

ივ. ჯავახიშვილის სახელობის
თბილისის სახელმწიფო უნივერსიტეტი

გიორგი ჯულაყიძე

რიცხვთა წარმოდგენა კვადრატურულ ფორმებით

The Presentation Of Numbers With Quadratic Forms

მათემატიკა

ნაშრომი შესრულებულია მათემატიკის მაგისტრის აკადემიური
ხარისხის მოსაპოვებლად

სამეცნიერო ხელმძღვანელი: ქეთევან შავგულიძე

ფიზიკა-მათემატიკის მეცნიერებათა დოქტორი

ასოცირებული პროფესორი

თბილისი 2013

ანოტაცია

ვთქვათ $r(n, f)$ აღნიშნავს n ნატურალური რიცხვის წარმოდგენათა რაოდენობას f მთელკოეფიციენტებიანი დადებითი კვადრატული ფორმით. იმისათვის, რომ ვიპოვოთ ზუსტი ფორმულა $r(n, f)$ ფუნქციისათვის, საჭიროა ცხადი სახით ავაგოთ გარკვეული ტიპის სფერულ ფუნქციები და ამ სფერული ფუნქციების შესაბამის თეტამწკრივთა სივრცის ბაზისი. პარაბოლური ფორმებისა და აიზენშტაინის მწკრივების შესახებ ჰეკეს შედეგების გათვალისწინებით შესაძლებელია მივიღოთ ფორმულები n ნატურალური რიცხვის f კვადრატული ფორმით წარმოდგენათა რაოდენობისათვის.

ნაშრომში განხილულია ზოგიერთ f კვადრატურული ფორმით რიცხვის წარმოდგენა, წარმოდგენათა აუცილებელი და საკმარისი პირობები და ბოლოს გამოყვანილია $q = [1, 0, 1]$ კვადრატურული ფორმით რიცხვის წარმოდგენათა რაოდენობის დასათვლელი ფორმულა.

შინაასი

1. რიცხვთა კვადრატურული ფორმები 3
2. რიცხვის კვადრატურული ფორმით წარმოდგენათა შესახებ 7
3. რიცხვის $q=[1,0,1]$ კვადრატურული ფორმით 14
წარმოდგენათა რაოდენობის შესახებ

§ 1

რიცხვთა კვადრატურული ფორმები

n ცვლადის კვადრატურული ფორმა ეწოდება ფუნქციას

$$f = f(x_1, x_2, x_3, \dots, x_n) = \sum_{i, k=1}^n a_{ik} x_i x_k$$

სადაც a_{ik} - ფორმის კოეფიციენტები მოცემული რიცხვებია, $x_1, x_2, x_3, \dots, x_n$ დამოუკიდებელი ცვლადებია. ასეთ ფორმებს ურთიერთცალსახად ეთანადება სიმეტრიული მატრიცი

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

კვადრატულ ფორმათა არითმეტიკულ თეორიაში $x_1, x_2, x_3, \dots, x_n$ დამოუკიდებელ ცვლადთა ცვლილებების არეს, თითქმის ყოველთვის წარმოადგენს მთელ რიცხვთა რგოლი ან მისი ესა თუ ის ქვესიმრავლე; a_{ik} კოეფიციენტები კი, საზოგადოდ, დამდვილი რიცხვებია, კერძოდ მთელი რაციონალური რიცხვები. უკანასკნელ შემთხვევაში ფორმას მთელკოეფიციენტებიანი ეწოდება.

მოცემულ m რიცხვს ეწოდება წარმოდგენადი

$$f(x_1, x_2, x_3, \dots, x_n)$$

ფორმით, თუ არსებობს $x_1, x_2, x_3, \dots, x_n$ ცვლადთა მთელი მნიშვნელობის ერთი მაინც სისტემა $(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n)$ რომლისთვისაც ადგილი აქვს ტოლობას

$$f(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) = m$$

მთელ რიცხვთა ყოველ ასეთ სისტემას ეწოდება m რიცხვის წარმოდგენა f ფორმით. წარმოდგენას ეწოდება საკუთრივი თუ ის ერთადერთია.

ამ წინასწარი ზოგადი განმარტების შემდეგ განვიხილოთ ორცვლადიანი, ბინარული ($n=2$) კვადრატული ფორმები, ე.ი. შემდეგი სახის ფორმები

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

ვინადან ყოველი ასეთი ფორმა ცალსახად განისაზღვრება მისი a, b, c დალაგებული კოეფიციენტებით, შეგვიძლია ვიხმართ აღნიშვნა

$$q = [a, b, c] \quad (1.2)$$

სადაც, როგორც უკვე ვთქვით ეს კოეფიციენტები მთელი რიცხვებია. წინამდებარე ნაშრომში შევისწავლით (1.1) ფორმას.

რიცხვს

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

ეწოდება q ფორმის დისკრიმინანტი. კვადრატული ფორმის სიმეტრიული მატრიცაა

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

ხოლო,

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

განვიხილოთ ნებისმიერი წრფივი ჩასმა

$$x = \alpha X + \beta Y \quad y = \gamma X + \delta Y \quad (1.3)$$

რომლის მატრიცა არის

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

ხოლო დეტერმინანტი

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

(1.3) ჩასმის შებრუნებული ჩასმაა

$$X = \frac{\delta}{\Delta}x - \frac{\beta}{\Delta}y \quad Y = -\frac{\gamma}{\Delta}x + \frac{\alpha}{\Delta}y$$

