O’QUVCHILARGA TUB VA MURAKKAB SONLARNI O’QITISH JARAYONIDA KASBIY QIZIQISHLARINI OSHIRISHGA QARATILGAN MATEMATIK MA’LUMOTLAR BILAN TANISHTIRISH

[1]A.A.Akmalov, [2]D.A.Abduvahobov

[1]Nizomiy nomidagi TDPU Matematika va uni o’qitish metodikasi kafedrasi dotsenti, p.f.n.

[2]Nizomiy nomidagi TDPU Matematika va uni o’qitish metodikasi kafedrasi o’qituvchisi

https://doi.org/10.5281/zenodo.8051985

Annotatsiya. *Matematika tarixiga nazar solinsa har bir qilingan ish asosi hayotiy vaziyatdagi muammolarni hal etishga qaratilgandir. Eng oddiy misol sifatida sanashda ishlatiladigan sonlarni keltirish mumkin. Bu orqali nafaqat qadimdagi muammolarning balki hozirgi kunda ham amaliyotda ko’plab muammolar yechimi bo’lib kelmoqda. Hozirgi axborot-kommunikatsion vositalar rivojlanayotgan bir davrda matematikani o’qitish asosida ularga matematikaning hayotiy vaziyatlarda qo’llash imkoniyati mavjud ekanligini tushuntirish lozim.*

Kalit so’zlar: *o’quvchi, tub son, murakkab son, kasbiy qiziqish, matematika.*

Hayot va matematikaning o’zari integratsiyasini matematika ta’limida amalga oshirish asosiy muammolardan biri bo’lib kelmoqda. Bu jarayonda matematik bilimlar berishda mavzular uzviyligini ta’minlash, o’quvchilarning yosh psixologik imkoniyatlarini hisobga olish, misol va masalalarda soddadan murakkabga tomon tuzilishi, amaliy va kasbiy masalalarni uyg’unlashtirish masalalarini keltirish mumkin. Xususan, Prezidentimizning 2020-yil 7-maydagi “Matematika sohasidagi ta’lim sifatini oshirish va ilmiy-tadqiqotlarni rivojlantirish chora-tadbirlari to’g’risida” gi PQ-4708 qarorida shunday keltirilgan: “Umumta’lim maktablarida matematika darsliklari o’quvchilarning yoshiga nisbatan fanni o’zlashtirishni qiyinlashtiruvchi murakkab masalalardan iborat va boshqa fanlarda o’tiladigan mavzular bilan uyg’unlashitirilmagan”

Matematika ta’limida o’rgatiladigan bilimlar tizimi turli fanlarda shuningdek hayotning turli sohalarida keng qo’llaniladi. O’quvchilarni kasbiy sohalarga yo’naltirishda aynan matematikaning tatbiqi tomonlaridan foydalanish talab etiladi. Bunda o’quvchilarga matematik bilimlar bilan bir qo’llanilish sohalari ham keltirib o’tilishi maqsadga muvofiqdir. Ulardan biri bo’lgan tub va murakkab sonlarning harbiy sohaga qo’llanishiga e’tibor qaratsak. Umumta’lim maktablarida “Tub va murakkab sonlar” mavzusi 6-sinfda o’rgatiladi va bu jarayonda natural sonlar to’plamida qaraladi. Keyinchalik EKUB va EKUK mavzulari o’rgatiladi lekin algebra va sonlar nazariyasining asosiy tushunchalaridan biri bo’lgan “Taqqoslamalar” oliy ta’limda davom ettiriladi. Keltirilgan mavzular o’zaro aloqadorlikda kriptografiyada qo’llaniladi.

Ta’rif. p-butun son 0 va yo 1 dan farqli bo’lib, faqat va faqat yo 1 va yo p bo’luvchilarga ega bo’lsa, u holda p-butun son ***tub son*** deyiladi.

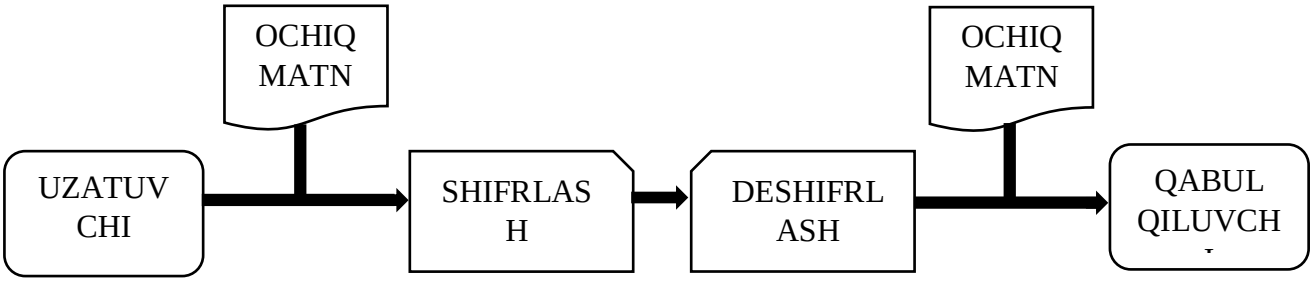
Tub sonlarga misol: -5, -3, -2, 2, 3, 5

Ta’rif. a-butun son 0 va yo 1 dan farqli bo’lib, yo 1 va yo a bo’luvchilardan tashqari yana bo’luvchilarga ega bo’lsa, u holda a-butun son ***murakkab son*** deyiladi.

