

O`zbekstan Respublikasi Xalq bilimlendiriw ministrliqi
A`jiniyaz atundag`ı No`kis ma`mlekettik pedagogikalıq instituti

Fizika-matematika fakul`teti

Ulwma matematika kafedrası

3-kurs Matematika oqıtw metodikası ta`lim bag`darı talabasının`

Algebra ha`m sanlar teoriyası pa`ninen

Kurs jumısı

Tema: Ferma teoremasının` dara jag`dayları

Orınladı:

Toreeva Eleonora

No`kis-2014

MAZMUNI:

Kirisiw.	3
§ 1. Ferma teoreması haqqında.	4
§ 2. $n = 4$ ko`rsetkishi ushın Ferma teoreması.	8
§ 3. $n = 3$ ko`rsetkishi ushın Ferma teoreması.	11
Juwmaqlaw.	23
A`debiyatlar.	24

Kirisiw

17-a`sirde jasag`an belgili matematik P`er Ferma (1601-1665)

$$x^n + y^n = z^n$$

ten`lemesi  $n \geq 3$  bolg`anda nol`den o`zgeshe pu`tin sanlarda sheshimge iye emes ekenligin aytıp ketken. Bul aytım Ferma teoreması degen at penen du`n`ya ju`zine ma`lim. Fermanın` o`zi bul teoremanı  $n = 4$  ko`rsetkishi ushın tolıq da`lillegen, biraq basqa jag`daylar ushın da`lillewin keltirmegen. Bul teoremanı 1768-jılı Eyler  $n = 3$  ko`rsetkishi ushın da`lillegen. Keyin, 1825-jılı Lejandr, al 1839-jılı Lame bul teoremanı sa`ykes $n = 5$ ha`m  $n = 7$  ko`rsetkishleri ushın da`lillegen [1].

Biz bul kurs jumısımızda Ferma teoremasının`  $n = 3$  ha`m $n = 4$ jag`dayları ushın da`lillewlerin keltiremiz. § 1 de bul teorema haqqında mag`lıwmatlar, § 2 de teoremanın` $n = 4$ ha`m § 3 de  $n = 3$  ko`rsetkishleri ushın da`lillewleri keltiriledi [1].

Bunda $n = 4$ ushın teorema elementar usıl menen da`lillenedi ha`m qısqa da`lillenedi.

$n = 3$ ushın teoremanın` da`lilleniwi elementar emes, yag`nıy bul jag`dayda teorema elementar usıllar menen da`lillenbeydi.

§ 1. Ferma teoreması haqqında

Ferma teoreması:

$$x^n + y^n = z^n, \quad x, y, z \in \mathbb{Z}, \quad (1)$$

ten`lemesi  $n \geq 3$  bolg`anda nol`den o`zgeshe sheshimge iye emes.

Bul teoremanın` toliq da`lilleniwi ha`zirge shekem baspada ja`riyalanbadı. Ha`r qıylı dara jag`daylardı 17-a`sirden baslap ha`zirge shekem da`lillenip kelmekte [1].

1851-jılı Kummer bul teoremanı $n < 100$, $n \neq 37, 59, 67$ ko`rsetkishleri ushın da`lilledi. 1858-jılı ol bul teoremanı $n = 37, 59, 67$ ko`rsetkishleri ushın da da`lilledi, biraq bul ju`da` quramalı (qıyın) da`lillew boldı. 1893-jılı Mirimanov  $n = 37$  ko`rsetkishi ushın an`sat da`lillew keltirdi.

1850-jılı Frantsuz ilimler akademiyası Ferma teoriyasın da`lillegen adamg`a 3500 frank sıylıq ajıratdı ha`m onı 1857-jılı Kummerge tapsırdı. Biraq teorema aqırına shekem da`lillenbey qaldı. Bunnan keyin ko`p waqıyalarg`a shekem bul tarawda ko`zge ko`rinetug`ınday na`tiyjeler alınbadı [1].

Da`slep (1) ten`leme to`mendegi eki jag`day ushın o`z-aldına qaraldı:

- 1) x, y, z lerdin` hesh qaysısı da  $n$  ge bo`linbeydi.
- 2) x, y, z lerdin` hesh bolmasa birewi  $n$  ge bo`linedi.

1823-jılı Sofi Jerman Ferma teoremasın 1) jag`day ushın  $n < 197$  ko`rsetkishleri ushın da`lilledi. 1858-jılı Kummer teoremanı  $B_{\ell-3}$  ha`m $B_{\ell-5}$ Bernulli sanlarının` alımları bo`linbeytug`ını  $\ell$  a`piwayı ko`rsetkishleri ushın da`lilledi. 1893-jıl Vendt qa`legen  $m \geq 1$  ushın  $D_m$  pu`tin sanın anıqladı ha`m to`mendegi teoremanı da`lilledi:

Teorema. Eger $\ell \geq 3$ a`piwayı sanı ushın  $m \geq 1$  sanı bar bolıp, to`mendegi sha`rtler orınlasa

- 1) $p = 2m\ell + 1$ sanı D_m sanın bo`lmeytug`ın a`piwayı san boladı.

