ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტი

მარიამ ნინუა

რიცხვთა წარმოდგენა კვადრატული ფორმებით

The representation of numbers by Quadratic forms

ნაშრომი შესრულებულია მათემატიკის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

სამეცნიერო ხელმძღვანელი: ქეთევან შავგულიძე

ფიზიკა-მათემატიკის მეცნიერებათა დოქტორი

ასოცირებული პროფესორი

თბილისი 2023

ანოტაცია

რიცხვთა ადიტიური თეორიის საგანს შეადგენს ნატურალურ რიცხვთა ამა თუ იმ სახის შესაკრებთა ჯამად დაშლის საკითხები. რიცხვთა ადიტიური თეორია მოიცავს ბევრ საინტერესო და საკმაოდ რთულ ამოცანებს. აქ არ არსებობს ამოცანათა ამოხსნის ერთი მთლიანი ზოგადი მეთოდი, მაგრამ არსებობს რამოდენიმე მეტ-ნაკლებად ზოგადი მეთოდი ცალკეული კლასის ამოცანათა ამოსახსნელად. ნაშრომში განვიხილავთ ასეთი ამოცანებიდან ერთ-ერთი კლასის ამოცანებს, კერძოდ ნატურალური რიცხვის წარმოდგენას კვადრატული ფორმით.

ნაშრომში განხილულია ცნებები, თუ რას ეწოდება n ცვლადის კვადრატული ფორმა, როდის ეწოდება რიცხვს წარმოდგენადი. განსაკუთრებით მნიშვნელოვანია დიაგონალური ფორმებით რიცხვთა წარმოდგენის საკითხი. ასევე განხილულია ორცვლადიანი (ბინარული n=2) კვადრატული ფორმები.

რიცხვთა წარმოდგენის შესახებ ჩამოყალიბებულია და დამტკიცებულია თეორემები , წარმოდგენათა აუცილებელი და საკმარისი პირობები რიცხვთა დაშლა ორი კვადრატის, სამი კვადრატის და ოთხი კვადრატის ჯამის სახით. ბოლოს გამოყვანილია $q = x^2 + y^2$ კვადრატული ფორმით ნატურალური რიცხვის წარმოდგენათა რაოდენობის გამოსათვლელი ფორმულები.

შინაარსი

თავი 1

კვადრატული ფორმები

კვადრატულ ფორმას უწოდებენ n ცვლადის შემცველ ერთგვაროვან კვადრატულ ფუნქციას

$$f = f(x_1, x_2, \dots, x_n) = \sum_{i,k=1}^{n} \alpha_{ik} x_i x_k \quad (\alpha_{ik} = \alpha_{ki}),$$

სადაც α_{ik}- ფორმის კოეფიციენტებია, ხოლო $x_1, x_2, \dots, x_n$- დამოუკიდებელი ცვლადებია. ამ სახის ფორმებს შეესაბამება სიმეტრიული მატრიცა

$$A_f = A = \|\alpha_{ik}\| \quad (\alpha_{ik} = \alpha_{ki}).$$

ფორმას ქვია დიაგონალური თუ $\alpha_{ik} = 0$, ყოველი $i \neq k$ წყვილისთვის, ანუ მას აქვს სახე

$$f = \sum_{k=1}^{n} \alpha_k x_k^2 \quad (\alpha_{kk} = \alpha_k, \alpha_{ik} = 0, i \neq k).$$

კვადრატულ ფორმათა არითმეტიკულ თეორიაში $x_1, x_2, \dots, x_n$ ცვლადთა ცვლილების არეს წარმოადგენს მთელ რიცხვთა რგოლი ან მისი ელემენტებისგან შემდგარი ესა თუ ის ქვესიმრავლე; აქ α_{ik} კოეფიციენტები მთელი რიცხვები არის და ფორმას ეწოდება მთელკოეფიციენტებიანი ან მთელი კვადრატული ფორმა

თუ არსებობს $x_1, x_2, \dots, x_n$ მთელი მნიშვნელობებისგან შემდგარი ერთი მაინც სისტემა $(x_1, x_2, \dots, x_n)$, რომლისთვისაც

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) = m.$$

m რიცხვს ეწოდება წარმოდგენადი $f(x_1, x_2, \dots, x_n)$ კვადრატული ფორმით, ხოლო მთელ რიცხვთა ყოველ ასეთ $(\alpha_1, \alpha_2, \dots, \alpha_n)$ სისტემას ეწოდება m რიცხვის წარმოდგენა f ფორმით.

$(\alpha_1, \alpha_2, \dots, \alpha_n)$ წარმოდგენას ეწოდება საკუთრივი, თუ $(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$.

ორ წარმოდგენას: $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ და $(\beta_1, \beta_2, \ldots, \beta_n)$ უწოდებენ განსხვავებულ წარმოდგენას, თუ არსებობს თუნდაც ერთი i $(i = 1,2, \ldots, n)$, რომლისთვისაც $\alpha_i \neq \beta_i$.

M_f-ით აღვნიშნოთ ყველა იმ m რიცხვა სიმრავლე, რომელიც წარმოდგენილი არის f ფორმით, ხოლო $r_f(m)$-ით აღვნიშნავთ m რიცხვის წარმოდგენათა რაოდენობა f კვადრატული ფორმით. ცხადია

$$r_f(m) = \begin{cases} > 0, \text{თუ } m \in M_f \\ 0, \text{თუ } m \notin M_f \end{cases}$$

ისტორიულად განსაკუთრებით მნიშვნელოვანია დიაგონალური ფორმებით რიცხვთა წარმოდგენის საკითხები, კერძოდ, ისეთი დიაგონალური ფორმებით, რომელთათვისაც ყოველი $\alpha_k = 1$, ე.ი.ფორმებით

$$f(x_1, x_2, \ldots, x_n) = x_1^2 + x_2^2 + \ldots + x_n^2 = \sum_{k=1}^{n} x_k^2$$

ცხადია, რომ თუ ნებისმიერი დიაგონალური ფორმისათვის

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = m$$

მაშინ

$$f(\pm\alpha_1, \pm\alpha_2, \ldots, \pm\alpha_n) = m$$

როგორიც არ უნდა იყოს ნიშანთა კომბინაცია ე.ი. თუ $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ არის m რიცხვის ერთ-ერთი წარმოდგენა დიაგონალური , კერძოდ კვადრატის ჯამების სახით, მაშინ ყოველი სისტემა $(\pm\alpha_1, \pm\alpha_2, \ldots, \pm\alpha_n)$ იქნება აგრეთვე წარმოდგენა. ასეთ წარმოდგენებს ეწოდებათ ერთმანეთისგან არა არსებითად განსხვავებული წარმოდგენები. ხოლო წარმოდგენა არსებითად განსხვავებულია, თუ განსხვავეება ცვლადთა შორის მხოლოდ ნიშანი არ არის.

ახლა განვიხილოთ ორცვლადიანი ანუ ბინარული $(n = 2)$ კვადრატული ფორმები, რომელსაც შემდეგი სახე აქვს:

$$q(x, y) = ax^2 + bxy + cy^2 \qquad (1.1)$$

თუ გავთვალისწინებთ, რომ ყოველი ასეთი ფორმა ცანსახად განისაზღვრება მისი a, b, c დალაგებული სამეულის კოეფიციენტებით, შეგვიძლია გამოვიყენოთ აღნიშვნა

$$q = [a, b, c] \tag{1.2}$$

სადაც იგულისხმება, რომ ეს კოეფიციენტები მთელი რიცხვებია.

რიცხვს

$$d_q = d = \begin{vmatrix} b & 2a \\ 2c & b \end{vmatrix} = b^2 - 4ac \tag{1.3}$$

ეწოდება q ფორმის დისკრიმინანტი.