ხოლო ამ უკანასკნელის მატრიცი და დეტერმინანტია

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

წრფივ ჩასმას ეწოდება მთელრიცხოვანი, თუ მისი ელემენტები მთელი რიცხვებია. მთელრიცხოვან ჩასმას ეწოდება უნიმოდულარული თუ მისი დეტერმინანტი უდრის ± 1 ანუ $\alpha, \beta, \gamma, \delta$ მთელი რიცხვებია და $\Delta_{\tau} = \pm 1$

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

თუ მოცემულ (1.1) კვადრატულ ფორმაში შევიტანთ (1.3) წრფივ ჩასმას, მივიღებთ ახალ კვადრატულ ფორმას ახალი ცვლადების მიმართ

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

სადაც

$$\begin{aligned} A &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ B &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ C &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

ამ შემთხვევაში ამოიღებენ q ფორმა (3) ჩასმას გადაყავს Q ფორმაში. კავშირი მათ დეტერმინანტებს შორის არის შემდეგი

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

ამ ფორმათა ეკვივალენტობას ასე ჩავწერთ $q \sim Q$ საწინააღმდეგო ფაქტს კი $q \neq Q$. ამ ყველაფრიდან გამომდინარე ცხადია რომ თუ რომელიმე m რიცხვი წარმოდგენადია რაიმე კვადრატული ფორმით, მაშინ ის წარმოდგენადი იქნება მისი ეკვივალენტური კვადრატურული ფორმითაც და ეკვივალენტური ფორმებით წარმოდგენათა რიცხვები ტოლია.

§ 2

რიცხვის კვადრატული ფორმით წარმოდგენათა შესახებ

წინასწარ შევნიშნოთ, რომ მთელი რიცხვის ამა თუ იმ მთელ კოეფიციენტებიანი ფორმით წარმოდგენადობა და წარმოდგენათა რიცხვი მჭიდრო კავშირში იმყოფება რიცხვის მულტიპლიკაციურ სტრუქტურასთან, რაც რიცხვთა ადიციურ და მულტიპლიკაციურ თვისებათა შორის კავშირის ერთ-ერთი გამოვლენაა. ეს ფაქტი, ნაწილობრივ, გამოჩნდება ქვემოთ გამხილულ მაგალითებში.

განვიხილოთ კვადრატული ფორმა $q = [1, 0, -1] = x^2 - y^2$

თეორემა 2.1 (ეილერის კრიტერიუმი)

ერთზე მეტი m კენტი რიცხვის ნატურალურ რიცხვთა კვადრატების სხვაობის სახით წარმოდგენათა რიცხვი მეტია ერთზე, თუ m შედგენილია, ხოლო უდრის ერთს, თუ m მარტივია.

დამტკიცება:

ვთქვათ $m=p$ მარტივი კენტია რიცხვია $p=x^2-y^2=(x-y)(x+y)$ საიდანაც გამოდის რომ $x-y=1$ და $x+y=p$ აქედან კი:

$$x = \frac{p+1}{2} \quad y = \frac{p-1}{2}$$
$$p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$$

ამგვარად კენტი მარტივი რიცხვი $[1, 0, -1]$ ფორმით წარმოდგენება ერთადერთი სახით. ახლა ვთქვათ $m=kp$ შედგენილი რიცხვია, სადაც k კენტია. $kp = x^2 - y^2 = (x-y)(x+y)$ საიდანაც გამოდის რომ $x-y=1$ და $x+y=kp$ ან $x-y=k$ და $x+y=p$ აქედან კი გვექნება:

$$x = \left(\frac{pk+1}{2}\right) \quad y = \left(\frac{pk-1}{2}\right)$$

და

$$x = \left(\frac{p+k}{2}\right) \quad y = \left(\frac{p-k}{2}\right)$$

$$m = kp = \left(\frac{kp+1}{2}\right)^2 - \left(\frac{pk-1}{2}\right)^2 = \left(\frac{k+p}{2}\right)^2 - \left(\frac{k-p}{2}\right)^2$$

ამგვარად მივიღეთ ერთზე მეტი წარმოდგენა.

თეორემა დამტკიცებულია

დამტკიცოთ შემდეგი იგივეობა:

$$(Ax^2+By^2)(Aa^2+Bb^2) = (Axa+Bby)^2+AB(ay-bx)^2 = (Axa-Bby)^2+AB(ay+bx)^2$$

(I)

$$\begin{aligned}(Ax^2+By^2)(Aa^2+Bb^2) &= (Axa)^2 + (Byb)^2 + AB(ya)^2 + AB(xb)^2 = \\ &= (Axa+Byb)^2 - 2ABxyab + AB(ya)^2 + AB(xb)^2 = (Axa+Byb)^2 + AB((ya)^2 - 2xyab + (xb)^2) = \\ &= (Axa+Byb)^2 + AB(ya - xb)^2\end{aligned}$$

როცა A და B უდრის ერთს, იგივეობა მიიღებს სახეს:

$$(x^2+y^2)(a^2+b^2) = (xa+by)^2 + (ay-bx)^2 = (xa-by)^2 + (ay+bx)^2$$

(II)

თეორემა 2.2 თუ m რიცხვი უშვებს ორ არსებითად განსხვავებულ წარმოდგენას $q=[1,0,1]$ ფორმით, მაშინ m შედგენილი რიცხვია.

