KVADRATIK TAQQOSLAMALAR: TUB MODUL BO’YICHA 2-DARAJALI TAQQOSLAMANI SODDA KO’RINISHGA KELTIRISH VA YECHIMLAR SONINI ANIQLASH

Diyoraxon Akramjonova*
Qo’qon davlat universiteti, Aniq fanlar va muhandislik fakulteti, Matematika kafedrasi 1-kurs magistranti
✉ diyoraxonakramjonova@gmail.com

ANNOTATSIYA

Maqolada p toq tub modul bo’yicha 2-darajali taqqoslamalar nazariyasining boshlang’ich bosqichi yoritilgan. Isbotlanishicha, p c_0 bo’lganda $c_0x^2 + c_1x + c_2 \equiv 0 \pmod p$ taqqoslama to’la kvadratni ajratish yo’li bilan $(x + c)^2 \equiv a \pmod p$ ko’rinishidagi ekvivalent taqqoslamaga, undan esa $z^2 \equiv a \pmod p$ ko’rinishiga keltiriladi. p a bo’lganda bu taqqoslama yo ikkita yechimga ega bo’ladi, yo birorta ham yechimga ega bo’lmaydi; yechimlar soni a sonning o’ziga emas, uning p modul bo’yicha sinfiga bog’liq. Natijalar misollar bilan tasdiqlangan hamda ularning o’qitish jarayonida mantiqiy va tanqidiy fikrlashni rivojlantirishdagi ahamiyati muhokama qilingan.

Kalit so‘zlar

kvadratik taqqoslama, tub modul, to’la kvadrat, chegirmalar sinfi, kvadratik chegirma, yechimlar soni, mantiqiy fikrlash, matematika ta’limi.

DOI: 10.5281/zenodo.24438010

Kirish

Taqqoslamalar nazariyasi sonlar nazariyasining asosiy bo'limlaridan biri bo'lib, undagi 1-darajali taqqoslamalardan keyingi tabiiy qadam — 2-darajali, ya'ni kvadratik taqqoslamalarni o'rganishdir [1]. Kvadrat ko'phadlarning tub modullar bo'yicha qiymatlari va ularning tub sonlarni ifodalash xossalari ham aynan shu nazariya bilan bog'liq [2]. Shu sababli kvadratik taqqoslamalarning yechilish shartlarini aniq bilish nazariy ham, amaliy ham ahamiyatga ega.

O'quv adabiyotlarida bu mavzu odatda tayyor ko'rinishda beriladi, talaba esa teoremaning mantiqiy tuzilishini emas, balki yakuniy natijani yodlab oladi. Holbuki, kvadratik taqqoslamaning yechimlari haqidagi mulohazalar — yechim mavjud bo'lmasligi mumkinligi, yechimlarning juft-juft kelishi, ularning sonining chegaralanganligi — mantiqiy va tanqidiy fikrlashni rivojlantirish uchun boy material beradi

Tadqiqotning maqsadi — p toq tub modul bo'yicha umumiy 2-darajali taqqoslamani $z^2 \equiv a \pmod p$ ko'rinishiga keltirish va bunday taqqoslama yechimlarining mavjudligi hamda sonini aniqlashdir.

Vazifalar:

1. p c_0 bo'lganda umumiy taqqoslamaning ekvivalent sodda ko'rinishini topish va isbotlash;
2. $z^2 \equiv a \pmod p$ taqqoslamaning yechimlari sonini a ning holatlari bo'yicha aniqlash;
3. olingan natijalarni sonli misollarda tekshirish va ularning didaktik ahamiyatini ko'rsatish.

Asosiy qism. Tadqiqot nazariy xarakterga ega. Quyidagi usullardan foydalanildi: chegirmalar sinflari ustida ekvivalent almashtirishlar; to'la kvadratni ajratish; hollarga bo'lib isbotlash (juft va toq koeffitsiyent); ”qarama-qarshisini faraz qilish” usuli; sinflar bo'yicha sonli tekshirish. Asosiy nazariy tayanch sifatida [1] dagi teoremalar — p c_0 bo'lganda 2-darajali taqqoslamani $x^2 + b_1x + b_2 \equiv 0 \pmod p$ ko'rinishga keltirish (144-teorema) va tub modul bo'yicha n-darajali taqqoslama n tadan ortiq yechimga ega bo'lmasligi (148-teorema) ishlatildi. Misollar [4] dagi kabi masalalar uslubida tanlandi va barcha sinflarni bevosita sinash orqali tekshirildi. Modul sifatida toq tub p olinadi: p = 2 bo'lganda yechimlar $\bar{0}$ va $\bar{1}$ sinflarni sinab ko'rish bilan topiladi. $p \mid c_0$ holda taqqoslama 1-darajali $c_1x + c_2 \equiv 0 \pmod p$ ga ekvivalent bo'lgani uchun faqat p c_0 holi qaraladi.