კვადრატული ფორმის სიმეტრიული მატრიცა

$$M_q = \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \tag{1.4}$$

(1.3) და (1.4) -ის გათვალისწინებით:

$$\det M_q = \begin{vmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{vmatrix} = -\frac{d}{4}$$

ეხლა განვიხილოთ ნებისმიერი წრფივი ჩასმა

$$\begin{aligned} x &= \alpha X + \beta Y \\ y &= \gamma X + \delta Y \end{aligned} \tag{1.5}$$

რომლის შესაბამისი მატრიცა არის

$$\tau = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

ხოლო წრფივი ჩასმის დეტერმინანტი

$$\Delta_\tau = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma$$

ამ ტიპის ყველა ჩასმათა სიმრავლე, რომელთა დეტერმინანტი არ უდრის ნულს, წარმოადგენს ჯგუფს გამრავლების მიმართ, რომლის ერთეულია იგიური ჩასმა: $x = X$, $y = Y$

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{და} \quad |e| = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

ერთეული მატრიცითა და 1-ის ტოლია დეტერმინანტით.

(1.5) ჩასმის შებრუნებული ჩასმაა

$$X = \frac{\delta}{\Delta}x - \frac{\beta}{\Delta}y$$

$$Y = -\frac{\gamma}{\Delta}x + \frac{\alpha}{\Delta}y$$

ხოლო ამ შებრუნებული ჩასმის მატრიცა და დეტერმინანტი შესაბამისად არის

$$\tau^{-1} = \begin{pmatrix} \frac{\delta}{\Delta} & -\frac{\beta}{\Delta} \\ -\frac{\gamma}{\Delta} & \frac{\alpha}{\Delta} \end{pmatrix},$$

$$|\tau^{-1}| = \frac{\delta}{\Delta}\cdot\frac{\alpha}{\Delta} - \frac{\beta}{\Delta}\cdot\frac{\gamma}{\Delta} = \frac{1}{\Delta^2}(\alpha\delta - \beta\gamma) = \frac{1}{\Delta} = \Delta^{-1}$$

წრფივ ჩასმას ეწოდება მთელი ჩასმა თუ მასში შემავალი ელემენტები მთელი რიცხვებია და მთელ ჩასმას ეწოდება უნიმოდულარული თუ მიღებული მატრიცის დეტერმინანტი ± 1-ს ტოლია. მაშასადამე, τ ჩასმა უნიმოდულარულია, თუ $\alpha, \beta, \gamma, \delta$ მთელი რიცხვებია და

$$\Delta_\tau = \det\tau = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma = \pm 1.$$

ჯგუფის განმარტებიდან გამომდინარე, შეგვიძლია ვთქვათ, რომ ყველა უნიმოდულარულ ჩასმათა სიმრავლე ჯგუფია, რომელიც ზემოთმოყვანილ ჩასმათა ჯგუფის ქვეჯგუფია. ასევე, ყველა იმ უნიმოდულარულ ჩასმათა სიმრავლე, რომლის დეტერმინანტი 1-ის ტოლია ჯგუფია, რომელიც ყველა უნიმოდულარულ ჩასმათა

ჯგუფის ქვეჯგუფია. ყოველი უნიმოდულარული ჩასმა ახდენს მთელ რიცხვთა დალაგებული წყვილების ურთიერთცალსახა გარდაქმნას.

მთელ რიცხვთა ორ წყვილს ვუწოდოთ ურთიერთეკვივალენტური, თუ არსებობს უნიმოდულარული ჩასმა, რომელსაც ერთი წყვილი გადაყავს მეორეში.

წყვილთა ეკვივალენტობის ამ დამოკიდებულებას ახასიათებს შემდეგი 3 თვისება:

1) $(x_1, y_1) \sim (x_1, y_1)$;
2) თუ $(x_1, y_1) \sim (x_2, y_2)$ მაშინ $(x_2, y_2) \sim (x_1, y_1)$;
3) თუ $(x_1, y_1) \sim (x_2, y_2), (x_2, y_2) \sim (x_3, y_3)$, მაშინ $(x_1, y_1) \sim (x_3, y_3)$;

მაშასადამ, ყველა მთელ რიცხვთა დალაგებული წყვილების სიმრავლე დაიყოფა არაგადამკვეთ ქვესიმრავლეებად ანუ ექვივალენტურ წყვილთა კლასებად.

თუ (1.1) კვადრატულ ფორმაში განვიხილავთ ნებისმიერ (1.5) წრფივ ჩასმას, მივიღებთ კვადრატულ ფორმას, რომელსაც აქვს შემდეგი სახე:

$$q(x, y) = q(\alpha X + \beta Y, \gamma X + \delta Y) = Q(X, Y) = AX^2 + BXY + CY^2$$

სადაც

$$A = a\alpha^2 + b\alpha\gamma + c\gamma^2 = q(\alpha, \gamma)$$

$$B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$$

$$C = a\beta^2 + b\beta\delta + c\delta^2$$

ამ შემთხვევაში ამბობენ რომ q ფორმა (1.5) ჩასმას გადაყავს Q ფორმაში.

განვიხილოთ q და Q კვადრატულ ფორმათა მატრიცი და დეტერმინანტი

$$M_Q = \begin{pmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{pmatrix}$$

$$\det M_Q = |M_Q| = \begin{vmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{vmatrix} = AC - \frac{1}{4}B^2$$

q და Q ფორმათა მატრიცებსა და დეტერმინანტებს შორის არის შემდეგი დამოკიდებულებები. $(\det\tau \neq 0)$

$$M_Q = \tau \cdot M_q \cdot \tau^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \cdot \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

$$\det M_Q = \begin{vmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{vmatrix} = AC - \frac{1}{4}B^2 = \begin{vmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{vmatrix} \begin{vmatrix} \alpha & \beta \\ \alpha & \beta \end{vmatrix} = \Delta^2 \left(ac - \frac{1}{4}b^2 \right).$$

თუ D აღნიშნავს Q ფორმის დისკრიმინანტს, კავშირი მათ დისკრიმინანტებს შორის არის შემდეგი

$$D = B^2 - 4AC = \Delta^2 d.$$

ორ ფორმას ეწოდება ეკვივალენტური, თუ არსებობს უნიმოდულარული ჩასმა, რომელსაც ერთი მეორეში გადაყავს, ანუ:

$$q \sim Q.$$

ხოლო თუ q და Q ფორმები არ არიან ეკვივალენტური, მაშინ ეს ჩაიწერება:

$$q \nsim Q$$

ვინაიდან ყველა უნიმოდალური ჩასმათა სიმრავლე ჯგუფს წარმოადგენს, კვადრატულ ფორმათა ეკვივალენტობის დამოკიდებულებას ახასიათებს შემდეგი სამი თვისება:

1) $q \sim q$, რეფლექსიურობა;
2) თუ $q \sim Q$, მაშინ $Q \sim q$, (სიმეტრიულობა);

3) თუ $q \sim Q, Q \sim R$, მაშინ $q \sim R$ (ტრანზიტულობა).

ამ თვისებებიდან გამომდინარე ყველა ბინარულ კვადრატულ ფორმათა სიმრავლე დაიყოფა კლასებად, კერძოდ, ეკვივალენტურ ფორმათა კლასებად. ცხადია, რომ ორ კლასს საერთო ელემენტი არ აქვს და თან ყოველი ფორმა q ცალსახად განსაზღვრავს ეკვივალენტურ ფორმათა იმ K_q კლასს, რომელსაც ის ეკუთვნის; ამგვარად $q \sim q'$ ნიშნავს $K_q = K_q{}'$.

თუ ექვივალენტურ ფორმათა ყოველი კლასიდან თითო ფორმას ავიღებთ, მივიღებთ არაეკვივალენტურ ფორმათა სრულ სისტემას.

ყველა ბინარულ ფორმათა კლასებად დაყოფა ჩაიწერება შემდეგნაირად:

$$\{q(x, y)\} = \{[a, b, c]\} = \bigcup K_q$$

აქედან გამომდინარე ცხადია რომ თუ რომელიმე m რიცხვი არის წარმოდგენადი რაიმე კვადრატული ფორმით, მაშინ ის წარმოდგენადი იქნება მისი ეკვივალენტური კვადრატული ფორმითაც და ექვივალენტური ფორმებით წარმოდგენათა რაოდენობები ტოლია.