დამტკიცება:

ვთქვათ $m=a^2+b^2$; $m=x^2+y^2$ სადაც $|a| \neq |x|$ და $|b| \neq |y|$ დავუშვათ საწინააღმდეგო, ვთქვათ $m=p$ მარტივი რიცხვია.

$$\begin{aligned}p &= a^2 + b^2, \quad b^2 = p - a^2, \quad 1 = \frac{p-a^2}{b^2}; \quad p = x^2 + y^2, \quad y^2 = p - x^2, \quad 1 = \frac{p-x^2}{y^2} \\ b^2(p-x^2) &= y^2(p-a^2) \\ p(b^2-y^2) &= (bx-ay)(bx+ay)\end{aligned}$$

აქედან კიდე გამოს რომ

$$p|(bx-ay) \text{ ან } p|(bx+ay) \quad (2.2.1)$$

(II) იგივეობის გათვალისწინებით გვექნება $p^2 = (xa \pm by)^2 + (ay \mp bx)^2$ ამ შემთხვევაში (2.2.1)-ის ძალით ვღებულობთ, რომ ადგილი აქვს ერთერთს შემდეგი ორი პირობიდან:

$$(xa \pm by)^2 = p^2 \text{ და } (ay \mp bx)^2 = 0 \quad \text{ან} \quad (ay \mp bx)^2 = p^2 \text{ და } (xa \pm by)^2 = 0$$

ვთქვათ ადგილი აქ მეორე შემთხვევას, (პირველის განხილვაც ანალოგიურად შეიძლება) მაშინ გვექნება:

$$ay \mp bx = \pm p \text{ და } xa = \pm by$$

და რადგან $(a,b)=(x,y)=1$ და $p=a^2+b^2=x^2+y^2$ გამოდის რომ $x/b, b/x, a/y, y/a$ საიდანაც გამოდის რომ $a=\pm x$ და $b=\pm y$ რაც ეწინააღმდეგება დაშვებას.

თეორემა დამტკიცებულია

ზემოთ დამტკიცებული თეორემიდან უშუალოდ გამომდინარეობს შემდეგი თეორემა

თეორემა 2.3 თუ p მარტივი რიცხვი წარმოიდგინება $q=[1,0,1]$ ფორმით, მაშინ ის ერთადერთია.

თეორემა 2.4 ნებისმიერი ორი რიცხვის კვადრატების ჯამს აქვს ერთ-ერთი სახე შემდეგთაგან: $4n, 4n+1, 4n+2$

დამტკიცება:

ვათქვათ x^2+y^2 დან 1) x ლუწია და y ლუწია 2) x კენტია და y ლუწი 3) x კენტია და y ლუწი;

$$1) (2k)^2 + (2t)^2 = 4k^2 + 4t^2 = 4(k^2 + t^2) = 4n$$

$$2) (2k+1)^2 + (2t)^2 = 4k^2 + 4k+1 + 4t^2 = 4(k^2 + t^2 + k) + 1 = 4n+1$$

$$3) (2k+1)^2 + (2t+1)^2 = 4k^2 + 4k+1 + 4t^2 + 4t+1 = 4(k^2 + t^2 + k + t) + 2 = 4n+2$$

თეორემა დამტკიცებულია

თეორემა 2.5 თუ m რიცხვი საკუთრივ წარმოიდგინება $q=[1,0,k]$ ფორმით, სადაც $k = 1, 2$

მაშინ მისი ნებისმიერი d გამყოფიც წარმოიდგინება იგივე ფორმით.

(ამ თეორემის შებრუნებული თეორემა უშუალოდ გამომდინარეობს (I) იგივეობიდან.)

დამტკიცება:

თეორემის დასამტკიცებლად საკმარისია დავამტკიცოთ თეორემა მარტივი p გამყოფისთვის.

ჯერ ვაჩვენოთ შემდეგი: $x^2 + ky^2$ სახის რიცხვის ყოველი მარტივი გამყოფი p წარმოადგენს $x^2 + k$ სახის რომელიმე რიცხვის გამყოფს. ე.ი

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

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

$$yz-pu=1, \quad (z,u)=1$$

$x^2 + ky^2$ გამოსახულების z^2 -ზე გამრავლება გვაძლევს

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

ამ ტოლობის მარცხენა მხარე და მარჯვენა მხარის ბოლო ორი შესაკრები იყოფა p -ზე, საიდანაც მივიღებთ რომ

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

ამის გამო ცხადია ვაჩვენოთ რომ $x^2 + k$ სახის ნებისმიერი რიცხვის ყოველი მარტივი p გამყოფი არის $u^2 + kv^2$ სახის. 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 უწყვეთ წილადად

$$\frac{x}{p} = [a_0; a_1, a_2, \dots, a_m] = \frac{p_m}{q_m}$$

როგორც ვიცით $q_0 < q_1 < q_2 < \dots < q_m = p$ ამიტომ არსებობს მეზობელ $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ მახლოვად წილადთა წყვილი, რომელთა მნიშვნელებისათვის ადგილი აქვს უტოლობას

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

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

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

თუ უკანასკნელ უტოლობას გავამრავლებთ $(pq_n)^2$ -ზე და მხედველობაში მივიღებთ $q_n^2 < p < q_{n+1}^2$ უტოლობას გვექნება

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

საიდანაც

$$(xq_n - pp_n)^2 + kq_n^2 < p + kq_n^2 \quad (2.5.1)$$

ვინაიდან $p/x^2 + k$, უკანასკნელი უტოლობის მარცხენა მხარე იყოფა p -ზე; მეორეს მხრივ, ვინაიდან $q_n^2 < p$, მარჯვენა მხარისთვის გვაქვს

$$p + kq_n^2 < p + kp = p(k+1) \quad (2.5.2)$$

ახლა განვიხილოთ ცალცალკე ა) $k=1$ და ბ) $k=2$ შემთხვევები;

ა) (2.5.2)-ის ძალით

$$p + kq_n^2 = p + q_n^2 < 2p \quad (2.5.2)_1$$

(2.5.1)-ის მარცხენა მხარე იყოფა p -ზე. ე.ი მას აქვს სახე $pt (t \geq 1)$; ამიტომ (2.5.2)₁-ის ძალით გვაქვს

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

საიდანაც ცხადია, რომ $t=1$, ე.ი

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

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

ბ) აქ გვაქვს ორი შემთხვევა:

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

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. თუ ადგილი აქვს მეორე ტოლობას, მაშინ გვაქვს

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

ვინაიდან ამ ტოლობის ორი (p და q_n^2) მთელი რიცხვია, ფრჩხილებში მოთავსებული გამოსახულებაც მთელია, ასე რომ, ამ შემთხვევაშიც p -ს აქვს $u^2 + kv^2$ სახე.

