MODULLI ARIFMETIKA VA KONGRUENSIYALAR NAZARIYASI

Turayev Ziyavutdin O‘ktamxonovich
Shahrisabz davlat pedagogika instituti
“Matematika va ta’limda axborot texnologiyasi”
kafedrasi o‘qituvchisi
e-mail: torayevziyovuddin6@gmail.com
Rovshanova Yulduz Shovkat qizi
Shahrisabz davlat pedagogika instituti
“Matematika ” yo‘nalishi 2-bosqich talabasi
Xolturayeva E’zoza Oybek qizi
Shahrisabz davlat pedagogika instituti
“Matematika ” yo‘nalishi 2-bosqich talabasi

Annotatsiya. *Ushbu maqola yoki ish modulli arifmetika va kongruensiyalar nazariyasi asoslarini, ularning matematik va amaliy ahamiyatini o‘rganishga bag‘ishlangan. Modulli arifmetika sonlar to‘plamini ma’lum bir modul bo‘yicha hisoblash qoidalarini o‘rganadi, bu esa sonlarning qoldiq bo‘yicha taqqoslanishini soddalashtiradi va raqamli tizimlar, kodlash, kriptografiya kabi sohalarda keng qo‘llaniladi. Kongruensiyalar nazariyasi esa modulli arifmetikaning fundamental tushunchalarini yanada chuqurlashtirib, sonlar orasidagi qoldiq munosabatlarini tahlil qilishga imkon beradi. Ishda kongruensiyalarni yechish usullari, teoremalari, va ularning son nazariyasi va zamonaviy hisoblash tizimlaridagi qo‘llanilishi misollar bilan tushuntiriladi. Shu bilan birga, modulli arifmetika va kongruensiyalar orqali murakkab sonlar munosabatlarini soddalashtirish va ularni amaliy masalalarda qo‘llash imkoniyatlari ko‘rib chiqilgan.*

Kalit so‘zlar. *Modulli arifmetika, kongruensiya, qoldiq, sonlar nazariyasi, qoldiq bo‘yicha hisoblash, kriptografiya, raqamli tizimlar, sonlar orasidagi munosabat, Teoremalar, amaliy qo‘llanilishi.*

Annotation. *This article or work is devoted to the study of the foundations of modular arithmetic and the theory of congruences, their mathematical and practical significance. Modular arithmetic studies the rules for calculating a set of numbers by a certain module, which simplifies the comparison of numbers by remainder and is widely used in such areas as digital systems, coding, cryptography. Congruence theory, on the other hand, deepens the fundamental concepts of modular arithmetic and allows you to analyze the residue relations between numbers. The work explains the methods of solving congruences, theorems, and their application in number theory and modern computing systems with examples. At the same time, the possibilities of simplifying the relations of*

complex numbers through modular arithmetic and congruences and their application in practical problems are considered.

Keywords. *Modular arithmetic, congruence, remainder, number theory, remainder calculation, cryptography, number systems, relationships between numbers, theorems, practical applications.*

Аннотация. *Данная статья посвящена изучению основ модульной арифметики и теории сравнений, их математического и практического значения. Модульная арифметика изучает правила вычисления множества чисел по некоторому модулю, что упрощает сравнение чисел с остатком и широко используется в таких областях, как цифровые системы, кодирование, криптография. Теория сравнений, с другой стороны, углубляет фундаментальные понятия модульной арифметики и позволяет анализировать отношения остатков между числами. В работе на примерах объясняются методы решения сравнений, теоремы и их применение в теории чисел и современных вычислительных системах. Одновременно рассматриваются возможности упрощения отношений комплексных чисел посредством модульной арифметики и сравнений и их применение в практических задачах.*

Ключевые слова: *модульная арифметика, сравнение, остаток, теория чисел, вычисление остатка, криптография, системы счисления, отношения между числами, теоремы, практические приложения.*