თავი 2

მთელ რიცხვთა წარმოდგენა კვადრატული ფორმით

დასაწყისში შევნიშნოთ, რომ მთელი რიცხვის მთელკოეფიციენტებიანი ფორმით წარმოდგენადობა და წარმოდგენათა რაოდენობა მჭიდრო კავშირში იმყოფება რიცხვის მულტიპლიკაციურ სტრუქტურასთან , რაც რიცხვთა ადიტიური და მულტიპლიკაციურ თვისებათა შორის კავშირის ერთ-ერთ გამოვლენას წარმოადგენს. ეს ფაქტი კარგად ჩანს ქვემოთ განხილულ მაგალითებში.

განვიხილოთ კვადრატული ფორმა $q = [1,0,-1] = x^2 - y^2$ და შემდეგი თეორემა, რომელიც ეილერის კრიტერიუმითაა ცნობილი:

თეორემა 2.1.

n მარტივი რიცხვია მაშინ და მხოლოდ მაშინ, თუ ის ერთადერთი გზით წარმოიდგინება კვადრატების სხვაობად.

დამტკიცება:

აუცილებლობა. ვთქვათ n მარტივი რიცხვია. ვაჩვენოთ რომ კვადრატების სხვაობად წარმოდგენა ერთადერთია. ვთქვათ

$$n = x^2 - y^2 = (x - y)(x + y)$$

რადგან n მარტივია, ამიტომ

$$\begin{cases} x - y = 1 \\ x + y = n, \end{cases}$$

ანუ

$$\begin{cases} x = \frac{n+1}{2} \\ y = \frac{n-1}{2} \end{cases},$$

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

ეს არის ერთადერთი წარმოდგენა მარტივი რიცხვისა კვადრატების სხვაობად.

საკმარისობა. ვთქვათ, $n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$. ეს ერთადერთი წარმოდგენაა კვადრატების სხვაობად და დავუშვათ წინააღმდეგი. ვთქვათ, $n = pq$. მაშინ

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

მივიღეთ n_ის სხვაგვარი დაშლა კვადრატების სხვაობად, ე.ი. ჩვენი დაშვება არ არის სწორი.

■

იმისთვის, რომ შევამოწმოთ n მარტივი რიცხვია თუ არა, განვიხილოთ შეიძლება თუ არა, რომ n გარდა წარმოდგენისა

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$$

წარმოდგეს სხვა კვადრატების სხვაობად. ამისთვის განვიხილოთ:

$$n + y^2 = x^2 \text{ ან } x^2 - n = y^2$$

და x-ს მივცეთ მნიშვნელობები

$$x > [\sqrt{n}] + 1 - \text{დან, ვიდრე } x = \frac{n+1}{2} - \text{მდე.}$$

თუ სხვაობა $x^2 - n$ გახდება სრული კვადრატი მაშინ n შედგენილია.

მაგალითად, 6077 –სათვის $77 < \sqrt{6077} < 78$. განვიხილოთ

$78^2 - 6077 = 7$

$79^2 - 6077 = 164$

$80^2 - 6077 = 323$

$81^2 - 6077 = 484 = 22^2$, ე.ი

$6077 = 81^2 - 22^2 = (81 - 22)(81 + 22) = 59 \cdot 103.$

ეს მეთოდი კარგია, თუ x და y ერთმანეთთან ახლოსაა. ლეჟანდრმა ყურადღება მიაქცია იმას, რომ ტოლობის ნაცვლად საკმარისია განვიხილოთ შედარება $x^2 \equiv y^2 (\mathrm{mod} n)$. ვიპოვოთ ამ შედარების ისეთი ამონახსნები, რომ $x \not\equiv \pm y (\mathrm{mod} n)$.

ვთქვათ x და y არის $x^2 \equiv y^2 (\mathrm{mod} n)$ შედარების ამონახსნები და აკმაყოფილებენ პირობას $x \not\equiv \pm y (\mathrm{mod} n)$. მაშინ $n | x^2 - y^2 = (x - y)(x + y)$, ანუ $n | (x - y)(x + y)$, $n \nmid (x - y)$ და $n \nmid (x + y)$. გვაინტერესებს უდიდესი საერთო გამყოფი n_ისა $x - y$_თან და $x + y$_თან : $(n, (x - y))$ და $(n, (x + y))$. ეს მოგვცემს n _ის დაშლას მარტივ მამრავლებად, ანუ ესენი იქნებიან n _ის გამყოფები.

დავამტკიცოთ შემდეგი იგივეობა:

$$(A\alpha^2 + B\beta^2)(Aa^2 + Bb^2) = (A\alpha a + Bb\beta)^2 + AB(a\beta - b\alpha)^2 = (A\alpha a - Bb\beta)^2 + AB(a\beta + b\alpha)^2 \quad (2.1)$$

$$\begin{aligned}(A\alpha^2 + B\beta^2)(Aa^2 + Bb^2) &= (A\alpha a)^2 + (B\beta b)^2 + AB(\beta a)^2 + AB(\alpha b)^2 \\ &= (A\alpha a + Bb\beta)^2 - 2ABab\alpha\beta + AB(a\beta)^2 + AB(\alpha b)^2 \\ &= (A\alpha a + Bb\beta)^2 + AB((a\beta)^2 - 2ab\alpha\beta + (\alpha b)^2) = (A\alpha a + Bb\beta)^2 + AB(a\beta - b\alpha)^2\end{aligned}$$

როცა B და A უდრის ერთს, იგივეობა მიიღებს სახეს:

$$(\alpha^2 + \beta^2)(a^2 + b^2) = (\alpha a + b\beta)^2 + (a\beta - b\alpha)^2 = (\alpha a - b\beta)^2 + (a\beta + b\alpha)^2 \quad (2.2)$$

თეორემა 2.2

თუ n რიცხვი უშვებს ორ ერთიმეორისაგან არსებითად განსხვავებულ წარმოდგენას

$$q(x,y) = [A,0,B] = Ax^2 + By^2 \tag{2.3}$$

ფორმით, რომლის A და B კოეფიციენტები ნატურალური რიცხვებია, მაშინ n შედგენილი რიცხვია.

დამტკიცება:

ვთქვათ, (α,β) და (a,b) არიან n რიცხვის არსებითად განსხვავებული წარმოდგენები

(2.3) ფორმით, ე.ი

$$n = Aa^2 + Bb^2,\ n = A\alpha^2 + B\beta^2,\ |\alpha| \neq |a|, |\beta| \neq |b| \tag{2.4}$$

და თან $|\alpha| \neq |b|$, როცა $A = B = 1$.

დავუშვათ საწინააღმდეგო, ე.ი $n = p$ მარტივი რიცხვია.

(2.4)ტოლობებიდან გვაქვს

$$B\beta^2 = p - A\alpha^2, \qquad Bb^2 = p - Aa^2$$

$$B = \frac{p - A\alpha^2}{\beta^2}, \qquad B = \frac{p - Aa^2}{b^2}$$

$$\frac{(p - A\alpha^2)b^2}{\beta^2} = p - Aa^2$$

$$(p - A\alpha^2)b^2 = \beta^2(p - Aa^2)$$

$$p(\beta^2 - b^2) = A(a^2\beta^2 - b^2\alpha^2) = A(a\beta - b\alpha)(a\beta + b\alpha) \tag{2.5}$$

(2.1) იგივეობისა და (2.4) ტოლობათა ძალით გვაქვს $(n = p)$

$$p^2 = (Aa\alpha \pm Bb\beta)^2 + AB(a\beta \mp b\alpha)^2$$

(2.4) ტოლობებიდან ცხადია, რომ $A < p$, მაშასადამე $p \nmid A$; აქედან კი (2.5)-ის ძალით ვასკვნით, რომ

$$p|a\beta - b\alpha \text{ ან } p|a\beta + b\alpha$$

1) ვთქვათ, $AB > 1$, ე.ი A ან B (ან ორივე) მეტია 1-ზე. მაშინ

$$a\beta - b\alpha = 0 \text{ ან } a\beta + b\alpha = 0.$$

თუ ადგილი აქვს ერთ-ერთ ამ ტოლობებიდან მაშინ+

$$\frac{a^2}{\alpha^2} = \frac{b^2}{\beta^2} = \frac{Aa^2}{A\alpha^2} = \frac{Bb^2}{B\beta^2} = \frac{Aa^2 + Bb^2}{A\alpha^2 + B\beta^2} = 1$$

საიდანაც $a = \pm\alpha, b = \pm\beta$, რაც პირობას ეწინააღმდეგება.