Murakkab sonlarga misol: -6, -4, 4, 6, 8, 9

Ta’rif. Z-butun sonlar halqasi bo’lib, m≥1 natural son bo’lsin. Agar Z halqaga tegishli a va b sonlarni m natural songa bo’lganda hosil bo’lgan qoldiqlar teng bo’lsa, yoki a-b ayirma m ga bo’linsa, u holda a va b son m modul bo’yicha taqqoslanadi deyiladi va u $a \equiv b(\mathrm{mod} m)$ ko’rinishida belgilanadi.

Kriptografiya – grekcha so’zdan olingan bo’lib, “maxfiy yozish” degan ma’noni anglatadi. Qo’llanilishiga ko’ra esa biror ma’lumotni maxfiy saqlash va himoyalash ishlarini amalga oshirishda xizmat qiladi. Bu jarayonda kriptografik usullar ko’plab maxfiylik imkoniyatlarini yaratib beradi. Ochiq ma’lumotlarni maxfiy saqlash va himoyalash quyidagicha amalga oshiriladi: (1-chizma)



1-chizma

Buning uchun Polig-Xelman, Mak-Elis, Rabin kabi ochiq kalitli shifrlash algoritmlaridan foydalaniladi. D.M [illegible] “Sonlar nazariyasi elementlarining assimmetrik kriptotizmlar asoslarida c [illegible] mli metodik qo’llanmasida Diffi va Xellmanning kalitlarni ochiq taqsimlash sistemasi algoritmidan foydalanilib ko’rsatilgan misolni keltiraylik:

Misol. Agar

p =13, g = 7

bo‘lsa, u holda Alisa va Bob uchun umumiy kalitni toping.

Yechish. Alisa va Bob quyidagi ketma-ketlikni amalga oshiradi:

1) Alisa tasodifiy x-soni, masalan $x=85$ tanlaydi va

$X= g^x(\text{mod } p) =7^{85}(\text{mod } 13) =(7^{13-1})^7 *7(\text{mod } 13)=1^7 *7 (\text{mod } 13)= 7$

qiymatni Bobga ochiq aloqa tarmog‘i orqali uzatadi.

2)Bob ham tasodifiy y - soni, masalan $y = 163$ tanlaydi va

$Y = g^y(\text{mod } p) = 7^{163} (\text{mod } 13)= (7^{13-1})^{13} * 7^7 (\text{mod } 13)= 1^{13}* 7^7(\text{mod } 13)= =49*49*49*7(\text{mod } 13)= 10*10*10*7(\text{mod } 13)= 6(\text{mod } 13) = 6$

qiymatni Alisaga ochiq aloqa tarmog‘i orqali uzatadi.

3)Alisa esa quyidagi qiymatni hisoblaydi

$K_1 = Y^x (\text{mod } p) =6^{85} (\text{mod } 13) =(6^{13-1})^7 * 6(\text{mod } 13)= 1^7*6(\text{mod } 13) = 6.$

4) Bob esa quyidagi qiymatni hisoblaydi

$K_2 =X^y (\text{mod p}) = 7^{163} (\text{mod } 13)= (7^{13-1})^{13} * 7^7 (\text{mod } 13)= 1^{13} * 7^7 (\text{mod } 13)= 6$

Demak,

$$K_1 = K_2 = 6$$

yani, Alisa va Bob uchun umumiy aloqa kaliti $K = 6$ ekan.

Misoldan ravshanki, matematikaning harbiy sohada mavjud bo’lib uning qo’llanishini esa maktab davridan oddiy elementlardan o’rgatib borish lozim. Yuqorida keltirilgan ma’lumotlarga ko’ra ma’lumotlarni maxfiy saqlashda sonlar nazariyasi elementlaridan foydalaniladi va bu ma’lumotni o’quvchilarga og’zaki yetkazishning o’zi ularning matematikaga bo’lgan qiziqishlarini hamda harbiy sohaga bo’lgan intilishlarini yanada oshiradi. Matematikaning real holatlarda mavjud muammolarni hal etishga qaratilgan tatbiqlari bilan o’quvchilarni tanishtirib borish esa ularning matematik va kasbiy kompetensiyalarini ham shakllantirib boradi.

REFERENCES

1. Куликов Л.Я. – Алгебра и теория чисел: Учеб. Пособия для педагогических институтов. – М.: Высш. Школа, 1979. -559 с.
2. Yunusova D. Algebra va sonlar nazariyasi. Oliy o’quv yurtlari uchun o’quv qo’llanma. – T.: «ILM ZIYO», 2009. -320 b.
3. КУРЬЯЗОВ Д.М. Сонлар назарияси элементларининг асимметрик криптотизмлар асосларида қўлланишлари. Т.: -2007, 76 б.