RAQAMLAR NAZARIYASI: MATEMATIKANING “TOJI” VA KRIPTOGRAFIYA SIRLARI

Qudratova Shaxnoza Baxtiyor qizi
Toshkent amaliy fanlar universiteti v.b dotsenti.
Negmatullayeva Amina Murodullo qizi
Toshkent amaliy fanlar universiteti talabasi.
qudratovashahnoza768@gmail.com
https://doi.org/10.5281/zenodo.18635574

Annotasiya. *Ushbu maqolada matematikaning eng qadimiy sohalaridan biri bo‘lgan Raqamlar nazariyasining asosiy tushunchalari, tub sonlar xossasi, modulyar arifmetika va bu nazariyaning zamonaviy kriptografiyadagi (axborot xavfsizligi) roli oddiy tilda tushuntirilgan.*

Maqola keng kitobxonlar ommasi, talabalar va matematikaga qiziquvchilar uchun mo‘ljallangan bo‘lib, fanning ham nazariy, ham amaliy ahamiyatini yoritib beradi

Tayanch so‘zlar: *Natural sonlar, Tub sonlar, Bo‘linish alomatlari, Yevklid algoritmi, Kriptografiya, RSA algoritmi, Modulyar arifmetika, Riman gipotezasi, Matematika tarixi, Butun sonlar.*

Аннотация. *В данной статье простым языком объясняются основные понятия теории чисел, одной из старейших отраслей математики, свойства простых чисел, модульная арифметика и роль этой теории в современной криптографии (информационной безопасности). Статья предназначена для широкой аудитории, студентов и всех, кто интересуется математикой, и подчеркивает как теоретическое, так и практическое значение этой науки.*

Ключевые слова: *Натуральные числа, Простые числа, Свойства делимости, Евклидов алгоритм, Криптография, Алгоритм RSA, Модульная арифметика, Гипотеза Римана, История математики, Целые числа.*

Annotation. *This article explains in simple language the basic concepts of Number Theory, one of the oldest branches of mathematics, the properties of prime numbers, modular arithmetic, and the role of this theory in modern cryptography (information security). The article is intended for a wide audience, students, and those interested in mathematics, and highlights both the theoretical and practical importance of the science*

Key words: *Natural numbers, Prime numbers, Divisibility properties, Euclidean algorithm, Cryptography, RSA algorithm, Modular arithmetic, Riemann hypothesis, History of mathematics, Integers.*

Matematika fanlar ichida eng aniq va mantiqiy fan bo‘lsa, Raqamlar nazariyasi (yoki Sonlar nazariyasi) uning eng qadimiy va jozibador sohasidir. Buyuk matematik Karl Fridrix Gauss "Matematika fanlarning malikasi, raqamlar nazariyasi esa matematikaning malikasidir" deb bejiz aytmagan. Bu soha asosan butun sonlar (Z = {..., -2, -1, 0, 1, 2, ...}) va ularning xossalarini o‘rganadi.

Garchi uzoq vaqt davomida bu fan "sof nazariy" va amaliyotdan yiroq deb hisoblangan bo‘lsa-da, bugungi kunda raqamli iqtisodiyot, internet xavfsizligi va blokcheyn texnologiyalarining barchasi aynan raqamlar nazariyasiga tayanadi.

Raqamlar Nazariyasining Tarixiy Ildizlari

Raqamlar nazariyasi insoniyat sivilizatsiyasi bilan birga shakllangan. Qadimgi Bobil va Misr matematiklari sonlarning ba'zi xossalarini bilishgan.

Biroq, tizimli o‘rganish Qadimgi Gretsiyada boshlangan. Pifagor va uning maktabi: Ular sonlarni shunchaki hisoblash vositasi emas, balki koinotning asosi deb bilishgan. "Hamma narsa bu — son" shiori ostida ular juft, toq, mukammal va do‘stona sonlarni tasniflashgan.