Kirish. Matematikaning sonlar nazariyasi bo‘limida modulli arifmetika va kongruensiyalar nazariyasi alohida o‘rin egallaydi. Ushbu nazariya sonlar orasidagi qoldiq munosabatlarini o‘rganishga va ularni turli amaliy masalalarda qo‘llashga imkon beradi. Modulli arifmetika oddiy qilib aytganda, sonlarni ma’lum bir modul bo‘yicha taqqoslash va ularga amallarni qo‘llash tizimidir. Masalan, sonlarni ma’lum bir butun son bilan bo‘lganda qolgan qoldiqni aniqlash orqali murakkab arifmetik amallarni soddalashtirish mumkin. Bu tushuncha raqamli tizimlar, kompyuter texnologiyalari, kriptografiya, kodlash va axborot xavfsizligi kabi sohalarda keng qo‘llaniladi.Kongruensiyalar nazariyasi modulli arifmetikaning eng muhim qismi bo‘lib, sonlar orasidagi qoldiq bo‘yicha tengliklarni tahlil qilish imkonini beradi. Kongruensiyalar yordamida murakkab hisob-kitoblarni qisqartirish, sonlar tizimini soddalashtirish va yechimlarni aniqlash mumkin bo‘ladi. Bu nazariya orqali matematik tafakkur va mantiqiy fikrlash rivojlanadi, chunki u abstrakt tushunchalarni amaliy masalalarga tatbiq etishni talab qiladi. Masalan, kongruensiyalar yordamida tub sonlarni aniqlash, modul bo‘yicha ekvivalent tenglamalarni yechish yoki katta sonlar ustida operatsiyalarni soddalashtirish mumkin.Shuningdek, modulli arifmetika va kongruensiyalar zamonaviy matematikaning turli sohalarida, xususan raqamli kodlash, ma’lumotlarni shifrlash, kompyuter algoritmlari va elektron hisoblash tizimlarida muhim vosita sifatida ishlatiladi. Kriptografiyada masalan, RSA algoritmi yoki Diffi-Hellman

kalit almashinuvi kabi jarayonlar modulli arifmetika va kongruensiyalarga asoslanadi. Shu bilan birga, bu nazariya matematik modellash va algoritmik yechimlarni ishlab chiqishda ham qo‘llaniladi.Modulli arifmetika va kongruensiyalarni chuqur o‘rganish orqali nafaqat matematik bilimlarni kengaytirish, balki real hayotdagi murakkab masalalarni hal qilish imkoniyati ham ortadi. Ular sonlar orasidagi munosabatlarni aniq va tizimli tarzda tahlil qilishga, murakkab tenglamalarni yechishga va raqamli tizimlarda xavfsizlikni ta’minlashga yordam beradi. Shu sababli, ushbu mavzu nafaqat nazariy qiziqish uyg‘otadi, balki amaliy ahamiyati bilan ham dolzarb hisoblanadi.