2) $\ell^{2m} - 1$ sanı p g'a bo'linbeydi,

onda

$$x^\ell + y^\ell = z^\ell$$

ten'lemesi nol'den o'zgeshe pu'tin sheshimlarga iye emes.

1905-jılı Mirimanov Ferma teoremasının 1) jag'dayın $B_{\ell-3}$, $B_{\ell-5}$, $B_{\ell-7}$ ha'm $B_{\ell-9}$ Bernulli sanlarının hesh bolmag'anda birewinin alımın bo'lmeytug'in ℓ a'piwayı ko'rsetkishi ushın da'lilledi. Bunnan 1) jag'dayda Ferma teoreması barlıq $\ell < 257$ a'piwayı ko'rsetkishleri ushın orınlanatug'ınlıg'ı kelip shıg'adı. 1909-jılı Viferix Mirimanovtın usılın paydalanıp to'mendegi teoremanı da'lilledi.

Teorema. 1) jag'dayda Ferma teoreması $2^{\ell-1} - 1$ sanı ℓ^2 qa bo'linbeytug'in barlıq $\ell \geq 3$ a'piwayı sanları ushın orınlı.

Bul teorema ju'da u'lken a'hmiyetke iye, sebebi onnan 1093 ha'm 3511 den basqa barlıq ≤ 200183 a'piwayı sanları ushın Ferma teoremasının orınlanatug'ınlıg'ı kelip shıg'adı. Viferixtın bul teoremanı da'lillewin keyin Mirimanov ha'm Frobenius a'piwayılastırdı ha'm teoremadag'ı 2 tiykarının ornına 3 tiykarın qoyıwg'a boltug'ınlıg'ın ko'rsetti. Demek 1) jag'dayda Ferma teoreması $2^{\ell-1} - 1$ ha'm $3^{\ell-1} - 1$ sanlarının hesh bolmasa birewi ℓ^2 qa bo'linbeytug'ınday barlıq a'piwayı $\ell \geq 3$ sanlar ushın orınlı eken.

1912-jılı Furtvengler Eyzenshteynnin o'z-aralıq nızamın qollanıp Viferix ha'm Mirimanov-Frobenius kriteriylerin ju'da qısqa jol menen da'lilledi. Bul teoremanı rawajlandırıp ha'm klasslar maydanlarının teoriyasın qollanıp, matematikler 1941-jılı Viferix kriteriyindegi 2 tiykarın qa'legen $p \leq 43$ a'piwayı sanı menen almastırıwg'a bolatug'ınlıg'ın da'lilledi. Bul usıl menen Ferma

teoreması 1) jag`dayda qa`legen $\ell < 6 \cdot 10^9$ ko`rsetkishleri ushın orınlı ekenligi ko`rsetildi.

1934-jılı Vandimer Ferma teoremasının` 1) jag`dayı ekinshi ko`beytiwshi  $h_2$  sanı  $\ell$  ge bo`linbeytug`ınday  $\ell$  a`piwayı ko`rsetkishleri ushın orınlı ekenligin ko`rsetti.

Ha`zirge shekem Ferma teoreması barlıq  $n < 100\ 000$  ko`rsetkishleri ushın da`lillengen [1].

Bunda da`slep bul teoremanın` ha`r qıylı ko`rsetikshleri ushın qandayda bir sha`rtler orınlanadı ha`m usı sha`rtler orınlang`an ko`rsetkishler ushın Ferma teoreması da`lillenedi. Keyin bunday sha`rtler basqa da ko`rsetkishler ushın tabıladı ha`m olardı qanaatlandırıatug`ın ko`rsetkishler ushın Ferma teoreması orınlanadı. Sonnan keyin, esaplaw mashinaları ja`rdeminde ko`rsetilgen sha`rtler tekserilip barıladı. Juwmag`ında teorema ha`zir barlıq $n < 100\ 000$ ushın da`lillenip bolındı.

§ 2. $n = 4$ ko`rsetkishi ushın Ferma teoreması

Ferma teoreması $n = 4$ ko`rsetkishi ushın elementar da`lillenedi. Biz bul paragrafta usınday da`lillewdi keltiremiz. Basqa jag`daylar ushın bul teoremanın elementar da`lilleniwi ha`zirshe joq (ha`m bolıwı da mu`mkin emes dep esaplaydı bir qansha belgili matematikler) [1].

Biz to`mendegi ten`lemenı qaraymız

$$x^2 + y^2 = z^2 \quad (1)$$

Lemma. Meyli $m > n > 0$, $(m, n) = 1$ ha`m  $m$  menen  $n$  sanlarının birewi taq san ha`m birewi jup san bolsın. Sonda

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2 \quad (2)$$

sanları (1) ten`lemenin` sheshimi boladı.

Kerisinshe, (1) ten`lemenin` x jup san bolg`an on` primitiv sheshimleri joqarıdag`ı qa`siyetke iye bolg`an (x, y, z) sanları boladı.

Da`lillew.

