო ჯერადი მოცემული რიცხვების ნამრავლის ტოლია. ორი რიცხვის უმცირესი საერთო ჯერადის შესახებ ნათქვამი შეიძლება განვავრცოთ რიცხვთა მეტ რაოდენობაზე. ვთქვათ, გვაქვს ν რიცხვი: m, n, p, q,..., r. როგორ ვიპოვოთ მათი უმცირესი საერთო ჯერადი? განვიხილოთ პირველი (m, n) წყვილი და მათი უმცირესი საერთო ჯერადი იყოს μ. ახლა m, n, p, q, ..., r რიცხვების უმცირესი საერთო ჯერადის პოვნა დაიყვანება $\nu-1$ რიცხვის μ, p, q, ..., r უმცირესი საერთო ჯერადის პოვნაზე. ვთქვათ, M არის მოცემული ν რიცხვის უმცირესი საერთო ჯერადი. მაშინ, ცხადია, რომ ამ რიცხვების ნებისმიერი ჯერადი იქნება M რიცხვის ჯერადი. თუ მოცემულია წყვილ-წყვილად თანამარტივ რიცხვთა სისტემა, მაშინ მათი უმცირესი საერთო ჯერადი ამ რიცხვების ნამრავლის ტოლი იქნება.

§ 5. დადებითი მთელი რიცხვები არსებობს დაშლადი და დაუშლადი. პირველადი * p რიცხვი გავიგოთ როგორც რიცხვი შემდეგი თვისებით: ორი a და b რიცხვების ნამრავლი მხოლოდ მაშინ იყოფა p-ზე, თუ ან a იყოფა p-ზე, ან b.

თ ე ო რ ე მ ა I. პირველადი და დაუშლელი რიცხვები ერთმანეთის იგივურია.

თ ე ო რ ე მ ა II. ვთქვათ, m რაიმე შედგენილი რიცხვია, მაშინ ის შეიძლება წარმოვადგინოთ შემდეგი ნამრავლის სახით

$$m=p_1\cdot p_2\cdot p_3\cdots p_{\nu-1}\cdot p_\nu\,, \tag{7}$$

სადაც p_1, p_2,..., $p_{\nu-1}$, $p\nu$ პირველადი რიცხვებია.

თ ე ო რ ე მ ა III. თუ m შედგენილი რიცხვია, მაშინ არსებობს მე-(7) დაშლა და ის ერთადერთია.

რადგან p ფაქტორი მე-(7) დაშლაში შეიძლება რამდენჯერმე შეგვხვდეს, ამიტომ m რიცხვის მამრავლებად დაშლის ყველაზე ზოგადი სახე ასეთია:

---

* პირველადი რიცხვი, თანამედროვე ტერმინოლოგიით, მარტივი რიცხვი (მთარგ. შენიშვნა).

$$m = p^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}} . \qquad (8)$$

§ 6. თ ე ო რ ე მ ა I. პირველადი რიცხვების სიმრავლე უსასრულოა.

თ ე ო რ ე მ ა II. თუ $m>1$, a და b მთელი დადებითი რიცხვებია, $p>2$, p პირველადი რიცხვია, მაშინ განტოლებას

$$2 \cdot 3 \cdot 5 \cdot \dots \cdot p = a^m + b^m$$

ამონახსნი არა აქვს. ეს თეორემა გამომდინარეობს ასეთი თეორემიდან: გამოსახულება $\alpha^q - \beta^q$, სადაც α და β მთელი რიცხვებია, ხოლო q პირველადი რიცხვია, ან q-სთან თანამარტივია, ან q^2-ზე იყოფა.

§ 7. ვთქვათ, გვაქვს შედგენილი m რიცხვი. როგორც ცნობილია, ეს რიცხვი შეიძლება წარმოვადგინოთ შემდეგი ნამრავლის სახით:

$$m = p^{\alpha} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}}$$

($p, p_1, p_2 \cdots p_{k-1}$ პირველადი რიცხვებია). ვთქვათ, n არის m რიცხვის რაიმე გამყოფი, ისე, რომ $m = nq$. მაშინ, ცხადია, n რიცხვს აქვს სახე:

$$n = p^{\alpha} p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}} , \qquad (9)$$

სადაც $a \geqslant \alpha_1$, $a_1 \geqslant \alpha_1, \dots, a_{k-1} \geqslant \alpha_{k-1}$.

m რიცხვის ყველა გამყოფს მივიღებთ, თუ მე-(9) ფორმულაში $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ არის რაიმე რიცხვები შემდეგი მწკრივიდან:

$$\begin{cases} \alpha: & 0,1,2,3, \dots, a \\ \alpha_1: & 0,1,2,3, \dots, a_1 \\ \alpha_2: & 0,1,2,3, \dots, a_2 \\ \alpha_{k-1}: & 0,1,2,3, \dots, a_{k-1} \end{cases} \qquad (10)$$

$n(\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1})$ სახის რიცხვების ერთობლიობა, სადაც $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1}$ ღებულობს ყველა შესაძლებელ მნიშვნელობას (10)-დან არის m რიცხვის ყველა გამყოფთა სიმრავლე.

თ ე ო რ ე მ ა I. $m = p^{\alpha} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}}$ სახის რიცხვის ყველა განსხვავებულ გამყოფთა რაოდენობა უდრის

$$(1+a)\,(1+a_1)\,(1+a_2) \dots (1+a_{k-1})$$

ნამრავლს. ეს რიცხვი $t(m)$ ფუნქციონალური ნიშნით აღინიშნება, ე. ი.

$$t(m)=(1+a)\ (1+a_1)\ (1+a_2)\cdots(1+a_{k-1}).$$

ჩვენ ვხედავთ, რომ $t(m)$ დამოკიდებული არ არის m რიცხვის პირველად გამყოფებზე. ის მხოლოდ $a,\ a_1,\ a_2,\ldots,\ a_{k-1}$ ხარისხებზე არის დამოკიდებული. ეს ხარისხები კი მიუთითებს, რამდენჯერ მეორდება ყოველი პირველადი რიცხვი m-ის დაშლაში.

თ ე ო რ ე მ ა II. მოცემული m რიცხვის ყველა გამყოფის ჯამი აღინიშნება $S(m)$ სიმბოლოთი და შემდეგი ნამრავლის ტოლია:

$$\frac{p^{a+1}-1}{p-1}\cdot\frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_{k-1}^{a_{k-1}+1}-1}{p_{k-1}-1}=S(m).$$

ეს ჯამი დამოკიდებულია პირველადი $p,\ p_1,\ p_2,\ \ldots,\ p_{k-1}$ ფაქტორებისაგან და იმ რიცხვებისაგან, რომლებიც მიუთითებენ, რამდენჯერ მეორდება პირველადი გამყოფები ნამრავლში

$$m=p^a\cdot p_1^{a_1}\cdot p_2^{a_2}\cdots p_{k-1}^{a_{k-1}}.$$

თ ე ო რ ე მ ა III. ამ გამყოფთა n-ური ხარისხების ჯამი ტოლია:

$$S_n(m)=\frac{p^{n(a+1)}-1}{p-1}\cdot\frac{p_1^{n(a_1+1)}-1}{p_1-1}\cdots\frac{p_{k-1}^{n(a_{k-1}+1)}-1}{p_{k-1}-1}.$$

თ ე ო რ ე მ ა IV. თუ m არ არის რაიმე რიცხვის კვადრატი, მაშინ მისი გამყოფთა რაოდენობა ლუწი 2λ რიცხვია; თუ m არის რაიმე რიცხვის კვადრატი, მაშინ მისი გამყოფთა რაოდენობა კენტი $2\lambda+1$ რიცხვია.

თ ე ო რ ე მ ა V. ვთქვათ, $m=qn$, მაშინ $m=nq$-ის ν-თი აღვნიშნოთ რიცხვი, რომელიც მიუთითებს, რამდენი არსებობს m რიცხვის ორ ფაქტორად დაშლა. ν ტოლია ან $\lambda+1$ ან λ-სი, იმის მიხედვით, m კვადრატია თუ არ არის კვადრატი. ე. ი. $\nu=\frac{1}{2}\ (t(m)+1)$ ან $\frac{1}{2}\ t(m)$.

თ ე ო რ ე მ ა VI. m რიცხვის ორი თანამარტივი ფაქტორის ნამ-

რაველად წარმოდგენათა რაოდენობა აღვნიშნოთ μ-თი, მაშინ $\mu=2^{k-1}$, სადაც k არის μ რიცხვის პირველადი გამყოფების რაოდენობა. მაშასადამე, ეს რიცხვი სრულებით არაა დამოკიდებული a, a_1, a_2, ..., a_{k-1} ხარისხის მაჩვენებლებზე. ამიტომ

$$m=p^a\cdot p_1^{a_1}\cdot p_2^{a_2}\dots p_{k-1}^{a_{k-1}} \quad \text{და} \quad m'=p\cdot p_1p_2\dots p_{k-1}$$

ორი რიცხვისათვის $\mu=\mu^1$.

§ 7. ვთქვათ, მოცემულია რამდენიმე რიცხვი m, m', m'',.. დავუშვათ, ჩვენთვის ცნობილია ამ რიცხვების პირველად ფაქტორებად დაშლა, მაშინ შეიძლება ვიპოვოთ ამ რიცხვების D უდიდესი საერთო გამყოფი და უმცირესი საერთო ჯერადი (უფრო სწორად, D და V-ს პირველად ფაქტორებად დაშლა).

$$D=p^\nu\cdot p_1^{\nu_1}\cdot p_2^{\nu_2}\dots,$$

სადაც p შედის m, m', m'',... რიცხვების დაშლაში a, a', a'', ... ხარისხებით შესაბამისად, ხოლო ν არის a, a', a'',... რიცხვებს შორის უმცირესი. შესაბამისად, იგივე ითქმის ν_1, ν_2,... რიცხვების შესახებ.

ასევე ვპოულობთ

$$V=p^\varepsilon\cdot p_1^{\varepsilon_1}\cdot p_2^{\varepsilon_2}\dots,$$

სადაც ε არის უდიდესი a, a', a'',... რიცხვებს შორის. ასეთივე გზით ვპოულობთ ε_1, ε_2,... რიცხვებს.

ვთქვათ, ახლა მოცემულია ორი რიცხვი m და m'. მათი უმცირესი საერთო ჯერადი $V=p^\varepsilon\cdot p_1^{\varepsilon_1}\cdot p_2^{\nu_2}\dots$ ხარისხები p^ε, $p_1^{\varepsilon_1}$,..., ან m რიცხვის დაშლაში შედის ან m'-ის დაშლაში ან ორივეში. ამიტომ V შეიძლება წარმოვადგინოთ μ და μ' ფაქტორების ნამრავლად ისე, რომ μ იყოს m-ის დაშლაში, ხოლო μ' კი m'-ის დაშლაში.

§ 8. ვთქვათ, მოცემულია ფაქტორიალი

$$n!=1\cdot2\cdot3\cdot4\cdots n.$$

ასეთი ნამრავლი იშლება პირველად ფაქტორებად, რომლებიც [1, 2, 3,..., n] მონაკვეთს ეკუთვნის. ვთქვათ, p ამ მონაკვეთის პირველადი რიცხვია. მაშინ ν ხარისხი, რომლითაც p შედის $n!$ რიცხვის პირველად მამრავლებად დაშლაში, ტოლია:

$$\nu = \left[\frac{n}{p}\right] + \left[\frac{n'}{p}\right] + \left[\frac{n''}{p}\right] + \ldots + \left[\frac{n^{i-1}}{p}\right],$$

სადაც

$$n' = \left[\frac{n}{p}\right], \qquad n'' = \left[\frac{n'}{p}\right], \ldots$$

ადგილი აქვს ლემას, რომელიც გვეუბნება: თუ n' არის $\frac{n}{a}$ წილადში მოთავსებული უდიდესი მთელი რიცხვი, n'' არის $\frac{n'}{b}$ წილადში მოთავსებული უდიდესი მთელი რიცხვი, მაშინ n'' აგრეთვე არის $\frac{n}{ab}$ წილადში მოთავსებული უდიდესი მთელი რიცხვი.

ამ ლემის თანახმად,

$$\nu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

ასეთი აღნიშვნა დასაშვებია, რადგან ამ მწკრივის წევრები, გარკვეული ადგილიდან დაწყებული, ნულის ტოლი იქნება.

§ 9. ვთქვათ, p და n რაიმე მთელი დადებითი რიცხვებია. ავიყვანოთ p თანამიმდევრობით 1, 2, 3,... ხარისხებში. მაშინ მივაღწევთ რაღაც h ხარისხს, ისეთს, რომ

$$p^h \leqslant n < p^{h+1}$$

p^h და p^{h+1} ხარისხებს შორის არის რიცხვები $2p^h$, $3p^h$,... $(p-1)p^h$, ამიტომ არსებობს ისეთი a რიცხვი, რომ

$$ap^h \leqslant n < (a+1)p^h$$

დავუშვათ, $n = ap^h + n'$, სადაც $0 \leqslant n' < p^h$.

ასე მოვიქცეთ n' რიცხვის მიმართაც. მივიღებთ ასეთ საბოლოო შედეგს:

$$n = ap^h + a_1 p^{h-1} + a_2 p^{h-2} + \ldots + a_{h-1} p + a_h,$$

სადაც კოეფიციენტები p-ზე ნაკლები მთელი რიცხვებია. n რიცხვის ეს წარმოდგენა p ფუძით გამოიყენება თვლის ათობით სისტემაში

$p=10$ კერძო შემთხვევის დროს. კოეფიციენტები a, a_1, a_2, ..., a_h ამ შემთხვევაში არის მოცემული რიცხვის ციფრები. მაშასადამე, თუ ჩვენ გვაქვს მოცემული რაიმე რიცხვი, მაშინ ერთი ფუძის დროს ვღებულობთ კოეფიციენტთა ერთ სისტემას, მეორე ფუძის დროს—მეორე სისტემას. ამდენად, საინტერესოა, როგორ შეიცვლება კოეფიციენტთა სისტემა, როცა ერთი ფუძიდან მეორე ფუძეზე გადავალთ. თანაც ამ დროს ადვილად ვიპოვით ინვარიანტულ თვისებებს, ე. ი. თვისებებს, რომლებიც ფუძისაგან არ არის დამოკიდებული.

განვიხილოთ ორი კერძო შემთხვევა:

I. $p=2$. მაშინ a_l ციფრები ან 0-ია ან 1. ამიტომ ყოველი დადებითი მთელი რიცხვი, რომელიც ნაკლებია 2^{h+1}, შეიძლება აღნიშნული გზით წარმოვადგინოთ როგორც 2^h, 2^{h-1}, ..., 2, 1 ხარისხების ჯამი, ციფრთა ჯამს $a+a_1+a_2+\ldots+a_h$ მოცემული რიცხვის ხარისხი ეწოდება.

II. $p=3$. ყოველი დადებითი მთელი რიცხვი $<3^{h+1}$ შეიძლება წარმოვადგინოთ როგორც 3^h, 3^{h-1},..., 3, 1 ხარისხების ჯამი გარკვეული კოეფიციენტებით.

ზემოთ მივიღეთ:

$$n=ap^h+a_1p^{h-1}+a_2p^{h-2}+\ldots+a_{h-1}p+a_h$$

ვთქვათ, p პირველადი რიცხვია, მაშინ

$$\left[\frac{n}{p}\right]=ap^{h-1}+a_1p^{h-2}+\ldots+a_{h-1},$$

$$\left[\frac{n}{p^2}\right]=ap^{h-2}+a_1p^{h-3}+\ldots+a_{h-2},$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\left[\frac{n}{p^h}\right]=a.$$

შევკრიბოთ ეს ტოლობები. მარცხენა მხარეში მივიღებთ $\sum_{l=1}^{\infty}\left[\frac{n}{p^l}\right]=$ $=\nu$ ჯამს, რომელზედაც საუბარი გვქონდა მე-8 პარაგრაფში, ე. ი.

$$\nu = a\frac{p^h-1}{p-1} + a_1\frac{p^{h-1}-1}{p-1} + \dots + a_{h-1}\frac{p-1}{p-1} .$$

ან

$$\nu = \frac{n-(a_1+a_2+\dots+a_{h-1}+a_h)}{p-1} .$$

ეს არის Legendre-ის ფორმულა. ამ ფორმულის უმარტივესი შემთხვევა მიიღება, როცა $p=2$.

§ 10. ცნობილია, რომ

$$(x+y+\dots)^m = \sum C^m_{q,r,s,\dots} x^q y^r z^s \dots ,$$

სადაც

$$C^m_{q,r,s,\dots} = \frac{m!}{q!\,r!\,s!\dots} , \quad q+r+s\dots = m .$$

წინა პარაგრაფებში ნათქვამის საფუძველზე შეიძლება ვაჩვენოთ, რომ ეს ბინომური კოეფიციენტები მთელი რიცხვებია. კერძოდ, თუ გვაქვს

$$(x+y)^m = \Sigma C_{q,r} x^q \cdot y^r, \quad \text{სადაც} \quad q+r=m,$$

მაშინ ბინომური კოეფიციენტები

$$\frac{m!}{q!\,r!} = \frac{1\cdot 2\cdot 3\dots(q+r)}{1\cdot 2\cdot 3\dots q\cdot 1\cdot 2\cdot 3\dots r}$$

მთელი რიცხვებია, ანუ

$$\frac{(q+1)(q+2)\dots(q+r)}{1\cdot 2\dots r}$$

არის მთელი რიცხვი, ე. ი. ნებისმიერი r მომდევნო რიცხვის ნამრავლი იყოფა პირველი r რიცხვის ნამრავლზე.

თუ ავიღებთ $(x+y)^p$ დაშლას, სადაც p პირველადი რიცხვია,

$$(x+y)^p = x^p + \frac{p}{1}x^{p-1}y + \frac{p(p-1)}{1\cdot 2}x^{p-2}y^2 + \dots + \frac{p}{1}xy^{p-1} + y^p ,$$

მაშინ ყველა კოეფიციენტი, პირველი და უკანასკნელის გარდა, გაიყოფა p-ზე.

$$C_q^{m,r,s\cdots}=\frac{m!}{q!\,r!\,s!\ldots}\ .$$

დავუშვათ, $q=r=s=\ldots=q$, მაშინ მივიღებთ, რომ $m=nq$ და

$$C_q^{m,q,\cdots}=\frac{(nq)!}{(q!)^n}\ .$$

მთელი რიცხვია. აღმოჩნდა, რომ არა მარტო წინა გამოსახულება, არამედ აგრეთვე $\dfrac{(nq)!}{n!(q!)^n}$ არის მთელი რიცხვი.

განვიხილოთ შეფარდება $\dfrac{(nq)!}{((n-1)q)!q!}$. ეს შეფარდება მთელი რიცხვია.

შეკვეცის შემდეგ იგი მიიღებს სახეს

$$\frac{((n-1)q+1)((n-1)q+2)((n-1)q+3)\ldots((n-1)q+q-1)}{1\cdot 2\cdot 3\ldots q}\ .$$

ამ ნამრავლის პირველი ფაქტორი მთელი რიცხვია. აღვნიშნოთ ეს მთელი რიცხვი q_n-ით. შემდეგ დავუშვებთ $n=n-1,\ n-2,\ldots,2,1$ და მივიღებთ მთელ რიცხვებს, რომლებსაც აღვნიშნავთ $q_{n-1},\ q_{n-2},\ldots,\ q_1\ (q_1=1)$. აღმოჩნდება, რომ

$$\frac{(nq)!}{n!(q!)^n}=q_1q_2\cdots q_n\ .$$

ეს ფორმულა გვაძლევს Weill-ის თეორემას. D. Andra-მ შემდეგ დაამტკიცა, რომ $\dfrac{(nq)!}{(q!)^n}$ იყოფა არა მარტო $n!$-ზე, არამედ $(n!)^k$-ზე, სადაც k არის კოეფიციენტთა ჯამი q რიცხვის p პირველადი ფუძით წარმოდგენაში.

Weill-ის თეორემა აქედან მიიღება როგორც კერძო შემთხვევა. ასე რომ, თუ მაგალითად, მოცემული q რიცხვის წარმოდგენას p პირველადი ფუძით აქვს სახე

$$q=\alpha+\beta p+\gamma p^2+\delta p^3+\cdots,$$

მაშინ

$$z \geqslant (\alpha+\beta+\gamma+\delta+\cdots)p(n), \qquad (11)$$

სადაც $\alpha+\beta+\gamma+\delta+\cdots=k$ არის მოცემული რიცხვის ხარისხი მოცემული ფუძის დროს, $p(n)$ არის რიცხვი, რომელიც მიუთითებს რამდენჯერ გვხვდება p რიცხვი $n!$-ის გაშლაში, ხოლო z—რამდენჯერ გვხვდება p შეფარდებაში $\frac{(nq)!}{(q!)^n}$. მე-(11) ტოლობიდან გამომდინარეობს, რომ Andre-ს დებულება სწორია.

§ 12. ვთქვათ, გვაქვს q და n რიცხვები. მათი წარმოდგენა p ფუძით ასეთია

$$q=\mu p^h+\mu_1 p^{h-1}+\cdots+\mu_h,$$
$$n=\nu p^h+\nu_1 p^{h-1}+\cdots+\nu^h,$$

სადაც კოეფიციენტები p-ზე ნაკლები რიცხვებია. შევკრიბოთ q და n, მივიღებთ დაშლას

$$q+n=\delta p^{h+1}+\delta p^h+\delta_1 p^{h-1}+\cdots+\delta_n.$$

გვექნება შემდეგი თეორემა I. q და n ორი რიცხვის ციფრთა ჯამი $q+n$ რიცხვის ციფრთა ჯამისაგან მიიღება p—1 რიცხვის ნამრავლით იმ ერთეულთა რაოდენობაზე, რომლებიც p-ს უფრო დაბალი ხარისხიდან უფრო მაღალ ხარისხზე გადადის (p ფუძეა).

თუ q და n რიცხვებს გავამრავლებთ, მივიღებთ შემდეგ

თ ე ო რ ე მ ა II-ს. ორი მოცემული რიცხვის ციფრთა ნამრავლი განსხვავდება ნამრავლის ციფრთა ჯამისაგან ერთეულთა რიცხვით, რომელიც ტოლია $(p-1)E$, ანუ

$$S(q)S(n)=S(qn)+(p-1)E. \qquad (12)$$

$S(x)$ სიმბოლოთი აღნიშნულია ციფრთა ჯამი რაიმე ფუძის დროს.

დავუბრუნდეთ Legendre-ის ფორმულას. თუ n რაიმე მთელი რიცხვია, p—პირველადი, ν-თი აღნიშნულია რიცხვი, რომელიც მიუთითებს, რა ხარისხით შედის $n!$-ში p, მაშინ

$$\nu=\frac{n-(a+a_1+a_2+\cdots+a_h)}{p-1},$$

სადაც a, a_1, a_2,.., a_h მოცემული რიცხვის კოეფიციენტებია p ფუძით გაშლაში.

გამოვიყენოთ ეს ფორმულა $\frac{(nq)!}{(q!)^n}$ შეფარდების მიმართ. Legendre-ის ფორმულით p მოთავსებულია ამ ნამრავლში ν-ჯერ.

