FAN, TA'LIM VA AMALIYOT INTEGRATSIYASI

ISSN: 2181-1776

**Z . Zaparov**

*Andijon qishloq xo'jaligi va agrotexnologiyalar instituti o'qituvchisi*

# TUB SONLARNI ANIQLASHNING AYRIM USULLARI

**Аннотация**

Ushbu maqolada tub sonlarni hosil qiluvchi bir nechta xususiy formulalar keltirilgan. Bu formulalarning barchasi xususiy formulalar bo'lib, bu formulalar bir nechta tub sonlar uchungina o'rinlidir. Tub sonlarni aniqlaydigan umumiy formula haligacha matematik olimlar tomonidan topilmagan. Ushbu maqolada tub sonlarni topish formulasi haqida so'z yuritiladi.

**Kalit so'zlar:** Tub son, murakkab son, o'zaro tub sonlar, eng katta umumiy bo'luvchi, murakkab sonni tub ko'paytuvchilarga ajratish, bo'luvchi, bo'linuvchi, Eratosfen g'alviri.

## KIRISH

Dastlab tub sonlar haqida qisqacha to'xtalib o'tamiz. Tub sonlar 1 dan va o'zidan boshqa bo'luvchilarga ega bo'lmagan, 1 dan katta butun musbat sonlardir. Ular quyidagi sonlardir: 2, 3, 5, 7,...va hokazo. 1 dan katta har qanday butun son yagona usulda Tub sonlar ko'paytmasiga yoyiladi.Tub sonlarning cheksiz ko'p ekanligini birinchi marta Yevklid isbotlagan.

Qadim zamondan buyon matematik olimlar tub sonlarning umumiy formulasini topish ustida bosh qotirib kelmoqdalar.

Bunday formulalardan juda ko'p taklif qilingan bo'lsada, ularning hech biri n ning hamma qiymatlari uchun o'rinli bo'lmagan. Quyida bunday formulalarning ayrimlarini keltiramiz [1]:

## ADABIYOTLAR TAHLILI VA METODOLOGIYA

Matematika faniga qiziqish uyg‘otish, mantiqiy fikrlashni yanada oshirish uchun o‘qituvchilar ba’zan nostandart masalalardan foydalanishadi.Nostandart masalalar, albatta, o‘quvchidan alohida yondashishni, o‘rganilgan qoidani yoki formulani yanada chuqurroq bilishni talab etadi.Biz bu maqolada tub sonlarni aniqlashning bir necha usullarini ko‘rib chiqamiz.

1. $n^2-n+41$ ko‘phad n=0,1,2,3,..,40 bo‘lganda tub son bo‘lib, n=41 bo‘lganda murakkab son hosil bo‘ladi. $n^2-n+41$formula yordamida hosil qilinadigan 2348 ta sonning yarmi tub son ekanligi ko‘rsatilgan. Shunday sonlar ichida millionning 0,475 qismini tub sonlar tashkil qilishi ko‘rsatilgan. $n^2-n+a$ifoda a>41 va n=1,2,3,…,a–2 bo‘lganda tub sonni beradimi, degan savol qo‘yilgan edi. Bu savolga hozirgacha to‘la javob yo‘q. Ammo a=3,5,11,17 bo‘lganda $n^2-n+a$ tub son bo‘lishi isbotlangan.

2. $2n^2+29$ ko‘phad n=0,1,2,3,..,28 bo‘lganda tub son bo‘lib, n=29 bo‘lganda murakkab son hosil bo‘ladi.

3. $n^2+n+17$ko‘phad n =0,1,2,3,…,16 bo‘lganda tub son n=17 da esa murakkab son hosil bo‘ladi.

4. Buyuk fransuz olimi Ferma (1601-1665 yy) $2^{2^n}+1$sonni har qanday natural n son uchun tub son bo‘lishini ko‘rsatib bergan. U 0,1,2,3,4 kabi qiymatlarni berib 3,5,17,257,65537 kabi tub sonlar hosil qilgan edi. n=5 bo‘lganda $2^{2^n}+1$soni juda katta son bo‘lgani uchun Ferma bu sonni tub yoki murakkab ekanligini aniqlay olmagan. 1739-yilda Eyler bu sonning murakkab ekanligini aniqladi.

5. Angliyalik matematik Risel Xans (1970-yilda) 4943+600708s ifoda s=0,1,2,3,…,12 bo‘lganda tub son bo‘lishini: 429983158710+k ifoda esa k=11,13,17,19,23,37,41,43,47,53,59 bo‘lganda tub son bo‘lishini ko‘rsatdi.