Yevklid: Uning "Ibtido" asarida tub sonlarning cheksizligi isbotlangan va bugungi kunda ham qo‘llaniladigan Yevklid algoritmi (EKUBni topish usuli) bayon etilgan.

Diofant: "Algebra otasi" sifatida tanilgan ushbu olim butun sonli yechimlarga ega tenglamalarni o‘rgangan.

O‘rta asrlarda musulmon dunyosi olimlari, xususan, Al-Xorazmiy va Abu Komil kabi bobokalonlarimiz sonlar ustidagi amallarni algoritmlashtirishga ulkan hissa qo‘shishgan.

Tub sonlar — o‘ziga va birga bo‘linadi, 1 dan katta natural sonlardir.

Tub sonlarning asosiy xususiyatlari:

2 — eng kichik va yagona juft tub son. Qolgan barcha tub sonlar toqdir.

1 soni tub son ham, murakkab son ham hisoblanmaydi.

Har bir natural sonni tub ko‘paytuvchilar bilan ifodalash mumkin.

1 dan 100 gacha bo‘lgan tub sonlar ro‘yxati (jami 25 ta):

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Tub sonlarni topishning eng mashhur usuli — Eratosfen g‘alviri deb ataladi. Kattaroq sonlarni tekshirish uchun WolframAlpha kabi matematik resurslardan foydalanishimiz mumkin.

Arifmetikaning asosiy teoremasi

Har qanday 1 dan katta natural sonni tub sonlarning ko‘paytmasi ko‘rinishida va faqat bir xil usulda yozish mumkin. Masalan:

Bu teorema tub sonlarni barcha sonlarning "qurilish bloklari" yoki "atomlari" ekanligini anglatadi.

Tub sonlar qatorida hech qanday aniq qonuniyat yo‘qdek ko‘rinadi. Ular gohida ketma-ket keladi (masalan, 11 va 13 "egizak tub sonlar"), gohida esa ular orasida millionlab sonlar farqi bo‘lishi mumkin. Riman gipotezasi tub sonlarning qanday taqsimlanganini tushuntirib beruvchi, hozirgacha yechilmagan eng buyuk matematik jumboqdir.

Bo‘linish va Qoldiqli Arifmetika

Raqamlar nazariyasining kundalik hayotdagi eng muhim qismi bu Modulyar arifmetikadir. Buni ko‘pincha "soat arifmetikasi" deb ham atashadi. Agar soat hozir 10:00 bo‘lsa, 5 soatdan keyin soat 15:00 emas, balki 3:00 bo‘ladi. Chunki biz 12 modulli tizimda ishlaymiz:

Ushbu oddiy tushuncha zamonaviy kompyuter texnologiyalarida ma'lumotlarni kodlash va xatolarni tuzatishda (masalan, bank kartalaridagi raqamlarni tekshirishda) ishlatiladi.

Buyuk teoremalar va jumboqlar

Raqamlar nazariyasi o‘zining sodda berilgan, lekin isboti nihoyatda murakkab bo‘lgan masalalari bilan mashhur.

Fermaning buyuk teoremasi — P. Fermaning yunon matematigi Diofantnutt tenglamasi yechimlari musbat butun sonlar bilan ifodalanmaydi, degan da’vosi tasdig‘i (bunda i — ikkidan katta butun son). P. Fermaning bu teoremaning isbotini bilganligi va yozishga joy bo‘lmagani uchun keltirilmagani haqida ma’lumot bergan bo‘lishiga qaramay, bu teoremani ingliz matematigi E. Uayls algebraik geometriyaning murakkab usullarini qo‘llab isbotladi (E. Uayls bu haqida 2002 i. Xitoyda bo‘lib o‘tgan matematiklarning butunjaqon kongressida e’lon qildi).

Bu oddiy gapni isbotlash uchun insoniyatga 358 yil kerak bo‘ldi (1994-yilda Endryu Uayls isbotladi).