თუ განვიხილავთ შეფარდებას $\frac{(nq)!}{(n!)^\lambda (q!)^n}$, მაშინ,

$$\nu' = \frac{nS(q) - S(nq)}{p-1} - \lambda\nu', \quad \text{სადაც} \quad \nu' = \frac{n - S(n)}{n-1}.$$

მე-(12) ტოლობის საფუძველზე,

$$\nu = (S(q) - \lambda)\nu' + E,$$

ან, როცა $E = \nu'\varepsilon + \rho$, $0 \leqslant \rho < \nu'$, მაშინ

$$\nu = (S(q) + \varepsilon - \lambda)\nu' + \rho.$$

წინა შეფარდებაში ჩვენ λ ნებისმიერი ავირჩიეთ, ახლა, თუ λ-ს ისე ავირჩევთ, რომ $S(q) + \varepsilon - \lambda < 0$, ან $\lambda > S(q) + \varepsilon$, მაშინ ეს შეფარდება აღარ იქნება მთელი რიცხვი. ამიტომ ეს შეფარდება მთელი რომ იყოს, აუცილებელია, შესრულდეს შემდეგი უტოლობა:

$$S(q) + \varepsilon - \lambda > 0.$$

§ 13. თ ე ო რ ე მ ა I (Catalan). ვთქვათ, m და n თანამარტივი მთელი და დადებითი რიცხვებია. მაშინ შეფარდება

$$Q = \frac{(m+n-1)!}{m!\,n!}$$

მთელი რიცხვია.

თ ე ო რ ე მ ა II (Catalan).

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

მთელი რიცხვია.

II თეორემა უფრო ზოგადი თეორემის კერძო შემთხვევას წარმოადგენს: შეფარდება

$$\frac{(km_1)!(km_2)!\ldots(km_h)!}{m_1!m_2!\ldots m_h!(m_1+m_2+\ldots+m_h)!}$$

მთელი რიცხვია, როცა $k \geqslant 2$.

III თ ა ვ ი

შედარებათა შესახებ

§ I. ზემოთ მითითებული იყო, რომ თუ მოცემულია ორი მთელი m და n რიცხვი, მაშინ ისინი ყოველთვის დაკავშირებულია შემდეგი ტოლობით:

$$m=qn+r, \quad 0\leqslant r\leqslant n-1.$$

თუ $r=0$, მაშინ m რიცხვი ეკუთვნის ($n\varepsilon$) მოდულს. ვთქვათ, m' და m'' ორი მთელი რიცხვია, მაშინ $m'=q'n+r'$, $m''=q''n+r''$. მათი სხვაობა—$m'-m''=(q'-q'')n+(r'-r'')$. თუ $m'-m''$ სხვაობა ($n\varepsilon$) მოდულს ეკუთვნის, მაშინ $r'=r''$; როცა $m'-m''$ არ ეკუთვნის ($n\varepsilon$) მოდულს, მაშინ r' განსხვავებულია r''-ისაგან.

ორ რიცხვს ეწოდება n მოდულით სადარი, თუ ამ რიცხვების სხვაობა ეკუთვნის ($n\varepsilon$) მოდულს. ეს აღინიშნება ასე:

$$m'\equiv m'' \pmod{n}.$$

ორი რიცხვი სადარია ან არ არის სადარი მოცემული მოდულით იმის მიხედვით, ტოლნაშთიანია ეს რიცხვები ამ მოდულით თუ არაა ტოლნაშთიანი.

სადარი რიცხვების განმარტებიდან გამომდინარეობს შემდეგი თეორემები: 1. თუ ორი რიცხვი მესამე რიცხვის სადარია რაიმე მოდულით, მაშინ ეს რიცხვები ერთმანეთის სადარია ამავე მოდულით. II, ისე, როგორც განტოლებაში, შედარებაში წევრები ერთი მხარიდან შეიძლება მეორე მხარეში გადავიტანოთ მოპირდაპირე ნიშნით.

ნათქვამის საფუძველზე, მთელი რიცხვები შეიძლება დავყოთ კლასებად. ერთი კლასის ორი რიცხვი სადარია მოცემული მოდულით, ხო-

ლო სხვადასხვა კლასების რიცხვები არ არის სადარი ამავე მოდულით.

ყოველ კლასს შეიძლება ტოლნაშთიანი ვუწოდოთ და რადგან ყოველი რიცხვი (mod n) უშვებს 0,1, 2,..., n—1 ნაშთებიდან ერთერთს, ამიტომ ნაშთთა კლასების რაოდენობა ზუსტად n-ის ტოლია. ყოველი ასეთი კლასიდან ავირჩიოთ ერთი რიცხვი. მიღებული n რიცხვი ქმნის ნაშთთა სრულ R სისტემას (mod n). ეს რიცხვები, ცხადია, არასადარია mod n. მოცემული a რიცხვის n მოდულით სადარი ნებისმიერი x რიცხვი წარმოიდგინება ასე:

$$x=a—ny.$$

თუ y-ს მივცემთ მთელ მნიშვნელობებს, მაშინ მივიღებთ a რიცხვის n მოდულით სადარ ყველა რიცხვს. ამ რიცხვებს შორის განსაკუთრებით საინტერესოა ორი რიცხვი: I. a რიცხვის n მოდულით სადარი უმცირესი დადებითი რიცხვი და II. უარყოფითი რიცხვი, რომლის აბსოლუტური სიდიდე ყველა სხვა რიცხვის აბსოლუტურ სიდიდეზე ნაკლებია. პირველ რიცხვს ეწოდება უმცირესი დადებითი ნაშთი, მეორე რიცხვს უმცირესი უარყოფითი ნაშთი. თუ ჩვენ ვსაუბრობთ ნაშთთა სრულ სისტემაზე, ცხადია,

$$0,\ 1,\ 2,\ 3,\ldots,\ n—1$$

ასეთი სისტემა არის. n ლუწი რიცხვის შემთხვევაში ნაშთთა სრული სისტემა იქნება აგრეთვე

$$—\frac{n}{2},\ —\frac{n—2}{2},\ldots,—1,\ 0,\ 1,\ 2,\ \ldots,\ \frac{n—2}{2},\ \frac{n}{2};$$

კენტი n-ის შემთხვევაში—

$$—\frac{n—1}{2},\ —\frac{n—3}{3},\ \ldots,\ —2,\ —1,\ 0,\ 1,\ 2,\ \ldots,\ \frac{n—1}{2}.$$

თუ $m'—m''$ ეკუთვნის (nz) მოდულს, ე. ი. n-ის ჯერადია და d არის n-ის გამყოფი, მაშინ $m'—m''$ რიცხვი აგრეთვე ეკუთვნის (dz) მოდულს, ე. ი., თუ

$$m'\equiv m'' \pmod{n},\ d/n,\ \text{მაშინ}\ m'\equiv m'' \pmod{d}.$$

ამიტომ თუ m' ეკუთვნის (dz) მოდულს, მაშინ n მოდულით მისი სადარი ყველა რიცხვიც ეკუთვნის (dz) მოდულს. მაშასადამე, თუ კლასის რომელიმე რიცხვი თანამარტივია n-თან, მაშინ ამ კლასის ყველა რიცხვი n-თან თანამარტივი იქნება. თუ გვაქვს n რიცხვი, მაშინ n მოდულით სადარი ყველა კლასიდან გამოვყოთ ის კლასები, რომლებიც თანამარტივია n-თან და თითოეული ასეთი კლასიდან ავირჩიოთ ერთი წარმომადგენელი. ასე აგებულ სისტემას ეწოდება ნაშთთა დაყვანილი სისტემა (mod n). ნაშთთა დაყვანილ სისტემას მივიღებთ, თუ 0, 1, 2,..., n—1 რიცხვებიდან გამოვყოფთ n-თან თანამარტივ რიცხვებს.

თუ $\varphi(n)$ არის n-თან თანამარტივი n-ზე ნაკლები დადებითი რიცხვების რაოდენობა, მაშინ ნაშთთა ყოველი დაყვანილი სისტემა შედგება $\varphi(n)$ რაოდენობის n მოდულით არასადარი რიცხვისაგან.

§ 2. ვთქვათ, გვაქვს (nz), $(n'z)$,.... მოდულების რიცხვები. რიცხვები, რომლებიც ყველა ამ მოდულს ეკუთვნის, თვითონ ქმნის მოდულს. ამიტომ, თუ N უმცირესი რიცხვია, რომელიც ყველა მოცემულ მოდულს ეკუთვნის, მაშინ ყველა ასეთი რიცხვი ეკუთვნის (Nz) მოდულს. ცხადია, რომ N არის n, n', n'',... რიცხვების უმცირესი საერთო ჯერადი. ამიტომ, თუ $m' \equiv m''$ (mod n), $m' \equiv m''$ (mod n'),... სადაც n, n',... თანამარტივი რიცხვებია, მაშინ $m' \equiv m''$ (mod nn'n'')..

თ ე ო რ ე მ ა 1. თუ $a \equiv b$ (mod n), $a' \equiv b'$ (mod n), მაშინ $aa' \equiv bb'$ (mod n) და $a \pm a' \equiv b \pm b'$ (mod n).

თ ე ო რ ე მ ა II. თუ $ma \equiv mb$ (mod n), m და n თანამარტივი რიცხვებია, მაშინ $a \equiv b$ (mod n); თუ m და n რიცხვების საერთო

გამყოფია d, მაშინ $a \equiv b \left(\text{mod } \frac{m}{d}\right)$.

თ ე ო რ ე მ ა III. თუ $f(x)$ არის X ცვლადის მთელი ფუნქცია

$$f(x) = ax^{\alpha} + a_1 x^{\alpha-1} + a_2 x^{\alpha-2} + \ldots\ldots + a_{\alpha-1} x + a_{\alpha},$$

სადაც a, a_1, a_2, $\cdots$, $a_{\alpha-1}$, a_{α} მთელი რიცხვებია და

$$m' = m'' \text{ (mod n)},$$

მაშინ $f(m') \equiv f(m'')$ (mod n).

§ 3. ვთქვათ, მოცემულია p ფუძით წარმოდგენილი რაიმე რიცხვი:

$$m=ap^h+a_1p^{h-1}+a_2p^{h-2}+\ldots+a_{h-1}\,p+a_h,$$

ამასთან, a, a_1, a_2,..., a_{h-1}, a_h მთელი რიცხვებია. თუ $p\equiv r \pmod n$, მაშინ

$$m\equiv ar^h+a_1r^{h-1}+\cdots+a_{h-1}r+a_h \pmod n. \qquad (1)$$

ამიტომ m იყოფა ან არ იყოფა n-ზე იმის მიხედვით, იყოფა თუ არა n-ზე (1) შედარების მარჯვენა მხარე, კერძოდ, დავუშვათ, $p=n+1$ ან $p=n-1$, მაშინ $p\equiv\pm1\pmod n$ და ამიტომ,

$$m\equiv(a+a_1+\cdots+a_h) \pmod{p-1}$$

და

$$m\equiv((-1)^ha+(-1)^{h-1}\,a_1+\cdots+a_h) \pmod{p+1}$$

ამ შედარებებიდან ვღებულობთ, რომ ათობით სისტემაში ჩაწერილი რიცხვი იყოფა 9-ზე, თუ ამ რიცხვის ციფრთა ჯამი იყოფა 9-ზე; ასევე, ათობით სისტემაში ჩაწერილი რიცხვი იყოფა 11-ზე, როცა ლუწ ადგილებზე მდგომი ციფრთა ჯამისა და კენტ ადგილებზე მდგომი ციფრთა ჯამის სხვაობა იყოფა 11-ზე.

თუ, მაგალითად, $p^h\equiv1\pmod n$, მაშინ (1)-დან გამომდინარეობს შემდეგი შედარება

$$m\equiv(a_h+a_{h-1}p+\cdots+a_{h-k+1}p^{h-1})+(a_{h-k}+a_{h-k+1}p+\cdots+a_{h-2k+1}p^{2k-1})+\cdots \pmod n.$$

თუ $p^h\equiv-1 \pmod n$, მაშინ

$$m\equiv(a_h+a_{h-1}p+\cdots+a_{h-k+1}p^{k-1})-(a_{h-k}+\cdots+a_{h-2k+1}p^{2k-1})+\cdots \pmod n.$$

§ 4. ვთქვათ, გვაქვს მთელი ფუნქცია

$$F(x)=ax^\alpha+a_1x^{\alpha-1}+a_2x^{\alpha-2}+\cdots+a_{\alpha-1}x+a_\alpha.$$

დავსვათ კითხვა: არსებობს თუ არა x, რომელიც აკმაყოფილებს შედარებას

$$f(x) \equiv 0 \pmod{n}. \qquad (2)$$

თუ ასეთი რიცხვი არსებობს, მას ეწოდება მე-(2) შედარების ამონახსნი. ადვილია იმის დანახვა, რომ, თუ m აკმაყოფილებს მე-(2) შედარებას, მაშინ ნებისმიერი m', რომელიც m-ის სადარია n მოდულით, აგრეთვე დააკმაყოფილებს მე-(2) შედარებას. ყველა ეს რიცხვი, თითქოს, ერთი რიცხვის როლს ასრულებს. ამიტომ ვუწოდოთ ყველა ამ რიცხვს მოცემული შედარების ამონახსნი ან შედარების ფესვი. აღვნიშნოთ ეს ასე: მოცემულ მე-(2) შედარებას აქვს ფესვი $x \equiv m \pmod{n}$.

თუ n მოდული პირველადი რიცხვია, მაშინ ადგილი აქვს შემდეგ თეორემას: თუ შედარების მოდული პირველადი რიცხვია, მაშინ შედარების ფესვთა რიცხვი შედარების რიგს (ხარისხს) არ აღემატება (Euler, Lagrange).

§ 5.I. თუ გვაქვს შედარება $ax \equiv c \pmod{n}$, სადაც a და n თანამარტივი რიცხვებია, მაშინ, როგორც უკვე ითქვა, შედარებას მხოლოდ ერთი ფესვი აქვს.

II. თუ ნაშთთა რომელიმე დაყვანილი სისტემის რიცხვებს გავამრავლებთ მოდულთა თანამარტივ a რიცხვზე, მივიღებთ კვლავ ნაშთთა დაყვანილ სისტემას მოცემული მოდულით.

თუ შედარებაში $ax \equiv c \pmod{n}$, a და n რიცხვები თანამარტივი არ არის, მაშინ საქმე სხვაგვარადაა. შედარების ამოხსნადობისათვის აუცილებელია, რომ n და c რიცხვებიც არ იყოს თანამარტივი.

III. ვთქვათ, გვაქვს შედარება $ax \equiv c \pmod{n}$ a, n და c თანამარტივი რიცხვები არ არის. დავუშვათ, a და c რიცხვების უდიდესი საერთო გამყოფი არის d, მაშინ მოცემულ შედარებას აქვს d განსხვავებული ამონახსნი. შედარება $ax \equiv c \pmod{n}$ ნიშნავს, რომ $c - ax$ არის n-ის ჯერადი. ამიტომ შედარება შეგვიძლია გადავწეროთ ასე: $c - ax = ny$. თუ n-ის მაგივრად სიმეტრიის მიზნით ჩავწერთ b-ს, მივიღებთ Diophante-ეს განუზღვრელ განტოლებას

$$ax + by = c. \qquad (3)$$

მაშასადამე, $ax \equiv c \pmod{n}$ შედარების ამოხსნის ამოცანა (3) განტოლების მთელი და დადებითი ამოხსნების პოვნის ტოლფასია.

გამოდიხ, რომ მე-(3) განტოლების ამონახსნი ჩაიწერება ასე:

$$x=\xi+\frac{b}{d}z\,, \qquad (a_x)$$

სადაც ξ არის რაიმე მნიშვნელობა, რომლისთვისაც $c-a\xi$ არის b რიცხვის ჯერადი, მაგ., უდრის $b\eta$-ს და $a\xi+b\eta=c$.
(a_x) ტოლობის საფუძველზე, მივიღებთ

$$y=\eta-\frac{a}{d}z\,. \qquad (a_y)$$

ე. ი. თუ არსებობს მე-(3) განტოლების ორი მთელი ამონახსნი ξ და η, მაშინ ყველა დანარჩენ მთელ ამონახსენს ექნება (a_x) და (a_y) სახე.

თუ გვაქვს განტოლება

$$ax+by=1,$$

სადაც a და b თანამარტივი რიცხვებია, მაშინ ეს განტოლება მთელ რიცხვებში ამოიხსნება, თუ არსებობს $ax\equiv 1 \pmod b$ შედარების ამონახსნი.

ვთქვათ, a' რაიმე რიცხვია, რომელიც აკმაყოფილებს $ax\equiv 1 \pmod b$ შედარებას, მაშინ $aa'\equiv 1 \pmod b$. a' რიცხვს, Euler-ის ტერმინით, ეწოდება „eine associirte Zahl“. ასევე a რიცხვი a'-ის მიმართ არის „assoriirte Zahl“, მაგრამ მას სხვა სახელწოდება აქვს: a რიცხვი a'-ის მიმართ არის „socin“ $\pmod b$.

ეს ასეც ჩაიწერება

$$a'\equiv\frac{1}{a}\pmod b, \qquad a\equiv\frac{1}{a'}\pmod b\,.$$

§ 6. ყველაფერი, რაც ზემოთ ვთქვით, საშუალებას გვაძლევს უკვეცი $\frac{m}{n}$ წილადი დავშალოთ ე. წ. კერძო (partialbinche) წილადებად. თუ $\frac{m}{n}$ მოცემული უკვეცი წილადია და n-ს წარმოვადგენთ ასე: $n=ab$, სადაც a და b თანამარტივი რიცხვებია, მაშინ

$$\frac{m}{n}=\frac{\alpha}{a}+\frac{\beta}{b}+h \qquad (h \text{ მთელია}, \ \alpha<a, \ \beta<b),$$

ამასთან, α და β ნულს არ უდრის და (α, a) და (β, b) წყვილები თანამარტივია.

თუ, საერთოდ, $\frac{m}{n}$-ის მნიშვნელი არის ნამრავლი $n=a\cdot b\cdot c\cdots$ (a, b, c,$\cdots$ თანამარტივი რიცხვებია), მაშინ

$$\frac{m}{n}=\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\cdots+h\,,$$

$\alpha<a$, $\beta<b$, $\gamma<c$, h მთელი რიცხვია. ასეთი წარმოდგენა არის ერთადერთი. თუ ახლა დავუშვებთ, $a=p^l$, $b=q^k$, $c=r^e$,$\cdots$, მაშინ α, β, γ,... რიცხვებს ექნება ფორმა

$$\alpha=\alpha_0+\alpha_1 p+\alpha_2 p^2+\cdots+\alpha_{l-1}p^{l-1};$$
$$\beta=\beta_0+\beta_1 q+\beta_2 q^2+\cdots+\beta_{k-1}q^{k-1};$$
$$\gamma=\gamma_0+\gamma_1 r+\gamma_2 r^2+\cdots+\gamma_{e-1}r^{l-1}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

ამ დაშლებში კოეფიციენტები არაუარყოფითი რიცხვებია და ნაკლებია p, q, r,... რიცხვებზე შესაბამისად. ახლა მივიღებთ:

$$\frac{m}{n}=\frac{m}{p^l q^k r^e\cdots}=\frac{\alpha_0}{p^l}+\frac{\alpha_1}{p^{l-1}}+\cdots+\frac{\alpha_{l-1}}{p}+\frac{\beta_0}{q^k}+$$
$$+\frac{\beta_1}{q^{k-1}}+\cdots+\frac{\beta_{k-1}}{q}+\frac{\gamma_0}{r^e}+\frac{\gamma_1}{r^{e-1}}+\cdots+\frac{\gamma_{e-1}}{r}+\cdots.$$

ეს დაშლა ცნობილია უკვეცი $\frac{m}{n}$ წილადის უმარტივეს წილადებად დაშლის სახელწოდებით. ასეთი დაშლა ერთადერთია. p, q, r,..., ამ წარმოდგენაში პირველადი რიცხვებია.

§ 7. შედარებათა თეორემების მეორე გამოყენება.

ა მ ო ც ა ნ ა:

ვიპოვოთ x რიცხვი, რომელიც მოცემული მოდულების მიმართ გვაძლევს მოცემულ ნაშთებს, ე. ი., ვიპოვოთ ისეთი x, რომელიც ერთდროულად აკმაყოფილებს შემდეგ შედარებებს:

$$x\equiv\alpha\pmod{a},\quad x=\beta\pmod{b},\quad x\equiv\gamma\pmod{c},\ldots$$

პირველი შედარებიდან გვექნება $x=\alpha+ay$; მეორე შედარება მოგვცემს $ay\equiv\beta-\alpha \pmod b$, ანუ $\frac{a}{d}y\equiv\frac{\beta-\alpha}{d}\left(\mod\frac{b}{a}\right)$. უკანასკნელ შედარებას აქვს ამონახსნი $y\equiv\eta\left(\mod\frac{b}{d}\right)$, მაშასადამე, $y=\eta+\frac{b}{d}z$ და ამიტომ $x=\alpha+a\eta+\frac{ab}{d}z$. ეს არის რიცხვი, რომელიც აკმაყოფილებს პირველ ორ შედარებას. თუ გავაგრძელებთ, ვნახავთ, რომ x, რომელიც პირველ სამ შედარებას აკმაყოფილებს, ასეთი სახისაა

$$x=\alpha+a\eta+\frac{ab}{d}\zeta+\frac{abc}{d\delta}n\,.$$

ამ გამოსახულებებში d არის a, $\beta-\alpha$ და b რიცხვების უდიდესი საერთო გამყოფი, ხოლო δ არის $\frac{ab}{d}$, $(\gamma-\alpha-a\eta)$ და c რიცხვების უდიდესი საერთო გამყოფი.

დასკვნა ასეთია: დასმული ამოცანა ყოველთვის ამოხსნადია, თუ a, b, c,... თანამარტივი რიცხვებია.

საერთოდ, თუ ვიპოვით ამ შედარებათა ერთ ξ ამონახსნს, მაშინ შედარებათა ზოგად ამონახსნს ექნება სახე

$$x\equiv\xi\left(\mod\frac{abc\ldots}{\alpha\delta\ldots}\right).$$

აქედან გამოდის, რომ, თუ მოდულები წყვილ-წყვილად თანამარტივია, მაშინ მოდული იქნება მოცემული მოდულების ნამრავლი.

თუ დავუშვებთ, $a=p^{l}p'^{l_1}\ldots$, მაშინ პირველი შედარება შეიძლება შევცვალოთ შედარებათა სისტემით. ეს შედარებები ყოველთვის ამოხსნადია. თუ b მოდულში p ფაქტორი რომელიმე k ხარისხში შედის, მაშინ $x\equiv\beta \pmod b$ შედარების ამოსახსნელად უნდა ამოიხსნას სხვა შედარებებთან ერთად $x\equiv\beta \pmod{p^{k}}$, ხოლო იმისათვის, რომ ერთდროულად ადგილი ჰქონდეს

$$x\equiv\alpha \pmod{p^{l}} \text{ და } x\equiv\beta \pmod{p^{k}}$$

შედარებებს, $k \leqslant i$ შემთხვევაში, აუცილებელია $\alpha \equiv \beta \pmod{p^k}$. თუ ეს პირობა არ შესრულდა, მაშინ სისტემის პირველ ორ შედარებას ერთდროულად ადგილი არ ექნება.