2) $AB = 1$, ე.ი $A = B = 1$, მაშინ კვადრატული ფორმა (2.3) იქნება კვადრატების ჯამი.

$$q(x, y) = [1,0,1] = x^2 + y^2$$

$$p^2 = (\alpha a \pm b\beta)^2 + (a\beta \mp b\alpha)^2$$

მაშასადამე ადგილი აქვს ერთ-ერთ შემდეგი ორი პირობიდან

$$(\alpha a \pm b\beta)^2 = p^2, a\beta \mp b\alpha = 0$$

ან

$$(\alpha a \pm b\beta)^2 = 0, a\beta \mp b\alpha = p^2$$

ვთქვათ, ადგილი აქვს მეორეს, მაშინ გვექნება

$$a\beta \mp b\alpha = \pm p, \qquad \alpha a \pm b\beta = 0, \qquad \alpha a = \pm b\beta$$

ამავე დროს, ვინაიდან (α, β) და (a, b) p-ს წარმოდგენებია $x^2 + y^2$ ფორმით, გვექნება

$$p = \alpha^2 + \beta^2 = a^2 + b^2, (\alpha, \beta) = (a, b) = 1.$$

ეს დამოკიდებულებები, წინა პირობასთან ერთად გვაძლევენ: $\alpha|b, b|\alpha, a|\beta, \beta|a$, საიდანაც

$$a = \pm\beta, b = \pm\alpha$$

რაც პირობას ეწინააღმდეგება.

თუ აღმოჩნდება, რომ რომელიმე n რიცხვი უშვებს ორ არსებითად განსხვავებულ წარმოდგენას $Ax^2 + By^2$ ფორმით, მაშინ დამტკიცებული თეორემის საფუძველზე ვასკვნით რომ ეს რიცხვი არის შედგენილი.

მაგალითად ვთქვათ $(p > 2)$ $n = p^4 + 4$ ე.ი.

$$n = (p^2)^2 + 2^2 = (p^2 - 2)^2 + (2p)^2$$

რაც ნიშნავს, რომ $p^4 + 4$ სახის ყოველი რიცხვი უშვებს ორ არსებითად განსხვავებულ წარმოდგენას $(p^2, 2)$ და $(p^2 - 2,2p)$ ორი კვადრატის ჯამის სახით, საიდანაც ვასკვნით რომ ეს რიცხვი შედგენილია.

■

თეორემა 2.3

თუ n რიცხვი საკუთრივ წარმოდგება

$$q = q(x, y) = [1,0, k] = x^2 + ky^2$$

ფორმით, სადაც $k = 1,2$ ან 3, მაშინ მისი ნებისმიერი d გამყოფიც წარმოდგება ამავე ფორმით

$$d = u^2 + kv^2,$$

ერთადერთი გამონაკლისით $d = 2$, იმ შემთხვევაში როცა $k = 3$, არაუარყოფითი u და v მთელი რიცხვები შეიძლება თანამარტივი არ იყვნენ.
(ამ თეორემის შებრუნებული თეორემა უშუალოდ გამომდინარეობს (2.1) იგივეობიდან).

დამტკიცება:

(2.1) იგივეობა შეიძლება შემდეგნაირად ჩაიწეროს $\left(\frac{B}{A} = s\right)$

$$(a^2 + sb^2)(\alpha^2 + s\beta^2) = (a\alpha \pm sb\beta)^2 + s(a\beta \mp b\alpha)^2$$

ამ იგივეობიდან გამომდინარეობს, რომ $x^2 + ky^2$ ფორმით წარმოდგენად ნებისმიერ ორ რიცხვთა ნამრავლი წარმოდგენადია ამავე ფორმით. ამიტომ საკმარისია ვაჩვენოთ თეორემის მართებულობა $x^2 + ky^2$სახის რიცხვის ნებისმიერი მარტივი გამყოფისათვის.

პირველ რიგში ვაჩვენოთ რომ: $x^2 + ky^2$ სახის რიცხვის ყოველი მარტივი გამყოფი p წარმოადგენს $x^2 + k$ სახის რომელიღაც რიცხვის გამყოფს. ე.ი.

$$\text{თუ } p|x^2 + ky^2 \text{ , მაშინ } p|x_1^2 + k$$

მართლაც, ვთქვათ $p|x^2 + ky^2$ $(x, y) = 1$; მაშინ ასევე $(p, y) = 1$, რადგან წინააღმდეგ შემთხვევაში, ე.ი. $p|y$, გვექნებოდა $p|x$, $(x, y) > 1$. ვინაიდან $(p, y) = 1$ არსებობს მთელი რიცხვების ისეთი წყვილი (z, u) რომ

$$yz - pu = 1, (z, u) = 1.$$

$x^2 + ky^2$ გამოსახულების z^2 ზე გამრავლებით მივიღებთ

$$x^2z^2 + k(yz)^2 = x^2z^2 + k(1 + pu)^2 = x^2z^2 + k + 2kpu + kp^2u^2$$

ამ ტოლობის მარცხენა მხარის და მარჯვენა მხარის ბოლო ორი შესაკრები იყოფა p ზე, საიდანაც მივიღებთ შემდეგს

$$p|x^2z^2 + k = (xz)^2 + k = x_1^2 + k, \quad p|x_1^2 + k$$

ეხლა ვაჩვენოთ, რომ $x^2 + k$ სახის ნებისმიერი რიცხვის ყოველი მარტივი p გამყოფს შემდეგი სახე აქვს $u^2 + kv^2$. ანუ

$$\text{თუ } p|x^2 + k, \text{ მაშინ } p = u^2 + kv^2$$

მართლაც, ვთქვათ $p|x^2 + k$; რაციონალური რიცხვი $\frac{x}{p}$ დავშალოთ უწყვეტ წილადად

$$\frac{x}{p} = [\alpha_0; \alpha_1; \alpha_2; \dots, \alpha_m] = \frac{p_m}{q_m}$$

როგორც ვიცით

$$q_0 < q_1 < q_2 < \dots < q_m = p$$

ამიტომ არსებობს მეზობელ $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ მახლობლად წილადთა წყვილი, რომელთა მნიშვნელებისთვის ადგილი აქვს უტოლობას

$$q_n^2 < p < q_{n+1}^2$$

რადგან , $\frac{x}{p} \in (\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}})$ გვექნება,

$$\left|\frac{x}{p} - \frac{p_n}{q_n}\right|^2 < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|^2 = \frac{1}{q_n^2 q_{n+1}^2}$$

თუ ამ უკანასკნელ უტოლობას გავამრავლებთ $(pq_n)^2$ ზე და მხედველობაში მივიღებთ

$$q_n^2 < p < q_{n+1}^2$$

უტოლობას მაშინ გვექნება

$$(xq_n - pp_n)^2 < \frac{p^2}{q_{n+1}^2} < p$$

საიდანაც

$$(xq_n - pp_n)^2 + kq_n^2 < p + kq_n^2 \qquad (2.6)$$

რადგან, $p|x^2 + k$, მოცემული უკანასკნელი უტოლობის მარცხენა მხარე იყოფა p-ზე.

მეორეს მხრივ, ვინაიდან $q_n^2 < p$, მარჯვენა მხარისათვის გვაქვს

$$p + kq_n^2 < p + kp = p(k+1) \qquad (2.7)$$

განვიხილოთ ცალ-ცალკე ყველა შესაძლებელი შემთხვევა.