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

ten`liginen (2) degi sanlar (1) din` sheshimi bolatug`ınlıg`ı kelip shıg`adı, bul jerde  $x$  -jup san. Eger bul sanlar  $\lambda \geq 2$  ulıwma bo`liwshige iye bolsa, onda λ sanı

$$2m^2 = (m^2 + n^2) + (m^2 - n^2),$$

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

sanların da bo`liwi kerek. Demek  $\lambda = 2$ , sebebi  $(m, n) = 1$ . Biraq, eger  $\lambda = 2$  bolsa  $y = m^2 - n^2$  sanı jup san, demek  $m^2$  ha`m n^2 sanları ekewi de birden taq yamasa jup sanlar. Bul mu`mkin emes, sebebi  $m$  ha`m n sanlarının` birewi taq ha`m birewi jup sanlar. Demek (2) primitiv (qısqarmaytug`ın) sheshim boladı.

Kerisinshe, meyli (x, y, z) on` primitiv sheshim bolsın, bul jerde  $x = 2a$  jup san.  $y$  ha`m z taq sanlar bolg`anı ushın,  $z + y$  ha`m $z - y$ sanları jup sanlar boladı.

Meyli

$$z + y = 2b, \quad z - y = 2c$$

bolsın, bunda b ha`m  $c$  on` sanlar. b ha`m  $c$  sanlarının` qa`legen ulıwma bo`liwshisi λ sanı $z = b + c$ ha`m  $y = b - c$  sanların bo`ledi.

Sonlıqtan $\lambda = \pm 1$ boladı, demek $(b, c) = 1$. Ekinshi jaqtan

$$4a^2 = x^2 = z^2 - y^2 = 4bc,$$

yag`nıy  $a^2 = bc$ . Demek  $(m, n) = 1$  ha`m birewi taq, birewi jup m ha`m n sanları bar bolıp

$$b = m^2, \quad c = n^2$$

boladı. Onda $a^2 = m^2 n^2$ yag`nıy  $a = mn$  ha`m

$$x = 2a = 2mn, \quad y = b - c = m^2 - n^2,$$

$$z = b + c = m^2 + n^2 \text{ ha`m } n < m.$$

Lemma da`lillendi. Endi biz Ferma teoremasın  $n = 4$  ko`rsetkishi ushın da`lilleymiz. Biz bul jag`day ushın ku`shlirek teoremanı da`lilleymiz:

Teorema.

$$x^4 + y^4 = z^2 \tag{3}$$

ten`lemesi nol`den o`zgeshe pu`tin sanlarda sheshimge iye emes.

**Da`lillew.** Meyli bunday sheshim bar dep oylayıq. Bunda  $x, y$  ha`m z sanların o`z-ara a`piwayı sanlar dep qarawg`a boladı. Natural sanlardın` qa`legen ko`pliginde en` kishi san bar bolg`anı ushın (3) ten`lemenin` sheshimlerinin` ishinde en` kishi z ke iye bolg`an (x, y, z) sheshimi bar boladı. Bul sheshimdi

dıqqat penen u`yreneyik. Bunda  $x$  ha`m y sanlarının` birewi jup san bolıwı kerek. Meyli x jup san bolsın.

$$(x^2)^2 + (y^2)^2 = z^2$$

bolg`anlıg`ı ha`m  $x^2, y^2, z$  sanları o`z-ara a`piwayı on` sanlar bolg`anlıg`ı ha`m  $x^2$  jup san bolg`anlıg`ı ushın joqarıdag`ı lemmadan $(m, n) = 1, n < m$ sonday-aq birewi taq, birewi jup m ha`m  $n$  sanları bar bolıp, to`mendegi ten`likler orınlanadı.

$$x^2 = 2mn$$

$$y^2 = m^2 - n^2$$

$$z = m^2 + n^2$$

Eger $m = 2k$ ha`m $n = 2\ell + 1$ bolsa

$$y^2 = 4(k^2 - \ell^2 - \ell - 1) + 3$$

kelip shıg`adı, biraq bul mu`mkın emes, sebebi taq sannın` kvadratı  $4k + 1$  tu`rinde boladı. Demek m taq, al n jup san boladı.

Meyli $n = 2q$ bolsın. Sonda $x^2 = 4mq$ ha`m sonlıqtan

$$mq = \left(\frac{x}{2}\right)^2$$

boladı. Bunnan, m ha`m  $q$  sanları o`z-ara a`piwayı bolg`anlıg`ı ushın

$$m = z_1^2, \quad q = t^2$$

ekenligi kelip shıg`adı, bunda  $z_1, t \in N$  ha`m $(z_1, t) = 1$.

Dara jag`dayda

$$y^2 = (z_1^2)^2 - (2t^2)^2$$

boladı, yag`nıy

$$(2t^2)^2 + y^2 = (z_1^2)^2.$$

t ha'm z_1 o'z-ara a'piwayı sanlar bolg'anı ushın, bul ten'likke ja'ne de joqarıda da'llengen lemmanı qollanıw mu'mkin. Demek, $0 < b < a$, $(a,b) = 1$ ha'm birewi taq, birewi jup a ha'm b sanları bar bolıp

$$2t^2 = 2ab \text{ yag'niy } t^2 = ab$$

$$y^2 = a^2 - b^2$$

$$z_1^2 = a^2 + b^2$$

ten'likleri orınlanadı. $(a,b) = 1$ bolg'anı ushın birinshi ten'likten

$$a = x_1^2, \quad b = y_1^2$$

bolatug'ınday x_1 ha'm y_1 pu'tin sanlarının bar bolatug'ınlıg'ı kelip shıg'adı.