თეორემა

დამტკიცებულია.

თეორემა 2.5 $k=1$ შემთხვევისთვის შეგვიძლია ასე ჩამოვყალიბოთ:

თეორემა 2.6 თუ მარტივი რიცხვი არის ორი ურთიერთ მარტივი რიცხვების კვადრატების ჯამის გამყოფი, თვითონაც წარმოადგენს ასეთი კვადრატების ჯამს.

თეორემა 2.5-ის შებრუნებული თეორემა, როგორც უკვე აღვნიშნეთ მარტივად გამოდის (I) იგივეობიდან და ჩამოყალიბდება შემდეგნაირად

თეორემა 2.7 თუ რომელიმე რიცხვის ყოველი მამრავლი ორი კვადრატის ჯამია, მაშინ ეს რიცხვიც ორი კვადრატის ჯამია.

თეორემა 2.8 (ვილსონი) $n/(n-1)! + 1$ მაშინ და მხოლოდ მაშინ როცა $n=p$ მარტივი რიცხვია.

ამ თეორემიდან გამოდის შემდეგი თეორემა

თეორემა 2.9 თუ $p=4k+1$ მარტივი რიცხვია, მაშინ

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

აქედან გამომდინარე შეგვიძლია შეგვიძლია ჩავწეროთ კიდე ერთი თეორემა

თეორემა 2.10 ყოველი $p=4k+1$ სახის მარტივი რიცხვი არის რაიმე $N^2 + 1^2$ სახის კვადრატების ჯამის გამყოფი.

თეორემა 2.11 არც ერთი $p=4k+3$ სახის მარტივი რიცხვი არ იშლება ორი კვადრატის ჯამად

დამტკიცება:

დავუშვათ საწინააღმდეგო, ვთქვათ $p = x^2 + y^2$ საიდანაც, ზოგადობის შეუზღუდავად $x=2n+1$ და $y=2m$, (წინააღმდეგ შემთხვევაში p მარტივი არ იქნება) მივიღებთ:

$$\begin{aligned} p=4k+3 &= x^2+y^2=(2n+1)^2+(2m)^2 \\ 4k+3 &= (2n+1)^2+(2m)^2 \\ 4k+3 &= 4n^2+4n+1+4m^2 \\ 2(n^2+m^2+n-k) &= 1 \\ n^2+m^2+n-k &= 0.5 \end{aligned}$$

რაც გამორიცხულია. მიღებული წინააღმდეგობა ამტკიცებს თეორემის მართებულობას.

ზემოთ დამტკიცებული თეორემების საფუძველზე მივიღეთ შემდეგი, რომ რადგან რიცხვი შეიძლება ჩავწეროთ $4n$, $4n+1$, $4n+2$, $4n+3$ აქედან მარტივი შეიძლება იყოს მხოლოდ $4n+1$ და $4n+3$, მაგრამ ეს უკანასკნელი კიდე არ წარმოიდგინება ორი კვადრატის ჯამად ამიტომ თუ მარტივი რიცხვი ისლება ორი კვადრატის ჯამად ის უნდა იყოს $4n+1$ სახის. ვილსონის თეორემა ამბობს, რომ ყოველი $p=4k+1$ სახის მარტივი რიცხვი ყოფს რომელიღაც ორი კვადრატის ჯამს. თუ გავითვალისწინებთ თეორემა 2.6-ს გამოვა რომ ყველა ასეთი სახის მარტივი რიცხვი წარმოდგება ორი კვადრატის ჯამად. ყოველივე ეს შეიძლება ჩამოვაყალიბოთ შემდეგი თეორემის სახით:

თეორემა 2.12 $4k+1$ სახის მარტივი რიცხვი ერთადერთი სახით იშლება ორი (ურთიერთ მარტივი) კვადრატის ჯამად. არც ერთი $4k+3$ სახის მარტივი რიცხვი არ იშლება ორი კვადრატის ჯამად.

ახლა განვიხილოთ შედგენილი რიცხვის ორი კვადრატის ჯამად წარმოდგენის საკითხი.

თეორემა 2.13 აუცილებელი და საკმარისი პირობა იმისა, რომ m რიცხვი წარმოსდგებოდეს ორი კვადრატის ჯამად, იმაში მდგომარეობს, რომ მის კანონიკურ დაშლაში $4k+3$ სახის ყოველი მარტივი რიცხვი შედიოდეს ლუწ ხარისხში.