§ 8. იმ შემთხვევაში, როცა a, b, c,... წყვილ-წყვილად თანამარტივი რიცხვებია, შეიძლება მივუთითოთ სხვა მეთოდზე, რომელსაც გარკვეული უპირატესობა გააჩნია § 7-ში მითითებულ მეთოდთან შედარებით.

ამ ახალ მეთოდში მნიშვნელოვან როლს ასრულებს r, s, t,... დამხმარე რიცხვები, რომლებიც უნდა აკმაყოფილებდეს შემდეგ შედარებებს:

$$r \equiv 1 \pmod{a} \equiv 0 \pmod{b} \equiv 0 \pmod{c} \equiv 0 \ldots$$
$$s \equiv 0 \pmod{a} \equiv 1 \pmod{b} \equiv 0 \pmod{c} \equiv 0 \ldots$$
$$t \equiv 0 \pmod{a} \equiv 0 \pmod{b} \equiv 1 \pmod{c} \equiv 0 \ldots$$

ყველა ეს შედარება ამოხსნადია. მაგ., $r = r'\,b\,c\ldots$, სადაც r' განისაზღვრება $r'bc\ldots \equiv 1 \pmod{a}$ შედარებიდან. ასევე ვპოულობთ s, t,..., მაშინ ასეთი გზით მიღებული r, s, t... დამხმარე რიცხვების საშუალებით მიღებული x აკმაყოფილებს ჩვენს შედარებებს და აქვს სახე:

$$x \equiv \alpha r + \beta s + \gamma t + \ldots \pmod{abc\ldots} \qquad (4)$$

ამ მეთოდის არსებითი უპირატესობა წინა მეთოდთან შედარებით იმაში გამოიხატება, რომ ყველა ამ ტიპის ამოცანაში, სადაც a, b, c მუდმივი რიცხვებია, ხოლო α, β, γ,..., იცვლება ნებისმიერად, შედარებათა სისტემისათვის გვაქვს მე-(4) ზოგადი ფორმულა, რომელშიც r, s, t,... მუდმივებია, ხოლო α, β, γ,... ცვლადი ფაქტორებია.

ზემოთ ნათქვამიდან გამომდინარეობს შემდეგი ზოგადი თეორემა:

თუ $\{\alpha\}$, $\{\beta\}$, $\{\gamma\}$,..., მე-(4) ფორმულაში წარმოადგენს a, b, c,... მოდულების ნაშთთა სრულ სისტემებს, შესაბამისად, მაშინ

$$\{\alpha r + \beta s + \gamma t + \cdots\}$$

წარმოადგენს $abc\ldots$ მოდულით ნაშთთა სრულ სისტემას.

ამ თეორიის გამოყენება შეიძლება შემდეგი ამოცანის ამოსახსნელად: ვთქვათ, მოცემულია შედარება $mx \equiv n \pmod{M}$, სადაც $M =$

$=abc\ldots$, a, b, $c,\ldots$ წყვილ-წყვილად თანამარტივი რიცხვებია. მაშინ გვექნება შედარებათა სისტემა

$$mx\equiv n(\mathrm{mod}\ a),\quad mx\equiv n\ (\mathrm{mod}\ b),\quad mx\equiv n\ (\mathrm{mod}\ c),\ldots$$

ვთქვათ, $x\equiv\alpha\ (\mathrm{mod}\ a)$, $x\equiv\beta\ (\mathrm{mod}\ b)$, $x\equiv\gamma\ (\mathrm{mod}\ c),\ldots$ ამ შედარებათა ამონახსნებია შესაბამისად, მაშინ მოცემული შედარების ამონახსნი ჩაიწერება ასეთი ფორმით:

$$x\equiv\alpha r+\beta s+\gamma t+\cdots\ (\mathrm{mod}\ M).$$

ახლა, თუ a, b, $c,\ldots$ დავშლით პირველად მამრავლებად და p^h არის ერთ-ერთი პირველადი მამრავლი, რომელიც შედის a-ს დაშლაში, მაშინ $mx\equiv n\ (\mathrm{mod}\ a)$ შედარების ამოსახსნელად უნდა ამოიხსნას შედარება $mx\equiv n\ (\mathrm{mod}\ p^h)$. ამ უკანასკნელის ამოხსნას მივყავართ $mx\equiv n\ (\mathrm{mod}\ p^{h-1})$ შედარების ამოხსნამდე.

მაგალითი:

$$x\equiv 3\ (\mathrm{mod}\ 17);\quad x\equiv 1(\mathrm{mod}\ 12)\quad x\equiv 4(\mathrm{mod}\ 5).$$

ვხსნით შედარებებს: $60r'\equiv 1(\mathrm{mod}\ 17)$, $85s^1\equiv 1(\mathrm{mod}\ 12)$, $204\,t^1\equiv 1(\mathrm{mod}\ s)$. ვღებულობთ: $r'=2$, $s'=1$, $t'=4$. ე. ი. $r=120$, $s=85$, $t=816$ და $x\equiv 3\cdot 120+1\cdot 85+4\cdot 816\ (\mathrm{mod}\ 1020)$.

$x\equiv 649\ (\mathrm{mod}\ 1020)$.

§ 9. ვიცით, რომ, თუ a, b, $c,\ldots$, წყვილ-წყვილად თანამარტივი მოდულებია, $\{\alpha\}$, $\{\beta\}$, $\{\gamma\},\ldots$, ნაშთთა სრული სისტემებია ამ მოდულებით შესაბამისად, მაშინ $\{\alpha r+\beta s+\gamma t+\cdots\}$ ნაშთთა სრული სისტემაა $abc\ldots$ მოდულით (r, s, $t,\ldots$ განსაზღვრულია წინა პარაგრაფში). ირკვევა, რომ, ამას გარდა, თუ $\{\alpha\}$, $\{\beta\}$, $\{\gamma\},\ldots$ ნაშთთა სრული დაყვანილი სისტემებია a, b, $c,\ldots$ მოდულებით შესაბამისად, მაშინ $\{\alpha r+\beta s+\gamma t+\cdots\}$ ნაშთთა სრული დაყვანილი სისტემაა $abc\ldots$ მოდულით.

ან სიმბოლურად

$$\varphi(abc\ldots)=\varphi(a)\cdot\varphi(b)\cdot\varphi(c)\ldots$$

კერძოდ, თუ $D(m,\ n)=1$, მაშინ $\varphi(m)\cdot\varphi(n)=\varphi(mn)$

ახლა აღვნიშნოთ Euler-ის φ ფუნქციის რამდენიმე საინტერესო თვისება:

I. ვთქვათ, $n=p^{\alpha}\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots$, სადაც p, p_1, p_2, p_3,... პირველადი ფაქტორებია. უნდა ვიპოვოთ $\varphi(n)$. ირკვევა, რომ თუ ცნობილია p, p_1, p_2,..., a, a_1, a_2,..., მაშინ $\varphi(n)$-ს ადვილად ვპოულობთ. სახელდობრ:

$$\varphi(n)=p^{a-1}(p-1)p_1^{a-1}(p_1-1)p_2^{a_2-1}(p_2-1)\ldots=$$

$$=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots=\frac{n}{pp_1p_2\ldots}(p-1)(p_1-1)\ldots, \quad (5)$$

ხოლო $\varphi(p)=p-1$.

II. გვქონდა, რომ თუ $D(m, n)=1$, მაშინ $\varphi(mn)=\varphi(m)\times\varphi(n)$. ვნახოთ, როგორ შეიცვლება ეს ფორმულა, როცა m და n არ არიან თანამარტივი რიცხვები. P-თი აღვნიშნოთ ყველა იმ პირველადი რიცხვის ნამრავლი, რომელიც შედის როგორც m-ის, ისე n-ის დაშლაში. M-ით აღვნიშნოთ ყველა პირველადი რიცხვის ნამრავლი, რომელიც მხოლოდ m-ის დაშლაში შედის, ხოლო N-ით მხოლოდ n-ის დაშლაში შემავალი ყველა პირველადი რიცხვის ნამრავლი. მაშინ, მე-(5) ტოლობის თანახმად,

$$\varphi(m)=\frac{m}{PM}\varphi(P)\varphi(M)\ ,$$

$$\varphi(n)=\frac{n}{PN}\varphi(P)\varphi(N)\ ,$$

$$\varphi(mn)=\frac{mn}{PMN}\varphi(P)\varphi(M)\varphi(N)\ .$$

აქედან ვღებულობთ ფორმულას

$$\varphi(mn)=\frac{P}{\varphi(P)}\varphi(m)\varphi(n)\ .$$

III. მიღებული ფორმულა შეიძლება განვაზოგადოთ ფაქტორთა უფრო დიდი რიცხვისათვის. მაგ., 3 რიცხვის შემთხვევაში

$$\varphi(m\cdot r\cdot s)=\varphi(m)\varphi(r)\varphi(s)\cdot\frac{P}{\varphi(P)}\cdot\frac{P'}{\varphi(P')}\ .$$

P არის m და rs რიცხვების საერთო პირველადი მამრავლების ნამრავლი, P' კი—r და s რიცხვების საერთო პირველადი მამრავლების ნამრავლი. P_1-ით აღვნიშნოთ იმ პირველადი გამყოფების ნამრავლი, რომლებიც საერთოა ამ სამი რიცხვიდან რომელიმე ორისათვის; ხოლო P_2-ით — სამივე რიცხვის საერთო პირველადი გამყოფების ნამრავლი, მაშინ გვექნება:

$$\varphi(m\cdot r\cdot s)=\varphi(m)\varphi(r)\varphi(s)\cdot\frac{P_1}{\varphi(P_1)}\cdot\left(\frac{P_2}{\varphi(P_2)}\right)^2.$$

§ 10. ვთქვათ, $n=p^{\alpha}\cdot p_1^{\alpha_1}\cdot p_1^{\alpha_2}\cdots p_{k-1}^{\alpha_{k-1}}$ მოცემული რიცხვია, $d=p^{\alpha}\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{k-1}^{\alpha_{k-1}}$, $0\leqslant\alpha\leqslant a$, $0\leqslant\alpha_1\leqslant a_1$, ..., $0\leqslant\alpha_{k-1}\leqslant a_{k-1}$, არის n რიცხვის რაიმე გამყოფი. მაშინ

$$\varphi(d)=p^{\alpha-1}\ (p-1)\cdot p_1^{\alpha_1-1}(p_1-1)\cdots p_{k-1}^{\alpha_{k-1}-1}(p_{k-1}-1).$$

თუ α_1, α_1, α_2,..., α_{k-1} რიცხვებს შევცვლით 0-დან a, a_1, a_2,..., a_{k-1} რიცხვებამდე შესაბამისად, მივიღებთ n რიცხვის ყველა გამყოფს. სამართლიანია ფორმულა

$$\sum_d\varphi(d)=p^{\alpha}\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots P_{k-1}^{\alpha_{k-1}}=n.$$

ცხადია, აგრეთვე

$$\sum_d\varphi\left(\frac{n}{d}\right)=n.$$

§ 11. $\varphi(m)$ ფუნქცია შეიძლება განზოგადდეს. მაგ., Schemmel-მა $\varphi(m)$ ფუნქცია განსაზღვრა შემდეგნაირად. ვთქვათ, n რაიმე რიცხვია. m არის n-ზე ნაკლები რიცხვი. შევადგინოთ შემდეგი რიცხვთა ჯგუფები:

$$1,\ 2,\ 3,\ldots,\ m$$
$$1+1,\ 2+1,\ 3+1,\ \ldots,\ m+1$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$1+(n-m-1),\ 2+(n-m-1),\ldots,\ m+(n-m-1).$$

განვსაზღვროთ ამ ცხრილის ის ჯგუფები, რომლებიც თანამარტივია n-

თან. ეს რიცხვი, ცხადია, იქნება n-ის ფუნქცია. ეს ფუნქცია აღვნიშნოთ $\varphi_m(n)$-ით. როცა $m=1$, მაშინ $\varphi_1(n)=\varphi(n)$ (Euler-ის ფუნქცია), თავის მხრივ, $\varphi_m(n)$ არის Lucas-ის მიერ მოცემული ფუნქციის კერძო სახე:

ვთქვათ, $e_1, e_2, \ldots, e_k$ რიცხვთა რაიმე მწკრივია. განვსაზღვროთ $\psi(n)$ რიცხვი ისეთი h—ებისა, რომლებიც ეკუთვნის $[1, 2, 3, \ldots, n]$ მონაკვეთს და რომელთათვის

$$h+e_1,\ h+e_2,\ \ldots,\ h+e_k$$

ჯამების ჯგუფი n-თან თანამარტივია. ცხადია, $e_1=1$, $e_2=2, \ldots$, $e_k=k$, მაშინ $\psi(n)=\varphi_k(n)$.

ირკვევა, რომ ψ ფუნქციას აქვს იგივე ძირითადი თვისება, რაც φ ფუნქციას. ე. ი. $\psi(mn)=\psi(m)\cdot\psi(n)$, თუ m და n თანამარტივია. ამ ფორმულიდან მივიღებთ $\psi(p^\alpha)=p^{\alpha-1}(p-\lambda)$. საერთოდ, თუ $n=p^\alpha\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{k-1}^{\alpha_{k-1}}$, მაშინ

$$\psi(n)=p^{\alpha-1}(p-\lambda)\cdot p_1^{\alpha_1-1}(p_1-\lambda_1)\cdots(p_{k-1}^{\alpha_{k-1}-1}(p_{k-1}-\lambda_{k-1}), \qquad (7)$$

λ რიცხვები მე-(7)ფორმულაში შემდეგნაირად განისაზღვრება: ვთქვათ, $e_1, e_2, \ldots, e_h$ მოცემული რიცხვებია, რომელთა მიმართ აიგება $\psi(n)$ ფუნქცია. ვთქვათ, ამ რიცხვებიდან λ რიცხვი არასადარია p მოდულით, λ_1—არასადარია p_1 მოდულით და ა. შ.

ვიპოვოთ ახლა $\varphi_k(n)$ გამოსახულება. ამისათვის დავუშვათ, $e_1=1$, $e_2=2$, $e_3=3, \ldots$ $e^k=k<n$. მაშინ, ცხადია, რომ $\lambda_1=\lambda_2=\ldots=\lambda_n=k$ (თუ k ნაკლებია n-ის ყველა პირველად გამყოფზე). მაშასადამე,

$$\varphi^k(n)=p^{\alpha-1}(p-k)p_1^{\alpha_1-2}(p_1-k)\cdots p_{k-1}^{\alpha_{k-1}-1}\ (p_{k-1}-k)\,.$$

იმ შემთხვევაში, როცა k მეტია n-ის პირველად გამყოფებზე, მაშინ $\varphi_k(n)=0$.

ვთქვათ, d არის n-ის რომელიმე გამყოფი. ის წარმოიდგინება $d=p^\alpha\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_{k-1}^{\alpha_{k-1}}$ სახით და

$$\psi(d)=p^{\alpha-1}(p-\lambda)p_1^{\alpha_1-1}(p-\lambda_1)\cdots p_{k-1}^{\alpha_{k-1}-1}\ (p_{k-1}-\lambda_{k-1}),$$

ანუ

$$\frac{\psi(d)}{\lambda^{\alpha}\cdot\lambda_1^{\alpha_1}\ldots\lambda_{k-1}^{\alpha_{k-1}}}=\frac{p^{\alpha-1}(p-\lambda)}{\lambda^{\alpha}}\cdot\frac{p_1^{\alpha_1-1}(p-\lambda_1)}{\lambda_1^{\alpha_1}}\cdots\frac{p_{k-1}^{\alpha_{k-1}-1}(p-\lambda_{k-1})}{\lambda_{k-1}^{\alpha_{k-1}}}.$$

თუ ამ ტოლობის ორივე მხარეს შევაჯამებთ, როცა α, α_1, α_2,.., α_{k-1} იცვლება 0-დან a, a_1, a_2,.., a_{k-1}-მდე, მივიღებთ

$$\sum_d\frac{\psi(d)}{\lambda^{\alpha}\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\ldots}=\frac{n}{\lambda^{a}\lambda_1^{a_1}\lambda_2^{a_2}\ldots}.$$

კერძო შემთხვევაში, როცა $(e_1, e_2,\ldots, e_k)=(1, 2, .., k)$, მაშინ $\psi(n)=\varphi^k(n)$ და

$$\sum_d\frac{\psi(d)}{k^{\alpha}k_1^{\alpha_1}k_2^{\alpha_2}\ldots}=\frac{n}{k^{a}k_1^{a_1}k_2^{a_2}\ldots}.$$

ეს ფორმულა პირველმა Schemmel-მა მიიღო.

IV თავი

FERMAt-ს და WILSON-ის თეორემები

§ I. მე-3 თავის § I-ში აღინიშნა, რომ ყოველი m რიცხვი n რიცხვის მიმართ წარმოიდგინება ასე: $m=qn+r$, სადაც $r<n$. ვთქვათ, $r_1, r_2,\ldots, r_{\varphi(m)}$ ნაშთთა დაყვანილი სისტემაა n მოდულით. თუ a და n თანამარტივია, მაშინ $ar_1, ar_2,\ldots, ar_{\varphi(n)}$, აგრეთვე ნაშთთა დაყვანილი სისტემაა n მოდულით. რადგან $r_1, r_2,\ldots, r_{\varphi(n)}$ და $ar_1, ar_2,\ldots, ar_{\varphi(n)}$ სისტემები ერთსა და იმავე ნაშთებს წარმოადგენენ, ამიტომ პირველთა ნამრაველი n მოდულით მეორეთა ნამრაველის სადარია. ე.ი.

$$a^{\varphi(n)}r_1\cdot r_2\cdots r_{\varphi(n)}\equiv r_1 r_2\cdots r_{\varphi(n)} \pmod{n}$$

მარცხენა მხარეში გადატანის შემდეგ გვექნება

$$(a^{\varphi(n)}-1)r_1\cdot r_2\cdots r_{\varphi(n)}\equiv 0 \pmod{n},$$

ე. ი.

$$a^{\varphi(n)}-1\equiv 0 \pmod{n}. \qquad \text{I}$$

მივიღეთ შემდეგი თეორემა: თუ a და n თანამარტივი რიცხვებია, მაშინ a რიცხვის $\varphi(n)$ ხარისხი I-ის სადარია n მოდულით.

კერძოდ, თუ n არის პირველადი p რიცხვი, მაშინ

$$\varphi(n)=\varphi(p)=p-1 \qquad \text{და ამიტომ}$$

$$a^{p-1}\equiv 1 \pmod{p}. \qquad \text{I}'$$

ან

$$a^p\equiv a \pmod{p}. \qquad \text{I}''$$

I'და I'' ფორმულები Fermat-ს თეორემაა (მოდული აუცილებლად პირველადი რიცხვია).

Fermat-ს თეორემა პირველად დაამტკიცა Euler-მა პირველადი

n-ისა და მთელი a-სათვის ბინომიური კოეფიციენტების უმარტივესი თვისებების გამოყენებით. შემდეგ Ganss-მა (Disg-An) მოგვცა ამ თეორემის მეორე დამტკიცება.

§ 2. Lagrange-ის თეორემა. ავიღოთ ნამრავლი

$$\Pi(x)=(x+1)\ (x+2)\cdots(x+p-1)$$

და დავშალოთ x-ის ხარისხების მიხედვით

$$\Pi(x)=x^{p-1}+A_1x^{p-2}+\cdots+A_{p-2}x+A_{p-1};$$

A_1, A_2,..., Ap_{-1} კოეფიციენტები მთელი რიცხვებია. ირკვევა, რომ A_1, A_2,..., A_{p-2} კოეფიციენტები იყოფა p-ზე, ამიტომ

$$(p-1)A_{p-1}=1+A_1+A_2+\cdots+A_{p-2}$$

ტოლობიდან გამოდის, რომ $A_{p-1}\equiv -1 \pmod p$. (1)

აქედან კი ვღებულობთ

$$(x+1)\ (x+2)\cdots(x+p-1)\equiv x^{p-1}-1 \pmod p. \quad (2)$$

თუ x ცვლადის მაგივრად შევიტანთ 1, 2, 3,..., $p-1$ მთელ რიცხვებს, მაშინ მარცხენა მხარე გაიყოფა p-ზე და მივიღებთ Fermat-ის თეორემას

$$x^{p-1}\equiv 1 \pmod p/ \quad (x \text{ არ იყოფა } p\text{-ზე})$$

(1) შედარებიდან ვღებულობთ Wilson-ის ძალიან მნიშვნელოვან თეორემას. თუ p რაიმე პირველადი რიცხვია, მაშინ

$$1\cdot 2\cdot 3\cdots(p-1)\equiv -1 \pmod p \quad (3)$$

(3) ფორმულით შეიძლება გავარკვიოთ, მოცემული n რიცხვი პირველადია თუ შედგენილი.

§ 3. § 1-ის დასაწყისში ვაჩვენეთ, რომ Euler-ის თეორემიდან $a^{\tau(n)}\equiv 1 \pmod n$ შეიძლება გამოვიყვანოთ $a^{p-1}\equiv 1 \pmod p$, სადაც p პირველადი რიცხვია. შეიძლება პირიქითაც—უკანასკნელი შედარებიდან გამოვიყვანოთ პირველი შედარება. ამ თეორემის განზოგადება ასე ხდება.

ვთქვათ, $n=p^\alpha q^\beta r^\tau\cdots a$ არის p, q, r,... რიცხვების თანამარტი-

ვი რაიმე მთელი რიცხვი. შევიტანოთ $\varphi(p^\alpha)$, $\varphi(p^\beta)$, $\varphi(r^\gamma)$ ფუნქციები. $\psi(n)$-ით აღვნიშნოთ ამ ფუნქციონალური გამოსახულებების უმცირესი საერთო ჯერადი. ნაშინ

$$a^{\psi(n)} \equiv 1 \pmod{n};$$

რადგან

$$\varphi(n) = \varphi(p^\alpha) \cdot \varphi(q^\beta) \cdot \varphi(r^\gamma) \ldots,$$

ამას გარდა, $\varphi(n)$ არის $\psi(n)$-ის ჯერადი, ამიტომ მივიღებთ Fermat-ის თეორემას ყველაზე ზოგადი სახით $a^{\varphi(n)} \equiv 1 \pmod{n}$.

უკანასკნელი ფორმულა მოგვცემს

$$m^{\varphi(n)} = 1 + nh, \quad m = a.$$

თუ ავიღებთ $nx - ny = 1$ განუზღვრელ განტოლებას, მივიღებთ ამ განტოლების ამონახსნს

$$y = h, \; x = m^{\varphi(n)-1}.$$

§ 4. Fermat-ს თეორემის შებრუნებული თეორემა შეიძლება ასე ჩამოვაყალიბოთ, ვთქვათ, $a^{n-1} \equiv 1 \pmod{n}$. შესაძლებელია ორი შემთხვევა.

I შემთხვევა, როცა $n-1$ უმცირესი ხარისხია, რომლისთვისაც ამ შედარებას აქვს ადგილი. მაშინ $\psi(n)$ და ე. ი. $\varphi(n)$ არის n-ის ჯერადი, აქედან გამოდის $n-1 = \varphi(n)$ და n პირველადი რიცხვია.