1) $k = 1$; (2.7) ტოლობის გათვალისწინებით

$$p + kq_n^2 = p + q_n^2 < 2p \qquad (2.8)$$

(2.6)-ის მარცხენა მხარე იყოფა p-ზე. ე.ი აქვს სახე pt $(t \geq 1)$; ამიტომ (2.8) ტოლობის გათვალისწინებით გვაქვს

$$pt < p + q_n^2 < 2p$$

საიდანაც ცხადია, რომ $t = 1$,

$$(xq_n - pp_n)^2 + kq_n^2 = p$$

რაც ნიშნავს რომ p არის $u^2 + kv^2$ სახის რიცხვი.

2) $k > 1$; მაშინ (2.6) და (2.7)-ის ძალით გვაქვს ((2.6)-ის მარცხენა მხარე იყოფა p-ზე, მაშასადამე, მეტია ან ტოლია $p - $ სი)

$$p \leq (xq_n - pp_n)^2 + kq_n^2 \leq kp \qquad (2.9)$$

განვიხილოთ ცალ-ცალკე ორივე შესაძლებელი შემთხვევა:

2)ა. $k = 2$ მაშინ

$$p = (xq_n - pp_n)^2 + kq_n^2$$

ან

$$(xq_n - pp_n)^2 + kq_n^2 = kp = 2p$$

თუ ადგილი აქვს პირველ ტოლობას, მაშინ ცხადია, რომ p-ს აქვს $u^2 + kv^2$ სახე.

ხოლო, თუ ადგილი აქვს მეორე ტოლობას მაშინ გვაქვს

$$p = kq_n^2 + k\left(\frac{xq_n - pp_n}{k}\right)^2$$

ვინაიდან ამ ტოლობის ორივე p და q_n^2 მთელი რიცხვებია, მაშინ ფრჩხილებში მოთავსებული გამოსახულებაც მთელი რიცხვი არის , ასე რომ ამ შემთხვევაშიც p-ს აქვს $u^2 + kv^2$ სახე.

2)ბ. $k = 3$ თუ (2.9)-ში ადგილი აქვს მარცხენა მხარეში ტოლობას, ე.ი. თუ

$$p = (xq_n - pp_n)^2 + kq_n^2$$

თეორემის მართებულება ცხადია; თუ ადგილი აქვს მარჯვენა მხარეში ტოლობას, ე.ი. თუ

$$kp = (xq_n - pp_n)^2 + kq_n^2$$

მაშინ, როგორც ზემოთ გვექნება

$$p = q_n^2 + k\left(\frac{xq_n - pp_n}{k}\right)^2 = u^2 + kv^2$$

მთელი u და v რიცხვებით; ამ შემთხვევაშიც თეორემა მართებულია.

ახლა განვიხილოთ შემთხვევა, როცა (2.9)-ს ორივე მხარეში ადგილი აქვს უტოლობას, ე.ი. როცა

$$2p = (xq_n - pp_n)^2 + 3q_n^2$$

ნებისმიერი მთელი რიცხვის კვადრატს აქვს ერთ-ერთი შემდეგი სახე: $4m, 4m + 1$. თუ q_n კენტია, მაშინ უკანასკნელი ტოლობის მარჯვენა მხარეში მდგომი ორივე შესაკრები კენტია; მაშინ მთელ მარჯვენა მხარეს ექნება სახე $4m$; ამავე სახის უნდა იყოს მარცხენა მხარე, ე.ი. $2p = 4m$, $p = 2m$, საიდანაც $p = 2$.

როცა $k = 3$ ე.ი. $x^2 + 3y^2$ ფორმის შემთხვევაში, დარჩა განსახილველი მარტივი გამყოფი $p = 2$; ვინაიდან $(x, y) = 1$, რიცხვები x და y ორივე ლუწი არაა. ამიტომ $p = 2$ თუ არის $x^2 + 3y^2$-ის გამყოფი , $2|x^2 + 3y^2$, მაშინ ორივე კენტი უნდა იყოს; ცხადია რომ პირიქით თუ x და y ორივე კენტია, მაშინ $2|x^2 + 3y^2$. მაგრამ $p = 2$ არ არის $x^2 + 3y^2$ სახის რიცხვი, ე.ი. განტოლებას $x^2 + 3y^2 = 2$ არა აქვს ამონახსნი მთელ რიცხვებში.

■

განვიხილოთ ფორმა

$$q = q(x, y) = [1,0,1] = x^2 + y^2$$

რომელიც $x^2 + ky^2$ და $Ax^2 + By^2$ფორმათა კერძო შემთხვევას წარმოადგენს.

თეორემა 2.4 (ვილსონი)

$n|(n-1)! + 1$ მაშინ და მხოლოდ მაშინ როცა $n = p$ არის მარტივი რიცხვი .

ვილსონის თეორემიდან ადვილად მიიღება შემდეგი თეორემა

თეორემა 2.5

თუ p მარტივ რიცხვს აქვს სახე $4k + 1$, $p = 4k + 1$ მაშინ

$$p\left|\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 = x^2 + 1\right.$$

მეორე მხრივ ცხადია, რომ ნებისმიერი ორი კვადრატის ჯამს აქვს ერთ-ერთი შემდეგი სახე: $4n,\ 4n + 1,\ 4n + 2$. ამიტომ თეორემა (2.5)-ის ძალით, ორი კვადრატის ჯამის ყოველ გამყოფსაც აქვს ერთ-ერთი ამავე სახეთაგანი; აქედან გამომდინარეობს, რომ ორი თანამარტივი რიცხვების კვადრატების ჯამს აქვს მხოლოდ $4n + 1$ სახის კენტი გამყოფი. ამის შემდეგ $x^2 + y^2$ ფორმისათვის მიღებული ყველა შედეგი შეიძლება შემდეგნაირად ჩამოყალიბდეს:

შედეგი 2.1 თუ p მარტივი რიცხვი იშლება ორი კვადრატის ჯამად, ეს დაშლა ერთადერთია.

შედეგი 2.2 თუ მარტივი რიცხვი არის ორი თანამარტივი კვადრატების ჯამის გამყოფი, მაშინ ეს რიცხვი წარმოადგენს ასეთი კვადრატების ჯამს.

შედეგი 2.3 თუ რომელიმე რიცხვის ყოველი მამრავლი ორი კვადრატის ჯამია, მაშინ ეს რიცხვიც ორი კვადრატის ჯამია.

შედეგი 2.4 ორი კვადრატის ნებიესმიერ ჯამს აქვს ერთ-ერთი შემდეგი სახე: $4n,\ 4n + 1,\ 4n + 2$.

შედეგი 2.5 ყოველი p მარტივი რიცხვი $4k + 1$ სახისა არის კვადრატების ჯამის $(N^2 + 1^2)$ გამყოფი.

შედეგი 2.1; 2.2; 2.4 და 2.5- დან გამომდინარეობს

თეორემა 2.6

$4k + 1$ სახის მარტივი რიცხვი ერთადერთი სახით იშლება ორი თანამარტივი კვადრატის ჯამად. არც ერთი $4k + 3$ სახის მარტივი რიცხვი არ იშლება ორი კვადრატის ჯამად.

ახლა განვიხილოთ შედგენილი რიცხვის ორი კვადრატის ჯამის სახით წარმოდგენის საკითხი.

თეორემა 2.7

აუცილებელი და საკმარისი პირობა იმისა რომ m რიცხვი წარმოდგებოდეს ორი კვადრატის ჯამად, იმაში მდგომარეობს, რომ მის კანონიკურ დაშლაში $4k + 3$ სახის ყოველი მარტივი რიცხვი შედიოდეს ლუწ ხარისხში.