დამტკიცება:

ვთქვათ შესგენილი რიცხვი იშლება ორი კვადრატი ჯამად და თან შეიცავს $p=4k+3$ სახის მარტივ გამყოფს. ანუ $m = x^2 + y^2$ და $p|m$
 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.

$$x = x_1 d, \quad y = y_1 d \quad m = x^2 + y^2 = d^2(x_1^2 + y_1^2), \quad p^{2t}|m, \quad (x_1, y_1) = 1$$

p^{2t} არის p -ს უმაღლესი ხარისხი შემავალი m -ში; მართლაც წინააღმდეგ შემთხვევაში გვექნება: $p^s|m$ $s>2t$ საიდანაც $p^s|d^2(x_1^2 + y_1^2)$, $p^{s-2t}|x_1^2 + y_1^2 = m_1$, $p|x_1^2 + y_1^2$; p მარტივი რიცხვი, როგორც კვადრატების გამყოფი თვითონაც უნდა წარმოადგენდეს კვადრატების ჯამს, რაც შეუძლებელია თეორემა 2.11-ის საფუძველზე.
 ამგვარად, თუ m შედგენილი რიცხვი იშლება ორი კვადრატის ჯამად, მის კანონიკურ დაშლას უნდა ქონდეს სახე:

$$m = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \dots q_u^{\alpha_u} p_1^{2\beta_1} p_2^{2\beta_2} \dots p_v^{2\beta_v} \quad (2.13.1)$$

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

ახლა ვაჩვენოთ რომ (2.13.1) პირობა საკმარისიკაა იმისათვის, რომ m რიცხვი წარმოდგეს ორი კვადრატის ჯამად. მართლაც

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

სადაც

$$m_1 = 2^{\alpha} q_1^{\alpha_1} q_2^{\alpha_2} \dots q_u^{\alpha_u} \quad m_2 = p_1^{\beta_1} p_2^{\beta_2} \dots p_v^{\beta_v}$$

m_1 ის ყოველი თანამამრავლი როგორც ვიცით ორი კვადრატის ჯამია, მაშასადამე, m_1 _იც ორი კვადრატის ჯამია.

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

თუ ამ ტოლობას m_2^2 _ზე გავამრავლებთ გვექნება

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

თეორემა დამტკიცებულია

თეორემა 2.14 ნატურალური რიცხვი ერთადერთი სახით (შესაკრებთა რიგისა და მათ ნიშნის სიზუსტით) იშლება ორი კვადრატის ჯამად მაშინ და მხოლოდ მაშინ, როცა ის არის $4k+1$ სახის მარტივი რიცხვი.

ეს თეორემა ადვილად გამომდინარეობს წინა დამტკიცებული თეორემებიდან და პასუხს ცემს კითხვას როდის წარმოიდგინება რიცხვი ორი კვადრატის სახით ერთადერთი გზით. რაც შეეხება ერთზე მეტ წარმოდგენას და მათ რიცხვს ჩვენ შემდეგ თავში განვიხიავთ.

§ 3

რიცხვის კვადრატურული ფორმით წარმოდგენათა რაოდენობის შესახებ

ამ თავში უკვე შევხებით რიცხვის კვადრატურული ფორმით წარმოდგენათა რაოდენობას.

$N(q=m)$ აღვნიშნოთ m რიცხვის წარმოდგენათა რაოდენობა.

შევსწავლოთ ზემოთ განხილული $q=[1,0,1]$ შემთხვევა.

როგორც უკვე ვაჩვენეთ $N(m)=1$, მაშინ და მხოლოდ მაშინ, როცა m მარტივი რიცხვია $4k+1$ სახისა და თუ შეიცავს $4k+3$ სახის მარტივ რიცხვს, ის უნდა იყოს ლუწი რაოდენობის.

თეორემა 3.1 ვთქვათ $m = m_1 \cdot t^{2k}$ სადაც m_1 შეიცავს მხოლოდ $4k+1$ სახის მარტივ მამრავლებს და t არის $4k+3$ სახის მარტივი რიცხვი, მაშინ $N(m) = N(m_1)$

დამტკიცება:

რადგან t არ იშლება ორი კვადრატის ჯამად, t^{2k} -ს წარმოდგენას ექნება ერთადერთი სახე

$$t^{2k} = (t^k)^2 + 0^2$$

(ასეთ წარმოდგენას *ნულშემცველი* ვუწოდოთ) ამიტომ m რიცხვის ყოველი $x_i^2 + y_i^2$ წარმოდგენა მიიღებს სახეს $(t^k x_i)^2 + (t^k y_i)^2$ საიდანაც ჩანს რომ წარმოდგენათა რიცხვი არ შეიცვლება.

თეორემა დამტკიცებულია

შედეგი 3.1 თეორემა (3.1)-დან უშუალოდ გამომდინარეობს, რომ რამდენ $4k+3$ სახის ლუწ რაოდენობა მარტივ მამრავლსაც არ უნდა შეიცავდეს m რიცხვი, მისი წარმოდგენათა რიცხვი, $q=[1,0,1]$ ფორმით, არ შეიცვლება.

წარმოდგენათა რაოდენობაზე ასევე გავლენას ვერ იქონიებს რიცხვში ორიანების რაოდენობა.

ადგილი ექნება შემდეგ თეორემას.

თეორემა 3.2 თუ $m = m_1 \cdot 2^k$ სადაც m_1 შეიცავს მხოლოდ $4k+1$ სახის მარტივ მამრავლებს, მაშინ $N(m) = N(m_1)$

დამტკიცება:

ა) ვთქვათ $k = 2s$, მაშინ რადგან 2 იშლება მხოლოდ ერთადერთი სახით $1^2 + 1^2$, 2^{2s} დაიშლება $(2^s)^2 + 0^2$ (რაც მარტივად გამოდის (II) იგვეობიდან). ამიტომ (3.1) თეორემის დამტკიცებაში ჩატარებული მსჯელობის საფუძველზე დავასკვნით, რომ ამ შემთხვევაშიც $N(m) = N(m_1)$

ბ) თუ $k = 2s + 1$, მაშინ 2^k შეგვიძლია წარმოვიდგინოთ $2^k = 2^{2s} \cdot 2 = ((2^s)^2 + 0^2) \cdot (1^2 + 1^2)$ და ისევ (II) იგვეობის საფუძველზე ვნახავთ რომ იარსებებს ერთადერთი წარმოდგენა კერძოდ

$$2^k = (2^s)^2 + (2^s)^2$$

და თუ ისევ გამოვიყენებთ (II) იგვეობას გვექნება:

$$m = m_1 \cdot 2^k = (x_i 2^s + y_i 2^s)^2 + (x_i 2^s - y_i 2^s)^2 = (x_i 2^s - y_i 2^s)^2 + (x_i 2^s + y_i 2^s)^2$$

ამით ვაჩვენებთ, რომ არც ასე იცვლება წარმოდგენათა რიცხვი.