Sonlıqtan u'shinshi ten'likni to'mendegishe jazıw mu'mkin

$$x_1^4 + y_1^4 = z_1^2$$

Bunnan (x_1, y_1, z_1) (3) ten'liginin on sanlardan turatug'ın primitiv sheshimi bolatug'ınlıg'ı kelip shıg'adı. Demek (x, y, z) sheshiminin saylap alınıwına baylanışlı

$$z_1 \geq z,$$

ha'm sonlıqtan

$$z_1^2 \geq z$$

bolıwı kerek, yag'niy

$$m \geq m^2 + n^2$$

bolıwı kerek. Biraq bul mu'mkin emes.

Kelip shıqqan qarama-qarsılıq (3) ten'lemenin nol'den o'zgeshe pu'tin sheshimleri bolmaytug'ınlıg'ın ko'rsitedi. Teorema da'llilendi.

§ 3. $n = 3$ ko`rsetkishi ushın Ferma teoreması

Eyler 1768-jılı Ferma teoremasın $n = 3$ ko`rsetkishi ushın da`lillegende to`mendegi lemmanı paydalandı:

Lemma (Eyler). Eger $(a, b) = 1$ bolıp, $a^2 + 3b^2$ sanı pu`tin sannın` kubı bolsa, onda sonday s ha`m  $t$  pu`tin sanları bar bolıp, olar ushın

$$a = s(s^2 - 9t^2), \quad b = 3t(s^2 - t^2)$$

boladı.

Biz da`slep bul lemmadan Ferma teoreması qalay kelip shıg`atug`ınlıg`ın ko`rseteyik.

Meyli, kerisinshe

$$x^3 + y^3 = z^3 \quad (1)$$

bolatug`ınday nol`den o`zgeshe  $x, y$  ha`m z pu`tin sanları bar dep boljayıq. Biz bunda  $x, y$  ha`m z sanların ekew-ara a`piwayı dep esaplay alamız, sonlıqtan olardıń tek birewi jup san bolıwı mu`mkin. Sonın` menen birge olardıń barlıg`ı birden taq san bolıwı mu`mkin emes, sebebi eki taq sannın` qosındısı jup san. Demek x, y ha`m  $z$  sanlarının` birewi ha`m tek g`ana birewi jup san boladı.

Biz bul jup sandı x dep qarawımız mu`mkin. Haqıyqatında da, eger  $y$  jup san bolsa, onda  $x$  ha`m y sanlarının` belgilewlerin o`zgertemiz. Eger z jup san bolsa

$$(-z)^3 + y^3 = (-x)^3$$

bolg`anı ushın $-z$ ti x dep, al $-x$ ti z dep belgileymiz.

(1) ten`lemenı qanaatlantıratug`ın barlıq (x, y, z) lerdin` ishinen  $(x - \text{jup san})$  en` kishi $|x|$ ke iye bolg`anın saylap alamız.  $y$  ha`m x taq sanlar bolg`anı ushın

$$p = \frac{z+y}{2} \text{ ha'm } q = \frac{z-y}{2}$$

sanları pu`tin sanlar boladı. Keyin

$$z = p + q, \quad y = p - q \quad (2)$$

bolg`anı ushın  $p$  ha'm  $q$  sanlarının` birewi taq, birewi jup san boladı, ja`nede  $(p, q) = 1$ . (1) ha'm (2) den to`mendegige iye bolamız:

$$x^3 = z^3 - y^3 = (p+q)^3 - (p-q)^3 = 6p^2q + 2q^3 = 2q(q^2 + 3p^2).$$

Bul jerde $x = 2n$ dep alsaq

$$u^3 = \frac{q}{4}(q^2 + 3p^2) \quad (3)$$

kelip shıg`adı.  $p$  ha'm  $q$  sanlarının` birewi taq, birewi jup san bolg`anı ushın  $q^2 + 3p^2$  sanı taq boladı. Sonlıqtan (3) ten  $q$  din` 4 ke bo`linetug`ınlıg`ı kelip shıg`adı (demek, q jup, al p taq san boladı).

Biz eger eki o`z-ara a`piwayı sannın` ko`beymesi qandayda bir sannın` kubına ten` bolsa, bul sanlardın` o`zleri de kubqa ten` bolatug`ınlıg`ın bilemiz. Sonın` menen birge $q/4$ ha'm $q^2 + 3p^2$ sanları o`z-ara a`piwayı bolıwı ushın q ha'm $3p^2 = (q^2 + 3p^2) - q^2$ sanları o`z-ara a`piwayı bolıwı za`ru`r ha'm jeterli. $(p, q) = 1$ bolg`anı ushın bul  $q$  sanı 3 ke bo`linbegende g`ana orınlı boladı. Sonlıqtan, eger biz  $q$  sanı 3 ke bo`linbeydi dep boljasaq, onda (3) ten $q/4$ ha'm $q^2 + 3p^2$ sanlarının` kub bolatug`ınlıg`ı kelip shıg`adı. Biraq, lemma boyınsha, eger $q^2 + 3p^2$ kub bolsa,

$$q = s(s^2 - 9t^2), \quad p = 3t(s^2 - t^2)$$

boladı, bul jerde s ha'm t -pu`tin sanlar.  $p$  taq san bolg`anı ushın

$$p = 3t(s^2 - t^2)$$

ten`liginen  $t$  nın` taq ha`m  $s$  tin` jup san bolatug`ınlıg`ı kelip shıg`adı. Keyin,  $(p, q) = 1$  bolg`anı ushın $(t, s) = 1$ boladı.