დამტკიცება:

ვთქვათ შედგენილი რიცხვი იშლება ორი კვადრატის ჯამად და თან შეიცავს $p = 4k + 3$ სახის მარტივ გამყოფს. ანუ

$$m = x^2 + y^2 \quad \text{და} \quad p|m$$

ვთქვათ $(x, y) = d$, მაშინ $(x^2, y^2) = d^2$. თუ p^t არის p-ს უმაღლესი ხარისხი შემავალი d-ში, მაშინ p^t იქნება p-ს უმაღლესი ხარისხი შემავალი d^2-ში.

$$x = x_1 d, \qquad y = y_1 d, \qquad m = x^2 + y^2 = d^2(x_1^2 + y_1^2)$$

$$p^{2t}|m, \qquad (x_1, y_1) = 1$$

p^{2t} არის p-ს უმაღლესი ხარისხი შემავალი m-ში. მართლაც, წინააღმდეგ შემთხვევაში გვექნება: $p^s|m \;\; s > 2t$ საიდანაც

$$p^s|d^2(x_1^2 + y_1^2), \qquad p^{s-2t}|x_1^2 + y_1^2 = m_1, \;\; p|x_1^2 + y_1^2;$$

p მარტივი რიცხვი როგორც კვადრატების ჯამის გამყოფი თვითონაც უნდა წარმოადგენდეს ორი კვადრატების ჯამს, რაც შეუძლებელია, რადგან $p = 4k + 3$

ამგვარად , თუ m შედგენილი რიცხვი იშლება ორი კვადრატის ჯამად, მის კანონიკურ დაშლას უნდა ქონდეს სახე:

$$m = 2^{\alpha} q_1^{\alpha_1} q_2^{\alpha_2} \dots \; q_u^{\alpha_u} p_1^{2\beta_1} p_2^{2\beta_2} \dots p_v^{2\beta_v} \qquad (2.10)$$

სადაც, ყოველი q_i არის $k + 1$ სახის, ხოლო ყოველი q_j არის $4k + 3$ სახის.

ვაჩვენოთ, რომ (2.10) პირობა არის საკმარისი იმისათვის, რომ m რიცხვი წარმოდგეს ორი კვადრატის ჯამად. მართლაც

$$m = m_1 \cdot m_2^2$$

სადაც,

$$m_1 = 2^{\alpha} q_1^{\alpha_1} q_2^{\alpha_2} \dots \; q_u^{\alpha_u}$$

$$m_2 = p_1^{\beta_1} p_2^{\beta_2} \dots p_v^{\beta_v}$$

m_1-ის ყოველი თანამამრავლი როგორც ვიცით ორი კვადრატის ჯამი არის, და მაშასადამე, m_1იც ორი კვადრატის ჯამი არის

$$m_1 = x_1^2 + y_1^2$$

თუ ამ ტოლობას m_2^2-ზე გავამრავლებთ, მაშინ მივიღებთ

$$m = m_1 \cdot m_2^2 = (x_1^2 + y_1^2)m_2^2 = (m_2 x_1)^2 + (m_2 y_1)^2 = x^2 + y^2;$$

■

თეორემა 2.8

ნატურალური რიცხვი ერთადერთი სახით (შესაკრებთა რიგისა და მათი ნიშნის სიზუსტით) იშლება ორი კვადრატის ჯამად, მაშინ და მხოლოდ მაშინ, როცა ის არის $4k + 1$ სახის მარტივი რიცხვი.

რიცხვთა სიმრავლის სამი კვადრატის ჯამის სახით დაშლის შესახებ სრულ პასუხს გვაძლევს შემდეგი თეორემა:

თეორემა.2.9

ნატურალური რიცხვი იშლება სამი კვადრატის ჯამად მაშინ და მხოლოდ მაშინ, როცა მას არა აქვს სახე

$$4^{n}(8m + 7),\ n,\ m = 0,1,2,3,\ldots. \tag{2.11}$$

ვამტკიცებთ მხოლოდ პირობის აუცილებლობას, ვთქვათ რიცხვს აქვს (2.11) სახე და ვაჩვენოთ რომ ის არ წარმოდგება სამი კვადრატის ჯამის სახით, ნებისმიერ მთელ რიცხვს აქვს შემდეგი სახეებიდან $4k, 4k + 1, 4k + 2, 4k + 3$ ერთ-ერთი, ანუ რაც იგივეა $4k, 4k + 1, 4k + 2, 4k - 1$ სახე. ამ რიცხვების კვადრატს აქვს

$$8q,\ 8q + 1,\ 8q + 4 \tag{2.12}$$

სახეებიდან ერთ-ერთი.

თუ განვიხილავთ ყველა შესაძლო ასეთი სამი რიცხვის ჯამს, ის ყველა მნიშვნელობას მიიღებს გარდა $8m + 7$ სახის რიცხვებისა, ანუ სხვაგვარად რომ ვთქვათ

$$x^2 + y^2 + z^2 \ = 8m + 7$$

განტოლებას ამონახსნი არა აქვს მთელ რიცხვთა სიმრავლიდან. პირობის აუცილებლობა დამტკიცებულია $n = 0$-ისთვის.

პირობის სრულად მართებულობა ვაჩვენოთ მათემატიკური ინდუქციის მეთოდის გამოყენებით, დავუშვათ რომ პირობა მართებულია მოცემული n ნატურალური რიცხვისთვის ე.ი

$$x^2 + y^2 + z^2 \ = 4^n(8m + 7) \tag{2.13}$$

და ვაჩვენოთ ფორმულის სამართლიანობა $n + 1$ -ისთვის.

$$x^2 + y^2 + z^2 \ = 4^{n+1}(8m + 7) \tag{2.14}$$

ანუ ვაჩვენოთ რომ ამ შემთხვევაშიც განტოლებას ამონახსნი მთელ რიცხვთა სიმრავლეში არ გააჩნია. დავუშვათ საწინააღმდეგო, ვთქვათ განტოლებას გააჩნია მთელი ამონახსნი და რადგან განტოლების მარჯვენა მხარე უნაშთოდ იყოფა 4-ზე, მარცხენაც უნდა გაიყოს, ეს შესაძლებელია მხოლოდ მაშინ როცა თითოეული x, y, z უნაშთოდ იყოფა 2-ზე, ანუ

$$x = 2x_1, \ \ y = 2y_1, \ \ z = 2z_1$$

(2.14) ტოლობაში ამ მნიშვნელობების შეტანით მიღებული განტოლების ყველა წევრი შეიკვეცება 4 ზე და მივითებთ განტოლებას:

$$x_1{}^2 + y_1{}^2 + z_1{}^2 \ = 4^n(8m + 7)$$

ე.ი. (x_1, y_1, z_1) სამეული აკმაყოფილებს (2.13) განტოლებას, რაც პირობას ეწინააღმდეგება.

■

განვიხილოთ რიცხვთა წარმოდგენა ოთხი კვადრატის ჯამის სახით

დირიხლეს თეორემა

ნებისმიერი მარტივი p-სათვის არსებობს ოთხი კვადრატის ჯამი რომელიც იყოფა p-ზე.

დამტკიცება:

შეგვიძლია დავამტკიცოთ, რომ არსებობს სამი კვადრატის ჯამი იყოფა p-ზე. განვიხილოთ კვადრატულ ნაშთა კლასების სიმრავლე მოდულით p. ჯერ x^2-ის და შემდეგ $-1-y^2$-ის. თითოეულ ამ სიმრავლეში შედის $\frac{p+1}{2}$ ელემენტი. ეს ორი სიმრავლე თანაიკვეთება, ესეიგი x^2 სადარია $-1-y^2$ მოდულით p. ეს იგივეა რაც x^2+y^2+1 სადარია 0 მოდულით p.

ოთხი კვადრატის ჯამის სახით რიცხვთა წარმოდგენისათვის განვიხილოთ ლაგრანჟის თეორემა

თეორემა 2.10 (ლაგრანჟის თეორემა)

ყოველი ნატურალური რიცხვი წარმოდგება 4 კვადრატის ჯამის სახით.