Goldbax gipotezasi (taxmini) matematika dunyosidagi eng eski va mashhur hal qilinmagan muammolardan biridir. 1742 yilda Kristian Goldbax bu farazni taklif qildi. Goldbax farazi ikki bo‘limdan iborat. Kuchli Goldbax farazi shuni aytadi: 2 dan katta har bir juft sonni ikki tub son yig‘indisi sifatida ifodalash mumkin.

Masalan, 4=2+2; 10=3+7 yoki 5+5; 28=11+17.

Kuchsiz Goldbax farazi shuni aytadi: 5 dan katta har bir toq sonni uchta tub son yig‘indisi sifatida ifodalash mumkin.Eslatma: Kuchsiz faraz 2013-yilda matematik Harald Xelfgott tomonidan to‘liq isbotlangan deb tan olingan. Hozirgi holat: Kuchli faraz hali ham isbotlanmagan. Matematiklar uni juda katta sonlargacha kompyuterlar yordamida tekshirib ko‘rishgan va u har doim to‘g'ri chiqqan, biroq umumiy matematik isbot topilmagan.Bu muammoni hal qilish uchun Arxiv.org kabi platformalarda ko‘plab ilmiy maqolalar e'lon qilinadi, ammo hozircha hech biri yakuniy akademik tasdiqni olmagan.Kriptografiya (yunoncha “kriptos” — yashirin va “grapho” — yozish) — bu ma'lumotlarning maxfiyligini, butunligini va haqiqiyligini saqlash uchun ularni shifrlash haqida bir fan. Oddiy qilib aytganda, bu ma'lumotni begonalardan himoya qilish maqsadida uni “tushunarsiz” holatga keltirish san'atidir.

Kriptografiya faqat xabarlarni yashirish emas; u to‘rtta asosiy ustunga tayanadi:

Maxfiylik (Confidentiality): Ma'lumotni faqat ruxsati bor shaxslargina o‘qiy oladi.

Butunlik (Integrity): Ma'lumot uzatishda o‘zgarmasligini tekshirish.

Haqiqiylik (Authentication): Jo‘natuvchi o‘zini tasdiqlash. Tasdiqlash jo‘natuvchi aytgan shaxs ekanligini ko‘rsatadi.

Inkor eta olmaslik (Non-repudiation): Ma'lumotni jo‘natgan shaxs keyin 'men yubormaganman' deb ayta olmaydi. Hozirgi kunda kriptografiya asosan ikki yo‘nalishga bo‘linadi:

1. Simmetrik shifrlash (Maxfiy kalitli)

Bu usulda ma'lumotni shifrlash va uni qayta o‘qish (deshifrlash) uchun bir xil kalitdan foydalaniladi.

Afzalligi: Juda tez ishlaydi.

Kamchiligi: Kalitni boshqa tomonga xavfsiz yetkazish qiyin.

Misollar: AES (Advanced Encryption Standard), DES.

Asimmetrik shifrlash (Ochiq kalitli)

Bu yerda ikkita kalit ishlaydi. Ikkita kalit bor: Ochiq kalit (Public key) va Yopiq kalit (Private key).

Ochiq kalit har bir odam uchun ochiq. Ochiq kalit ma'lumotni shifrlashda ishlatiladi.

Mening fikrimcha, yopiq kalit faqat egasida bo‘ladi. Yopiq kalit egasiga ma’lumotni o‘qish imkonini beradi.

Misollar: RSA, ECC. Kriptografiyadan har kuni foydalanamiz, bilmasdan.

Messengerlar: Telegram va WhatsApp'dagi "End-to-end encryption" (uchma-uch shifrlash).

Bank tizimi: Plastik kartalar va onlayn to‘lovlar.

Internet xavfsizligi: Brauzerda sayt manzili yonidagi “qulf” belgisi menandakan.

Kriptovalyutalar: Blockchain texnologiyasi butunlay kriptografiyaga asoslangan.