თეორემა დამტკიცებულია

განმარტება 3.1 ვთქვათ $m = x_i^2 + y_i^2$ წარმოდგენას ვუწოდოთ *საკუთრივი* თუ $(x_i ; y_i) = 1$

ახლა ვთქვათ $p^\alpha = 4k+1$ სახის მარტივი რიცხვია, რომელიც, როგორც თეორემა 2.12_დან ვიცით, ერთადერთი სახით იშლება ორი კვადრატის ჯამად, როცა $\alpha = 1$ და თან დაშლა იქნება საკუთრივი. ვთქვათ ეს წყვილი არის $\tau_1^1 = (x_1 ; y_1)$ (სადაც ზედა ინდექსი p -ს ხარისხს აღნიშნავდეს, ხოლო ქვედა ინდექსი წყვილის ნომერს. ასევე შემოვიტანოთ აღნიშვნა Δ^α - რომლითაც აღვნიშნოთ ასეთი ტაუების სიმრავლე)

განვიხილოთ $\alpha = 2$ შემთხვევა, ანუ ვნახოთ რას უდრის $N(p^2)$. (II) იგვეობიდან გვექნება

$$p^2 = (x_i^2 + y_i^2)^2 + 0^2 = (x_i^2 - y_i^2)^2 + (2x_i y_i)^2$$

და

$$\Delta^2 = \{\tau_1^2 ; \tau_2^2\}$$

მივიღებთ, რომ $N(p^2) = 2$ კერძოდ $\tau_1^2 = (p^2 ; 0)$ $\tau_2^2 = (x_i^2 - y_i^2 ; 2x_i y_i)$

$\alpha = 3$ შემთხვევაში $p^3 = p^2 \cdot p^1$ ამ სახით წარმოვიდგინოთ, წესით Δ^3 უნდა უდრიდეს $\Delta^2 \times \Delta^1 = \{(\tau_1^1 \cdot \tau_1^2); (\tau_1^1 \cdot \tau_2^2)\}$ და რადგან (II) იგივეობის გათვალისწინებით თითო წყვილი საზოგადოდ წარმოშობს ორ დაშლას, Δ^3 უნდა იყოს ასეთი სიმრავლე $\{\tau_1^3; \tau_2^3; \tau_3^3; \tau_4^3\}$ მაგრამ რადგან Δ^2 -ში τ_1^2 არის ნულშემცველი წარმოდგენა ის არ წარმოშობს ორ წყვილს არამედ ერთ $\tau_1^3 = \tau_2^3$ წყვილს. $\tau_1^1 \cdot \tau_2^2$ -ის შედეგად მიღებული წყვილებიდან ერთი τ_2^3 ასევე დაემთხვევა $\tau_1^3 = \tau_2^3$ წყვილს. (რაც მიიღება (II) იგივეობიდან) ამინ რეალურად

$$\Delta^3 = \{\tau_1^3; \tau_2^3\} \text{ ანუ } N(p^3) = 2$$

უნდა ყოფილიყო ოთხი წარმოდგენა მაგრამ „ჩაიყლაპა“ ორი და დარჩა ორი წარმოდგენა. იგივე მეთოდით თუ გავყვებით სქემას გვექნება ასეთი სურათი:

$$N(p^1) = 1$$

$$N(p^2) = N(p^1 \cdot p^1) = 2, \text{ „ჩაიყლაპა“ } 1$$

$$N(p^3) = N(p^2 \cdot p^1) = 2, \text{ „ჩაიყლაპა“ } 1$$

$$N(p^4) = N(p^3 \cdot p^1) = 3, \text{ „ჩაიყლაპა“ } 2$$

$$N(p^5) = N(p^4 \cdot p^1) = 3, \text{ „ჩაიყლაპა“ } 2$$

$$N(p^6) = N(p^5 \cdot p^1) = 4, \text{ „ჩაიყლაპა“ } 3$$

$$N(p^7) = N(p^6 \cdot p^1) = 4, \text{ „ჩაიყლაპა“ } 3$$

$$N(p^8) = N(p^7 \cdot p^1) = 5, \text{ „ჩაიყლაპა“ } 4$$

$$N(p^9) = N(p^8 \cdot p^1) = 5, \text{ „ჩაიყლაპა“ } 4$$

$$N(p^{10}) = N(p^9 \cdot p^1) = 6, \text{ „ჩაიყლაპა“ } 5$$

ზოგადი სახე კი იქნება შემდეგი:

$$N(p^{2\alpha}) = N(p^{2\alpha-1} \cdot p^1) = \alpha + 1, \text{ „ჩაიყლაპა“ } \alpha$$

$$N(p^{2\alpha+1}) = N(p^{2\alpha} \cdot p^1) = \alpha + 1, \text{ „ჩაიყლაპა“ } \alpha$$

აქედან გამომდინარე შესაძლებელია ჩამოვყალიბოთ შემდეგი თეორემა:

თეორემა 3.3 ვქვით მოცემულია $m = p^t$, სადაც $p = 4k+1$ სახის მარტივი რიცხვია.