II შემთხვევა, როცა $n-1$ არ არის უმცირესი ხარისხი, რომლისთვისაც ამ შედარებას აქვს ადგილი. მაშინ, ვთქვათ, d არის ასეთი უმცირესი ხარისხი. როგორც პირველ შემთხვევაში, შეგვიძლია ვაჩვენოთ, რომ $n-1$ არის d რიცხვის ჯერადი.

მივიღეთ, თუ $a^x - 1$ იყოფა n-ზე, როცა $x = n-1$ და არ იყოფა n-ზე, როცა $x < n-1$, მაშინ n პირველადი რიცხვია.

§ 5. Fermat-ს თეორემით, თუ p პირველადი რიცხვია, მაშინ ნებისმიერი a-სათვის, რომელიც p-ზე არ იყოფა, გვაქვს

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Jacobi-მ აჩვენა, რომ ეს შედარება შესრულდება p^2-სთვის, თუ a არის ერთ-ერთი $1, 2, 3, \ldots, p-1$ რიცხვებიდან.

ცხადია, $\frac{a^{p-1}-1}{p}$ არის მთელი რიცხვი. ამ რიცხვის p-სთან შეფარდების მთელი ნაწილი აღვნიშნოთ Θ-თი, ხოლო ნაშთი $q(a)$-თი, მაშინ გვექნება

$$\frac{a^{p-1}-1}{p} = \Theta p + q(a) ,$$

ანუ

$$a^{p-1} \equiv 1 + q(a)p \pmod{p^2}.$$

II ხარისხის შედარებები

მე-2 ხარისხის შედარება მიიყვანება

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

სახეზე. შეიძლება დავუშვათ, $a + m$, რადგან წინააღმდეგ შემთხვევაში მივიღებთ $bx + c \equiv 0 \pmod{m}$ პირველი ხარისხის შედარებას.

ასეთ სახეზე მიყვანილი შედარების ორივე მხარე გავამრავლოთ $4a$-ზე, მივიღებთ

$$4a^2x^2 + 4abx + b^2 + 4ac - b^2 \equiv 0 \pmod{4am}$$

ან

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}.$$

დავუშვათ, $2ax + b = z$, $b^2 - 4ac = q$, მაშინ

$$z^2 \equiv q \pmod{4am}.$$

შემდეგ, $2ax + b = z \pmod{4am}$ შედარებიდან ვპოულობთ x-ს. უკანასკნელი შედარება რომ ამოხსნადი იყოს, უნდა შესრულდეს პირობა $2a \mid (z - b)$. თუ ვიპოვეთ ამონახსნი $x \equiv a \pmod{4am}$, მაშინ ეს კლასი უნდა განვავრცოთ m მოდულით კლასებზე. განვიხილოთ დაწვრილებით

$$x^2 \equiv q \pmod{m}$$

შედარება. თუ ეს შედარება ამოხსნადია, მაშინ ამბობენ, რომ q არის m მოდულით კვადრატული ნაშთი; თუ ეს შედარება ამოუხსნადია, მაშინ q არის კვადრატული არანაშთი (Rest ან Nichtrest).

ვთქვათ, q კვადრატული ნაშთია და $D(q, m)=\delta$, მაშინ $D(x, m)=\delta$. შემდეგში განვიხილავთ მხოლოდ იმ შემთხვევას, როცა $D(x,m)=1$.

დავამტკიცოთ ახლა თეორემა:

თუ $x^2\equiv q \pmod m$ შედარებას აქვს ამონახსნი $x\equiv\xi \pmod m$, მაშინ მისი ამონახსნი იქნება აგრეთვე

$$x\equiv m-\xi \pmod m.$$

მართლაც, თუ კვადრატში ავიყვანთ, მივიღებთ

$$(m-\xi)^2=m^2-2m\xi+\xi^2.$$

ამ გამოსახულების პირველი და მეორე შესაკრები 0-ის სადარია m მოდულით, ხოლო უკანასკნელი q-ს სადარია m მოდულით.

შემდეგ. თუ z არის $z\equiv 1 \pmod m$ შედარების ამონახსნი, მაშინ $x\equiv\xi z \pmod m$ იქნება მოცემული შედარების ამონახსნი, რადგან

$$x^2\equiv\xi^2z^2\equiv q\cdot 1 \pmod m.$$

პირიქით, თუ $\xi^2\equiv q \pmod m$ და $\xi'^2\equiv q \pmod m$, მაშინ $\xi'=\xi z$. რადგან $D(\xi, m)=1$ და $D(\xi', m)=1$, ამიტომ ყოველთვის ვიპოვით ξ რიცხვის socin-ს. ვთქვათ, $\xi\eta\equiv 1 \pmod m$, რადგან $\xi^2\equiv\xi'^2 \pmod m$, ამიტომ $(\xi'\eta)^2\equiv(\xi'\eta)^2 \pmod m$. ე. ი. $(\xi'\eta)^2\equiv 1$ და $\xi'\eta$ არის $z^2\equiv 1 \pmod m$ შედარების ერთ-ერთი ფესვი, $z\equiv\xi^1\eta \pmod m$. თუ ორივე მხარეს გავამრავლებთ ξ-ზე, მივიღებთ

$$\xi z\equiv\xi'(\eta\xi) \pmod m,$$

ანუ $\xi'\equiv\xi z \pmod m$, რაც უნდა დაგვემტკიცებინა.

დამტკიცებული თეორემა გვიჩვენებს, რომ $z^2\equiv 1 \pmod m$ შედარების ამონახსნთა რიცხვი დამოკიდებულია მხოლოდ m-ზე.

დაგვრჩა მოვძებნოთ პირობა, რომლის შესრულებისას $x^2\equiv q \pmod m$ ამოხსნადია. ვთქვათ,

$$m=2^\omega\cdot p^\pi\cdot p_1^{\pi_1}\cdots$$

მაშინ ჩვენი შედარების ამოხსნადობისათვის აუცილებელია და საკმარისია, ამოხსნადი იყოს შემდეგი შედარებები

$$x^2\equiv q \pmod{2^\omega},\ x^2\equiv q \pmod{p^\pi},\ldots$$

ვთქვათ, ამ შედარებათა ამოხსნებია α, β, γ,...,

$$\alpha^2 \equiv q \pmod{2^\omega},\ \beta^2 \equiv q \pmod{p^\pi},\ \gamma^2 \equiv q \pmod{p_1^{\pi_1}},\ldots$$

თუ x არის

$$x \equiv \alpha \pmod{2^\omega},\ x \equiv b \pmod{p^\pi},\ x \equiv \gamma \pmod{p_1^{\pi_1}},\ldots$$

სისტემის ამონახსნი, მაშინ ის იქნება მოცემული სისტემის ამონახსნიც. მართლაც, თუ ამ შედარებებს კვადრატში ავიყვანთ, მივიღებთ

$$x^2 \equiv q \pmod{2^\omega},\ x^2 \equiv q \pmod{p^\pi},\ldots$$

რაც იმას ნიშნავს, რომ

$$x^2 \equiv q \pmod{2^\omega\ p^\pi \cdot p_1^{\pi_1}\ldots}$$

შემდგომში ჩვენ შეგვიძლია განვიხილოთ მხოლოდ $m=2^\omega$ და $m=p^\pi$ შემთხვევები, სადაც p მარტივი რიცხვია.

ჯერ განვიხილოთ

$$x^2 \equiv p \pmod{2^\omega}$$

სახის შედარება. ვუშვებთ, რომ $D(q,\ 2^\omega)=1$, მაშასადამე, $D(x,\ 2^\omega)=1$. დავიწყოთ $\omega=1$, $x^2 \equiv q \pmod 2$ შემთხვევის განხილვით. ცხადია, q კენტი რიცხვია, ამიტომ ნებისმიერი $x=2n+1$ სახის რიცხვი შედარებას დააკმაყოფილებს.

2) ვთქვათ, $\omega=2$, $x^2 \equiv q \pmod 4$. x შეიძლება იყოს მხოლოდ კენტი რიცხვი. თუ $x=2n+1$, მაშინ $x^2=4n^2+4n+1$, ე. ი. $x^2 \equiv 1 \pmod 4$. თუ $q=4k+1$ სახის რიცხვია, მაშინ შედარებას ნებისმიერი კენტი რიცხვი აკმაყოფილებს. თუ $q=4k+3$, მაშინ შედარებას ამონახსნი არა აქვს.

3) ვთქვათ, $\omega=3$, $x^2 \equiv q \pmod 8$. რადგან x კენტი რიცხვია, ამიტომ $x=4z\pm1$, $x^2=16z^2\pm8z+1$, ე. ი. $x^2 \equiv 1 \pmod 8$ და $q \equiv 1 \pmod 8$. შედარებას $x^2 \equiv q \pmod 8$ აკმაყოფილებს ნებისმიერი $x \equiv 1, 3, 5, 7 \pmod 8$, თუ $q \equiv 1 \pmod 8$.

$\omega>3$ შემთხვევა განიხილება იმ დაშვებით, რომ $x^2 \equiv q \pmod{2^{k-1}}$, სადაც $k-1 \geqslant 3$ შედარება ამოხსნადია. ვთქვათ, ξ ამ შედარების ერთ-ერთი ამონახსნია, მაშინ $\xi^2 - q = 2^{k-1} L$. შემდეგ,

$$x \equiv \xi \pmod{2^{k-1}},$$

$$x=\xi+z\cdot 2^{k-1}=\xi+z_1 2^{k-2}$$

ვნახოთ, შეიძლება თუ არა z შევარჩიოთ ისე, რომ დაკმაყოფილდეს შედარება $x^2\equiv q \pmod{2^k}$.

გვაქვს,

$$(\xi+z_1 2^{k-2})^2\equiv q \pmod{2^k}, \quad \xi^2-q=2^{k-1}L,$$

ანუ

$$\xi^2+2\xi z_1\cdot 2^{k-2}+z_1^2\cdot 2^{2k-4}\equiv q \pmod{2^k}.$$
$$2^{k-1}L+2^{k-1}\xi z_1+z_1^2\cdot 2^{2k-4}\equiv 0 \pmod{2^k}.$$

თუ ამ შედარების ორივე მხარეს და მოდულს გავყოფთ 2^{k-1}-ზე, მივიღებთ:

$$L+\xi\cdot z_1+z_1^2\cdot 2^{k-3}\equiv 0 \pmod 2.$$

თუ მოვიშორებთ მოდულის ჯერად რიცხვებს, მივიღებთ

$$L+\xi z_1\equiv 0 \pmod 2.$$

რადგან $D(\xi, 2)=1$, ამიტომ უკანასკნელ შედარებას ყოველთვის აქვს ფესვი და ამიტომ ფესვი ექნება $x^2\equiv q \pmod{2^\alpha}$ შედარებასაც.

გადავიდეთ $x^2\equiv q \pmod{p^\pi}$ სახის შედარების განხილვაზე. თუ ამ შედარებას ფესვი აქვს, მაშინ ექნება ფესვი ამ შედარებას p-ს უფრო დაბალი ხარისხის შემცველი მოდულებისათვის, კერძოდ, $p\pi-(\pi-1)=p$, ე. ი. q აუცილებლად უნდა იყოს კვადრატული ნაშთი p მოდულით. ვაჩვენოთ, რომ ეს პირობა საკმარისიც არის.

ვაჩვენოთ ისევ, რომ თუ $x^2\equiv q \pmod{p^{k-1}}$ შედარების ამონახსნი ცნობილია, მაშინ შეიძლება ვიპოვოთ $x^2\equiv q \pmod{p^k}$ შედარების ამონახსნიც. ვთქვათ, $x\equiv\xi \pmod{p^{k-1}}$ არის პირველი შედარების ამონახსნი. მაშინ $\xi^2-q=p^{k-1}\cdot L$, $x=\xi+p^{k-1}z$, ამიტომ

$$(\xi+p^{k-1}z)^2\equiv q \pmod{p^k},$$
$$\xi^2+2p^{k-1}\xi z+p^{2k-2}z^2-q\equiv 0 \pmod{p^k},$$
$$p^{k-1}L+2p^{k-1}\xi z+p^{2k-2}z^2\equiv 0 \pmod{p^k}.$$

შეკვეცის შემდეგ მივიღებთ

$$p^{k-1}z^2+L+2\xi z\equiv 0 \pmod p, \quad L+2\xi z\equiv 0 \pmod p.$$

რადგან $D(2\xi, q)=1$, ამიტომ უკანასკნელი შედარების ამონახსნი ცნობილია.

ახლა შეიძლება ჩამოვაყალიბოთ $x^2\equiv q \pmod m$ შედარების ამოხსნადობის ზოგადი პირობა. თუ $D(m, q)=1$, $\omega=1$ შემთხვევაში, აუცილებელი და საკმარისია q იყოს $p_1, p_2,\ldots$ მარტივი რიცხვების კვადრატული ნაშთი; თუ $\omega=2$, დამატებითი პირობაა $q\equiv 1 \pmod 4$; ხოლო თუ $\omega\geqslant 3$, მაშინ $q\equiv 1 \pmod 8$. თუ ეს პირობები შესრულებულია, მაშინ $x^2\equiv q \pmod m$ შედარებას აქვს $\chi(m)$ ფესვი, ამასთან, ძნელი არ არის განვსაზღვროთ $\chi(m)$ ყოველი m-სთვის.

განვთავისუფლდეთ ახლა $D(q, m)+1$ პირობისაგან. ვთქვათ, გვაქვს შედარება $x^2\equiv q \pmod m$, სადაც $D(q, m)=d$, $q=q'd$, $m=m',d$. ვთქვათ, $d=p_1^{2k_1+\xi}\cdot p_2^{2k_2+\varepsilon_2}\ldots$, სადაც $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ ან 0-ა, ან 1. d წარმოვადგინოთ ასე

$$d=\Pi p_i^{2k_i+\varepsilon_i}$$

შედარება რომ ამოხსნადი იყოს, x^2 უნდა გაიყოს $\Pi p_i^{2k_i+\varepsilon_i}$, ამას კი ადგილი ექნება, თუ x იყოფა $\Pi p_i k_i+\varepsilon i$. მაშასადამე, x წარმოიდგინება ასე

$$x=\Pi p_i^{k_i+\varepsilon_i}\cdot y.$$

თუ ყველა ამ სიდიდეს შედარებაში ჩავსვამთ, მივიღებთ

$$\Pi p_i^{2k_i+2\varepsilon_i}\cdot y^2\equiv q'd \pmod{m'd}$$

d-ზე შეკვეცის შემდეგ მივიღებთ:

$$\Pi p_i^{\varepsilon_i}\cdot y^2\equiv q' \pmod{m'} \qquad (1)$$

აქ $D(m', q')=1$, ამიტომ შედარების ამოხსნადობისათვის უნდა შესრულდეს

$$D(\Pi p_i^{\varepsilon_i}, m')=1 \qquad (2)$$

პირობა.

შემოვიტანოთ ახალი უცნობი $z=\Pi p_i^{\varepsilon_i} y$, მაშინ $z^2=\Pi p_i^{2\varepsilon_i} y^2$. თუ (1) შედარებას გავამრავლებთ $\Pi p_i^{\varepsilon_i}$, მივიღებთ

$$(\Pi p_i^{\varepsilon_i} y)^2=z^2\equiv q'\Pi p_i^{\varepsilon_i} \pmod{m'}. \qquad (3)$$

ე. ი. $q'\Pi p_i^{\varepsilon_i}$ უნდა იყოს კვადრატული ნაშთი m' მოდულით. თუ ეს პირობები შესრულებულია, მაშინ ჩვენი შედარება ამოხსნადია. მე-(2) ტოლობის თანახმად, ყოველთვის ამოხსნადია შედარება

$P \cdot \Pi p_i^{\nu_i'} \equiv 1 \pmod{m'}$, სადაც P არის $\Pi p_i^{\nu_i'}$ რიცხვის socius-ვიპოვოთ ასეთი P და მე-(3) შედარება გავამრავლოთ P^2-ზე. მივიღებთ

$$(Pz)^2 \equiv q' P^2 \Pi p_i^{\nu_i'} \equiv P q' \pmod{m'} \qquad (4)$$

მაგრამ $z^2 = \Pi p^{2\varepsilon_i} y^2$, ე. ი. (4)-ის თანახმად,

$$y^2 \equiv P q' \pmod{m'}.$$

ეს მოგვცემს (1) შედარების ამოხსნას, ე. ი. $x^2 \equiv q \pmod{m}$ შედარების ამოხსნასაც. მაშასადამე, მოცემული ორი პირობა საკმარისია $x^2 \equiv q \pmod{m}$ შედარების ამოსახსნელად და მისი ამოხსნა დაიყვანება მე-(3) შედარების ამოხსნაზე, სადაც მარჯვენა მხარე მოდულთან თანამარტივია.

განვიხილოთ ახლა შემთხვევა, როცა $x^2 \equiv q \pmod{m}$ შედარებას აქვს ან ერთი ამონახსნი, ან ორი, ან ამოუხსნადია. ვთქვათ, p/q, მაშინ p/x და $x \equiv 0 \pmod{p}$. მოცემული პირობის დროს ეს ერთადერთი ამონახსნია. ადრე ვნახეთ, რომ თუ $x \equiv \alpha \pmod{p}$ არის შედარების ამონახსნი, მაშინ $x \equiv p - \alpha \pmod{p}$ აგრეთვე ამონახსნია, როცა $D(q, p) = 1$. ე. ი. ამ პირობებში კვადრატულ უტოლობას აქვს ან ორი ამონახსნი, ან ამოუხსნადია. შედარებები $x \equiv \alpha \pmod{p}$ და $x \equiv p - \alpha \pmod{p}$ ყოველთვის განსხვავებული ამონახსნებია, რადგან რომ დავუშვათ $\alpha \equiv p - \alpha \pmod{p}$, მივიღებთ $2\alpha \equiv p \pmod{p}$, ამასთან, $D(2, p) = 1$. გამოდის, რომ $\alpha \equiv 0 \pmod{p}$. ეს კი ეწინააღმდეგება პირობას, $D(q, p) = 1$.

ახლა ისმება კითხვა, როგორ გავიგოთ, მოცემულ შედარებას ორი ამონახსნი აქვს თუ ამოუხსნადია? ადრე გვქონდა კრიტერიუმი ამონახსნთა მაქსიმალური რიცხვის დასადგენად. ვისარგებლოთ ამ კრიტერიუმით. $x^p - x$ გავყოთ $(x^2 - q)$-ზე. დავწეროთ იგივეობა

$$x^p - x = [(x^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}} + q^{\frac{p-1}{2}} - 1]\, x,$$

სადაც $\frac{p-1}{2}$ მთელია p-ს კენტობის გამო. გავყოთ ეს იგივეობა $(x^2 - q)$-ზე. ნაშთი, ცხადია, იქნება $x\,(q^{\frac{p-1}{2}} - 1)$. რადგან ამონახსნთა მაქსიმალური რიცხვისათვის ეს ნაშთი ნულის ტოლი უნდა იყოს x-სგან

$\frac{p-1}{2}$

დამოუკიდებლად, ამიტომ $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. მაშასადამე, თუ ამ შედარებას ადგილი აქვს, მაშინ კვადრატულ შედარებას ორი ფესვი აქვს, და თუ არა აქვს ადგილი, მაშინ კვადრატული შედარება ამოუხსნადია.

Fermat-ს თეორემის თანახმად, თუ q არ იყოფა p-ზე, მაშინ

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

გვექნება

$$q^{p-1} - 1 \equiv 0 \equiv \left(q^{\frac{p-1}{2}} - 1 \right)\left(q^{\frac{p-1}{2}} + 1 \right) \pmod{p}.$$

თუ კვადრატული შედარება ამოუხსნადია, მაშინ $q^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}$, ე. ი. $q^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$, ე. ი. ჩვენ ვხედავთ, რომ ან $q^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ ან $q^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$. ამ ორ შედარებას ერთდროულად არ შეიძლება ჰქონდეს ადგილი, რადგან მაშინ მივიღებდით, რომ $2 \equiv 0 \pmod{p}$, რაც შეუძლებელია.

მაშასადამე, თუ $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, მაშინ q კვადრატული ნაშთია.

მაგალითი: $x^2 \equiv 6 \pmod{7}$; $6^{\frac{7-1}{2}} = 216$; $216 \equiv -1 \pmod{7}$, ამიტომ მოცემულ შედარებას ამონახსნი არა აქვს.

p და q რიცხვების დიდი მნიშვნელობებისათვის $q^{\frac{p-1}{2}}$ გამოთვლა ძნელდება, ამიტომ მიღებული კრიტერიუმი, Legendre-მა სხვა კრიტერიუმით შეცვალა. მან შემოიღო სიმბოლო $\left(\frac{q}{p}\right) = \pm 1$ და ჩათვალა, რომ $\left(\frac{q}{p}\right) = 1$, როცა q კვადრატული ნაშთია p მოდულით და $\left(\frac{q}{p}\right) = -1$, როცა q კვადრატული არანაშთია. მაშასადამე, Legendre-ის სიმბოლო განისაზღვრება პირობით

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}, \quad \left|\left(\frac{q}{p}\right)\right| = 1.$$

დავამტკიცოთ Legendre-ის სიმბოლოს ორი თვისება.

თ ე ო რ ე მ ა I. თუ $q \equiv q' \pmod{p}$, მაშინ $\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right)$.

მართლაც, $q^{\frac{p-1}{2}} \equiv q'^{\frac{p-1}{2}} \pmod{p}$, $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$,

$q'^{\frac{p-1}{2}} \equiv \left(\frac{q'}{p}\right) \pmod{p}$, ამიტომ $\left(\frac{q}{p}\right) \equiv \left(\frac{q'}{p}\right) \pmod{p}$. რადგან Legendre-ის სიმბოლოს მხოლოდ ორი მნიშვნელობა აქვს, ამიტომ შესაძლებელია შემდეგი შემთხვევები

$$\pm 1 \equiv \pm 1 \pmod{p}, \quad \pm 1 \equiv \mp 1 \pmod{p}.$$

მეორე შემთხვევა გვაძლევს $\pm 2 \equiv 0 \pmod{p}$, რაც შეუძლებელია, ამიტომ $\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right)$. თეორემა დამტკიცებულია.

თ ე ო რ ე მ ა II. თუ $q = q_1 \cdot q_2$, მაშინ $\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)$.

გვაქვს, $q^{\frac{p-1}{2}} \equiv q_1^{\frac{p-1}{2}} \cdot q_2^{\frac{p-1}{2}}$, ანუ $\left(\frac{q}{p}\right) \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \pmod{p}$.

წინა მსჯელობის მსგავსი მსჯელობით დავრწმუნდებით, რომ შედარება შეიძლება შეიცვალოს ტოლობით.

თუ ვისარგებლებთ დამტკიცებული თეორემებით, გამარტივდება Legendre-ის სიმბოლოს გამოთვლა. მეორე თეორემა შეიძლება ასე განვაზოგადოთ: თუ $q = q_1 q_2 \cdots q_n$, მაშინ $\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \cdots$ $\cdots \left(\frac{q_n}{p}\right)$. როცა $q_1 = q_2 = \cdots = q_n$, მაშინ $\left(\frac{q}{p}\right) = \left(\frac{q_n}{p}\right)^n$.