დამტკიცება:

ამ წარმოდგენაში დაგვეხმარება ეილერის იგივეობა:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$$
$$=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4+x_4y_3)^2$$
$$+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$$

ამ იგივეობის თამახმად ოთხი კვადრატის ჯამის სახით წარმოდგენილი ორი რიცხვის ნამრავლი წარმოდგენადია ოთხ რიცხვთა კვადრატის ჯამის სახით. აქედან გამომდინარე საკმარისია ვაჩვენოთ ნებისმიერი მარტივი რიცხვის ოთხ კვადრატთა ჯამის სახით წარმოდგენადობა.

$p=2$-ს ერთადერთი ლუწი მარტივი რიცხვია და იგი იშლება ოთხი მთელი რიცხვის კვადრატთა ჯამის სახით:

$$2=1^2+1^2+0^2+0^2$$

ეხლა განვიხილოთ ნებისმიერი კენტი p მარტივი რიცხვი და ვაჩვენოთ მისი წარმოდგენა ოთხი მთელი რიცხვის კვადრატთა ჯამის სახით, ამიტომ განვიხილოთ შემდეგი ორი დებულება:

1) არსებობს ისეთი ნატურალური $m < p$ რიცხვი, რომლისთვისაც mp ნამრავლი წარმოადგენს ოთხი კვადრატის ჯამს.
2) თუ mp ოთხი მთელი რიცხვის კვადრატთა ჯამია და $m > 1$, მაშინ არსებობს $n(0 < n < m)$ რიცხვი, რომლისთვისაც np-ც ოთხი კვადრატის ჯამია.

ამ ორი დებულებიდან გამომდინარე გვექნება შემდეგი ტოლობები:

$$mp = x_{01}^2 + x_{02}^2 + x_{03}^2 + x_{04}^2,$$
$$m_1 p = x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2, \quad 0 < m_1 < m,$$
$$m_2 p = x_{21}^2 + x_{22}^2 + x_{23}^2 + x_{24}^2, \quad 0 < m_2 < m_1,$$

და ა.შ.

რადგან $m > m_1 > m_2 > \ldots$, უტოლობათა ეს მიმდევრობა სასრულია. ის წყდება ტოლობაზე, რომლისთვისაც $m_k = 1$; უკანასკნელ ტოლობას ექნება სახე

$$p = x_{k_1}^2 + x_{k_2}^2 + x_{k_3}^2 + x_{k_4}^2 = p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

რაც ნიშნავს, რომ p რიცხვი წარმოდგენადია ოთხი კვადრატის ჯამის სახით.

პირველი დებულების დასამტკიცებლად საკმარისია ვაჩვენოთ, რომ მოცემული p კენტი მარტივი რიცხვისთვის არსებობს x და y რიცხვები $x < \frac{p}{2}, y < \frac{p}{2}$ ისეთი რომ მათი კვადრატების ჯამი p-ზე გაყოფისას ნაშთში იძლევა 1-ს

$$x < \frac{p}{2},\ y < \frac{p}{2},\ x^2 + y^2 = mp - 1 \qquad (2.15)$$

მართლაც

$$mp = x^2 + y^2 + 1^2 + 0^2, \qquad 0 < mp < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2, \qquad m < p$$

ე.ი m რიცხვი აკმაყოფილებს პირველი დებულების მოთხოვნას.

ამგვარად პირველი დებულების დასამტკიცებლად საკმარისია ვაჩვენოთ (2.15) პირობით განსაზღვრული x და y რიცხვების არსებობა. ამისათვის განვიხილოთ სისტემა

$$0,1,2,3,\ldots,\frac{p-1}{2}$$

რომელიც შეიცავს $\frac{p+1}{2}$ წევრს. განვიხილოთ მათი კვადრატებისგან შემდგარი სისტემა

$$0, 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \tag{2.16}$$

ეს რიცხვები წყვილ-წყვილად ურთიერთ არასადარი არიან მოდულით p. თუ განვიხილავთ საწინააღმდეგოს დაშვების მეთოდს მივიღებთ რომ

$$x_1^2 \equiv x_2^2 (\mathrm{mod}\ p), \qquad x_1^2 = pk_1 + r, \qquad x_2^2 = pk_2 + r, \qquad 0 \le r \le p-1,$$

საიდანაც

$$x_1^2 - x_2^2 = (k_1 - k_2)p, \qquad p|(x_1 - x_2)(x_1 + x_2)$$

მაგრამ $0 < x_1 + x_2 \le p - 1 < p$, საიდანაც $p|x_1 - x_2$ რაც შეიძლება მხოლოდ მაშინ როცა $x_1 = x_2$. (2.16) რიცხვები p-ზე გაყოფისა იძლევა სხვადასხვა ნაშთს, აქედან გამომდინარე

$$-1, -1^2 - 1, -2^2 - 1, -3^2 - 1, \ldots, -\left(\frac{p-1}{2}\right)^2 - 1 \tag{2.17}$$

p-ზე გაყოფისას იძლევიან სხვადასხვა ნაშთს. x_i^2 იყოს (2.10.2)-ის ნებისმიერი წევრი, მაშინ (2.17) შესაბამისი წევრი იქნება $-1 - x_i^2$ $(i = 1,2\ldots\frac{p-1}{2})$. (2.16) და (2.17) სისტემების რიცხვთა საერთო რაოდენობა არის $p + 1$. თან თითოეული სისტემის რიცხვები წყვილ-წყვილად ურთიერთარასადარი არიან მოდულით p, მაგრამ p-ზე გაყოფისას განსხვავებულ ნაშთა რიცხვი არის p. ამიტომ (2.16) სისტემის ერთი მაინც რიცხვი სადარი იქნება (2.17) სისტემის სათანადო რიცხვისა. ე.ი

$$x_i^2 = -1 - x_j^2 (\mathrm{mod} p), \qquad x_i^2 = sp + r, \qquad -1 - x_j^2 = tp + r,$$

საიდანაც

$$x_i^2 + x_j^2 + 1 = (s - t)p$$

ჩანს რომ $s - t > 0$. ამავე დროს

$$x_i \le \frac{p-1}{2} < \frac{p}{2}, \qquad x_j \le \frac{p-1}{2} < \frac{p}{2}, \qquad 0 \le |s| < \frac{p}{2}, \qquad 0 \le |t| < \frac{p}{2}.$$

ამგვარად გვაქვს

$$x_i^2 + x_j^2 = mp - 1, \qquad 0 < x_i, \qquad x_j < \frac{p}{2}, \qquad 0 < m = s - t < p,$$

საიდანაც გამომდინარეობს პირველი დეგულების მართობულობა.

ახლა ვაჩვენოთ მეორე დებულების მართებულობა, რაც ნიშნავს m მამრავლის შემცირების შესაძლებლობას განვიხილოთ mp ნამრავლის ერთ-ერთი წარმოდგენა ოთხი კვადრატის ჯამად

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \tag{2.18}$$

აღვნიშნოთ y_k-თი x_k რიცხვის აბსოლუტურად უმცირესი ნაშთის აბსოლუტური სიდიდე მოდულით m და თუ q_k და r_k აღნიშნავს x_k-ს m-ზე გაყოფისას მიღებულ განაყოფსა და ნაშთს მაშინ

$$y_k = \begin{cases} r_k, \text{თუ } 0 \le r_k \le \dfrac{m}{2}, \\ m - r_k, \text{თუ } r_k > \dfrac{m}{2} \end{cases}$$

y_k რიცხვთა განმარტების ძალით გვაქვს

$$x_k = mq_k \pm y_k, \qquad 0 \le y_k \le \frac{m}{2},$$

$$x_k^2 = m^2 q_k^2 \pm 2mq_k y_k + y_k^2 = mQ_k + y_k^2, \quad (Q_k = mq_k^2 \pm 2q_k y_k).$$

თუ x_k რიცხვების ამ რიცხვებს შევიტანთ (2.18)-ში, გვექნება

$$mp = mq + y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

ან

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2, n = p - q. \tag{2.19}$$

(2.18) და (2.19) იგივეობათა გადამრავლება, ეილერის იგივეობის ძალით გვაძლევს

$$m^2pn = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 \tag{2.20}$$

მარჯვენა მხარეში მდგომი ყველა ფრჩხილში მოთავსებული გამოსახულება m-ის ჯერადია, ამიტომ მთლიანად გამოსახულება m^2-ის ჯერადია.