ა) თუ t - ლუწია, მაშინ $N(m) = \frac{t}{2} + 1$;

ბ) თუ t - კენტია, მაშინ $N(m) = \frac{t+1}{2}$;

თეორემა 3.4 თუ $m_1 = x_1^2 + y_1^2$ და $m_2 = x_2^2 + y_2^2$ საკუთრივი წარმოდგენებია, მაშინ $m = m_1 m_2 = x^2 + y^2$ წარმოდგენაც იქნება საკუთრივი.

დამტკიცება:

დაუშვათ საწინააღმდეგო, ვთქვათ

$$m = m_1 m_2 = x^2 + y^2 = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - y_1 x_2)^2 = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + y_1 x_2)^2$$

არაა საკუთრივი წარმოდგენები და (საკმარისია განვიხილოთ მხოლოდ ერთი წარმოდგენა)

$$((x_1 x_2 + y_1 y_2), (x_1 y_2 - y_1 x_2)) = d$$

ანუ

$$d \mid x_1 x_2 + y_1 y_2 \text{ და } d \mid x_1 y_2 - y_1 x_2$$

საიდანაც მივიღებთ რომ

$$x_1 x_2 + y_1 y_2 = kd \text{ და } x_1 y_2 - y_1 x_2 = td$$

$$x_1^2 x_2^2 + y_1^2 y_2^2 + 2x_1 x_2 y_1 y_2 = k^2 d^2$$

$$x_1^2 y_2^2 + y_1^2 x_2^2 - 2x_1 x_2 y_1 y_2 = t^2 d^2$$

თუ უკანასკნელ ორ ტოლობას შევკრებთ და მამრავლებად დავშლით მივიღებთ:

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = d^2(k^2 + t^2)$$

საიდანაც გამოდის რომ d ყოფს m_1 -ს და m_2 -ს რაც ეწინააღმდეგება პირობას.

გამოდის რომ დაშვება არასწორია, სადანაც გამომდინარეობს თეორემის სამართლიანობა.

თეორემა დამტკიცებულია

თეორემა 3.5 თუ $m = p_1 p_2 \dots p_n$ სახის რიცხვია, სადაც ყოველი p_i განსხვავებულია ერთმანეთიგან და არის $4k+1$ სახის, მაშინ $q = [1, 0, 1]$ წარმოდგენისთვის

$$N(m) = 2^{n-1}$$

დამტკიცება:

თეორემის დამტკიცება ადვილად გამომდინარეობს თეორემა 2.12 და თეორემა 3.4 _დან.

$$m = p_1 p_2 \text{ დროს } N(m) = 2^1$$

$$m = p_1 p_2 p_3 \text{ დროს } N(m) = 2^2$$

$$m = p_1 p_2 p_3 p_4 \text{ დროს } N(m) = 2^3$$

სადაც კარგად ჩანს, რომ ორის ხარისხი ერთით ნაკლებია მამრავლების რაოდენობაზე.
თეორემა დამტკიცებულია

მივადექით ყველაზე მთავარს, რას უდრის $N(m)$ მაშინ როცა

$$m = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \dots q_u^{\alpha_u} p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} t_1^{2\gamma_1} t_2^{2\gamma_2} \dots t_v^{2\beta_v}$$

სადაც ყოველი q_i და p_i არის $4k+1$ სახის და t_j არის $4k+3$ სახის. ყოველი α_i კენტია, ხოლო β_i ლუწია.

ასევე შემოვიტანოთ აღნიშვნები:

$$m_0 = 2^\alpha t_1^{2\gamma_1} t_2^{2\gamma_2} \dots t_v^{2\beta_v}$$

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

$$m_2 = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

განვიხილოთ $N(m_1)$ შემთხვევა.

რადგან ყოველი q_i ერთმანეთისგან განსხვავებული მარტივი რიცხვია, ყველა $q_i^{\alpha_i}$ იქნება ურთიერთ მარტივი ერთმანეთთან. ამიტომ $q_1^{\alpha_1} q_2^{\alpha_2} \dots$ -ის ორი კვადრატის ჯამად წარმოდგენათა რაოდენობა იქნება

$$2 \cdot \frac{(\alpha_1 + 1)}{2} \cdot \frac{(\alpha_2 + 1)}{2} = \frac{(\alpha_1 + 1)(\alpha_2 + 1)}{2}$$

თეორემა 3.3-ის ბ) პუნქტიდან გამომდინარე. $q_1^{\alpha_1} q_2^{\alpha_2} q_3^{\alpha_3}$ -ის ორი კვადრატის ჯამად წარმოდგენათა რაოდენობა კი

$$2 \cdot \frac{(\alpha_1 + 1)(\alpha_2 + 1)}{2} \cdot \frac{(\alpha_3 + 1)}{2} = \frac{(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1)}{2}$$

აქედან გამომდინარე საბოლოოდ $N(m_1)$ დაითვლება:

$$N(m_1) = \frac{1}{2} \prod_{i=1}^u (\alpha_i + 1)$$

ახლა განვიხილოთ $N(m_2)$ შემთხვევა.