Bugungi kunda Kvamt kriptografiyasi rivojlanmoqda. Kvamt kompyuterlari kelajakda hozirgi RSA kabi qiyin shifrlarni soniyalarda buzishi mumkin. Bu sababli olimlar “Post-kvant kriptografiyasi” ustida ishlamoqda.

Qiziqarli fakt: Tarixdagi eng mashhur shifrlash qurilmalaridan biri Ikkinchi jahon urushida natsistlar tomonidan ishlatilgan Enigma mashinasi bo‘lgan.RSA algoritmi (Rivest, Shamir, Adleman) - bu asimmetrik kriptografiyaga asoslangan mashhur ochiq kalitli shifrlash usuli. RSA algoritmi xabar yuborish (shifrlash) va elektron imzo (digital signature) uchun keng qo‘llaniladi. RSA algoritmi shifrlash va dekriptlash uchun ochiq va maxfiy kalitlarni ishlatadi.

RSA algoritmi ikkita katta tub sonni tanlaydi, ularning ko‘paytmasini (N) hisoblaydi, keyin Euler funksiyasi yordamida ochiq (e) hamda maxfiy (d) kalitlarni aniqlaydi. Asosiy xususiyatlari Asimmetrik: Ochiq kalit shifrlash uchun, maxfiy kalit dekriptlash uchun mavjud.

Ochiq kalitli sistema: Ochiq kalitni hamma bilan bo‘lishish mumkin, maxfiy kalitni esa faqat egasi saqlaydi. Xavfsizlik: Katta sonlarni tub ko‘paytuvchilarga ajratish qiyinligiga asoslanadi; bu muammo hal bo‘lmaguncha tizim xavfsiz. Ishlatilishi TLS/SSL: Veb-sayt xavfsizligini HTTPS orqali ta’minlaydi. PGP, S/MIME: Elektron pochta shifrlash va imzolash uchun ishlatiladi. IPsec: Tarmoq darajasida xavfsizlikni ta’minlaydi. Qanday ishlaydi (soddalashtirilgan misol).

Sonlar va san’at bir-biriga bog‘liq. Bog‘liq qadimiy, chuqur ildizga ega. Sonlar va san’at uyg‘unligini “Matematik estetika” deb atash mumkin.

San’atda sonlarning qo‘llanilishi bo‘yicha asosiy yo‘nalishlar:

Oltin kesim: Taxminan 1.618 ga teng bo‘lgan Oltin kesim soni tabiatda ham san’atda ham ideal mutanosiblik sifatida tanilgan. Leonardo da Vinchi (Mona Liza) va Salvador Dali kabi rassomlar Oltin kesim nisbatini asarlarini vizual mukammallikka erishish uchun ishlatishgan

Fibonachchi ketma-ketligi: Har bir son o‘zidan oldingi ikki sonning yig‘indisiga teng bo‘lgan (1, 1, 2, 3, 5, 8...) bu qonuniyat musiqiy ritmlarda, arxitektura kompozitsiyalarida va rasm chizishda spiral shakllarni yaratishda ishlatiladi.

Fraktal san’at: Matematik formulalar yaratadi cheksiz takrorlanuvchi geometrik shakllar.

Bugun raqamli san’atda algoritmlar yaratadi murakkab va go‘zal vizual tasvirlar.

Musiqa va Matematika: Musiqa aslini olganda "eshitiladigan matematika"dir. Notalar orasidagi masofa, intervallar, ritm va garmoniya qat’iy matematik hisob-kitoblarga asoslanadi

Islomiy naqshlar: Sharq san’atida, ayniqsa me’morchilikda murakkab geometrik shakllar va simmetriya sonlar uyg‘unligining eng yuqori cho‘qqisi hisoblanadi.

Xulosa qilib aytganda, raqamlar nazariyasi shunchaki sonlar bilan o‘yin emas, deb o‘ylayman, u zamonaviy raqamli dunyoning asosiy poydevori.