$q / 4$ sanı kub bolg`anı ushın

$$2q = 8 \cdot \frac{q}{4}$$

sanı da kub boladı. Bunnan

$$2s(8^2 - 9t^2) = 2s(s - 3t)(3 + 3t)$$

sanı da kub ekenligi kelip shıg`adı.  $2s$ ,  $s - 3t$  ha`m $s + 3t$ sanları o`z-ara a`piwayı. Haqıyqatında da, eger $2s$ ha`m  $s \pm 3t$  sanları a`piwayı ulıwma bo`liwshi  $\lambda$  ge iye bolsa, onda  $\lambda \neq 2$ , sebebi  $s \pm 3t$  taq san. Demek  $\lambda$  sanı  $s$  ha`m $\pm 3t = (s \pm 3t) - s$ sanların bo`ledi. Biraq,  $t$  ha`m s sanları o`z-ara a`piwayı bolg`anlíg`ı ushın, bul tek $\lambda = 3$ bolg`anda g`ana mu`mkin. Tap sonday, eger  $s + 3t$  ha`m $s - 3t$ a`piwayı ulıwma bo`liwshi λ g`a iye bolsa, onda  $\lambda \neq 2$ , sebebi bul eki san taq sanlar. Ekinshiden,  $2s = (s + 3t) + (s - 3t)$  ha`m $6t = (s + 3t) - (s - 3t)$ sanları λ g`a bo`linedi, biraq bul tek $\lambda = 3$ bolg`anda g`ana mu`mkin. Solay etip, eki jag`dayda da s sanı, demek q sanı da $\lambda = 3$ ke bo`linedi, biraq bul boljamg`a qarma-qarsı keledi.

$2s$, $s - 3t$ ha`m  $s + 3t$  o`z-ara a`piwayı sanlarının` ko`beymesi kub bolg`anı ushın, olardıń ha`r qaysısı kub boladı. Demek sonday  $x_1, y_1$  ha`m z_1 pu`tin sanları bar bolıp

$$x_1^3 = 2s,$$

$$y_1^3 = -(s + 3t),$$

$$z_1^3 = s - 3t$$

ten`likleri orınlanadı. Demek

$$x_1^3 + y_1^3 = z_1^3$$

Solay etip biz (1) din` sheshimi bolg`an (x, y, z) ten basqa (x, y, z) sheshimin aldıq ha`m bul jerde x_1 - jup san.

$$x^3 = 2q(q^2 + 3p^2)$$

bolg`anı ushın  $|q| < \frac{|x^3|}{2}$  ha`m

$$q = s(s^2 - 9t^2)$$

bolg`anı ushın $|s| \leq |q|$. Demek

$$|x_1^3| = 2|s| < |x^3|,$$

sonlıqtan $|x_1| < |x|$. Bul (x, y, z) tin` minimallıg`ına qarama-qarsı keledi. Kelip shıqan qarama-qarsılıq q din` 3 ke bo`linetug`ınlıg`ın ko`rsetedi:  $q = 3r$ , bul jerde  $r$  sanı 4 ke bo`linetug`ın pu`tin san. Onda (3) ten to`mendegi ten`lik kelip shıg`adı

$$u^3 = \frac{3}{4}r(9r^2 + 3p^2) = \frac{9}{4}r(3r^2 + p^2) \quad (4)$$

Eger $\frac{9}{4}r$ ha`m  $3r^2 + p^2$  pu`tin sanları a`piwayı ulıwma bo`liwshi λ ge iye bolsa, onda $\lambda \neq 3$, sebebi bolmasa p sanı 3 ke bo`liner edi, onda ol  $q$  menen o`z-ara a`piwayı bolmas edi.  $\lambda \neq 3$  bolg`anı ushın λ sanı r di, demek $p^2 = (3r^2 + p^2) - 3r^2$ sanın bo`ledi, onda ol  $q$  ha`m p nı da bo`ledi. Bul mu`mkın emes. Demek, $\frac{9}{4}r$ ha`m  $3r^2 + p^2$  o`z-ara a`piwayı sanlar.

Onda (4) ten bul sanlardın` kub bolatug`ınıg`ı kelip shıg`adı, bunnan Lemmag`a sa`ykes $(3r^2 + p^2)$ sanına qollang`an) to`mendegi ten`likler kelip shıg`adı.

$$p = s(s^2 - 9t^2), \quad r = 3t(s^2 - t^2), \quad (5)$$

bul jerde s ha`m  $t$  pu`tin sanlar ha`m  $(s, t) = 1$ .  $r$  jup san boladı ushın  $t$  jup san bolg`anı, demek s taq san boladı. Bunnan tısqarı

$$\frac{8}{27} \cdot \frac{9}{4} r = \frac{2}{3} r = 2t(s^2 - t^2) = 2t(s + t)(s - t)$$

sanı kub boladı.