მაგალითი. $\left(\frac{38}{13}\right) = \left(\frac{12}{13}\right) = \left(\frac{2}{13}\right)^2 \cdot \left(\frac{3}{13}\right) = \left(\frac{3}{13}\right) = 1$,

რადგან $\left(\frac{2}{13}\right)^2 = 1$ და $13^{\frac{13-1}{2}} \equiv 1 \pmod{13}$. ე. ი. $x^2 \equiv$ $\equiv 38 \pmod{13}$ შედარებას აქვს ორი ამონახსნი.

ადვილად გამოითვლება $\left(\frac{-1}{p}\right)$ სიმბოლო. მართლაც, $\left(\frac{-1}{p}\right) \equiv$

$\equiv (-1)^{\frac{p-1}{2}} \pmod p$, ეს კი გვაძლევს ტოლობას $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$; ე. ი. $\left(\frac{-1}{p}\right)=1$, როცა $p=4n+1$ და $\left(\frac{-1}{p}\right)=-1$, როცა $p=4n+3$.

შემდეგ, ცხადია, $\left(\frac{1}{p}\right)=1$ ნებისმიერი p-სთვის. ე. ი. 1 კვადრატული ნაშთია ნებისმიერი მოდულით, $x^2\equiv 1 \pmod p$ ყოველთვის ამოხსნადია და მისი ამოხსნებია $x\equiv 1 \pmod p$, $x\equiv p-1 \pmod p$.

თუ $q\equiv q_1 \pmod p$, ე. ი. $q=np+q_1$, მაშინ $\left(\frac{q}{p}\right)=\left(\frac{q_1}{p}\right)$, ამიტომ Legendre-ის სიმბოლოს ყოველთვის შეიძლება ისეთი ფორმა მივცეთ, როცა მრიცხველი მნიშვნელზე ნაკლებია, მნიშვნელი კი მარტივი რიცხვია.

$\left(\frac{q}{p}\right)$ და $\left(\frac{p}{q}\right)$ სიმბოლოებს შორის თანაფარდობა მოცემულია რიცხვთა თეორიის ერთ-ერთი ყველაზე შესანიშნავი კანონით—შექცევადობის კანონით.

ამ კანონის დასამტკიცებლად ჯერ დავამტკიცოთ Gauss-ის ლემა, განვიხილოთ მწკრივი q, $2q$, $3q$,..., $\frac{p-1}{2}\,q$, სადაც p და q კენტი მარტივი რიცხვებია და $D(p, q)=1$. გავყოთ ამ მწკრივის რიცხვები p-ზე და ვთქვათ, ნაშთებია r_1, r_2,..., $r_{\frac{p-1}{2}}$ შესაბამისად. ადვილად შეიძლება ვაჩვენოთ, რომ ეს ნაშთები ეკუთვნის სხვადასხვა კლასებს. გავყოთ ისინი ორ ჯგუფად. პირველ ჯგუფს მივაკუთვნოთ $\frac{p}{2}$-ზე ნაკლები რიცხვები, მეორე ჯგუფს—$\frac{p}{2}$-ზე მეტი. ვთქვათ, ნაშთთა რიცხვი პირველ ჯგუფში არის μ, ხოლო მეორე ჯგუფში—ν. ვთქვათ, ეს რიცხვებია α_1, α_2,..., α_μ; β_1, β_2,..., β_ν, სადაც $\mu+\nu=\frac{p-1}{2}$.

β რიცხვები შევცვალოთ უარყოფითი ნაშთებით

$$p-\beta_1,\ p-\beta_2,\ldots,\ p-\beta\nu.$$

$\alpha_1, \alpha_2,\ldots,\ \alpha\mu, p-\beta_1, p-\beta_2,\ldots, p-\beta\nu$ განსხვავებული რიცხვებია. ამ რიცხვებს შორის არ არის ნული და მათი რიცხვი არის $\frac{p-1}{2}$.

მაშასადამე, ეს არის 1, 2, 3,..., $\frac{p-1}{2}$ რიცხვები, მოცემული გარკვეული თანამიმდევრობით. რადგან ეს ასეა, ამიტომ

$$\alpha_1\alpha_2\ldots\alpha\mu(p-\beta_1)(p-\beta_2)\cdots(p-\beta\nu)\equiv 1\cdot 2\cdot 3\ldots\frac{p-1}{2}\pmod p,$$

ან $(-1)^\nu\alpha_1\alpha_2\cdots\alpha\mu\cdot\beta_1\beta_2\cdots\beta\nu\equiv 1\cdot 2\cdot 3\cdots\ \frac{p-1}{2}\pmod p$.

ე. ი. $1.\ 2.\ 3.\ldots.\frac{p-1}{2}\cdot q^{\frac{p-1}{2}}\equiv(-1)^\nu 1\cdot 2\cdot 3\ldots.\ \frac{p-1}{2}\pmod p$.

შევკვეცოთ $\left(\frac{p-1}{2}\right)!$, მივიღეთ $q^{\frac{p-1}{2}}\equiv(-1)^\nu\pmod p$,

ე. ი. $\left(\frac{q}{p}\right)\equiv(-1)^\nu\pmod p$. როგორც წინათ ვიქცეოდით, შედარება შევცვალოთ ტოლობით, მივიღებთ $\left(\frac{q}{p}\right)=(-1)^\nu$. Gauss-ის ლემა: თუ ν ლუწია, მაშინ q კვადრატული ნაშთია. წინა ტოლობა ამტკიცებს ამ ლემას.

გადავდივართ შეკვეთადობის კანონის დამტკიცებაზე. მოყვანილი დამტკიცება Gauss-ს ეკუთვნის და Eisenstein-ის მიერ არის სახეშეცვლილი. თუ ვისარგებლებთ E სიმბოლოთი, მივიღებთ შემდეგ ტოლობებს:

$$1\cdot q=p\cdot E\left(\frac{1\cdot q}{p}\right)+r_1,\ 2q=p\cdot E\left(\frac{2q}{p}\right)+r_2,\ldots,\ \frac{p-1}{2}\cdot q=$$

$$=p\cdot E\left(\frac{\frac{p-1}{2}\cdot q}{p}\right)+r_{\frac{p-1}{2}}.$$

თუ ამ გამოსახულებებს შევკრებთ, მივიღებთ

$$\frac{p^2-1}{8}q=p\Sigma+r_1+r_2+\cdots+r_{\frac{p-1}{2}}, \qquad \text{I}$$

სადაც Σ არის $E\left(\frac{kq}{p}\right)$ ფუნქციათა ჯამი, როცა $k=1, 2, 3, \ldots, \frac{p-1}{2}$.

ჩვენ ვიცით, რომ $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ არის სხვა მიმდევრობით აღებული $\alpha_1, \alpha_2, \ldots, \alpha_\mu$; $\beta_1, \beta_2, \ldots, \beta_\nu$ რიცხვები, ამიტომ $\alpha_1+\alpha_2+\cdots+\alpha_\mu+p-\beta_1+p-\beta_2+\cdots+p-\beta_\nu=1+2+3+\cdots+\frac{p-1}{2}$,

ე. ი. (I′) $\Sigma\alpha+\nu p-\Sigma\beta=\frac{p^2-1}{8}$. შევნიშნოთ, რომ $\Sigma\alpha+\Sigma\beta=\Sigma r$ და I ტოლობას გამოვაკლოთ I′. მივიღებთ

$$-\frac{p^2-1}{8}(q-1)=p\Sigma+2\Sigma\beta-\nu\cdot p. \qquad \text{II}$$

ახლა განვიხილოთ ორი შემთხვევა:

1) $q=2$; 2) q კენტი მარტივი რიცხვია.

1) $q=2$; მაშინ $\Sigma=0$ და $\frac{p^2-1}{8}=2\Sigma\beta-\nu p$, რაც ნიშნავს, რომ $\frac{p^2-1}{8}\equiv-\nu p \pmod 2$, ე. ი. $\frac{p^2-1}{8}\equiv\nu \pmod 2$. Gauss-ის ლემის თანახმად, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

8-ის ტოლი მოდულით ნებისმიერ კენტ რიცხვს ექნება შემდეგი ოთხი სახიდან ერთ-ერთი: $8n+1$, $8n+3$, $8n+5$, $8n+7$. თუ p-ს მაგიერად ამ გამოსახულებებს ჩავსვამთ, მივიღებთ, რომ თუ $p=8n+3$ ან $p=8n+5$, მაშინ $\left(\frac{2}{p}\right)=-1$. ე. ი. 2 არის $8n\pm1$ სახის მარტივი რიცხვების კვადრატული ნაშთი და $8n\pm3$ მარტივი რიცხვების კვადრატული არანაშთი.

2) ვთქვათ, q კენტი მარტივი რიცხვია. მაშინ $(q-1)\cdot\frac{p^2-1}{8}$ ლუწი რიცხვია და II ტოლობა გვაძლევს

$$p\Sigma \equiv p\nu \pmod 2, \quad \text{ანუ} \quad \Sigma \equiv \nu \pmod 2.$$

გამოვიდა, რომ Σ და ν რიცხვებს ერთნაირი ლუწკენტოვნება აქვს.

თუ ვისარგებლებთ Gauss-ის ლემით, დავწერთ:

$$\left(\frac{q}{p}\right)=(-1)^{E\left(\frac{1\cdot q}{p}\right)+E\left(\frac{2q}{p}\right)+E\left(\frac{p-1/2q}{p}\right)+\dots}$$

თუ $q=2^{\omega}\cdot q'$, მაშინ, ზემოთ ნათქვამის საფუძველზე, მივიღებთ

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p^2-1}{8}\omega+\sum_{k=1}^{p-1/2}E\left(\frac{kq}{p}\right)}.$$

განვიხილოთ მაგალითი:

$$\left(\frac{11}{13}\right)=(-1)^{E\left(\frac{11}{13}\right)+E\left(\frac{22}{13}\right)+E\left(\frac{33}{13}\right)+E\left(\frac{44}{13}\right)\times}$$

$$\times(-1)^{+E\left(\frac{55}{13}\right)+E\left(\frac{66}{13}\right)}=(-1)^{0+1+2+3+4+5}=-1\ .$$

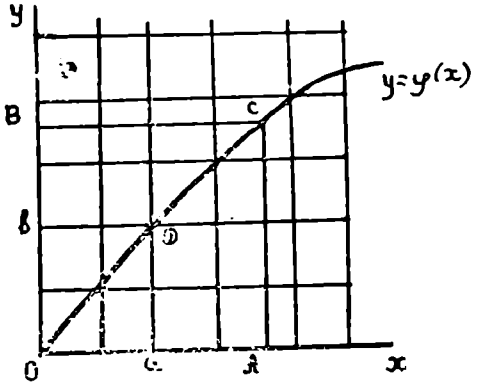
ახლა სიბრტყეზე მართკუთხა საკოორდინატო სისტემის მიმართ განვიხილოთ $y=\varphi(x)$ წირი, სადაც $\varphi(x)$ ცალსახა ფუნქციაა (ან ჩვენ ავირჩევთ გარკვეულ შტოს), უწყვეტია და გადაკვეთს საკოორდინატო ღერძების პარალელურ წრფეებს ერთ წერტილში და $\varphi(0)=0$. კოორდინატთა სათავე აღვნიშნოთ 0-ით, ღერძებზე გადავზომოთ მონაკვეთები 1, 2, 3,..., და მათ ბოლოებზე გავატაროთ ღერძების პარალელური წრფეები. მთელი სიბრტყე დაიყოფა კვადრატებად. მათ წვეროებს ვუწოდოთ კვანძები და განვიხილოთ AOBC ფიგურა. დავთვალოთ, რამდენი კვანძია AOBC კონტურის შიგნით. კონტური გავყოთ ორად და ჯერ განვიხილოთ AODC ფიგურა.

პირველი ორდინატი იქნება $\varphi(1)$, მეორე—$\varphi(2)$ და ა. შ. უკანასკნელი $\varphi(E(a))$. შევთანხმდეთ, არ ჩავთვალოთ კვანძები, რომლებიც ღერძებზე მდებარეობს. კვანძების რაოდენობა პირველ ორდინატზე

იქნება $E(\varphi(1))$, მეორეზე—$E(\varphi(2))$... უკანასკნელზე—$E(\varphi(E(a)))$. კვანძების საერთო რიცხვი არის

$$E(\varphi(1))+E(\varphi(2))+\cdots+E(\varphi E(a)).$$

ვთქვათ, ახლა, მოცემული ფუნქცია ამოვხსენით x-ის მიმართ და მივიღეთ $x=\psi(y)$.



განვიხილოთ აბსცისები $\psi(1)$, $\psi(2)$,..., $\psi(E(b))$. კვანძთა რაოდენობა OBCDO-ზე იქნება

$$E(\psi(1))+E(\psi(2)+\cdots+E(\psi(E(b)).$$

თუ ამ გამოსახულებებს შევკრებთ, მივიღებთ კვანძთა რაოდენობას მართკუთხედის შიგნით, გადიდებულს N რიცხვით, რადგან ის კვანძები, რომლებიც თვითონ წირზე მდებარეობს, თვლის დროს აბსცისებშიც შევა და ორდინატებშიც.

მაშასადამე,

$$E(\varphi(1))+E(\varphi(2))+\cdots+E(\varphi(E(a)))+E(\psi(1))+$$
$$+E(\psi(2)+\cdots+E(\psi(E(b)))=E(a)E(b)+N,$$

ან მოკლედ დავწერთ ასე

$$\sum_{1}^{E(\varphi(a))} E\,(\varphi(n)) + \sum_{1}^{E(\psi(b))} E(\psi(n))=E(a)\,E(b)+N\ .$$

φ ფუნქციად ავირჩიოთ $y=\frac{q}{p}x$, სადაც p და q კენტი მარტივი რიცხვებია. ავიღოთ $a=\frac{p}{2}$ და $b=\frac{q}{2}$, მაშინ

$$E(a)=\frac{p-1}{2}, \quad E(b)=\frac{q-1}{2}, \quad \psi(y)=x=\frac{p}{q}y .$$

თუ წრფე გადის კვანძის წერტილზე, მაშინ $\frac{x}{p}=\frac{y}{q}$ და $y=qh$, $x=ph$. ყველა ეს რიცხვი მთელია, ამიტომ ნახაზის შიგნით ჩვენი წრფე არ გაივლის კვანძის წერტილებზე, რადგან უდიდესი ორდინატი არის $\frac{q}{2}$ და უდიდესი აბსცისა — $\frac{p}{2}$, ამიტომ N=1, მაშასადამე,

$$E\left(\frac{q}{p}\right)+E\left(\frac{2q}{p}\right)+\ldots+E\left(\frac{\frac{p-1}{2}\cdot q}{p}\right)+E\left(\frac{p}{q}\right)+$$

$$+E\left(\frac{1\cdot p}{q}\right)+\ldots+E\left(\frac{\frac{q-1}{2}\cdot p}{q}\right)=\frac{p-1}{2}\cdot\frac{q-1}{2} .$$

ადრე გვქონდა, რომ

$$\left(\frac{q}{p}\right)=(-1)^{E\left(\frac{q}{p}\right)+E\left(\frac{2q}{p}\right)+\ldots+E\left(\frac{\frac{p-1}{2}\cdot q}{p}\right)};$$

$$\left(\frac{p}{q}\right)=(-1)^{E\left(\frac{p}{q}\right)+E\left(\frac{2p}{q}\right)+\ldots+E\left(\frac{\frac{q-1}{2}\cdot q}{q}\right)} .$$

თუ ამ ორ უკანასკნელ ტოლობას გადავამრავლებთ და მხედველობაში მივიღებთ წინა ფორმულას, გვექნება

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} .$$

ამ ფორმით შეკცევადობის კანონი პირველად ჩამოაყალიბა Legendre-მ. თუ ამ ფორმულით ვისარგებლებთ, მაშინ Legendre-ს სიმბოლოს გამოთვლა დაიყვანება $\left(\frac{-1}{p}\right)$, $\left(\frac{1}{p}\right)$ და $\left(\frac{2}{p}\right)$ სიმბოლოების დათვლაზე.

მაგალითი.

$$\left(\frac{609}{103}\right)=\left(\frac{94}{103}\right)=\left(\frac{2}{103}\right)\cdot\left(\frac{47}{103}\right)=-\left(\frac{9}{47}\right)=$$
$$=-\left(\frac{3}{47}\right)^2=-1\,.$$

ახლა შემოვიღოთ Iacobi-ს სიმბოლო. მას ფორმალური ხასიათი აქვს. ვთქვათ, P და Q ორი თანამარტივი რიცხვია, ამასთან, $P=p\cdot p'\cdot p''\cdots p^{(n)}$. მაშინ Iacobi-ს სიმბოლოდ მიღებულია

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p}\right)\left(\frac{Q}{p_1}\right)\cdot\left(\frac{Q}{p''}\right)\cdots\left(\frac{Q}{p^{(n)}}\right).$$

დავამტკიცოთ რამდენიმე თეორემა Iacobi-ს სიმბოლოს შესახებ.

თ ე ო რ ე მ ა I. ვთქვათ, $Q\equiv Q'\pmod P$, მაშინ

$$\left(\frac{Q}{P}\right)=\left(\frac{Q'}{P}\right).$$

მართლაც, მოცემული შედარებიდან ვღებულობთ

$$\left(\frac{Q}{p}\right)=\left(\frac{Q'}{p}\right),\ \left(\frac{Q}{p'}\right)=\left(\frac{Q'}{p'}\right),\ \ldots,\ \left(\frac{Q}{p^{(n)}}\right)=\left(\frac{Q'}{p^{(n)}}\right).$$

თუ გადავამრავლებთ, მივიღებთ $\left(\frac{Q}{P}\right)=\left(\frac{Q'}{P'}\right)$.

ანალოგიურად დამტკიცდება:

$$\left(\frac{QQ'}{P}\right)=\left(\frac{Q}{P}\right)\cdot\left(\frac{Q'}{P}\right);\quad\left(\frac{1}{P}\right)=1\,.$$

გამოვიყვანოთ ახლა $\left(\frac{-1}{P}\right)$ და $\left(\frac{2}{P}\right)$ Iacobi-ს სიმბო-

ლებისათვის Legendre-ის სიმბოლოების ანალოგიური ფორმულები. დავიწყოთ $\left(\frac{-1}{P}\right)$ სიმბოლოთი. ვთქვათ, $P = p \cdot p' \cdot p'' \cdots$ $\cdots p^{(n)}$, მაშინ

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p}\right)\left(\frac{-1}{p'}\right)\left(\frac{-1}{p''}\right)\cdots\left(\frac{-1}{p^{(n)}}\right).$$

ამიტომ

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{p-1}{2}+\frac{p'-1}{2}+\cdots+\frac{p^{(n)}-1}{2}}.$$

საბოლოო ფორმულის მისაღებად ვიყენებთ ხელოვნურ ხერხს. გვაქვს: $P=p\cdot p'p''\cdots p^{(n)}$, ანუ $P=((p-1)+1)\cdot((p'-1)+1)\cdots$ $(p^{(n)}-1)+1)$. ფრჩხილების გახსნის შემდეგ გვექნება

$$P=4A+(p-1)+(p'-1)+\cdots+(p^{(n)}-1)+1,$$

სადაც 4A-ში შედის 4-ის ჯერადი ყველა რიცხვი. აქედან

$$\frac{P-1}{2}=2A+\frac{p-1}{2}+\frac{p'-1}{2}+\ldots+\frac{p^{(n)}-1}{2}.$$

და რადგან

$$(-1)^{\frac{P-1}{2}}=(-1)^{\frac{p-1}{2}+\frac{p'-1}{2}+\cdots+\frac{p^{(n)}-1}{2}},$$

ე. ი. $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$.

განვიხილოთ ახლა $\left(\frac{2}{P}\right)$ სიმბოლო. განსაზღვრის ძალით,

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p}\right)\left(\frac{2}{p'}\right)\cdots\left(\frac{2}{p^{(n)}}\right).$$

ვიცით, რომ

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}},\ \left(\frac{2}{p'}\right)=(-1)^{\frac{p'^2-1}{8}},\ \ldots,\left(\frac{2}{p^{(n)}}\right)=$$

$$= (-1)^{\frac{p^{(n)2}-1}{8}}.$$

შემდეგ დავწეროთ იგივეობა:

$$P^2 = ((p^2-1)+1)\ ((p'^2-1)+1)\cdots((p^{(n)2}-1)+1).$$

ვაჩვენოთ, რომ ნებისმიერი სხვაობა ამ იგივეობაში 8-ის ჯერადია. რადგან P კენტი მარტივი რიცხვია, ამიტომ მას აქვს $4n+1$ ან $4n+3$ სახე, ანუ $4n\pm1$ სახე. $p^2 = 16n^2 \pm 8n + 1$, საიდანაც ჩანს, რომ $8 \mid (P^2-1)$. ამიტომ,

$$P^2 = 64A + (p^2-1) + (p'^2-1) + \cdots + (p^{(n)2}-1) + 1.$$

და, როგორც წინა შემთხვევაში, ვპოულობთ, რომ

$$\left(\frac{2}{p}\right) = (-1)^{\frac{P^2-1}{8}}.$$

ახლა განვიხილოთ გამოსახულება

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \left(\frac{P}{q'}\right)\left(\frac{P'}{q''}\right)\cdots\left(\frac{P}{q^{(n)}}\right)\cdot\left(\frac{Q}{p'}\right)\left(\frac{Q}{p''}\right)\cdots$$
$$\cdots\left(\frac{Q}{p^{(n)}}\right),$$

სადაც P და Q კენტი მარტივი რიცხვებია, $P = p'p''\cdot p'''\cdots p^{(n)}$, $Q = q'q''\cdots q^{(n)}$.

თუ Legendre-ის სიმბოლოებს დავშლით, მივიღებთ

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \Pi\left(\frac{p^{(i)}}{q^{(i)}}\right)\Pi\left(\frac{q^{(i)}}{p^{(i)}}\right) = \Pi(-1)^{\frac{p^{(i)}-1}{2}\cdot\frac{q^{(i)}-1}{2}} =$$

$$= (-1)^{\Sigma\frac{p^{(i)}-1}{2}\cdot\frac{q^{(i)}-1}{2}}.$$

ჩვენ დამტკიცებული გვაქვს, რომ

$$(-1)^{\frac{P-1}{2}} = (-1)^{\Sigma\frac{p^{(i)}-1}{2}} \quad \text{და} \quad (-1)^{\frac{Q-1}{2}} = (-1)^{\Sigma\frac{q^{(i)}-1}{2}},$$

საიდანაც ვღებულობთ

$$(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} = (-1)^{\Sigma\frac{p^{(i)}-1}{2}\cdot\frac{q^{(i)}-1}{2}}.$$

მართლაც, ვნახეთ, რომ

$$\frac{P-1}{2} \equiv \Sigma\frac{p^{(i)}-1}{2} \pmod 2 \quad \text{და} \quad \frac{Q-1}{2} \equiv \Sigma\frac{q^{(i)}-1}{2} \pmod 2 .$$

ამ შედარებების გადამრავლება მოგვცემს

$$\frac{P-1}{2}\cdot\frac{Q-1}{2} \equiv \Sigma\frac{p^{(i)}-1}{2}\cdot\frac{q^{(i)}-1}{2} \pmod 2 .$$

აქედან კი პირდაპირ გამოდის

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Jacobi-სა და Legendre-ის სიმბოლოებში განიხილავენ უარყოფით რიცხვებსაც. უშვებენ, რომ $\left(\frac{Q}{-P}\right)=\left(\frac{Q}{P}\right)$. ამ დროს ძალაში რჩება თეორემები: $\left(\frac{Q}{P}\right)=\left(\frac{Q'}{P}\right)$, თუ $Q\equiv Q' \pmod P$ და $\left(\frac{QQ'}{P}\right)=\left(\frac{Q}{P}\right)\left(\frac{Q'}{P}\right)$, ხოლო თეორემა $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$ შეიძლება არასწორი აღმოჩნდეს.