აქ რადგან m_2 -ში შემავალი ყველა მამრავლი ლუწი რაოდენობისაა, გვექნება ნულშემცველი წარმოდგენები, (რომელიც სხვა წარმოდგენასთან დაწყვილებისას წარმოშობს მხოლოდ ერთ წარმოდგენას) ამიტომ $p_1^{\beta_1} p_2^{\beta_2}$ -ის ორი კვადრატის ჯამად წარმოდგენათა რაოდენობა იქნება

$$2 \cdot \frac{\beta_1}{2} \cdot \frac{\beta_2}{2} + \frac{\beta_1}{2} + \frac{\beta_2}{2} + 1 = \frac{1}{2}(\beta_1 \beta_2 + \beta_1 + \beta_2) + 1$$

თეორემა 3.3-ის ა) პუნქტიდან გამომდინარე. $p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3}$ -ის ორი კვადრატის ჯამად წარმოდგენათა რაოდენობა

$$\begin{aligned} & 2 \cdot \frac{1}{2}(\beta_1 \beta_2 + \beta_1 + \beta_2) \cdot \frac{\beta_3}{2} + \frac{1}{2}(\beta_1 \beta_2 + \beta_1 + \beta_2) + \frac{\beta_3}{2} + 1 \\ &= \frac{1}{2}(\beta_1 \beta_2 \beta_3 + \beta_1 \beta_2 + \beta_1 \beta_3 + \beta_2 \beta_3 + \beta_1 + \beta_2 + \beta_3) + 1 \end{aligned}$$

ამ სქემაზე გაყოლა $p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} p_4^{\beta_4}$ -ისთვის იქნება

$$\begin{aligned} & \frac{1}{2}(\beta_1 \beta_2 \beta_3 \beta_4 + \beta_1 \beta_2 \beta_3 + \beta_1 \beta_3 \beta_4 + \beta_2 \beta_3 \beta_4 + \beta_1 \beta_2 \beta_4 + \beta_1 \beta_2 + \beta_1 \beta_3 + \beta_2 \beta_3 + \beta_1 \beta_4 + \beta_2 \beta_4 \\ &+ \beta_3 \beta_4 + \beta_1 + \beta_2 + \beta_3 + \beta_4) + 1 \end{aligned}$$

თუ შემოვიტანთ აღნიშვნას $\beta = \beta_1 \beta_2 \cdots \beta_n$, მივიღეთ, რომ საბოლოოდ $N(m_2)$ დაითვლება:

$$N(m_2) = \frac{1}{2} \sum_{d|\beta} d + 1$$

სადაც d გაირბენს β -ს ყველა გამყოფს.

თუ გავითვალისწინებთ თეორემა 3.2 და შედეგი 3.1-ს გამოვა, რომ

$$N(m_1 m_2) = N(m_0 m_1 m_2)$$

საბოლოო ფორმულა შეიძლება გამოვსახოთ შემდეგ თეორემაში

თეორემა 3.6 მოცემული $m = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \dots q_u^{\alpha_u} p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} t_1^{2\gamma_1} t_2^{2\gamma_2} \dots t_v^{2\beta_v}$ რიცხვისთვის, (სადაც ყოველი q_i და p_i არის $4k+1$ სახის და t_j არის $4k+3$ სახის. ყოველი α_i კენტი, ხოლო β_i ლუწია.)

$$N(m) = 2 \cdot N(m_1) \cdot N(m_2) - N(m_1)$$

სადაც

$$N(m_1) = \frac{1}{2} \prod_{i=1}^u (\alpha_i + 1)$$

და

$$N(m_2) = \frac{1}{2} \sum_{d|\beta} d + 1$$

შესავალში ჩვენ აღვნიშნეთ, რომ თუ რომელიმე m რიცხვი წარმოდგენადია რაიმე კვადრატული ფორმით, მაშინ ის წარმოდგენადი იქნება მისი ექვივალენტური კვადრატურული ფორმითაც და ექვივალენტური ფორმებით წარმოდგენათა რიცხვები ტოლია. ანუ $N_q(m) = N_Q(m)$ სადაც $q \sim Q$

განვიხილოთ $Q = [2, 2, 1]$ ანუ $2X^2 + 2XY + Y^2$

$$2X^2 + 2XY + Y^2 = X^2 + X^2 + 2XY + Y^2 = X^2 + (X + Y)^2$$

თუ შემოვიღებთ აღნიშვნას $X = x$ და $X + Y = y$ Q გადავა q -ში რადგან ის შესაძლებელია წარმოვიდგინოთ ორი კვადრატის ჯამის სახითაც, გამოდის რომ $q \sim Q$ და m რიცხვის Q ფორმით წარმოდგენათა რიცხვიც შესაძლებელია დაითვალოს ზემოთ მიღებული ფორმულით.

განვიხილოთ $Q = [2, 6, 5]$ ანუ $2X^2 + 6XY + 5Y^2$

$$2X^2 + 6XY + 5Y^2 = X^2 + 2XY + Y^2 + X^2 + 4XY + 4Y^2 = (X + Y)^2 + (X + 2Y)^2$$

თუ შემოვიღებთ აღნიშვნას $X + Y = x$ და $X + 2Y = y$ Q გადავა q -ში რადგან ისიც შესაძლებელია წარმოვიდგინოთ ორი კვადრატის ჯამის სახითაც, გამოდის რომ m რიცხვის Q ფორმით წარმოდგენათა რიცხვიც შესაძლებელია დაითვალოს ზემოთ მიღებული ფორმულით.

შევნიშნოთ რომ ორივე შემთხვევაში Q და q ფორმათა დისკრიმინანტები ტოლია.

გამოყენებული ლიტერატურა

- [1]. პ. კოლონია, ა. ლურსმანაშვილი - „რიცხვთა თეორიის კურსი“ 1967წ.
- [2]. Л.Е Диксон - „Введение в теорию чисел“ 1941 г.
- [3]. ა. ბენდუქიძე - „მათემატიკა სერიოზული და სახალისო“ 1988წ.
- [4]. ინტერნეტი:
<https://en.wikipedia.org>
https://en.wikipedia.org/wiki/Number_theory
- [5]. <https://www.google.com/>