Tub sonlarning murakkabligi va modulyar arifmetika qoidalari haqida maqolada gap bor, bugun ular ma'lumotlarni shifrlashda va kiberxavfsizlikda asosiy rol o‘ynaydi. Yevklid davridan boshlab bunday izlanishlar RSA algoritmi orqali endi kundalik hayotimizning bir qismiga aylandi, bu sof matematika va amaliyotning qanchalik bog'liq ekanligini ko‘rsatadi.

Insoniyat tafakkurining eng katta natijalaridan biri raqamlar nazariyasi, garchi biz bo‘linish alomatlari va Yevklid algoritmi kabi narsalarni o‘rgangan bo‘lsak ham.

Riman gipotezasi kabi hali yechimi topilmagan masalalar bor, bu sohaning ufqlari juda keng ekanligini anglatadi, menimcha. Kelajakda kvant hisoblash rivojlanganda, raqamlar nazariyasining yangi tomonlari ochilishi mumkin va kriptografiyada katta o‘zgarishlar bo‘lishi shubhasiz, ammo bu qanday bo‘lishini to‘liq tasavvur qilish qiyin.Raqamlar nazariyasi shunchaki quruq hisob-kitoblar to‘plami emas. Bu insoniyat tafakkurining cho‘qqisi bo‘lib, u koinot sirlarini o‘rganishdan tortib, shaxsiy ma'lumotlarimiz xavfsizligigacha bo‘lgan barcha sohalarni qamrab oladi. Garchi ko‘p sirlari hali ochilmagan bo‘lsa-da, bu fan o‘zining soddaligi va ayni paytda cheksiz chuqurligi bilan yangi avlod matematiklarini chorlashda davom etadi.

Raqamlar nazariyasi haqida o‘ylaganimda, bu matematikaning eng qadimiy qismi bo‘lib, ammo hech qachon eskirib qolmagan degan fikr keladi. Texnologiyalar rivojida u yangi bosqichga chiqdi, xuddi shunday. Menimcha, bu matematik tafakkurning eng go‘zal qismi.

Yana bir narsasi, bu sohada hali ko‘p sirlar bor. Riman gipotezasi yoki tub sonlar orasidagi masofalar haqidagi muammolar yechilmagan.

Umuman, raqamlar nazariyasini o‘rganish faqat matematiklar uchun emas, IT mutaxassislari, muhandislar va mantiqiy fikrlashni yaxshi ko‘ruvchilar uchun ham zarur. Sonlar olami insoniyatga koinotning tartibini ko‘rsatadi, cheksiz qonuniyatlari bilan. Bu doim davom etadi, o‘ylaymanki.

Adabiyotlar:

1. Neal Koblitz - "Raqamlar nazariyasi va kriptografiya kursi"
2. David M. Burton - "Elementar raqamlar nazariyasi"
3. S. X. Sirojiddinov "Algebra va sonlar nazariyasi"
4. Qudratov, B. (2024). O’ZBEKISTONNING VA TOJIKISTON O’RTASIDA SIYOSIY SOHADAGI HAMKORLIK VA HAMFIKRLIK. *Modern Science and Research*, *3*(9), 70-74.
5. Qudratova, S., & Azizova, D. (2024). BOSHLANG’ICH SINF O’QUVCHILARIDA MATEMATIK TASAVVURLARNI SHAKLLANTIRISH. *Modern Science and Research*, *3*(12), 305-311.
6. Atenov, J., & Dustov, M. (2024). Ikki va uch o ‘lchovli shakllarni chizishda amaliy dasturlardan foydalanib talabalarning matematik savodxonligini rivojlantirish. *Modern Science and Research*, *3*(1), 1-3.
7. Sotiboldiyeva, S., & Sadarova, N. (2025). THE SIGNIFICANCE OF FOLK ORAL LITERATURE IN PRIMARY SCHOOL EDUCATION. *International Journal of Artificial Intelligence*, *1*(4), 115-118.