დაბოლოს, თუ P და Q რიცხვები თანამარტივი არ არის, მაშინ $\left(\frac{P}{Q}\right)=0$. Iacobi-ს სიმბოლოს გამოყენება ამარტივებს Legendre-ის სიმბოლოს.

მაგალითი. $\left(\frac{242}{97}\right)=\left(\frac{48}{97}\right)=\left(\frac{2}{97}\right)^4\left(\frac{3}{97}\right)=\left(\frac{3}{97}\right)=$

$$=\left(\frac{1}{3}\right)=1;$$

$$\left(\frac{336}{97}\right)=\left(\frac{45}{97}\right)=\left(\frac{97}{45}\right)=\left(\frac{45}{7}\right)=\left(\frac{3}{7}\right)=\left(\frac{-1}{3}\right)=-1 .$$

Jacobi-ს სიმბოლო იმით არის მოხერხებული, რომ საჭირო არ არის რიცხვის დაშლა მარტივ მამრავლებად, რაც დიდი რიცხვებისთვის საკმაოდ ძნელია.

ჩვენ განვიხილეთ მე-2 ხარისხის შედარებები და ვნახეთ, რომ მათ ან აქვთ ფესვები, ან არა. ახლა ვნახოთ, როგორ ვიპოვოთ ეს ფესვები მათი არსებობის შემთხვევაში. I ხარისხის შედარებისთვის ჩვენ მივიღეთ ზოგადი ფორმულა

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

ირკვევა, რომ მე-2 ხარისხის შედარებისთვის ზოგადი ფორმულის დაწერა არ ხერხდება. მაგრამ მარტივი მოდულის დროს ზოგიერთ კერძო შემთხვევაში ვახერხებთ ზოგადი ფორმულის გამოყვანას. ვთქვათ, $p=4m+3$ მარტივი რიცხვია და შედარება $x^2 \equiv q \pmod{p}$ ამოხსნადია.

განტოლების ამოხსნადობის პირობაა $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. ჩვენს შემთხვევაში გამოდის, $q^{2m+1} \equiv 1 \pmod{p}$. ე. ი. $q^{2m+2} \equiv q \pmod{p}$, $(q^{m+1})^2 \equiv q \pmod{p}$. უკანასკნელი შედარება გვაძლევს, რომ, თუ ავიღებთ $x = q^{m+1}$, მაშინ დაკმაყოფილდება ჩვენი შედარება. მივიღეთ შედარების ერთი ამონახსნი. თუ α-თი აღვნიშნავთ ნაშთს, რომელიც მიიღება q^{m+1}-ის p რიცხვზე გაყოფის დროს, მაშინ შედარების ამონახსნები ჩაიწერება ასე:

$$x \equiv \alpha \pmod{p}, \quad x \equiv p - \alpha \pmod{p}.$$

ე. ი. $4m+3$ სახის მარტივი მოდულისათვის ჩვენ ვიცით შედარების ამონახსნების პოვნა.

შემდეგში გავეცნობით ნებისმიერი ხარისხის შედარების ამოხნის ზოგად მეთოდს. ახლა კი გადავიდეთ სხვა საკითხების შესწავლაზე.

რიცხვთა ალგებრული თეორია

რაციონალურობის არე

შემოვიღოთ რაციონალურობის არის ცნება. რაციონალურობის არე ეწოდება იმ რიცხვთა ერთობლიობას, რომლებიც მიიღება α რიცხვზე რაციონალური ოპერაციების ჩატარებით. ეს არე აღინიშნება

$R(\alpha)$ სიმბოლოთი. შეიძლება განვიხილოთ რაციონალურობის არეები, რომლებშიც ძირითადი ელემენტია არა α, არამედ რამდენიმე რიცხვი $\alpha, \beta, \ldots, \omega$. ასეთი არე $R(\alpha, \beta, \ldots \omega)$ სიმბოლოთი აღინიშნება. მის ყოველ ელემენტს ექნება სახე:

$$\frac{P(\alpha,\beta,\ldots,\omega)}{Q(\alpha,\beta,\ldots,\omega)}.$$

სადაც P და Q რაციონალურკოეფიციენტებიანი მთელი მრავალწევრებია. ადვილად დავინახავთ, რომ ნებისმიერ რაციონალურობის არეში შევა ყველა რაციონალური რიცხვი; მათ შორის 0 და 1. თუ რიცხვთა თეორიის სულისკვეთებით ვიმსჯელებთ, მაშინ რაციონალურობის არიდან შეიძლება გამოიყოს მთელობის არე, რომელიც შეკრების, გამოკლებისა და გამრავლების ოპერაციებით მიიღება. მთელობის არეს $R[\alpha]$ ან $[\alpha]$ სიმბოლოთი აღვნიშნავთ. $R[\alpha, \beta-\ldots, \omega]$ არის ელემენტებს აქვს სახე $R[\alpha, \beta, \gamma,\ldots, \omega]$, სადაც P მთელი მრავალწევრია მთელი კოეფიციენტებით.

მთელობის არე შეიძლება დამოუკიდებლად განვმარტოთ წინა აზრით, როგორც $[1, \alpha, \beta,\ldots, \omega]$. თვითონ I არ მიიღება დანარჩენი ელემენტებისგან სამი მოქმედების შესრულებით. უმარტივესი მთელობის არე არის [1]—ყველა მთელ რიცხვთა არე. რიცხვთა ალგებრული თეორია განიხილავს $[1, \alpha]$ სახის არეს, სადაც α რაიმე ალგებრული განტოლების ფესვია. ეს თეორია განავითარეს Dedekind-მა, Klosterman-მა და მათმა მოწაფეებმა.

ჩვენ მოდულს ვუწოდებთ ისეთი სიდიდეების სისტემას, რომელთა ჯამი და სხვაობა კვლავ ამ სისტემაში შედის. მოდულის მაგალითი უკვე განვიხილეთ [1] არეში. ახლა განვიხილოთ სხვა ხასიათის მოდულები. ვთქვათ, μ მარტივი რიცხვია, ხოლო $\varphi(x)$ მთელკოეფიციენტებიანი მრავალწევრია, რომლის კოეფიციენტები არ იყოფა p-ზე.

განვიხილოთ გამოსახულება

$$pf(x)+\varphi(x)\psi(x).$$

ასეთი გამოსახულებების ერთობლიობა ქმნის მოდულს. შევნიშნოთ შემდეგი: ვთქვათ, მოცემულია $[1, \alpha, \beta,\ldots, \omega]$ და ავირჩიეთ k ელემენტი $M_1M_2,\ldots, M_k$, მაშინ

$$C_1M_1+C_2M_2+\cdots+C_kM_k$$

სახის გამოსახულება, სადაც c_i მოცემული არის ელემენტებია, ქმნის მოდულს. მართლაც, ვთქვათ, გვაქვს ორი ასეთი სახის გამოსახულება

$$\sum_1^k C_i M_i \quad \text{და} \quad \sum_1^k C_i' M_i ,$$

მაშინ

$$\sum_1^k C_i M_i \pm \sum_1^k C_i' M_i = \sum_1^k (C_i + C_i') M_i = \sum_1^k C''_i M_i .$$

რაც უნდა დაგვემტკიცებინა.

პირველადი ფორმების შესახებ

შემოვიღოთ პირველადი ფორმის ცნება. ვთქვათ, გვაქვს m ხარისხის შედარება $a_0 x^m + a_1 x^{m-1} + \cdots + a_m \equiv 0 \pmod p$.

თუ a_0 არ იყოფა p-ზე (ეს ყოველთვის ასეა), მაშინ შეიძლება ვიპოვოთ a_i' $(1, 2, \ldots, m)$ რიცხვები, რომლებიც აკმაყოფილებს შედარებას $a_0 \cdot a_i' \equiv a_i \pmod p$ და $a_0 x + yp = a_i$. ჩვენი შედარება შემდეგ სახეს მიიღებს

$$a_0 (x^m + a_1' x^{m-1} + \cdots + a'_m) \equiv 0 \pmod p,$$

ანუ

$$x^m + a'_1 x^{m-1} + \cdots + a'm \equiv \pmod p.$$

ასეთ შედარებას, რომლის უმაღლესი ხარისხის კოეფიციენტი 1-ის ტოლია, ეწოდება პირველადი ფორმა.

ვთქვათ, გვაქვს ორი შედარება.

$$\varphi(x) \equiv \alpha_0 x^\mu + \alpha_1 x^{\mu-1} + \cdots + \alpha\mu \pmod p$$

და

$$\psi(x) \equiv \beta_0 x^\nu + \beta_1 x^{\nu-1} + \cdots + \beta\nu \pmod p.$$

ვაჩვენოთ, რომ ამ შედარებათა ნამრავლის ხარისხი შესაბამისი ხარისხების ჯამის ტოლია, მართლაც,

$$\varphi(x)\psi(x) \equiv \alpha_0\beta_0 x^{\mu+\nu} + (\alpha_0\beta_1 + \beta_0\alpha_1) x^{\beta+\upsilon-1} + \cdots \pmod p$$

რადგან α_0 და β_0 არ იყოფა p-ზე, ამიტომ უკანასკნელი შედარების ხარისხი არის $\mu+\nu$, რაც უნდა დაგვემტკიცებინა.

შედეგი: თუ $\varphi(x)\cdot\psi(x)$ ნამრავლი იგივურად ნულის სადარია p მოდულით, მაშინ ამ ფაქტორებიდან ერთ-ერთი მაინც იგივურად ნულის სადარია ამ მოდულით. მართლაც, თუ $\varphi(x)$ და $\psi(x)$ არც ერთი არ არის იგივურად 0-ის სადარი p მოდულით, მაშინ თითოეულს ექნება გარკვეული ხარისხი და ნამრავლის ხარისხიც განსაზღვრული რიცხვი იქნება. ეს კი შეუძლებელია.

მრავალწევრი დავშალოთ მამრავლებად p მოდულის მიხედვით. ვთქვათ, გვაქვს შედარება $f(x)\equiv 0 \pmod p$ და ξ რიცხვი მისი ფესვია, მაშინ

$$f(x)\equiv(x-\xi)f_1(x) \pmod p,$$

სადაც $f_1(x)$ არის მთელკოეფიციენტებიანი მრავალწევრი, რომლის კოეფიციენტები არ აღემატება $f(x)$ მრავალწევრის კოეფიციენტებს, თუ $f(x)$-ის ხარისხია m, მაშინ $f_1(x)$-ის ხარისხია $m-1$. თუ ვიპოვით მოცემული შედარების მეორე ამონახსნს, კიდევ გამოვყოფთ ფაქტორს და ა.შ. ამ პროცესს იმ აზრამდე მივყავართ, რომ განვიხილოთ შემდეგი სახის შედარებები

$$f(x)\equiv\varphi(x)\psi(x) \pmod p.$$

ამ შემთხვევაში ამბობენ, რომ $f(x)$ იშლება p მოდულით ფაქტორებად, ე. ი.

$$f(x)=\varphi(x)\psi(x)+pf(x).$$

ეს გამოსახულება ასეც ჩაიწერება

$$f(x)\equiv 0 \pmod{pf(x)}.$$

მივიღეთ შედარება ორმაგი მოდულით. ჩვენ ვხედავთ, რომ $f(x)$ არის ორმაგი მოდულის ერთ-ერთი ელემენტი. მნიშვნელოვანია კიდევ ერთი ცნება. თუ გვაქვს შედარება

$$f(x)\equiv\psi(x)\psi(x) \pmod p,$$

მაშინ ამბობენ, რომ $\varphi(x)$ და $\psi(x)$ არის $f(x)$-ის გამყოფები p მოდულით. ვაჩვენოთ, რომ ნებისმიერი რიცხვი, რომელიც p-ზე არ იყოფა, $f(x)$-ის გამყოფია. ვთქვათ, $D(a, p)=1$. ვიპოვოთ a რიცხვი socin p მოდულით, ე. ი. ისეთი a_1 რიცხვი, რომ $aa_1\equiv 1 \pmod p$, გავამრავლოთ $f(x)\equiv f(x) \pmod p$ შედარების ორივე მხარე წინა შედარებაზე. მივიღებთ $f(x)\equiv aa_1 f(x) \pmod p$. ან სხვა აღნიშვნით

$$(f(x) \equiv a.\ f_1 \cdot (x) \pmod{p}.$$

ეს კი ნიშნავს, რომ a არის $f(x)$-ის გამყოფი p მოდულით. რადგან ეს a რიცხვები (ე. ი. ნული ხარისხის ფუნქციები, რომლებიც არასადარია p მოდულით) ისეთი ყოფაქცევისაა, როგორც ერთიანი მთელ რიცხვთა თეორიაში, ამიტომ მათ p მოდულით ერთიანი ეწოდება, ხოლო $f_1(x)$-ს ეწოდება $f(x)$-საგან განსხვავებული არაარსებითი გამყოფი. არც ერთიანს, არც არაარსებით გამყოფებს ჩვენ გამყოფებად არ ჩავთვლით. თუ $f(x)$ მრავალწევრს არ გააჩნია ერთიანის გარდა არც ერთი გამყოფი, რომელიც არსებითად განსხვავდება თვითონ ფუნქციისაგან, მაშინ $f(x)$ ფუნქციას ეწოდება p მოდულით დაუყვანადი. ასეთი ფორმით განმარტება აღებულია ალგებრიდან, მხოლოდ ტოლობის ნიშანი შედარების ნიშნით არის შეცვლილი. შემდეგში ვნახავთ, რომ დაუყვანადი ფუნქციები მარტივი რიცხვების როლს ასრულებს.

ჩვენ შეგვიძლია p მოდულით სადარი ყველა მრავალწევრი ერთ კლასში მოვათავსოთ. ასეთი კლასების რიცხვი უსასრულო იქნება, რადგან არსებობს p მოდულით სადარი ნებისმიერი ხარისხის მრავალწევრები. თუ დავსვამთ კითხვას, რამდენი არსებობს მოცემული m ხარისხი p მოდულით არასადარი მრავალწევრი, ე. ი. ისეთი მრავალწევრები, რომლებიც სხვადასხვა კლასს ეკუთვნის, მაშინ მივიღებთ სრულიად გარკვეულ პასუხს. ასეთი სახის ყველა მრავალწევრს ექნება სახე:

$$a_0x^m + a_1x^{m-1} + \ldots + a_m,$$

სადაც a_0 არ იყოფა p-ზე. რადგან ორი მრავალწევრი p მოდულით სადარია ან არა, იმის მიხედვით, სადარია თუ არა შესაბამისი კოეფიციენტები, ამიტომ ჩვენ მივიღებთ p მოდულით არასადარ m ხარისხის ყველა არასადარ ფუნქციას, თუ ყველა კოეფიციენტს მივცემთ 1, 2, 3, ..., (p—1) მნიშვნელობას. ყოველი კომბინაცია მოგვცემს ერთ ფუნქციას და სულ ასეთი კომბინაციების რაოდენობა იქნება $(p-1)p^m$.

პირველად ფორმებში პირველი კოეფიციენტი არის 1, ამიტომ m მოდულით არასადარი m ხარისხის პირველადი ფორმების რაოდენობა იქნება p^m.

დავუბრუნდეთ მრავალწევრთა გაყოფადობის საკითხს. განვიხილოთ ორი მრავალწევრის საერთო გამყოფები p მოდულით და განვმარტოთ უდიდესი საერთო გამყოფი. თუ გვაქვს ორი შედარება

$$f_1(x) \equiv f_1'(x)\varphi(x) \pmod{p},$$
$$f_2(x) \equiv f_2'(x)\varphi(x) \pmod{p},$$

მაშინ ამბობენ, რომ $\varphi(x)$ არის f_1 და f_2 ფუნქციების საერთო გამყოფი p მოდულით. საერთო გამყოფების საპოვნელად არსებობს მთელ რიცხვთა სიმრავლეში ევკლიდის ალგორითმის ანალოგიური ალგორითმი.

ვთქვათ, f_2-ის ხარისხი არ აღემატება f_1-ის ხარისხს, მაშინ $f_1(x)$ შეიძლება ასე წარმოვადგინოთ:

$$f_1(x) \equiv f_2(x)\varphi(x) + f_3(x) \pmod{p},$$

სადაც $f_3(x)$-ის ხარისხი ნაკლებია $f_2(x)$-ის ხარისხზე. ამაში შეიძლება თანდათანობით დავრწმუნდეთ. ვთქვათ, a_0 და b_0 არის $f_1(x)$ და $f_2(x)$ მრავალწევრების უფროსი კოეფიციენტები შესაბამისად. c_0 რიცხვი ავირჩიოთ $a_0 \equiv b_0 c_0 \pmod{p}$ პირობიდან და შევადგინოთ გამოსახულება

$$f_1(x) - c_0 x^{m_1 - m_2} f_2(x),$$

სადაც m_1 და m_2 არის $f_1(x)$ და $f_2(x)$ მრავალწევრების ხარისხები შესაბამისად. თუ ამ გამოსახულებას p მოდულით განვიხილავთ, შევნიშნავთ, რომ უფროსი წევრი გაბათილდება და გამოსახულების ხარისხი ნაკლებია ან ტოლი $(m_1 - 1)$-ის. ამის შემდეგ $(f_1(x) - c_0 x^{m_1 - m_2} f_2(x))$ გამოსახულებას გამოვაკლოთ შესაბამის კოეფიციენტზე გამრავლებული $f_2(x)$. ხარისხი ისევ დაიწევს. თუ ასე რამდენჯერმე მოვიქცევით, მივაღწევთ იმას, რომ გამოსახულების ხარისხი ნაკლები გახდება m_2-ზე. ავიღოთ ახლა ყველა წევრი, რომელიც $f_1(x)$-ს აკლდება, $f_2(x)$ გავიტანოთ ფრჩხილებს გარეთ. მივიღებთ:

$$f_1(x) - f_2(x)\,(c_0 x^{m_1 - m_2} + c_0' x^{m_1' - m_2} + \ldots + c_0^{(l)} x^{m_1^{(l)} - m_2})$$

ფრჩხილებში მოთავსებული გამოსახულება აღვნიშნოთ $\varphi_1(x)$-ით. მივიღებთ

$$f_1(x) - f_2(x)\varphi_1(x) = f_3(x) + pf(x),$$

ანუ

$$f_1(x) \equiv f_2(x)\varphi_1(x) + f_3(x) \pmod{p}.$$

ახლა იგივე გავიმეოროთ $f_2(x)$ და $f_3(x)$-ის მიმართ. მაშინ გვექნება

$$f_2(x) \equiv f_3(x)\varphi_2(x) + f_4(x) \pmod{p}.$$

$f_i(x)$ ფუნქციის ხარისხი მცირდება ნომრის გაზრდასთან ერთად. უკანასკნელის წინა გამოსახულება ასეთი მიიღება

$$f_{k-3}(x)\equiv f_{k-2}(x)q_{k-3}(x)+f_{k-1}(x) \pmod p.$$

ხოლო უკანასკნელი

$$f_{k-2}(x)\equiv f_{k-1}(x)q_{k-2}(x) \pmod p.$$

რადგან პროცესი სასრულია, ამიტომ უკანასკნელ გამოსახულებას აუცილებლად მივიღებთ. თუ განვიხილავთ მიღებულ შედარებებს, შევნიშნავთ, რომ $f_1(x)$ და $f_2(x)$-ის ყოველი საერთო გამყოფი არის $f_{k-1}(x)$-ის გამყოფი და პირიქით. მაშასადამე, $f_{k-1}(x)$-ის გამყოფები და მხოლოდ ისინი არის $f_1(x)$ და $f_2(x)$ ფუნქციების საერთო გამყოფები p მოდულით. ეს შედეგი საშუალებას გვაძლევს $f_{k-1}(x)$ ფუნქციას ვუწოდოთ $f_1(x)$ და $f_2(x)$ მრავალწევრების უდიდესი საერთო გამყოფი p მოდულით. ჩატარებული მსჯელობიდან გამომდინარე, უდიდესი საერთო გამყოფის შესახებ ყველა თეორემა, რომელიც არითმეტიკაში მტკიცდება, სამართლიანი იქნება ჩვენს შემთხვევაშიც. მაგალითად, p მოდულით მოცემული შედარებებიდან ადვილად ვღებულობთ თანაფარდობას

$$f_1(x)F_1(x)+f_2(x)F_2(x)\equiv D(x) \pmod p.$$

სადაც $D(x)=f_{k-1}(x)$, ხოლო $F_1(x)$ და $F_2(x)$ მთელი მრავალწევრებია. თუ ორი ფუნქციის უდიდესი საერთო გამოყოფი p მოდულით არის ერთიანი, მაშინ ამ მრავალწევრებს p მოდულით თანამარტივი მრავალწევრები ეწოდება. ამ შემთხვევაში წინა შედარებას ექნება სახე

$$f_1(x)F_1(x)+f_2(x)F_2(x)\equiv e \pmod p.$$

ამ შედარების ორივე მხარე გავამრავლოთ e-ს socin e'-ზე და დავუშვათ, $F_1(x)e'=f'_1(x)$, $F_2(x)e'=f'_2(x)$. მივიღებთ

$$f_1(x)f'_1(x)+f_2(x)f'_2(x)\equiv 1 \pmod p.$$

ეს შედარება მრავალ საინტერესო შედეგს იძლევა. მაგ., თუ $f_1(x)$ და $f_2(x)$ p მოდულით თანამარტივი მრავალწევრებია, მაშინ ყოველთვის ამოხსნადია შედარება

$$f_1(x)\chi_1+f_2(x)\chi_2\equiv 1 \pmod p. \qquad (1)$$

ანალოგიური სურათია არითმეტიკაში. თუ a და b თანამარტივი რიცხვებია, მაშინ $ax+by=1$ განტოლებას ყოველთვის გააჩნია მთელი

ამონახსნი. შემდეგ, თუ $f_1(x)$ და $f_2(x)$ p მოდულით თანამარტივი მრავალწევრებია, ხოლო $\varphi(x)$ მთელი მრავალწევრია, მაშინ $f_1(x)$ $\varphi(x)$ და $f_2(x)$ მრავალწევრების საერთო გამყოფები p მოდულით იქნება $\varphi(x)$ და $f_2(x)$ მრავალწევრების საერთო გამყოფი. ე. ი.

$$D(f_1(x)\cdot\varphi(x),\ f_2(x))=D(\varphi(x),\ f_2(x)),\ \text{თუ}\ D(f_1(x),\ f_2(x))=1$$

მართლაც, გავამრავლოთ (1) შედარების ორივე მხარე $\varphi(x)$-ზე. მივიღებთ

$$f_1(x)\varphi(x)f'_1(x)+f_2(x)\varphi(x)f'_2(x)\equiv\varphi(x)\pmod p.$$

ეს კი იმას ნიშნავს, რომ $f_1(x)$ $\varphi(x)$ და $f_2(x)$ მრავალწევრების ნებისმიერი საერთო გამყოფი არის $\varphi(x)$-ის გამყოფი p მოდულით.

