ISSN 2181-3187

SONLAR NAZARIYASI

Shermatova Charosxon
Andijon davlat universiteti Matematika va mexanika fakulteti
Matematika yo'nalishi 4M2-guruh talabasi

Kirish

Asosiy Tamoyillar va Zamonaviy Tatbiqotlar

Sonlar nazariyasi – bu matematikaning eng qadimiy va bir vaqtning o'zida eng zamonaviy tarmoqlaridan biri bo'lib, sonlarning xossalarini va ularning bir-biri bilan munosabatlarini o'rganadi. Bu nazariya qadimgi zamonlardan boshlab olimlarning e'tiborini o'ziga tortib kelgan. Qadimgi yunon matematiklari, jumladan, Pifagor va Evklid, oddiy sonlar va ularning o'ziga xos xususiyatlariga oid dastlabki tadqiqotlarni amalga oshirgan. Hozirgi kunda esa sonlar nazariyasi ko'plab zamonaviy texnologiyalar, jumladan, kriptografiya va algoritmik hisoblashlar asosida yotadi.

Sonlar Nazariyasining Asosiy Tamoyillari

1. Oddiy sonlar va ularning ahamiyati

Oddiy sonlar (prime numbers) – bu 1 va o'zidan boshqa bo'luvchiga ega bo'lmagan sonlar. Ular sonlar nazariyasining asosiy elementlaridan biri hisoblanadi. Evklidning isboti bo'yicha oddiy sonlar cheksiz ko'p bo'lib, ular barcha boshqa butun sonlarni yaratish uchun asosiy "qurilish bloki" hisoblanadi.

Masalan:

1. 2, 3, 5, 7, 11 kabi sonlar oddiy sonlardir.
2. Har qanday butun sonlarni oddiy sonlarning ko'paytmasi shaklida ifodalash mumkin (masalan, $60 = 2 \times 2 \times 3 \times 5$).

2. Sonlarning bo'linishi va Evklid algoritmi

Evklid algoritmi ikki butun sonning eng katta umumiy bo'luvchisini (EKUB) topish uchun ishlatiladi. Bu algoritm nafaqat matematik tadqiqotlar, balki kompyuter hisoblashlari uchun ham muhimdir.

Misol: EKUB(48, 18) = 6, chunki 6 48 va 18 sonlarining eng katta umumiy bo'luvchisidir.

ISSN 2181-3187

3. Modulyar arifmetika

Modulyar arifmetika ("soat arifmetikasi" deb ham ataladi) sonlar nazariyasida keng qo‘llaniladigan tamoyildir. Bu yondashuvda sonlarning bo‘linish qoldiqlari asosida ishlanadi.

Masalan, 17 mod 5 = 2, chunki 17 ni 5 ga bo‘lganda qoldiq 2 bo‘ladi. Modulyar arifmetika kriptografiya, kodlash va kompyuter tarmoqlari uchun asosiy vosita hisoblanadi.

Sonlar Nazariyasining Zamonaviy Tatbiqotlari

1. Kriptografiya va ma’lumotlarni himoya qilish

Sonlar nazariyasi zamonaviy kriptografiyaning, ayniqsa RSA algoritmining asosini tashkil qiladi. RSA shifrlash tizimida ikkita katta oddiy sonni ko‘paytirish orqali hosil qilingan sonlardan foydalaniladi. Ushbu jarayon sonlarni faktorlarga ajratishning murakkabligi sababli xavfsiz hisoblanadi.

2. Kompyuter xavfsizligi va internet texnologiyalari

Hozirgi kunda sonlar nazariyasidan HTTPS protokollari, elektron imzolar va xavfsiz ma’lumot uzatish tizimlarida keng foydalaniladi. Masalan, Diffi-Xellman protokoli orqali shifrlash kalitlari almashinuvi amalga oshiriladi.

3. Kriptovalyutalar va blokcheyn texnologiyalari

Kriptovalyutalar, masalan, Bitcoin, sonlar nazariyasiga asoslangan hash funksiyalari va modulyar arifmetikadan foydalanadi. Bu texnologiyalar ma’lumotlarning xavfsizligini ta’minlash va tranzaksiyalarni tasdiqlashda ishlatiladi.

4. Signal va ma’lumotlarni qayta ishlash

Sonlar nazariyasi turli xil kodlash tizimlari, xususan, ma’lumotlarni uzatish va siqishda foydalaniladi. Shanonning axborot nazariyasi va Hamming kodlari sonlar nazariyasiga asoslangan.

5. Ilmiy tadqiqotlar va muhandislik

ISSN 2181-3187

Sonlar nazariyasi kvant kompyuterlash va fizika sohalarida ham foydalanilmoqda. Ayniqsa, kvant kriptografiyasi sonlar nazariyasidagi tamoyillar asosida rivojlanmoqda.