თუ x_k-ს შევცვლით $mq_k \pm y_k$ გამოსახულებით, შევამჩნევთ რომ ყოველი ფრჩხილი m-ის ჯერადია. (2.20) ტოლობის m^2-ზე შეკვეცით გვექნება

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

ბოლოს ვაჩვენოთ რომ $0 < n < m$. მართლაც, როგორც ვიცით, $0 \le y_k \le \frac{m}{2}$. ამავე დროს არსებობს k-ს ერთი მაინც მნიშვნელობა $k = I$, რომლისთვისაც $0 \le y_i < \frac{m}{2}$. $\left(1 < m < \frac{p}{2}\right)$. ამიტომ $0 \le y_k \le \frac{m}{2}$ უტოლობათა კვადრატში აყვანითა და შეკრებით ვღებულობთ

$$0 \le y_1^2 + y_2^2 + y_3^2 + y_4^2 < m^2,$$

ეს უტოლობა (2.19)-თან ერთად გვაძლევს

$$mn < m^2, \qquad n < m.$$

ამასთანავე $n > 0$ რადგან წინააღმდეგ შემთხვევაში გვექნებოდა $y_1 = y_2 = y_3 = y_4 = 0$ რაც ნიშნავს რომ ყოველი x_k არის m-ის ჯერადი და მათი კვადრატების ჯამი

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

გაიყოფა m^2-ზე რაც შეუძლებელია რადგან $m > 1$.

ამგვარად თუ არსებობს $m(1 < m < p)$, რომლისთვისაც ამოხსნადია განტოლება $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ მაშინ არსებობს $n(1 \le n < m)$, რომლისთვისაც ამოხსნადია სათანადო განტოლება

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

მაშასადამე 2) დებულება დამტკიცებულია.

ასევე შეიძლება ამ თეორემის გამოყვანა სამი კვადრატის თეორემიდან. ვიცით, რომ თუ რიცხვს არა აქვს სახე $4^a + (8b + 7)$, მაშინ ის შეიძლება წარმოვადგინოთ სამი კვადრატის ჯამის სახით ანუ ოთხი კვადრატის ჯამად წარმოდგინდება. ხოლო თუ მას აქვს სახე $4^a(8b + 7)$, მაშინ $8b + 3$ წარმოვადგინოთ სამი კვადრატის ჯამად და დავუმატოთ 2^2 ანუ მივიღებთ $8b + 3 + 2^2 = 8b + 7$. შემდეგ გავამრავლოთ მიღებული ჯამი $(2^a)^2$.

თავი 3

ნატურალური რიცხვის წარმოდგენათა რაოდენობა კვადრატული ფორმით.

ამ თავში განვიხილავ რიცხვის კვადრატული ფორმით წარმოდგენათა რაოდენობას. განასხვავებენ წარმოდგენათა რიცხვის ასიმპტოტურ და ზუსტ ფორმულებს. პირველი იძლევა რიცხვთა სათანადო კვადრატული ფორმით წარმოდგენათა $r(n)$ რაოდენობის, როგორც n-ის არითმეტიკული ფუნქციის ასიმპტოტურ ყოფაქცევას, მის ასიმპტოტურ გამოსახულებას, ხოლო მეორე -ამავე $r(n)$ ფუნქციის ზუსტ გამოსახულებას.

მოვიყვანოთ, დაუმტკიცებლად, წარმოდგენათა რაოდენობის რამდენიმე ფორმულა ზოგიერთი უმარტივესი ფორმისათვის.

თუ $q = q(x_1, x_2, \dots, x_m)$ მოცემული კვადრატული ფორმაა, მაშინ სიმბოლოთი $N(q = n) = r_q(n) = r(n)$ აღვნიშნოთ n რიცხვის q ფორმით ყველა წარმოდგენათა რაოდენობა, ე.ი. $q(x_1, x_2, \dots, x_m) = n$ განუზღვრელი განტოლების ამონახსნთა რაოდენობა. მაშინ ადგილი აქვს შემდეგ ტოლობებს

1) $N(x^2 + y^2 = n) = 4E(n)$,

სადაც

$$E(n) = \sum_{\substack{d|n \\ d\equiv 1 (\mathrm{mod} 4)}} 1 - \sum_{\substack{d|n \\ d\equiv 3 (\mathrm{mod} 4)}} 1 = \sum_{d|n} (-1)^{\frac{d-1}{2}}$$

სიტყვიერად: n რიცხვის ორი კვადრატის ჯამი სახით წარმოდგენათა რაოდენობა უდრის n-ის $4k + 1$ სახის გამყოფთა რაოდენობისა და მისივე $4k + 3$ სახის გამყოფთა რაოდენობის სხვაობის გაოთხკეცებულს.

2) $N(x^2 + 2y^2 = n) = 2g(n)$

სადაც

$$g(n) = \sum_{\substack{d|n \\ d\equiv 1,3 (\mathrm{mod} 8)}} 1 - \sum_{\substack{d|n \\ d\equiv 5,7 (\mathrm{mod} 8)}} 1$$

3) $N(x^2 + 3y^2 = n = 2^k u = \begin{cases} 0, & \text{თუ } k - \text{კენტია}, \\ 2e(u), & \text{თუ } k = 0, \\ 6e(u), & \text{თუ } k \geq 2 \text{ ლუწია} \end{cases}$

სადაც

$$e(n) = \sum_{\substack{d|n \\ d\equiv 1 (\mathrm{mod} 3)}} 1 - \sum_{\substack{d|n \\ d\equiv 2 (\mathrm{mod} 3)}} 1$$

4) $N(x^2 + xy + y^2 = n) = 6e(n)$

$$e(2^k u) = \begin{cases} 0, & \text{თუ } k - \text{კენტია}, \\ e(u), & \text{თუ } k - \text{ლუწია} \end{cases}$$

5) $N = (x^2 + y^2 + z^2 + t^2 = n = 2^\alpha u) = \begin{cases} 8\sigma(u), & \text{თუ } \alpha = 0 \\ 24\sigma(u), & \text{თუ } \alpha \geq 1 \end{cases}$;

სიტყვიერად: რიცხვის ოთხ კვადრატთა ჯამის სახით წარმოდგენათა რაოდენობა უდრის ყველა მის გამყოფთა 8-ჯერად ჯამს, თუ ეს რიცხვი კენტია და ყველა კენტი გამყოფების 24-ჯერად ჯამს, თუ ლუწია.

ამ ფორმულებიდან ჩანს, რომ რიცხვთა აღნიშნული ფორმებით წარმოდგენათა რაოდენობა დამოკიდებულია ამ რიცხვის მულტიპლიკაციურ სტრუქტურაზე, რაც მიუთითებს იმ კავშირზე, რომელიც არსებობს რიცხვთა ადიციურ და მულტიპლიკაციურ თვისებათა შორის.

გამოყენებული ლიტერატურა

1. კოლონია პ. ლურსმანაშვილი ა., რიცხვთა თეორიის კურსი, 1967.
2. შავგულიძე ქ., რიცხვთა თეორია და კრიპტოლოგია, თბილისი, 2018.
3. Диксон Л.Е., Введение в теорию чисел, Изд. Акад. наук Груз., 1941г.
4. Доценко В., Арифметика квадратичних форм, Москва, Издательство МЦНМО, 2007.
5. Kaplan J., Binary Quadratic Forms, Genus Theory, and Primes of the Form $p = x^2 + ny^2$, 2014.
6. Koninck J., Mercier A., 1001 Problems in Classical Number Theory, AMS, 2007;
7. Rosen K., Elementary Number Theory and its Applications, Addison-Wesley Publishing company, 1988.