$(s, t) = 1$ ha`m  $s$  ha`m t sanlarının` jup-taqlıg`ı ha`r qıylı bolg`anlıg`ı ushın  $2t$ ,  $s + t$  ha`m $s - t$ sanları o`z-ara a`piwayı. Sonlıqtan olardıń ha`r biri kub boladı, demek sonday  $x_1, y_1$  ha`m z_1 pu`tin sanları bar bolıp,

$$\begin{aligned} x_1^3 &= 2t, \\ y_1^3 &= s - t, \\ z_1^3 &= s + t \end{aligned}$$

ten`likleri orınlanadı. Demek

$$x_1^3 + y_1^3 = z_1^3$$

boladı, ha`m

$$|x_1^3| = 2|t| \leq \frac{2}{3}|r| = \frac{2}{9}|q| < 2|q| < |x^3|,$$

yag`nıy $|x_1| < |x|$.

Solay etip, bul jag`dayda da biz  $(x, y, z)$  tin` minimallıg`ına qarama-qarsı kelemiz.

Sonlıqtan $x^3 + y^3 + z^3$ ten`lemesi nol`den o`zgeshe pu`tin (x, y, z) sheshimge iye bolmaydı.

Ferma teoremasın $n = 3$ ko`rsetkishi ushın tolıq da`lillew ushın endi joqarıda keltirilgen lemmanı da`lillew qaldı.

Eyler lemmasının` da`lilleniwi.

Biz to`mendegi ko`plikti qaraymız

$$D_3 = \{A + B\xi | A, B \in \mathbb{Z}\},$$

bul jerde $\xi^3 = 1$ ha`m  $\xi^2 = -1 - \xi$  demek  $\xi$  sanı  $x^2 + x + 1$  ten`lemesinin` koreni. Bul ko`pliktin` kol`tso du`zetug`ınlıg`ın tekserip ko`riw qıyın emes. Meyli endi

$$K_3 = \{A + B\xi | A, B \in \mathbb{Z}\},$$

bolsın, bul jerde ξ joqarıdag`ıday,  $Q$  - ratsional sanlar ko`pligi. Bul ko`pliktin` maydan bolatug`ınlıg`ın tekserip ko`riw qıyın emes.

D_3 ha`m  $K_3$  ko`pliklerinin` elementleri  $A + B\xi$  tu`rinde bir ma`nisli ko`rsetiledi. Sebebi, eger $A + B\xi = A_1 + B_1\xi$ ha`m $B \neq B_1$ bolsa

$$\rho = -\frac{A - A_1}{B - B_1}$$

bolar edi. Biraq ξ haqıyqıy san bolmag`anı ushın bul mu`mkin emes, demek $A = A_1, B = B_1$.

Anıqlama. Eger $\alpha = A + B\xi \in K_3$ bolsa

$$N\alpha = \alpha\bar{\alpha} = A^2 - AB - B^2 = \frac{(2A - B)^2 + 3B^2}{4}$$

sanı α sanının` norması dep ataladı.  $N\alpha \geq 0$  ratsional san boladı ( $\alpha \in D_3$  bolsa  $N\alpha$  pu`tin san) $\alpha = 0$ bolsa $N\alpha = 0$ boladı.

$$N(\alpha\beta) = N\alpha \cdot N\beta, \quad \alpha, \beta \in K_3$$

boladı, haqıyqatında da

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta \cdot \bar{\alpha}\bar{\beta} = \alpha\bar{\alpha} \cdot \beta\bar{\beta} = N\alpha \cdot N\beta.$$

Keyin,

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

ten`lemesinin` koren`leri to`mendegishe boladı:

$$-\frac{1 \pm \sqrt{-3}}{2}$$

Bulardın` qa`legenin ξ dep alıwg`a boladı.

Meyli

$$\xi = \frac{1 \pm \sqrt{-3}}{2}$$

bolsın. Sonda

$$A + B\xi = \frac{(2A - B) + B\sqrt{-3}}{2}$$

Demek K_3 maydanının` ha`r bir elementi $a + b\sqrt{-3}$ tu`rinde jazıladı, bul jerde  $a, b$  ratsional sanlar,  $D_3$  kol`tsosının` ha`rbir elementi

$$\frac{p + q\sqrt{-3}}{2} \tag{7}$$

tu`rinde jazıladı, bul jerde  $p$  ha`m q jup-taqlıg`ı birdey pu`tin sanlar. Eger p ha`m q jup sanlar bolsa

$$a + b\sqrt{-3}$$

tu`rindegi Eyler sanları kelip shıg`adı, demek bul sanlar (7) tu`rindegi sanlardın` dara jag`dayı eken.

Anıqlama. Eger $\varepsilon \cdot \varepsilon^{-1} = 1$ bolatug`ınday  $\varepsilon^{-1} \in D$  elementi bar bolsa  $\varepsilon$  elementi  $D$  kol`tsosının` kerili (keri elementke iye) elementi dep ataladı.

Teorema-1. $\alpha \in D_\varepsilon$ kerili element bolıwı ushın $N\alpha = 1$ bolıwı za`ru`r ha`m jeterli.