Sonlar Nazariyasi: Asosiy Tamoyillar va Zamonaviy Tatbiqotlar

Sonlar nazariyasi – bu matematikaning eng qadimiy va bir vaqtning o‘zida eng zamonaviy tarmoqlaridan biri bo‘lib, sonlarning xossalarini va ularning bir-biri bilan munosabatlarini o‘rganadi. Bu nazariya qadimgi zamonlardan boshlab olimlarning e’tiborini o‘ziga tortib kelgan. Qadimgi yunon matematiklari, jumladan, Pifagor va Evklid, oddiy sonlar va ularning o‘ziga xos xususiyatlariga oid dastlabki tadqiqotlarni amalga oshirgan. Hozirgi kunda esa sonlar nazariyasi ko‘plab zamonaviy texnologiyalar, jumladan, kriptografiy va algoritmik hisoblashlar asosida yotadi.

Sonlar Nazariyasining Asosiy Tamoyillari

1. Oddiy sonlar va ularning ahamiyati

Oddiy sonlar (prime numbers) – bu 1 va o‘zidan boshqa bo‘luvchiga ega bo‘lmagan sonlar. Ular sonlar nazariyasining asosiy elementlaridan biri hisoblanadi. Evklidning isboti bo‘yicha oddiy sonlar cheksiz ko‘p bo‘lib, ular barcha boshqa butun sonlarni yaratish uchun asosiy "qurilish bloki" hisoblanadi.

Masalan:

1. 2, 3, 5, 7, 11 kabi sonlar oddiy sonlardir.
2. Har qanday butun sonlarni oddiy sonlarning ko‘paytmasi shaklida ifodalash mumkin (masalan, $60 = 2 \times 2 \times 3 \times 5$).

2. Sonlarning bo‘linishi va Evklid algoritmi

Evklid algoritmi ikki butun sonning eng katta umumiy bo‘luvchisini (EKUB) topish uchun ishlatiladi. Bu algoritm nafaqat matematik tadqiqotlar, balki kompyuter hisoblashlari uchun ham muhimdir.

Misol: EKUB(48, 18) = 6, chunki 6 48 va 18 sonlarining eng katta umumiy bo‘luvchisidir.

3. Modulyar arifmetika

ISSN 2181-3187

Modulyar arifmetika ("soat arifmetikasi" deb ham ataladi) sonlar nazariyasida keng qo‘llaniladigan tamoyildir. Bu yondashuvda sonlarning bo‘linish qoldiqlari asosida ishlanadi.

Masalan, 17 mod 5 = 2, chunki 17 ni 5 ga bo‘lganda qoldiq 2 bo‘ladi. Modulyar arifmetika kriptografiya, kodlash va kompyuter tarmoqlari uchun asosiy vosita hisoblanadi.

4. Fermatning kichik teoremasi va Eylerning teoremasi

Bu teoremalar oddiy sonlar va modulyar arifmetika bilan bog‘liq bo‘lib, ularning ko‘plab amaliy qo‘llanmalari mavjud. Fermatning kichik teoremasi shuni ko‘rsatadiki, agar ppp oddiy son bo‘lsa va a p ga bo‘linmasa, unda:

$$a^{P-1} = 1 \quad (\text{mod} \quad p)$$

Sonlar Nazariyasining Zamonaviy Tatbiqotlari

1. Kriptografiya va ma’lumotlarni himoya qilish

Sonlar nazariyasi zamonaviy kriptografiyaning, ayniqsa RSA algoritmining asosini tashkil qiladi. RSA shifrlash tizimida ikkita katta oddiy sonni ko‘paytirish orqali hosil qilingan sonlardan foydalaniladi. Ushbu jarayon sonlarni faktorlarga ajratishning murakkabligi sababli xavfsiz hisoblanadi.

2. Kompyuter xavfsizligi va internet texnologiyalari

Hozirgi kunda sonlar nazariyasidan HTTPS protokollari, elektron imzolar va xavfsiz ma’lumot uzatish tizimlarida keng foydalaniladi. Masalan, Diffi-Xellman protokoli orqali shifrlash kalitlari almashinuvi amalga oshiriladi.

3. Kriptovalyutalar va blokcheyn texnologiyalari

Kriptovalyutalar, masalan, Bitcoin, sonlar nazariyasiga asoslangan hash funksiyalari va modulyar arifmetikadan foydalanadi. Bu texnologiyalar ma’lumotlarning xavfsizligini ta’minlash va tranzaksiyalarni tasdiqlashda ishlatiladi.

4. Signal va ma’lumotlarni qayta ishlash

ISSN 2181-3187

Sonlar nazariyasi turli xil kodlash tizimlari, xususan, ma’lumotlarni uzatish va siqishda foydalaniladi. Shanonning axborot nazariyasi va Hamming kodlari sonlar nazariyasiga asoslangan.