Natijalar: *1. Umumiy taqqoslamani to'la kvadratga keltirish.* 2-darajali taqqoslamaning umumiy ko'rinishi:

$c_0x^2 + c_1x + c_2 \equiv 0 \pmod p$. (1)

Teorema. $p > 2$ va $p \nmid c_0$ bo'lganda (1) taqqoslama quyidagi ko'rinishdagi biror taqqoslamaga ekvivalent:

$(x + c)^2 \equiv a \pmod p$. (2)

Isbot. $p \nmid c_0$ bo'lgani uchun (1) taqqoslamani c_0 ning teskarisiga ko'paytirib, uni quyidagi ko'rinishga keltirish mumkin [1, 144-teorema]:

$x^2 + b_1x + b_2 \equiv 0 \pmod p$. (3)

Ikki holni qaraymiz.

1) Agar $2 \mid b_1$ bo'lsa, (3) taqqoslamani quyidagicha yozish mumkin:

$(x + b_1/2)^2 \equiv (b_1/2)^2 - b_2 \pmod p$.

2) Agar $2 \nmid b_1$ bo'lsa, (3) ni ekvivalent $x^2 + (b_1 + p)x + b_2 \equiv 0 \pmod p$ taqqoslama bilan almashtiramiz. p toq bo'lgani uchun $2 \mid b_1 + p$, shu sababli:

$(x + (b_1 + p)/2)^2 \equiv ((b_1 + p)/2)^2 - b_2 \pmod p$.

Ikkala holda ham dastlabkisiga ekvivalent (2) ko'rinishdagi taqqoslama hosil bo'ldi. □

$x + c$ ni z bilan belgilasak, har qanday 2-darajali taqqoslama uchun yechimlar mavjudligi va ularni topish masalasi $z^2 \equiv a \pmod p$ taqqoslamani tekshirishga keltiriladi. Quyida uni $x^2 \equiv a \pmod p$ ko'rinishda yozamiz:

$x^2 \equiv a \pmod p$, $p \nmid a$. (4)

2. (4) taqqoslamaning yechimlari.

- *Nol sinf.* Agar $a \in \bar{0}$, ya'ni $p \mid a$ bo'lsa, (4) faqat bitta $x \equiv 0 \pmod p$ yechimga ega: $x \not\equiv 0$ bo'lganda $x^2 \not\equiv 0 \equiv a$.
- *Yechim bo'lmasligi mumkin.* $p \nmid a$ bo'lganda (4) yechimga ega bo'lmasligi mumkin. Masalan, $x^2 \equiv 2 \pmod 5$ taqqoslamani 5 modul bo'yicha sinflarning birortasi ham qanoatlantirmaydi.
- *Yechimlar juft-juft keladi.* Agar $p \nmid a$ va $\bar{x}_0$ yechim bo'lsa, $-\bar{x}_0$ sinf ham yechim: $(-x_0)^2 \equiv a \pmod p$. Bunda $p \nmid a$ bo'lgani uchun $p \nmid x_0^2$, demak $p > 2$ da $2x_0 \not\equiv 0$, ya'ni $x_0 \not\equiv -x_0 \pmod p$: $\bar{x}_0$ va $-\bar{x}_0$ turlicha yechimlardir.
- *Ikkitadan ko'p emas.* (4) taqqoslama ikkitadan ortiq yechimga ega bo'la olmaydi [1, 148-teorema].

Shunday qilib, $p \nmid a$ bo'lganda (4) taqqoslama **yo ikkita yechimga ega, yo birorta ham yechimga ega emas**. Agar biror a da ikkita yechim mavjud bo'lsa, a ga p modul bo'yicha taqqoslanadigan har qanday b uchun ham ikkita yechim mavjud bo'ladi; shu sababli (4) ni alohida sonlar uchun emas, mos sinflar uchun qarash tabiiydir.

Natija. p toq tub bo'lsa, nolga teng bo'lmagan sinflar orasida (4) yechimga ega bo'ladiganlari soni $(p - 1)/2$ ga teng. *Isbot:* $p - 1$ ta nolmas x sinfning har biri qandaydir a sinfni beradi va yechimga ega har bir a aynan ikkita x dan hosil bo'ladi (x va $-x$), demak bunday a lar soni $(p - 1)/2$.

3. Sonli misollar. 5 va 7 modullar bo'yicha x^2 ning qiymatlari 1-jadvalda keltirilgan.

1-jadval. $x^2 \pmod p$ qiymatlari va yechimga ega sinflar

p	x = 1, …, p − 1 uchun $x^2 \pmod p$	Yechimga ega a sinflar	Yechimga ega bo'lmagan a sinflar
5	1, 4, 4, 1	$\bar{1}$ ($x \equiv \pm 1$), $\bar{4}$ ($x \equiv \pm 2$)	$\bar{2}$, $\bar{3}$
7	1, 4, 2, 2, 4, 1	$\bar{1}$ ($x \equiv \pm 1$), $\bar{2}$ ($x \equiv \pm 3$), $\bar{4}$ ($x \equiv \pm 2$)	$\bar{3}$, $\bar{5}$, $\bar{6}$

Jadval $(p - 1)/2$ qonuniyatini tasdiqlaydi: $p = 5$ da 2 ta, $p = 7$ da 3 ta sinf yechimga ega. Teoremaning qo'llanishi 2-jadvalda ko'rsatilgan.