Mavzuga doir adabiyotlar tahlili. Modulli arifmetika va kongruensiyalar nazariyasi bo‘yicha mavjud adabiyotlar son nazariyasi, algebra va amaliy matematikaga oid keng doiradagi manbalarni o‘z ichiga oladi. O‘zbek tilidagi ilmiy va pedagogik manbalar ushbu mavzuni o‘rganishda asosiy ma’lumotlarni beradi va nazariy tushunchalarni amaliy masalalarga tatbiq etishga yordam beradi.Masalan, G‘. Xo‘jayevning “Sonlar nazariyasi asoslari” asari modulli arifmetika va kongruensiyalarni bosqichma-bosqich tushuntirib, har bir teorema va qoidani misollar bilan mustahkamlaydi. Muallif kongruensiyalarni yechish algoritmlari, modul bo‘yicha qo‘llaniladigan amallar va ularning son nazariyasidagi ahamiyatini batafsil bayon etadi. Shu bilan birga, A. Islomovning “Algebra va sonlar nazariyasi” kitobida modulli arifmetika raqamli tizimlar va kompyuter texnologiyalarida qo‘llanilishi misollar bilan ko‘rsatilgan. Bu manba nazariy bilimlarni amaliy jihatlar bilan bog‘lashda foydalidir.Bundan tashqari, B. Qodirovning maqolalarida kongruensiyalarning turli turlari, ularni yechish usullari va tub sonlarni aniqlashdagi roli tahlil qilingan. Mualliflar modulli arifmetikaning tarixiy rivojlanishi va mashhur matematiklarning hissasini ham yoritib beradi. Shu tarzda, nazariya va amaliy masalalarni bog‘lovchi ilmiy ishlar mavzuni yanada chuqurroq tushunishga imkon yaratadi.O‘zbek tilidagi ta’limiy adabiyotlarda ko‘pincha modulli arifmetika va kongruensiyalar nazariyasi maktab va universitet darajasidagi o‘quv dasturlarida o‘rganiladi. Masalan, N. Toshpulatovning “Matematika fanidan qo‘llanma” kitobida modulli arifmetika va kongruensiyalar asosiy tushunchalar, amaliy masalalar va yechim metodlari bilan keng yoritilgan. Shu bilan birga, zamonaviy tadqiqotlarda bu mavzu kriptografiya, raqamli signallarni kodlash va algoritmik hisoblash sohalarida qo‘llanilishi ko‘rsatib o‘tiladi.Umuman olganda, adabiyotlar tahlili shuni ko‘rsatadiki, modulli arifmetika va kongruensiyalar nazariyasi nafaqat nazariy qiziqish uyg‘otadi, balki amaliy masalalarda, xususan, sonlarni tahlil qilish, kodlash, shifrlash va kompyuter texnologiyalarida keng qo‘llaniladi. Shu bois, mavzuni o‘rganishda turli adabiyotlarni integratsiyalash va ularning amaliy jihatlarini o‘rganish muhim ahamiyatga ega.

Tadqiqotlar metodologiyasi. Ushbu tadqiqot modulli arifmetika va kongruensiyalar nazariyasini o‘rganish va ularning amaliy qo‘llanilishini tahlil qilishga qaratilgan. Tadqiqot metodologiyasi nazariy va amaliy usullarni birlashtirib, mavzuning chuqur o‘rganilishini ta’minlaydi. Asosiy maqsad — modulli arifmetika va kongruensiyalarning matematik qonuniyatlarini aniqlash, ularni yechish usullarini o‘rganish va zamonaviy

ilovalarda qo‘llash imkoniyatlarini ko‘rsatish.Tadqiqotda analitik metod asosiy o‘rinni egallaydi. Bu metod sonlar orasidagi qoldiq munosabatlarini, kongruensiyalarni yechish qoidalarini va modullar bo‘yicha tenglamalarni tahlil qilishga imkon beradi. Masalalar va teoremalarning amaliy misollari orqali nazariy bilimlar mustahkamlanadi. Shuningdek, taqqoslash va umumlashtirish metodlari ishlatiladi: turli modullar va kongruensiyalar bo‘yicha olingan natijalar solishtiriladi, umumiy qonuniyatlar va xususiyatlar aniqlanadi.Tadqiqotning yana bir muhim qismi — amaliy metodlar. Ular orqali modulli arifmetika va kongruensiyalarni real masalalarda, masalan, raqamli kodlash, kriptografik algoritmlar, tub sonlarni aniqlash va algoritmik hisoblash tizimlarida qo‘llash imkoniyati ko‘rib chiqiladi. Masalalar yechimlari bosqichma-bosqich tahlil qilinadi, formulalar va qoidalar misollar orqali tasdiqlanadi.Bundan tashqari, tadqiqotda historik-metodik yondashuv ham qo‘llaniladi. Bu modulli arifmetika va kongruensiyalar nazariyasining tarixiy rivojlanishini, mashhur matematiklarning hissasini o‘rganishga yordam beradi va mavzuning ilmiy kontekstini tushunishga imkon beradi. Shu tariqa, nazariy va amaliy bilimlar birlashtiriladi, o‘quvchi yoki tadqiqotchi mavzuni kompleks tarzda o‘rganadi.Tadqiqot metodologiyasining yakuniy maqsadi — modulli arifmetika va kongruensiyalar nazariyasini chuqur tushunish, ularni yechish usullarini o‘rganish va amaliy jihatlarini tahlil qilish orqali mavzuni mukammal o‘rganishga erishishdir. Shu metodologiya orqali olingan natijalar nafaqat matematik nazariyani boyitadi, balki real hayotdagi masalalarni hal qilishda ham qo‘llanilishi mumkin.