Da`lillew. Eger $\alpha \cdot \alpha^{-1} = 1$ bolsa

$$N\alpha \cdot N\alpha^{-1} = N(\alpha \cdot \alpha^{-1}) = N1 = 1$$

Demek $N\alpha = N\alpha^{-1} = 1$. Egerde $N\alpha = 1$ bolsa, yag`nıy  $\alpha \cdot \bar{\alpha} = 1$  bolsa  $\alpha$ -kerili element:  $\alpha^{-1} = \bar{\alpha}$ .  $\alpha = A + B\xi$  sanının` norması

$$N\alpha = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4}$$

bolg`anı ushın  $N\alpha = 1$  ten`ligi tek g`ana to`mendegi jag`daylarda orınlanadı:

I) $B = 0, A = \pm 1$

II) $B = \pm 1, (A - B)^2 = 1$, yag`nıy $A = B = \pm 1$

III) $A = 0, B = \pm 1$

Solay etip D_3 kol`tsosı 6 kerili elementke iye:

$$\begin{aligned} 1, \quad \xi, \quad 1 + \xi = -\xi^2, \\ -1, \quad -\xi, \quad -1 - \xi = \xi^2 \end{aligned}$$

Bulardın` barlıg`ı da 1 din` 6-da`rjeli koren`leri boladı. Sonın` menen birge bular

$$1 + \xi = \frac{1 + \sqrt{-3}}{2}$$

kerili elementinin` da`rejeleri boladı:

$$\begin{aligned}(1+\xi)^2 &= 1+\xi, & (1+\xi)^2 &= \xi, & (1+\xi)^3 &= -1 \\ (1\xi)^4 &= -1-\xi, & (1+\xi)^5 &= -\xi, & (1+\xi)^6 &= 1.\end{aligned}$$

Анықлама. Егер $\alpha = \beta\gamma$ болса α elementi jikleniwshi element dep ataladı. Jiklenbeytug`ın element a`piwayı element dep ataladı.

Анықлама. Егер D kol`tsosının` qa`legen elementi a`piwayı ko`beytiwshilerge bir ma`nisli jiklense, D kol`tsosında arifmetikanın` tiykarg`ı teoreması orınlanadı delinedi.

Анықлама. Егер D kol`tsosının` qa`legen  $\alpha$  ha`m $\beta \neq 0$ elementleri ushın sonday γ ha`m ρ elementleri bar bolıp

$$\alpha = \beta\gamma + \rho$$

ten`ligi orınlansa ha`m bunda $\rho \neq 0$ ushın $|\rho| < |\beta|$ болса ($||$ bel-gisi D kol`tsosında berilgen norma), onda  $D$  kol`tsosı Evklid kol`tsosı dep ataladı.

Теорема-2. Qa`legen Evklid kol`tsosında arifmetikanın` tiykarg`ı teoreması orınlanadı.

Теорема-3. D_3 kol`tsosı Evklid kol`tsosı boladı.

**Da`lillew.**  $D_3$  kol`tsosındag`ı normanı Evklid kol`tsosındag`ı norma dep qabıl etemiz. Biz qa`legen α ha`m $\beta \neq 0$ elementleri ushın

$$\alpha = \beta\gamma + \rho, \quad N_\rho < N_\beta$$

bolatug`ınday  $\gamma$  ha`m ρ elementleri bar bolatug`ınlıg`ın da`lillewimiz kerek.

Lemma. Qa`legen $\varepsilon \in K_3$ ushın

$$N(\varepsilon - \gamma) \leq \frac{3}{4}$$

bolatug`ınday $\gamma \in D_3$ elementi bar boladı.

Da`lillew. Meyli

$$\varepsilon = A + B\xi,$$

ha'm $a, b \in Z$ bolip,

$$|A - a| \leq \frac{1}{2}; \quad |B - b| \leq \frac{1}{2}$$

bolsin. Onda

$$\gamma = a + b\xi \in D_3$$

sanı ushın to'mendegige iye bolamız:

$$\begin{aligned} N(\varepsilon - \gamma) &= (A - a)^2 - (A - a)(B - b) + (B - b)^2 \leq |A - a|^2 + \\ &+ |A - a| |B - b| + |B - b|^2 \leq \left(\frac{1}{2}\right)^2 + \frac{1}{2} \cdot \frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4}. \end{aligned}$$

Lemma da'lillendi. Endi teoremanı da'lilleyik. Lemmanı $\varepsilon = \frac{\alpha}{\beta}$ sanına

qollanıp ha'm $\rho = \alpha - \beta\gamma$ dep alıp biz

$$\alpha = \beta\gamma + \rho,$$

$$N\rho N(\alpha - \beta\gamma) = N\beta \cdot N(\varepsilon - \gamma) \leq \frac{3}{4}N\beta < N\beta$$

ekenligine iye bolamız. Teorema da'lillendi.

Saldar. D_3 kol'tsosında arifmetikanın tiykarg'ı teoreması orınlanadı.