5. Ilmiy tadqiqotlar va muhandislik

Sonlar nazariyasi kvant kompyuterlash va fizika sohalarida ham foydalanilmoqda. Ayniqsa, kvant kriptografiyasi sonlar nazariyasidagi tamoyillar asosida rivojlanmoqda.

Sonlar Nazariyasidagi Dolzarb Muammolar

1. **Oddiy sonlarni topish va tekshirish algoritmlari**
Oddiy sonlarni aniqlash algoritmlari, xususan, katta sonlar uchun samarali usullarning izlanishi davom etmoqda.
2. **Riman gipotezasi**
Bu nazariyada hali ham hal qilinmagan eng qiyin masalalardan biri bo‘lib, oddiy sonlarning taqsimlanishini tushunishga yordam beradi. Riman gipotezasi isbotlansa, u sonlar nazariyasida ulkan yutuq bo‘ladi.

Xulosa

Sonlar nazariyasi – bu matematikaning eng chuqur va keng qamrovli yo‘nalishlaridan biri. Uning asosiy tamoyillari oddiy va murakkab sonlar bilan ishlashga asoslangan bo‘lsa-da, amaliy qo‘llanmalari zamonaviy dunyoda juda muhim o‘rin egallaydi. Internet xavfsizligidan boshlab, ilmiy tadqiqotlar va texnologik taraqqiyotga qadar sonlar nazariyasi ko‘plab sohalarda inqilobiy o‘zgarishlarga asos bo‘lmoqda. Oddiy sonlarning xossalaridan tortib, modulyar arifmetikadagi algoritmlargacha bo‘lgan tamoyillar zamonaviy texnologiyalarning xavfsizligini ta’minlaydi. Internet orqali ma’lumot uzatish, moliyaviy tranzaksiyalarni himoya qilish, shuningdek, blokcheyn texnologiyalaridagi kriptovalyutalar sonlar nazariyasiga asoslangan. Ayniqsa, Riman gipotezasi kabi hal qilinmagan masalalar bu nazariyaning ilmiy dunyodagi ahamiyatini yana-da oshiradiSonlar nazariyasining universal ahamiyati uni nafaqat matematiklar, balki muhandislar, dasturchilar va fiziklar uchun ham muhim qiladi. Hozirgi davrda bu fan nafaqat nazariy muammolarni hal qilish, balki real hayotdagi murakkab muammolarni yechishda ham asosiy vosita hisoblanadi.Ushbu fan nafaqat nazariy bilimlarni boyitadi, balki kundalik hayotda ham dolzarb masalalarni yechishda asosiy

rol o‘ynaydi. Shu sababli, sonlar nazariyasini o‘rganish nafaqat matematiklar, balki texnologiya va muhandislik sohasida ishlayotgan har bir kishi uchun muhimdir.

FOYDALANILGAN ADABIYOTLAR

1.Нишонов Туланмирза Сойибжонович. Эҳтимоллар назарияси фанини ўқитишда назария билан амалиётнинг боғлиқлик тамойилидан фойдаланиш имкониятлари. Journal of innovations in pedagogy and psychology, Vol. 7, Issue 3, 2020, pp.91-96.

2. Nishonov T.S. Professional approach to teaching of elements of probability theory for students of economics. Наука и образование сегодня № 12 (59), 2020. 85-87 pp.

3.Ахлимирзаев А., Нишонов Т.С. Роль и значение практическо-профессионального подхода обучения теории вероятностей и математической статистики в подготовке будущих экономистов // Universum: психология и образование : электрон. научн. журн. 2021. 2(80). 12-17 с.to‘plami.

4. **Evklid** – *"Elementlar"* (O‘rta asr yunon matematikasining asosiy asari).
Al-Xorazmiy – *"Hisob al-jabr val-muqobala"* (Algebra fanining boshlang‘ich asosi).

5. Nyuton, I. va Leybnits, G. – Differensial va integral hisoblash bo‘yicha asarlar.
Axundov, T. – *"Matematik tahlil asoslari"* (O‘quv qo‘llanma, zamonaviy matematik tadqiqotlar bo‘yicha).

6.Zeldovich, Ya. B. – *"Matematika va uning qo‘llanilishi"* (Ilmiy-ommabop nashr).
Xorijiy universitetlarning ochiq darsliklari: Massachusetts Institute of Technology (MIT) – *"OpenCourseWare: Mathematics"*.

7.O‘zbekiston Fanlar Akademiyasi Nashrlari – Matematika rivoji va qo‘llanilishi haqida ilmiy maqolalar.
Kapitsa, P. L. – *"Matematikaning hayotiy o‘rni"* (ilmiy-ommabop darslik).

8.Kriptografiya asoslari: Rivest, R. L., Shamir, A. va Adleman, L. – RSA algoritmlari haqida ilmiy maqola.

9.Andijon Davlat Universiteti uchun maxsus darsliklar va ilmiy maqolalar