Natija va muhokama. Tadqiqot natijalariga ko‘ra, modulli arifmetika va kongruensiyalar nazariyasi sonlar nazariyasi sohasida muhim o‘rin egallashi va amaliy masalalarni yechishda keng qo‘llanilishi aniqlangan. Modulli arifmetika yordamida sonlar orasidagi murakkab munosabatlar soddalashtiriladi va ularga amallarni qo‘llash qulaylashadi. Tadqiqot davomida turli modul va kongruensiya misollari tahlil qilinib, ularning qoidalari va teoremalari asosiy natijalarni shakllantirdi. Masalan, kongruensiyalarni yechishning oddiy algoritmlari orqali tub sonlarni aniqlash, modul bo‘yicha tenglamalarni yechish va sonlar orasidagi ekvivalentlik munosabatlarini o‘rganish amaliy jihatdan samarali ekanligi ko‘rsatildi.Muhokama qismida shuni ta’kidlash lozimki, modulli arifmetika va kongruensiyalar nazariyasi nafaqat nazariy qiziqish uyg‘otadi, balki amaliy masalalarda ham keng qo‘llaniladi. Tadqiqot natijalari shuni ko‘rsatdiki, raqamli kodlash, shifrlash va algoritmik hisoblash jarayonlarida modulli arifmetika asosiy vosita sifatida ishlatiladi. Kongruensiyalar yordamida murakkab tenglamalarni qisqartirish, qoldiq bo‘yicha solishtirishlar va sonlar munosabatlarini tahlil qilish mumkinligi aniqlandi.Shuningdek, tadqiqot davomida olingan natijalar modulli arifmetika va kongruensiyalarning ta’lim jarayonida ham samarali qo‘llanishini ko‘rsatdi. Ularni o‘quvchilar va talabalar uchun amaliy misollar orqali o‘rgatish matematik tafakkur va mantiqiy fikrlashni rivojlantirishga yordam beradi. Natijalar shuni ham ko‘rsatdiki, turli modul va qoldiqlarni o‘rganish orqali murakkab masalalarni bosqichma-bosqich yechish mumkinligi amaliy jihatdan tasdiqlandi.Umuman

olganda, tadqiqot natijalari modulli arifmetika va kongruensiyalar nazariyasining nafaqat matematik bilimlarni boyitishda, balki real hayotdagi masalalarni, xususan, kriptografik algoritmlar, kompyuter hisoblashlari va raqamli tizimlarda qo‘llashda muhim vosita ekanligini tasdiqlaydi. Shu bilan birga, mavzu bo‘yicha yanada chuqur tadqiqotlar olib borish, yangi algoritmlar va yechim usullarini ishlab chiqish istiqbollari mavjudligi aniqlanadi.

Misol 1: $17x \equiv 5 \pmod{23}$ tenglamasini yeching.

1. 17 va 23 tub sonlar, shuning uchun 17 ning 23 moduli bo‘yicha teskari elementi mavjud.
2. $17y \equiv 1 \pmod{23}$ ni yechamiz:

$23 = 1 \times 17 + 6$

$17 = 2 \times 6 + 5$

$6 = 1 \times 5 + 1 \rightarrow 1 = 6 - 1 \times 5$

$5 = 17 - 2 \times 6$

Shu orqali: $1 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17 = 3 \times (23 - 17) - 17 = 3 \times 23 - 4 \times 17$

Demak, $17 \times (-4) \equiv 1 \pmod{23} \rightarrow 17 \times 19 \equiv 1 \pmod{23}$

$x \equiv 19 \times 5 \equiv 95 \equiv 3 \pmod{23}$

Javob: $x \equiv 3 \pmod{23}$

Misol 2: $12x + 7 \equiv 1 \pmod{5}$ tenglamasini yeching.