Endi biz Eyler lemmasın da'lilleyik.

$$a^2 + 3b^2 = (a + b\sqrt{-3})(a - b\sqrt{-3}) \quad (8)$$

Bul ten'liktin shep jag'ı kub bolg'anı ushın, on jag'ındag'ı ha'r bir o'z-ara a'piwayı ko'beytiwshiler de kub bolıwları kerek. Dara jag'dayda

$$a + b\sqrt{-3} = (s + t\sqrt{-3})^3, \quad s, t \in Z$$

Bul ten'likti kubqa ko'terip to'mendegige iye bolamız.

$$a + b\sqrt{-3} = s^2 - 9st^2 + (3s^2t - 3t^2)\sqrt{-3}$$

Demek

$$a = s^3 - 9st^2 = s(s^2 - 9t^2)$$

$$b = 3s^2t - 3t^3 = 3t(s^2 - t^2)$$

Endi $a + b\sqrt{-3}$ ha'm $a - b\sqrt{-3}$ elementleri D_3 kol'tsosında o'z-ara a'piwayı elementler bolatug'inlig'in ko'rsetiw qaldı.

Da'slep a nın 3 ke bo'linbeytug'inlig'in da'lilleyik. Haqıyqatında da, a sanı 3 ke bo'linse, kub bolg'an $a^2 + 3b^2$ sanı da 3 ke bo'liner edi, yag'nıy 27 ge bo'liner edi. Onda $a = 3a_1$ ha'm $a^2 + 3b^2 = 27n$ dep alsaq $9a_1^2 + 3b^2 = 27n$ demek $b^2 = 3(3n - a_1^2)$ boladı. Solay etip b^2 , demek b sanı 3 ke bo'liner edi. Bul $(a, b) = 1$ ekenligine qarama-qarsı keledi.

Meyli endi $a + b\sqrt{-3}$ ha'm $a - b\sqrt{-3}$ sanları $\gamma \in D_3$ sanına bo'linsin.

Onda γ g'a

$$2a = (a + b\sqrt{-3}) + (a - b\sqrt{-3}),$$

$$2b\sqrt{-3} = (a + b\sqrt{-3}) - (a - b\sqrt{-3})$$

sanları da belinedi, bunnan, normalarg'a o'tip, biz $N\gamma$ sanı $N(2a) = 4a^2$ ha'm $N(2b\sqrt{-3}) = 12b^2$ sanların, demek olardın' en' u'lken ulıwma bo'liwshisin bo'letug'inlig'ına iye bolamız. a ha'm b sanları o'z-ara a'piwayı ha'm a sanı 3 ke bo'linbeytug'inlig'ı sebepli bul en' u'lken ulıwma bo'liwshi 4 ke ten' boladı. Demek $N\gamma = 4$, $N\gamma = 2$ yamasa $N\gamma = 1$ bolıwı mu'mkin.

Eger $N\gamma = 4$ bolsa $N(\frac{\gamma}{2}) = 1$ yag'nıy $\gamma = 2\varepsilon$ boladı, bul jerde ε - kerili

element. Bul jag'dayda $\gamma = 2$ boladı, biraq bul bizge kerek emes, sebebi $a + b\sqrt{-3}$ sanı D_3 kol'tsosında 2 ge bo'liniwi ushın a ha'm b sanları da 2 ge

bo`liniwi kerek ha`m kerisinshe. $N\gamma = 2$ bolıwı mu`mkin emes, sebebi  $x^2 - xy + y^2 = 2$  pu`tin sheshimlerge iye emes. Solay etip $N\gamma = 1$ bolıwı sha`rt. Onda  $\gamma$  kerili element boladı. Demek  $a + b\sqrt{-3}$  ha`m $a - b\sqrt{-3}$ elementleri o`z-ara a`piwayı.

Eyler lemması, demek Ferma teoremsı $n = 3$ ko`rsetkishi ushın da`lillendi.

Juwmaqlaw

Solay etip biz Ferma teormasının $n = 3$ ha'm $n = 4$ bolg'andag'ı jara jag'dayların qaradıq ha'm bul jag'daylar ushın teoremanın da'lillewlerin keltirdik. Joqarıda aytqanımızday, Ferma teoreması ha'zir barlıq $n < 100\,000$ ko'rsetkishleri ushın da'llengen. Biraq bul da'lillewler ju'da quramalı. Bul teoremanı da'lillew barısında sanlardın algebralıq teoriyası boyınsha birqansha a'hmiyetli na'tiyjeler alındı, klasslar maydanları teoriyası rawajlandı. Birqansha matematikler Ferma teoremasın da'lillew barısında alıng'an algebralıq rezul'tatlar teoremanın o'zinen de a'hmiyetlirek dep qaraydı [1].

Usının menen biz bul kurs jumısımızdı juwmaqlaymız.

A`debiyatlar

1. Postnikov M.M. Vvedenie v teoriyu algebraicheskix chisel. M., «Nauka», 1982.
2. Buxshtab A.A. Teoriya chisel. M., «Prosveshenie», 1966.
3. Vinogradov I.M. Osnovi teorii chisel. M., «Nauka», 1974
4. Kostrikin A.I. Vvedenie a algebru. M., «Nauka», 1977.
5. Nazarov R.N. va boshq. Algebra va sonlar nazariyasi. T., «Uqituvchi» I-qism, 1993; II-qism, 1995.