თ ე ო რ ე მ ა I. თუ $D(f_1,\ f_2)=1$, $f_1\cdot\varphi$ იყოფა f_2-ზე, მაშინ φ იყოფა f_2-ზე p მოდულით.

თ ე ო რ ე მ ა II. თუ $D(f_1,\ f_2)=1$, $D(\varphi,f_2)=1$, მაშინ $D(f_1\cdot\varphi_1f_2)=1$.

თ ე ო რ ე მ ა III. თუ რამდენიმე მრავალწევრის ნამრავლი p მოდულით იყოფა დაუყვანად მრავალწევრზე, მაშინ მასზე გაიყოფა ერთი თანამამრავლი მაინც.

თეორემის დასამტკიცებლად გავიხსენოთ, რომ დაუყვანად მრავალწევრებს აქვს ორი არაარსებითად განსხვავებული გამყოფი—ერთიანი და თავისი თავი. ვთქვათ, ახლა $f(x)\varphi(x)$ იყოფა p მოდულით $P(x)$ დაუყვანად მრავალწევრზე. შესაძლებელია ასეთი შემთხვევები: ან $f(x)$ იყოფა $P(x)$-ზე და თეორემა დამტკიცებულია, ან $f(x)$ და $P(x)$ მრავალწევრების საერთო გამყოფი მხოლოდ ერთიანია. მაშინ $f(x)$ და $P(x)$ თანამარტივი მრავალწევრებია და II თეორემის თანახმად, $\varphi(x)$ იყოფა $P(x)$-ზე p მოდულით. თეორემა დამტკიცებულია. ამ თეორემის გამოყენებით ადვილად ვამტკიცებთ მრავალწევრის დაუყვანად მრავალწევრებად დაშლის ერთადერთობას.

სურათი იმგვარია, როგორც არითმეტიკაში. მოცემული ფუნქცია ან დაუყვანადია p მოდულით, ან გამყოფებად აქვს ორი ან რამდენიმე მრავალწევრი, რომლებიც არსებითად განსხვავდება $f(x)$-სგან. ამ გამყოფების ხარისხი $f(x)$-ის ხარისხზე ნაკლებია. ვთქვათ, ერთერთი ასეთი ფუნქცია არის $P_0(x)$. მაშინ

$$f(x)\equiv P_0(x)f_1(x)\pmod p.$$

თუ $P_0(x)$ უმცირესი ხარისხის გამყოფია, მაშინ ის დაუყვანადი მრავალწევრია, რადგან წინააღმდეგ შემთხვევაში გვექნება

$$P_0(x) \equiv \varphi(x)\psi(x), \pmod{p}$$

და $\varphi(x)$ და $\psi(x)$ მრავალწევრების ხარისხები ნაკლებია $P_0(x)$-ის ხარისხზე, ეს კი პირობას ეწინააღმდეგება.

ანალოგიურად მოვიქცეთ $f_1(x)$-ის შემთხვევაში. დაერწმუნდებით, რომ

$$f_1(x) \equiv P_1(x) f_2(x) \pmod{p}$$
$$f_2(x) \equiv P_2(x) f_3(x) \pmod{p}$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$f_{n-1}(x) \equiv P_{n-1}(x) f_n(x) \pmod{p},$$

სადაც $f_n(x)$ არის დაუყვანადი მრავალწევრი $P_n(x)$. თუ ამ შედარებებს გავითვალისწინებთ, მივიღებთ

$$f(x) \equiv P_0(x) P_1(x) \cdots P_n(x) \pmod{p}.$$

ყოველი დაუყვანადი მრავალწევრი შეიძლება მივიყვანოთ პირველად ფორმამდე.

$$P_i(x) \equiv a_i \Pi_i(x) \pmod{p}.$$

თუ აღვნიშნავთ $\alpha = a_0 a_1 \cdots a_n$, მივიღებთ $f(x)$-ის დაშლას პირველად დაუყვანად მრავალწევრებად

$$f(x) \equiv \alpha \Pi_0(x) \Pi_1(x) \cdots \Pi_n(x) \pmod{p},$$

სადაც α ერთიანია p მოდულით. ზუსტად ისე, როგორც არითმეტიკაში. მტკიცდება ამ დაშლის ერთადერთობა.

მოდულთა სისტემის მოკლე თეორია

ჩვენ მოდული ვუწოდეთ ისეთ ელემენტთა სიმრავლეს, რომელთა ჯამი და სხვაობა კვლავ ამ სიმრავლეს ეკუთვნის. [1] არისთვის მოდული მარტივ საბეზე მიიყვანება. ეს არის zd სახის რიცხვები, თვითონ d-საც მოდული ეწოდება. ვნახოთ ახლა, როგორ შეიძლება განვაზოგადოთ მოდულის ცნება და შემოვიღოთ მოდულური სისტემის ცნება. ჩვენი არიდან ავირჩიოთ μ ელემენტი $M_1, M_2, \ldots, M_\mu$ და შევადგინოთ შემდეგი სახის ელემენტები

$$c_1 M_1 + c_2 M_2 + \cdots + c_\mu M_\mu,$$

სადაც c_i ამავე არის ნებისმიერი ელემენტია. როგორც ვხედავთ, ასეთ ელემენტთა სიმრავლე $\sum_1^m c_i M_i$ ქმნის მოდულს. ეს მოდული სავსებით ხასიათდება $M_1, M_2, \ldots, M\mu$ ელემენტებით. ამ μ ელემენტთა ერთობლიობას ეწოდება მოდულური სისტემა და აღინიშნება $(M_1, M_2, \ldots, M\mu)$ ან მოკლედ (M).

ასეთი სისტემები შეიძლება [1] არისთვისაც განვიხილოთ, მაგრამ ახალს ვერაფერს მივიღებთ. ირკვევა, რომ ამ არეში ყოველი მოდულური სისტემა ერთი რიცხვის ტოლფასია. ზოგად დამტკიცებაზე არ შევჩერდებით. განვიხილავთ მხოლოდ მაგალითს. ავიღოთ მოდულური სისტემა $(8, 6)$, ე. ი. $8c_1+6c_2$ სახის რიცხვები, სადაც c_1 და c_2 ნებისმიერი მთელი რიცხვებია. ცხადია, ყოველი ასეთი რიცხვი $2z$ რიცხვის ეკვივალენტურია და $(8, 6)$ მოდულური სისტემა ემთხვევა რიცხვს 2-ს.

ზოგად შემთხვევაში მოდულური სისტემა ყოველთვის არ შეიცვლება ერთი ელემენტით. შემოვიღოთ ზოგიერთი ახალი ცნება. თუ ცნობილია რაიმე არე, ვიმბობთ, რომ A ელემენტი M ელემენტზე იყოფა, თუ მოიძებნება ისეთი c ელემენტი, რომ $A=MC$.

ვთქვათ, $A=M_1C_1+M_2C_2+\cdots+M\mu C\mu$. მაშინ ამბობენ, რომ A იყოფა (M) მოდულურ სისტემაზე და ამ ფაქტს აღნიშნავენ ასე $(M)/A$ ან $A\equiv 0 \pmod{M_1, M_2, \ldots, M\mu}$. შემდეგ ვამბობთ, რომ $A\equiv B \pmod{(M)}$, თუ $(M)/(A-B)$. ჩავთვალოთ, რომ ორი ასეთი ელემენტი ერთ კლასს ეკუთვნის (M) მოდულური სისტემით. ამ შეთანხმების შემდეგ მივიღებთ თეორემებს, რომლებიც ზუსტად ისე მტკიცდება, როგორც შედარებათა თეორიაში.

I. ყოველი ელემენტი თავისი თავის სადარია ნებისმიერი მოდულური სისტემით.

II. თუ $A\equiv B \pmod{(M)}$, $B\equiv C \pmod{(M)}$, მაშინ $A\equiv C \pmod{(M)}$.

III. შედარებები მოდულური სისტემით ემორჩილება ჩვეულებრივი შედარებების კანონებს: ისინი შეიძლება შეკრიბოთ და გავამრავლოთ.

მე-2 თეორემა ადასტურებს კლასებად დაშლის კანონიერებას.

აღვნიშნოთ განსხვავება მოდულსა და მოდულურ სისტემას შორის. მოდული განსაზღვრავს უბრალოდ არის რიცხვს, მოდულური სისტემა აღარ არის მოცემული არის ელემენტი, ის სრულიად სხვა რამეა. ეს დასკვნა ძალიან მნიშვნელოვანია. ვთქვათ, გვაქვს ორი მოდულური

სისტემა (ω)=(M$_1$, M$_2$,...,Mμ) და (D)=(D$_1$, D$_2$,..., Dυ). ჩვენ ვიტყვით, რომ (ω) მოდულური სისტემა იყოფა (D)-ზე, თუ მისი ყოველი ელემენტი იყოფა (D)-ზე, ე. ი. წრფივად გამოისახება D$_1$, D$_2$,..., Dυ მოდულური სისტემით.

თ ე ო რ ე მ ა. თუ შედარებას ადგილი აქვს რაიმე მოდულური სისტემით, მაშინ მას ადგილი ექნება ნებისმიერი მოდულური სისტემით, რომელიც პირველის გამყოფია.

ვთქვათ, A≡B (mod M$_1$, M$_2$,..., Mμ). ეს ნიშნავს, რომ

$$A-B=C_1M_1+C_2M_2+\cdots+C\mu M\mu.$$

თუ (D) /(ω), მაშინ

$$\begin{aligned}
M_1&=\gamma_1^{(1)}D_1+\gamma_2^{(1)}D_2+\cdots+\gamma_\upsilon^{(1)}D\upsilon\\
M_2&=\gamma_1^{(2)}D_1+\gamma_2^{(2)}D_2+\cdots+\gamma_\upsilon^{(2)}D\upsilon\\
&\cdots\cdots\cdots\cdots\\
M\mu&=\gamma_1^{(\mu)}D_1+\gamma_2^{(\mu)}D_2+\cdots+\gamma_t^{(\mu)}D\upsilon.
\end{aligned}$$

თუ ამ გამოსახულებას წინა ტოლობაში ჩავსვამთ, მივიღებთ

$$A-B=C'_1D_1+C'_2D_2+\cdots+C'\upsilon D\upsilon,$$

ეს კი ამტკიცებს თეორემას.

მეორე მნიშვნელოვანი თეორემა შემდეგში მდგომარეობს: თუ მოდულურ სისტემას მივუერთებთ ახალ სისტემას, მაშინ მიღებული სისტემა მოცემული სისტემის გამყოფია.

ვთქვათ, გვაქვს მოდულური სისტემა (M$_1$, M$_2$,..., Mμ), M$_0$ ჩვენი არის რაიმე ელემენტია. პირველი სისტემის ყოველი ელემენტი შეიძლება წარმოვადგინოთ შემდეგი სახით

$$Mi=C_0^{(i)}M_0+C_1^{(i)}M_1+C_2^{(i)}M_2+\cdots+C\mu^{(i)}M_\mu,$$

სადაც $C_0^{(i)}=0$. ეს კი გვიჩვენებს, რომ (M$_1$, M$_2$,..., Mμ) მოდულური სისტემა იყოფა (M$_0$, M$_1$, M$_2$,..., Mμ) მოდულურ სისტემაზე.

ახლა შემოვიღოთ ექვივალენტობის ცნება, (ω) და (R) მოდულურ სისტემებს ექვივალენტური ვუწოდოთ, თუ პირველი სისტემა იყოფა მეორე სისტემაზე და მეორე იყოფა პირველზე. მთელ რიცხვთა არეში ექვივალენტობა დადის რიცხვთა ტოლობის ცნებაზე. სხვა არეებში ეს ასე არ არის. მოდულური სისტემების ექვივალენტობა აღვნიშნოთ ასე:

$$(M_1,\ M_2,\ldots,\ M\mu)\sim(N_1,\ N_2,\ldots,\ N\upsilon).$$

არსებობს კი ასეთი სისტემები? არსებობს და მაგალითად მოვიყვანთ Kroneker-ის მიერ მოცემულ ორ მოდულურ სისტემას. ავიღოთ $[1, \alpha]$ არე და განვიხილოთ (M_1, M_2) და (N_1, N_2) მოდულური სისტემები.

$$M_1=21\alpha^3+14\alpha^2+4\alpha,\quad M_2=7\alpha^2+3\alpha$$
$$N_1=3\alpha^2+5\alpha,\quad N_2=2\alpha^2-\alpha$$

უშუალო შემოწმებით ვრწმუნდებით შემდეგი ტოლობების სამართლიანობაში

$$M_1=C_1N_1+C_2N_2,\quad M_2=C'_1N_1+C'_2N_2,$$
$$N_1=\gamma_1M_1+\gamma_2M_2,\quad N_2=\gamma'_1M_1+\gamma'_2M_2,$$

სადაც

$$C_1=3\alpha+1,\quad C_2=\alpha+1,\quad C'_1=1,\quad C'_2=2,\quad \gamma_1=2,$$
$$\gamma_2=-6\alpha-1,\quad \gamma'_1=-1,\quad \gamma'_2=3\alpha+1.$$

მოდულური სისტემების თეორიაში ძნიშვნელოვან როლს ასრულებს შემდეგი თეორემა: თუ მოცემული არის M_0 ელემენტი იყოფა $(M_1, M_2,\ldots, M\mu)$ მოდულურ სისტემაზე, მაშინ ამ სისტემისათვის M_0 ელემენტის მიერთებით მიღებული მოდულური სისტემა მოცემული მოდულური სისტემის ექვივალენტურია.

წინა თეორემიდან ჩვენ ვიცით, რომ

$$(M_0,\ M_1,\ M_2,\ldots,\ M\mu)/(M_1,\ M_2,\ldots,\ M\mu). \qquad (ა)$$

თეორემის პირობით, $(M)/M^\circ$, ე. ი. (M_0, M_1, M_2, M_μ) მოდულური სისტემის ნებისმიერი ელემენტი იყოფა მოცემულ სისტემაზე. ამიტომ ახალი სისტემა იყოფა ძველ სისტემაზე, ე. ი.

$$(M_1,\ M_2,\ldots,\ M\mu)/(M_0,\ M_1,\ M_2,\ldots,\ M\mu) \qquad (ბ)$$

(ა) და (ბ) ამტკიცებს თეორემას.

ამ თეორემიდან გამომდინარეობს, რომ მოდულური სისტემის ექვივალენტობის დაურღვეველად, შეგვიძლია გამოვრიცხოთ ის ელემენტი, რომელიც იყოფა დანარჩენი ელემენტებისაგან შედგენილ მოდულურ სისტემაზე. ამ დებულების დასამტკიცებლად საკმარისია წინა თეორემის შედეგი ბოლოდან წავიკითხოთ. ეს თეორემები საშუალებას

გვაძლევს გავამარტივოთ მოდულური სისტემა. მათ საფუძველზე შეიძლება უმარტივეს ფორმაზე დავიყვანოთ მოდულური სისტემა. რომელიც შეიცავს ერთიანს. განვიხილოთ მოდულური სისტემა (1, M_1, M_2,..., $M\mu$). რადგან ყოველი ელემენტი 1-ზე იყოფა, ამიტომ შეგვიძლია დავწეროთ:

$$(1, M_1, M_2,..., M\mu)\sim(1, M_2, M_3,..., M\mu)\sim\cdots\sim(1)\sim 1.$$

ე. ი. ყოველი მოცემული მოდულური სისტემა, რომელიც ერთიანს შეიცავს, ექვივალენტურია (1) სისტემისა. ისმება კითხვა, რა არის (1)? ადვილი მისახვედრია, რომ ამ მოდულურ სისტემას შეესაბამება ჩვენი არე, ე. ი. ეს შემთხვევა განსაკუთრებულ ინტერესს არ იწვევს.

ვაჩვენოთ, რომ თუ გვაქვს შედარება ერთი მოდულური სისტემით, ის შეიძლება შეიცვალოს მისი ექვივალენტური მოდულური სისტემით.

ვთქვათ, $(\omega)\sim(R;$ და $A\equiv B \pmod{(\omega)})$,

$(\omega)=(M_1, M_2,..., M\mu)$, $R=(N_1, N_2,..., N\upsilon)$. რადგან ჩვენი სისტემები ექვივალენტურია, ამიტომ $(N_1, N_2,\cdots N\upsilon)/(M_1, M_2,..., M\mu)$, ხოლო ასეთ შემთხვევაში დამტკიცებული გვაქვს, რომ

$$A\equiv B \pmod{N_1, N_2,..., N\upsilon}.;$$

ვაჩვენოთ, რომ სამართლიანია შებრუნებული დებულება. თუ ყველა შედარებას (ω) მოდულური სისტემით ადგილი აქვს (R) სისტემით და პირიქით, მაშინ ეს მოდულური სისტემები ექვივალენტურია.

მართლაც,

$$M_i\equiv 0 \pmod{M_1, M_2, M_3,.., M\mu}, \quad i=1, 2,..., \mu.$$

პირობის თანახმად,

$$Mi\equiv 0 \pmod{(N_1, N_2,..., N\upsilon)}, \quad i=1, 2,..., \mu.$$

ე. ი.

$$\sim (R)/(\omega) \qquad (\alpha)$$

შემდეგ,

$$Nj\equiv 0 \pmod{N_1, N_2,..., N\upsilon}, \; j=1, 2,..., \upsilon$$

და

$$Nj\equiv 0 \pmod{M_1, M_2,..., M\mu}, \quad j=1, 2, ..., \upsilon.$$

ეს ნიშნავს, რომ $(\omega)/(R)$.

(α) და (β) გვაძლევს, რომ $(\omega)\sim(R)$. (β).

ამ ცნებების დადგენის შემდეგ გადავდივართ მოდულური სისტემების საერთო გამყოფისა და უდიდესი საერთო გამყოფის განსაზღვრაზე. ორი რიცხვის უდიდესი საერთო გამყოფი ჩვენ გვესმის როგორც რიცხვი, რომელიც ყოფს მოცემულ რიცხვებს და იყოფა ამ რიცხვების ყველა საერთო გამყოფზე. ვნახოთ, ხომ არ შეიძლება ამ ცნების განზოგადება მოდულური სისტემებისთვის. ამისათვის განვიხილოთ ორი მოდულური სისტემა (ω) და (R). შევქმნათ ახალი მოდულური სისტემა ამ მოდულური სისტემების ელემენტთა სიმრავლეებისაგან.

$$(\omega,\ R)=(M)=(M_1,\ M_2,\ldots,\ M\mu,\ N_1,\ N_2,\ldots,\ N\upsilon).$$

ვაჩვენოთ, რომ ჩვენი სისტემების ნებისმიერი საერთო გამყოფი (D) გაყოფს (M) სისტემასაც. რადგან (D) არის (ω) და (R) მოდულური სისტემების საერთო გამყოფი, ამიტომ, თუ $(D)=(D_1,\ D_2,\ldots,\ D_\delta)$, მაშინ

$$M_i=c_1D_1+c_2D_2+\cdots+c_\delta D_\delta,\quad i=1,\ 2,\ldots,\ \mu,$$
$$N_j=\gamma_1D_1+\gamma_2D_2+\cdots+\gamma_\delta D_\delta,\quad j=1,\ 2,\ldots,\ \upsilon,$$

(M) სისტემის M_i და N_j ელემენტები იყოფა (D)-ზე, ამიტომ (M) სისტემა გაიყოფა (D)-ზე. შემდეგ, ზემოთ დამტკიცებული თეორემის თანახმად, $(M)/(\omega)$ და $(M)/(R)$, ე. ი. (M) სისტემას აქვს უდიდესი საერთო გამყოფის ყველა თვისება. ამიტომ (M) სისტემას ეწოდება (ω) და (R) სისტემების უდიდესი საერთო გამყოფი.

გადავდივართ გამრავლების (cosmoposition) ანალოგიური ოპერაციის განსაზღვრაზე. ვთქვათ, გვაქვს ორი მოდულური სისტემა (ω) და (R). გავამრავლოთ პირველი სისტემის ყოველი ელემენტი მეორე სისტემის ყოველ ელემენტზე და მიღებული ელემენტებით ავაგოთ ახალი მოდულური სისტემა

$$(\omega)\cdot(R)=(M_1N_1,\ M_1N_2,\ldots,M_1N\upsilon,\ldots,\ M\mu N_1,$$
$$M\mu N_2,\ldots,\ M_\mu N_\nu)$$

პირდაპირ ჩანს, რომ

$$(\omega)/(\omega)\cdot(R)\ \text{და}\ (R)/(\omega)\cdot(R).$$

განმარტებული ოპერაცია უშვებს კომუტაციურობის კანონს

$$(\omega)\cdot(R)—(R)\cdot(\omega).$$

იმ კერძო შემთხვევაში, როცა $\mu=\upsilon=1$, მივიღებთ ჩვეულებრივ გამრავლებას.

დავამტკიცოთ თეორემა: თუ $(\omega)\sim(\omega')$, მაშინ $(\omega)\cdot(R)\sim(\omega')\cdot(R)$.

$(\omega)\sim(\omega')$, ამიტომ

$$M_i'=C_1M_1+C_2M_2+\cdots+C\mu M\mu,\ i=1,\ 2,\ldots,\ \mu_1)$$

განვიხილოთ $(\omega')\cdot(R)$. მის ყოველ ელემენტს აქვს სახე

$$M'iN_k=C_1M_1N_k+C_2M_2N_k+\cdots+C\mu M\mu N_k.$$

ეს ნიშნავს, რომ $(\omega)\cdot(R)/(\omega')\cdot(R)$. ზუსტად ასევე დავრწმუნდებით, რომ $(\omega')\cdot(R)/(\omega)\cdot(R)$, ე. ი. $(\omega)\cdot(R)\sim(\omega)\cdot(R)$.

რრგორც წინა თეორემის შედეგს, მივიღებთ უფრო ზოგად თეორემას: თუ $(\omega)\sim(\omega')$ და $(R)\sim(R')$, მაშინ $(\omega).\ (R)\sim(\omega')\cdot(R')$.

დავამტკიცოთ კიდევ ორი საინტერესო დებულება, რომლებიც ჩვენთვის ნაცნობი თეორემების განზოგადებაა.

ვთქვათ, $(\omega)/(L)$, $(R)/(L)$. თუ შევადგენთ გამოსახულებას $(L)\cdot(\omega,\ R)$, მაშინ ეს გაიყოფა $(\omega)\cdot(R)$-ზე.

ეს თეორემა არითმეტიკაში ასე იკითხება: თუ b/m, l/h, მაშინ $l\cdot D\ (m,\ n)/\cdot mn$.