2-jadval. Taqqoslamalarni keltirish va yechish

Taqqoslama	Keltirish	Xulosa
$x^2 + 2x - 3 \equiv 0 \pmod 7$	$b_1 = 2$ juft: $(x+1)^2 \equiv 1 + 3 = 4$	$x + 1 \equiv \pm 2$, ya'ni $x \equiv 1$ va $x \equiv 4 \pmod 7$
$x^2 + 3x + 1 \equiv 0 \pmod 7$	$b_1 = 3$ toq, $3 + 7 = 10$: $(x+5)^2 \equiv 25 - 1 = 24 \equiv 3$	$\overline{3}$ yechimga ega emas, taqqoslama yechimsiz
$3x^2 + x + 2 \equiv 0 \pmod 7$	$\overline{3}$ ning teskarisi 5: $x^2 + 5x + 3 \equiv 0$; $b_1 = 5$ toq, $5 + 7 = 12$: $(x+6)^2 \equiv 36 - 3 = 33 \equiv 5$	$\overline{5}$ yechimga ega emas, taqqoslama yechimsiz

Birinchi taqqoslamada $x = 1$ va $x = 4$ ni qo'yib tekshirish: $1 + 2 - 3 = 0$ va $16 + 8 - 3 = 21 \equiv 0 \pmod 7$. Qolgan ikkitasi uchun barcha 7 ta sinfni bevosita sinash yechim yo'qligini tasdiqladi.

Muhokama

Olingan natijalar klassik bo'lib, [1] da bayon etilgan; ushbu maqolada ular yagona mantiqiy zanjir sifatida — umumiy taqqoslamadan (4) ga o'tish, so'ngra yechimlar sonini (0 yoki 2) asoslash tarzida — tizimlashtirildi va misollar bilan to'ldirildi. Muhim jihat shuki, (4) ning yechimga ega bo'lishi a ning sinfiga bog'liq, shuning uchun ”qaysi sinflar yechimga ega” degan savol tabiiy ravishda paydo bo'ladi. $(p-1)/2$ natijasi bunday sinflar yarmini tashkil etishini ko'rsatadi, ularni aniqlashning umumiy mezoni (Eyler mezoni, Lejandr belgisi) esa keyingi tadqiqot mavzusidir.

Didaktik nuqtai nazardan isbotning har bir bosqichi talabadan mustaqil mulohazani talab qiladi: nega toq b_1 holida b_1 ni $b_1 + p$ bilan almashtirish mumkin; nega $\bar{x}_0$ va $-\bar{x}_0$ turlicha; nega yechim bo'lmasligi mumkin. [3, 387-b.] da PISA topshiriqlari misolida ko'rsatilganidek, bunday vazifalar o'quvchini tayyor formulani qo'llashdan yangi yo'l izlashga o'tkazadi, shaxsning o'z faoliyatini tahlil qilish va xatolarini aniqlash ko'nikmasini mustahkamlaydi. Mavzuni o'rganishda [4] dagi kabi masalalar to'plamidan foydalanish, talabaning o'zi sinflar jadvalini tuzishi (yuqoridagi jadvalga o'xshash) mantiqiy fikrlashni amaliy mashqlar bilan bog'laydi. Bu xulosa nazariy mulohazaga asoslangan; uning samaradorligini pedagogik tajriba orqali tekshirish alohida tadqiqotni talab qiladi.

Xulosa

Isbotlandiki, $p > 2$ va p c_0 bo'lganda har qanday 2-darajali taqqoslama to'la kvadratni ajratish orqali $(x + c)^2 \equiv a \pmod p$ ko'rinishga, so'ngra $z^2 \equiv a \pmod p$ ga keltiriladi. p a bo'lganda bu taqqoslama yo ikkita ($\bar{x}_0$ va $-\bar{x}_0$), yo birorta ham yechimga ega emas; $p \mid a$ bo'lganda yagona $x \equiv 0$ yechim mavjud. Yechimlar soni a ning o'ziga emas, uning p modul bo'yicha sinfiga bog'liq, nolmas sinflar orasida yechimga egalari $(p-1)/2$ ta. Sonli misollar ($p = 5$ va $p = 7$) bu xulosalarni tasdiqladi. Mavzuni isbotning mantiqiy bosqichlari va sinflar jadvali orqali o'rgatish talabalarda mantiqiy va tanqidiy fikrlashni rivojlantirishga xizmat qiladi; bu ta'sirni tajribada tekshirish va yechimlilik mezonlarini (Eyler mezoni, Lejandr belgisi) o'rganish keyingi tadqiqot yo'nalishlaridir.

FOYDALANILGAN ADABIYOTLAR

1. Бухштаб А.А. Теория чисел. — М.: Просвещение, 1970. — URL: https://mahalex.net/teaching/algebra/Buchstab.pdf
2. Boston N., Greenwood M.L. Quadratics representing primes. — URL: https://share.google/vuMw0eUPbXxJIoSxQ
3. Корешков Н.А., Насрутдинов М.Ф. Сборник задач по теории чисел. — URL: https://share.google/ikQuU5zQ8KNbkQZfy