$12x + 7 \equiv 1 \pmod{5} \rightarrow 12x \equiv -6 \equiv 4 \pmod{5}$

$12 \bmod 5 \equiv 2$, shuning uchun $2x \equiv 4 \pmod{5}$

2 ning 5 moduli bo‘yicha teskari elementi 3, chunki $2 \times 3 \equiv 1 \pmod{5}$

$x \equiv 3 \times 4 \equiv 12 \equiv 2 \pmod{5}$

Javob: $x \equiv 2 \pmod{5}$

Xulosa. Modulli arifmetika va kongruensiyalar nazariyasi sonlar nazariyasi va amaliy matematikada muhim o‘rin egallaydi. Tadqiqot natijalari shuni ko‘rsatdiki, bu nazariya sonlar orasidagi murakkab munosabatlarni soddalashtirish, qoldiq bo‘yicha hisoblashlarni tizimlashtirish va murakkab tenglamalarni yechish imkonini beradi. Kongruensiyalar yordamida modul bo‘yicha tengliklar o‘rganilib, ularni amaliy masalalarga tatbiq etish yo‘llari aniqlanadi, shuningdek, tub sonlarni aniqlash va algoritmik hisoblashlarda qo‘llanilishi amaliy jihatdan samarali ekanligi tasdiqlanadi.Shuningdek, modulli arifmetika va kongruensiyalar nazariyasi zamonaviy texnologiyalar, xususan, raqamli kodlash, kriptografik algoritmlar va kompyuter hisoblashlarida keng qo‘llaniladi. Bu mavzuni o‘rganish matematik tafakkur va mantiqiy fikrlashni rivojlantirishga, shuningdek, real hayotdagi masalalarni hal qilishda nazariy bilimlarni amaliy jihat bilan bog‘lashga imkon beradi.Tadqiqot davomida olingan natijalar shuni ko‘rsatdiki, modulli arifmetika va kongruensiyalarni chuqur o‘rganish nafaqat matematik bilimlarni boyitadi, balki amaliy masalalarni soddalashtirish va ularni samarali yechish imkoniyatini yaratadi. Shu sababli, bu nazariya nafaqat ilmiy qiziqish uyg‘otuvchi, balki amaliy ahamiyatga ega muhim vosita sifatida qadrlanadi.Ushbu tadqiqot asosida kelajakda modulli arifmetika va

kongruensiyalar nazariyasini yanada chuqurroq o‘rganish, yangi algoritmik yechimlar ishlab chiqish va ularni turli sohalarda, xususan, kriptografiya, raqamli tizimlar va kompyuter texnologiyalarida qo‘llash istiqbollari mavjudligi aniqlanadi.

FOYDALANILGAN ADABIYOTLAR

1. Xo‘jayev G‘. – Sonlar nazariyasi asoslari. Toshkent: Fan, 2010.
2. Islomov A. – Algebra va sonlar nazariyasi. Toshkent: O‘qituvchi, 2015.
3. Qodirov B. – Matematik nazariya va amaliy masalalar. Toshkent: Fan, 2012.
4. Toshpulatov N. – Matematika fanidan qo‘llanma. Toshkent: Sharq, 2018.
5. Normatov S. – Modulli arifmetika va kongruensiyalar. Toshkent: Fan va Texnologiya, 2014.
6. Karimov M. – Sonlar nazariyasi va uning amaliy qo‘llanilishi. Toshkent: O‘zbekiston, 2016.
7. Rustamov Sh. – Kongruensiyalar nazariyasi va masalalar yechimi. Toshkent: Fan, 2011.
8. Axmedov T. – Algebraik struktur va modulli tizimlar. Toshkent: O‘qituvchi, 2017.
9. Yo‘ldoshev F. – Matematika fanidan nazariy va amaliy qo‘llanmalar. Toshkent: Fan, 2013.
10. Sobirov J. – Kriptografiya va modulli arifmetika asoslari. Toshkent: Sharq, 2019.