ჩვენი თეორემის სამართლიანობა იქიდან გამომდინარეობს, რომ თუ დავწერთ შედარებას

$$(M_1L_1,\ M_2L_2,\ldots,\ M\mu Li,\ldots,\ NiL_j,\ldots,\ N\upsilon L_k)\equiv 0 \mod (M_1N_1,\ldots,\ M\mu N\upsilon)$$

ეს სამართლიანი იქნება, რადგან M_kLi და N_kLj შეიცავს $(M.\ N_1,\ldots,\ M\mu N\upsilon)$ გამყოფებს. ეს შედარება კი გაშლილი სახით არის დასამტკიცებელი თეორემა.

ახლა ასეთი თეორემა დავამტკიცოთ: თუ $(L)\cdot(R)$ იყოფა (ω)-ზე, მაშინ $(L,\ \omega)\cdot(R)$ იყოფა (ω)-ზე.

თეორემის დასამტკიცებლად გამოსახულება $(L,\ \omega)\ (R)$ დავწეროთ გაშლილი სახით

$$(L_1N_1,\ L_2N_1,\ldots,\ LiN_k,\ldots,\ L_\mu N\upsilon,\ M_1N_1,\ldots,\ M_mN_k,\ldots,\ M\mu N\upsilon).$$

ჩვენ ვხედავთ, რომ აქა გვაქვს LiN_k და MiN_k სახის ელემენტები. პირველი კატეგორიის ყველა ელემენტი იყოფა (ω)-ზე, რადგან $(\omega)/(L,\ \omega)\cdot(R)$, მეორე კატეგორიის ელემენტები, ცხადია, იყოფა (ω)-ზე. მივიღეთ დასამტკიცებელი.

მთელ რიცხვთა არეში ამ თეორემას შეესაბამება ასეთი თეორემა: თუ m/nl, მაშინ $m/\mathrm{D}\ (m,\ l)\cdot n$.

როგორც დავინახეთ, მთელ რიცხვთა არის ბევრი თვისება სამართლიანია ზოგად არეში, მაგრამ სრული ანალოგია აქ არ არის.

მაგალითად, ჩვენ ვაჩვენეთ, რომ ორი მოდულური სისტემის ნამრავლი ხანდახან იყოფა მესამეზე, მაგრამ აქედან არ გამომდინარეობს, რომ პირველი ორი სისტემიდან რომელიმე იყოფა მესამე სისტემაზე. ზუსტად ასე, არ ემთხვევა ჯამის ცნება.

ახლა გადავიდეთ ისეთი მოდულური სისტემების განხილვაზე, რომელთა ელემენტებია ერთი ცვლადის ფუნქციები. ვთქვათ, ჩვენს მოდულურ სისტემას აქვს სახე:

$$(f_1\ (x),\ f_2(x),\ldots,\ f\mu(x)).$$

ჩვენი არის ნებისმიერი A ელემენტი, რომელიც ნულის სადარია ამ მოდულური სისტემით, ასეთი სახისაა:

$$\mathrm{A}=f_1(x)\psi_1(x)+f_2(x)\psi_2(x)+\cdots+f_\mu(x)\cdot\psi_\mu^{(x)},$$

სადაც $\psi_i(x)$, ისე როგორც $f_i(x)$, x-ის მთელი, მთელ კოეფიციენტებიანი მრავალწევრია. ასეთი უმარტივესი მოდულური სისტემა იქნება ერთი ელემენტისაგან შედგენილი $(f(x))$. მისი თვისებები ჩვენ შევისწავლეთ, როცა განვიხილეთ ფუნქციათა შედარება p მოდულით. ერთი შეხედვით შეიძლება მოგვეჩვენოს, რომ ყოველი მოდულური სისტემა შეიძლება შეიცვალოს $(f(x))$-ის ეკვივალენტური სისტემით. შემდეგში ვნახავთ, რომ ეს ყოველთვის ასე არ არის.

განვიხილოთ სირთულით მომდევნო შემთხვევა. ვთქვათ, გვაქვს მოდულური სისტემა $(f_1(x),\ f_2(x))$. ამ შემთხვევაში შეიძლება გამოვიყენოთ უდიდესი საერთო გამყოფის პოვნის ევკლიდის ალგორითმის ანალოგიური მეთოდი. ალგებრისაგან განსხვავება იმაშია, რომ განვიხილავთ მხოლოდ მთელკოეფიციენტებიან მრავაწევრებს და ჩვენს არეში რომ დავრჩეთ, ამიტომ შემოგვაქვს განსაკუთრებული გამყოფები.

ვთქვათ, $f_1(x)$-ის ხარისხი არის m_1; $f_2(x)$-ის —m_2 და $m_1 > m_2$. ვყოფთ $f_1(x)$ მრავალწევრს $f_2(x)$-ზე და ვღებულობთ

$$f_1(x)=f_2(x)\mathrm{Q}_1(x)+\mathrm{R}_1(x) \qquad (\alpha)$$

$\mathrm{Q}_1(x)$ და $\mathrm{R}_1(x)$ მრავალწევრებს შეიძლება ჰქონდეს წილადი კოეფი-

ციენტები. ვპოულობთ ამ კოეფიციენტების საერთო მნიშვნელს და შემოგვაქვს აღნიშვნები

$$Q_1(x)=\frac{\varphi_1(x)}{n_1}\ , \qquad R_1(x)=\frac{f_3(x)}{n_1}\ ,$$

(α) გამოსახულება მიიღებს სახეს

$$n_1f_1(x)=f_2(x)\varphi_1(x)+f_3(x),$$

სადაც ყველა კოეფიციენტი მთელი რიცხვია. თუ ამ გამოსახულებას ასე გადავწერთ

$$f_3(x)=n_1\ f_1(x)-\varphi_1\ (x)f_2(x),$$

დავინახავთ, რომ $f_3(x)/(f_1(x),\ f_2(x))$. მაშასადამე,

$$(f_1(x),\ f_2(x))\sim(f_1(x),\ f_2(x),\ f_3(x)).$$

თუ ამ პროცესს გავაგრძელებთ, მივიღებთ თანაფარდობებს

$$\begin{aligned}
&n_1f_1=f_2\varphi_1+f_3\\
&n_2f_2=f_3\varphi_2+f_4\\
&\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\
&n_{v-2}f_{v-2}=f_{v-1}\varphi_{v-1}+f_v\\
&n_{v-1}f_{v-1}=f_v\cdot\varphi_v
\end{aligned} \qquad (I)$$

ეს თანაფარდობები შეიძლება წარმოვადგინოთ შედარებების ფორმით:

$$f_3\equiv 0\ (\mathrm{mod}\ (f_1,\ f_2)),\ldots,\ n_{v-1}\varphi_{v-1}\equiv 0\ (\mathrm{mod}\ (f_v,\ \varphi_v) \qquad I'$$

(I)-დან შეიძლება მივიღოთ

$$f_v\equiv 0\ (\mathrm{mod}\ (f_1,\ f_2)), \qquad (ა)$$

ხოლო (I′)-დან

$$\begin{aligned}
&n_1n_2\cdots n_{v-1}f_1\equiv 0\ (\mathrm{mod}\ f_v)\\
&n_1n_2\cdots n_{v-1}f_2\equiv 0\ (\mathrm{mod}\ f_v)
\end{aligned} \qquad (ბ)$$

აქ ვხვდებით იმ თავისებურებებს, რომელსაც ადგილი არა აქვს რიცხვთა თეორიაში. სახელდობრ, $(f_1,\ f_2)\sim f_v$ ყოველთვის არ სრულდება. ეს რომ შესრულდეს, აუცილებელია f_v/f_1, f_v/f_2 და $(f_1,\ f_2)/f_v$. ჩვენთან, (ა)-ს თანახმად, უკანასკნელი პირობა სრულდება. რაც შეეხება პირველ ორ პირობას, (ბ)-დან ჩანს, რომ მის შესასრულებლად f_1 და f_2 უნდა გამრავლდეს გარკვეულ v_1 და v_2 მამრავლებზე. ეს მამრავლები კი, საერთოდ, არ არის უმცირესი რიცხვები, რომლებსაც ეს

თვისება აქვს. ვთქვათ, ასეთი უმცირესი მამრავლებია S_1 და S_2, მაშინ სამართლიანია დებულება:

ვთქვათ, f_1 და f_2 მთელკოეფიციენტებიანი მრავალწევრებია. მაშინ თანმიმდევრული გაყოფით ყოველთვის შეიძლება ვიპოვოთ f_v მრავალწევრი და S_1 და S_2 ისეთი რიცხვები, რომ ადგილი ჰქონდეს თანაფარდობებს

$$fv \equiv 0 \pmod{(f_1, f_2)} \text{ და } S_1 f_1 \equiv S_2 f_2 \equiv 0 \pmod{fv}.$$

fv ფუნქცია იქნება f_1 და f_2 მრავალწევრების უდიდესი საერთო გამყოფი მაშინ და მხოლოდ მაშინ, როცა $S_1 = S_2 = 1$.

ნათქვამიდან გამომდინარეობს, რომ ორელემენტიანი მოდულური სისტემა ყოველთვის ვერ შეიცვლება ექვივალენტური ერთელემენტიანი სისტემით. ეს დასკვნა გავრცელდება $(f_1, f_2, \ldots, fv)$ ზოგადი სახის მოდულურ სისტემაზე. ვეღებულობთ ასეთ ძირითად დებულებას:

$(f_1, f_2, \ldots, fv)$ სახის ყველა მოდულური სისტემა იყოფა ორ კლასად: მოდულური სისტემები, რომლებიც ექვივალენტურია ერთელემენტიანი მოდულური სისტემის და მოდულური სისტემები, რომლებიც არაა ერთელემენტიანი მოდულური სისტემის ექვივალენტური.

პირველი სახის მოდულურ სისტემებს ვუწოდოთ I საფეხურის, II სახისას—II საფეხურის. I საფეხურის მოდულური სისტემები მოცემული არის ელემენტებია. მოვიყვანოთ II საფეხურის მოდულური სისტემის მაგალითი. ვთქვათ, გვაქვს სისტემა $(m, x—n)$, სადაც m და n მთელი რიცხვებია და $m > 1$. ეს რომ I საფეხურის მოდულური სისტემა იყოს, მაშინ გვექნებოდა $(m, x—n) \sim a$, a/m, $a/(x—n)$, ეს კი ნიშნავს, რომ $a = 1$. ახლა ვაჩვენოთ, რომ $(m, x—n) \sim 1$. დავუშვათ წინააღმდეგი. ვთქვათ, $(m, x—n) \sim 1$, მაშინ

$$f_1(x)m + f_2(x) \cdot (x—n) = 1.$$

თუ $x = n$, მივიღებთ, $f_1(n) \cdot m = 1$, რაც შეუძლებელია, რადგან ამ ორი მთელი რიცხვის ნამრავლი არ შეიძლება იყოს ერთი (ვიცით, რომ $m > 1$). მაგალითი გვარწმუნებს, რომ არსებობს II საფეხურის მოდულური სისტემები. შეიძლება მოვახდინოთ II საფეხურის მოდულური სისტემების შემდგომი კლასიფიკაცია. თუ მოდულური სისტემის ყველა fi ელემენტი შეიცავს I საფეხურის ერთსა და იმავე D გამყოფს, მაშინ მოდულურ სისტემას შერეული ვუწოდოთ, წინააღმდეგ შემთხვევაში კი—წმინდა. გასაგებია, რომ შერეული მოდულური სისტე-

ძის შემთხვევაში D გამყოფი არ უნდა გაიყოს ამ მოდულურ სისტემაზე, რადგან წინააღმდეგ შემთხვევაში გვექნებოდა $D\sim(f_1, f_2,\ldots, f\mu)$ და ჩვენი სისტემა I საფეხურისა აღმოჩნდება. თუ $(\varphi_1, \varphi_2,\ldots, \varphi_\mu)$ შერეული სისტემაა და ელემენტების საერთო გამყოფია D, მაშინ დავუშვებთ, რომ $D f_i=\varphi_i$, მივიღებთ ცხად თანაფარდობას.

$$(\varphi_1, \varphi_2,\ldots, \varphi_\mu)\sim D(f_1, f_2,\ldots, f\mu).$$

აქ $(f_1, f_2,\ldots, f\mu)$ II საფეხურის მოდულური სისტემაა, რადგან ის რომ I საფეხურისა ყოფილიყო, მაშინ $D(f_1, f_2,\ldots, f\mu)$ იქნებოდა I საფეხურის მოდულური სისტემა, ეს კი ეწინააღმდეგება პირობას, რომ $(\varphi_1, \varphi_2,\ldots, \varphi\mu)$ II საფეხურის მოდულური სისტემაა.

ყველაფერ ნათქვამს მივყავართ ასეთ დასკვნამდე: თუ II საფეხურის სისტემა შერეულია, მაშინ ის შეიძლება დავიყვანოთ მის ექვივალენტურ II საფეხურის წმინდა მოდულურ სისტემაზე.

გადავდიგართ II საფეხურის მოდულური სისტემების შესწავლაზე. დავიწყოთ მოდულური სისტემის პირველად ელემენტებად დაშლით. პირველადი ელემენტი გავიგოთ როგორც ელემენტი, რომელიც არ იყოფა ამ არის არც ერთ სხვა ელემენტზე. თუ მოცემულია $f(x)$ ფუნქცია, რომლის კოეფიციენტებს აქვს საერთო გამყოფები, მაშინ შეგვიძლია დავწეროთ $f(x)=\varphi(x)\cdot m$, სადაც m არის $f(x)$-ის კოეფიციენტების უდიდესი საერთო გამყოფი. ცხადია, $\varphi(x)$ არ გაიყოფა რაიმე რიცხვზე (გარდა I-ისა). ვეძებოთ $\varphi(x)$-ის სხვა ტიპის გამყოფები. დავიწყოთ უველაზე მცირე ხარისხის, ე. ი. $ax+b$ სახის გამყოფებით და გადავიდეთ უფრო მაღალ ხარისხებზე. ვთქვათ, $P(x)$ უმცირესი ხარისხის გამყოფია. ის იქნება ჩვენი არის პირველადი ელემენტი, რადგან, წინააღმდეგ შემთხვევაში, იგი დაიშლებოდა უფრო მცირე ხარისხის მამრავლებად. თუ გამოვყოფთ უმცირესი ხარისხის გამყოფებს, მივიღებთ დაშლას

$$f(x)=mP(x)P_1(x)\cdots P_h(x).$$

თუ ახლა m-ს დავშლით მარტივ მამრავლებად და ჯერადობებს გავითვალისწინებთ, მივიღებთ

$$f(x)=P_1^{h_1}\cdot P_2^{h_2}\cdots P e^{h}\epsilon\Pi_{1a_1}(x)\Pi_2^{a^2}(x)\cdots\Pi_k^{a^k}(x),$$

სადაც $P\iota$ და $\Pi\iota(x)$ საძიებელი პირველადი ელემენტებია. ისინი მოცემულ არეში არ დაიშლება. ე.ი. პირველადი ელემენტები ჩვენს არეში

მარტივი რიცხვების როლს ასრულებს. ვაჩვენოთ, რომ თუ AB ნამრავლი იყოფა პირველად ელემენტზე, მაშინ ერთ-ერთი ფაქტორი აუცილებლად გაიყოფა მასზე. ამ თეორემით შემდეგ ვისარგებლებთ პირველად ელემენტებად დაშლის ერთადერთობის დასამტკიცებლად. როცა საუბარი გვქონდა შედარებებზე P მოდულით. დავამტკიცეთ, რომ შედარება

$$\psi(x)\varphi(x)\equiv 0 \pmod{p}$$

გვაძლევს $\varphi(x)\equiv 0 \pmod{p}$ და $\psi(x)\equiv 0 \pmod{p}$ შედარებებიდან ერთ-ერთს.

დავამტკიცოთ თეორემა: თუ $\varphi(x)$ ფუნქცია არ არის რიცხვითი ფაქტორი და $m\mathrm{F}(x)\equiv 0 \pmod{\Phi(x)}$, მაშინ აუცილებლად ადგილი ექნება შედარებას $\mathrm{F}(x)=0 \pmod{\Phi(x)}$, სადაც m და $\mathrm{F}(x)$ მოცემულ არეს ეკუთვნის.

მოცემული შედარების თანახმად, ადგილი აქვს თანაფარდობას $m\mathrm{F}(x)=\Phi(x)\varphi(x)$. უნდა დავამტკიცოთ, რომ $\varphi(x)$ იყოფა m-ზე. თუ $\mathrm{F}(x)=m\varphi(x)$, მაშინ $\mathrm{F}(x)=\Phi(x)\varphi(x)$ და თეორემა დამტკიცდება. ვთქვათ, $\varphi(x)$ იყოფა არა m-ზე, არამედ m-ის რომელიმე d გამყოფზე, მაშინ $m\mathrm{F}(x)=\Phi(x)\varphi(x)$ შევკვეცოთ d-ზე, მივიღებთ

$$m_1\mathrm{F}(x)=\Phi(x)\varphi_1(x).$$

მარჯვენა მხარე უკვე აღარ იყოფა არც ერთ რიცხვით ფაქტორზე, გარდა 1-ისა, ე.ი. $m_1=1$ და $\mathrm{F}(x)=\Phi(x)\varphi(x)$ ან, რაც იგივეა, $\mathrm{F}(x)=0 \pmod{\Phi(x)}$.

ახლა დავამტკიცოთ თეორემა: თუ $p(x)$ პირველადი ელემენტია და ადგილი აქვს შედარებას $\Phi(x)\psi(x)\equiv 0 \pmod{p(x)}$, მაშინ $\psi(x)$ და $\Phi(x)$ ფუნქციებიდან ერთ-ერთი $\mathrm{P}(x)$-ის ჯერადია.

უნდა დავამტკიცოთ, რომ თუ ერთი თანამამრავლი, მაგალითად, $\Phi(x)$ არ იყოფა $p(x)$-ზე, მაშინ $\varphi(x)$ აუცილებლად გაიყოფა $p(x)$-ზე. დასამტკიცებლად გამოვიყენოთ ევკლიდის სახეშეცვლილი ალგორითმი, რომელზედაც ზემოთ გვქონდა საუბარი. მივიღებთ შემდეგ სამ ფორმულას:

$$\psi(x)\equiv 0 \pmod{(p(x),\ \Phi(x))} \qquad (a)$$

$$m\mathrm{P}(x)\equiv 0 \pmod{\psi(x)} \qquad (b)$$

$$\mu\ \Phi(x)\equiv 0 \pmod{\psi(x)} \qquad (c)$$

სადაც μ და m განსაზღვრული მთელი რიცხვებია, ხოლო $\psi(x)$ ეკუთვნის ჩვენს არეს. ამ ფორმულებიდან გამომდინარე, ვაჩვენოთ, რომ $\psi(x)$ არ არის დამოკიდებული x-ზე. ვთქვათ, $\psi(x)=r\varphi(x)$, სადაც $\varphi(x)$ მთელი ფუნქციაა, რომელიც არ იყოფა რიცხვით ფაქტორზე. (*b*) ტოლობისა და წინა თეორემის თანახმად, $P(x)$ იყოფა $\varphi(x)$-ზე, ეს კი შესაძლებელია მხოლოდ მაშინ, თუ $P(x)=\varphi(x)$. (*c*) ტოლობიდან გამოდის, რომ $\Phi(x)$ იყოფა $\varphi(x)$-ზე და ე. ი. $\Phi(x)$ იყოფა $p(x)$-ზე. ეს კი პირობას ეწინააღმდეგება. მაშასადამე, $\varphi(x)$ არ არის x-სგან დამოკიდებული და, ე. ი. მთელი რიცხვია. ახლა (*a*) შედარება გავამრავლოთ ψ-ზე. შედეგი ასე წარმოვადგინოთ

$$\psi\psi(x)\equiv 0 \pmod{P(x)\cdot\psi,\ \Phi(x)\cdot\psi}.$$

ამ მოდულური სისტემის ორივე ელემენტი იყოფა $P(x)$-ზე, ამიტომ

$$\psi\psi(x)\equiv 0 \pmod{P(x)}.$$

აქ ψ რიცხვითი მამრავლია, ამიტომ, წინა თეორემის თანახმად,

$$\psi(x)\equiv 0 \pmod{P(x)}.$$

თეორემა დამტკიცებულია.

ახლა ადვილად ვაჩვენებთ,რომ $f(x)$ ფუნქციის დაშლა პირველად ელემენტებად ერთადერთია. ვთქვათ, ერთდროულად ადგილი აქვს ფორმულებს.

$$f(x)=p_1^{h_1}p_2^{h_2}\cdots P_c^{h_c}\Pi_1^{a_1}(x)\,\Pi_2^{a_2}(x)\cdots\Pi_k^{a_k}(x)$$

და

$$f(x)=q_1^{g_1}q_2^{g_2}\cdots q_e^{g_e}Q_1^{b_1}(x)\,Q_2^{h_2}(x)\cdots Q_s^{b_s}(x)$$

თუ შევადარებთ ამ ფორმულების მარჯვენა მხარეებს, ზუსტად ისე, როგორც რიცხვთა თეორიაში, მივიღებთ

$$p_i=q_l,\quad h_i=g_i,\quad e=c;\quad \Pi_i=Q_i,\quad a_i=b_l,\quad k=s,$$

რაც ამტკიცებს ჩვენს დებულებას.

ამით ჩვენ არსებითად დავამთავრეთ არის დაშლა. ვხედავთ, რომ განსხვავება ჩვეულებრივ არითმეტიკასთან შედარებით იმაში მდგომარეობს, რომ აქ, საზოგადოდ, ორ ელემენტს ყოველთვის არა აქვს უდიდესი საერთო გამყოფი. თუ დაშლას ჩავატარებთ, კვლევა საგრძნობლად გამარტივდება.

შ ი ნ ა ა რ ს ი

მკითხველთა საყურადღებოდ

უნივერსიტეტის გამომცემლობა გამოსაცემად ამზადებს ანდრია რაზმაძის კიდევ ერთ ნაშრომს—„ინტეგრალური აღრიცხვის კურსი“ (ნაწ. II, „განსაზღვრული ინტეგრალები“), პროფ. ი. ქარცივაძის რედაქციით; უახლოეს ხანში გამოვა კრებული — „ანდრია რაზმაძე. მოგონებები, წერილები“, მიძღვნილი ანდრია რაზმაძის დაბადებიდან 100 წლისთავისადმი.

Размадзе Андрей Михайлович

КОНСПЕКТ ТЕОРИИ ЧИСЕЛ

(на грузинском языке)

Издательство Тбилисского университета
Тбилиси 1992

გამომცემლობის რედაქტორი ა. სტურუა
ხამხატვრო რედაქტორი ი. ჩიქვინიძე
მხატვარი გ. ავსაჯანიშვილი
ტექრედაქტორი თ. ფირცხელანი
კორექტორი ნ. ელიზბარაშვილი

გადაეცა წარმოებას 29.05.92. ხელმოწერილია დასაბეჭდად 21.09.92. საბეჭდი ქაღალდი $60\times84^1/_{16}$ პირობითი ნაბეჭდი თაბახი 5,25. საღრ.-საგამომც. თაბახი 3,51. ტირაჟი 1200. შეკვეთის № 331.

ფასი 8 მან.

თბილისის უნივერსიტეტის გამომცემლობა.
თბილისი, 380028, ი. ჭავჭავაძის პროსპექტი, 14.

თბილისის უნივერსიტეტის სტამბა,
თბილისი, 380028, ი. ჭავჭავაძის პროსპექტი, 1.