## MUHOKAMA VA NATIJALAR

**Masalaning qo‘yilishi.** Berilgan sonni ko‘paytuvchilarga ajratish sonlar nazariyasining eng dastlabki masalalaridan biri hisoblanadi. Berilgan sonni (yoki to‘plamni) biror amal yoki xususiyatga ko‘ra uning tashkil etuvchilari orqali ifodalanishi, shu sonni (yoki to‘plamni) faktorlash (ajratish) deyiladi. Sonni ko‘paytuvchilarga ajratish qiyin jarayon emas, ammo ko‘paytuvchilarga ajratilishi kerak bo‘lgan sonning qiymati kattalashib borishi bilan, uni ko‘paytuvchilarga ajratish jarayoniga sarflanadigan vaqt ham ko‘payib boradi. Shunday bo‘lsada, ko‘paytuvchilarga ajratish jarayonini tezlashtiruvchi quyidagi algoritmlar mavjud [2]:

1. Elliptik egri chiziq usuli–o‘nlik sanoq tizimida tub ko‘paytuvchilarining razryadi (raqamlari soni) 43 tadan ko‘p bo‘lmagan sonlarni ko‘paytuvchilarga ajratishda foydalanilgan;
2. Pollardning Monte-Karlo usuli–amalda kam ishlatiladi;
3. Uzluksiz kasrlar usuli–qo‘llashga ko‘p vaqt sarflanadi;
4. Tanlab bo‘lish usuli–eng dastlabki usullardan bo‘lib, ko‘paytuvchilarga ajratilishi kerak bo‘lgan sonning kvadrat ildiziga teng va undan kichik bo‘lgan har bir tub sonni berilgan sonni qoldiqsiz bo‘lishi yoki bo‘lmasligi tekshirib chiqilishi natijasida, berilgan sonning tub ko‘paytuvchilari aniqlanadi.

5. Sonli maydon umumiy g‘alvir usuli –o‘nlik sanoq tizimida 110 ta va undan ko‘p raqamli sonlarni ko‘paytuvchilarga ajratishning ma’lum bo‘lgan eng samarali (tez, kam vaqt sariflanadigan) algoritmi;
6. Kvadratik g‘alvir usuli–o‘nlik sanoq tizimida 110 tadan kam bo‘lmagan razryadli (raqamli) sonlarni ko‘paytuvchilarga ajratishning ma’lum bo‘lgan eng samarali (tez va kam vaqt sarflanadigan) algoritmi;

Axborot texnologiyalarining ma’lumotlarni kodlashtirish, shifrlash, siqish va ishonchli uzatish masalalari yechimlarida xarakteristikasi tub sondan iborat bo‘lgan chekli maydonlarda hamda xarakteristikasi n tub sonlar ko‘paytmasidan iborat $n = p \cdot q$ bo‘lib, p va q tub sonlari noma’lum bo‘lgan chekli maydonlarda amallar bajarishga asoslanadi [3- 6].

Xususan tub sonlarning amaliy tadbiqlari bilan bog‘liq quyidagi texnologiyalarni keltirish mumkin.

**Modul n bo‘yicha kvadrat ildiz.** Agarda maydon xarakteristikasini ifodalovchi n soni ikkita tub sonning ko‘paytmasidan iborat bo‘lsa, u holda sonning kvadrat ildizini modul n bo‘yicha topish masalasini yechish n sonini ko‘paytuvchilarga ajratish masalasini yechish hisoblash nuqtai nazaridan teng kuchli masalalar hisoblanadi.Ya’ni, maydon xarakteristikasini ifodalovchi n sonining ko‘paytuvchilari ma’lum bo‘lsa, berilgan ixtièriy sonning kvadrat ildizini modul n bo‘yicha hisoblash qiyinchilik tug‘dirmaydi, aks holda hisoblashlar n sonining tub ko‘paytuvchilarini topish masalasi kabi murakkabliklarni o‘z ichiga oladi. Maydon xarakteristikasi yetarlicha katta bo‘lganda kriptobardoshliligi kvadrat ildizni hisoblash masalasining murakkabligiga asoslangan ochiq kalitli kriptoalgoritmlar mavjud.

**Tub sonlar generasiyasi (ishlab chiqarish).** Ochiq kalitli kriptoalgoritmlar asoslari yaratilishida tub sonlarning xossalaridan foydalaniladi. Biror berilgan sonni tub ko‘paytuvchilarga ajratish, uni tub yoki tub emasligini aniqlashga nisbatan murakkab bo‘lgan masala. Yetarli katta razryaddagi toq sonni tasodifiy tanlab olib, uni ko‘paytuvchilarga ajratish bilan tub yoki tub emasligini aniqlashdan ko‘ra, uni tubligini biror mavjud usul bilan tekshirish osonroq. Buning uchun turli ehtimollik testlari mavjud bo‘lib [2] sonning tubligini berilgan darajadagi ishonch bilan aniqlab beradi. Kriptobardoshliligi yetarli darajada katta razryadli sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga asoslangan ochiq kalitli kriptoalgoritmlar mavjud [3-6].

**Masalaning yechimi.** Yuqorida yetarli katta sonni tub yoki tub emasligini aniqlashning yagona formulasi yo‘qligi, mavjud usullar katta hajmdagi hisob-kitoblarni talab qilib hisoblash va vaqt bilan bog‘liq murakkabliklar keltirib chiqaradi. Yetarli katta tub sonlarni axborot texnologiyalaridagi tadbiqlari sohalari haqida so‘z yuritilganda yuqoridagi fikr va mulohazalar yetarli katta tub sonni topishning samarali usullarini yaratish dolzarb ilmiy tadqiqot ishlardan ekanligini asoslaydi. Quyidagi tasdiq ushbu yo‘nalishdagi ilmiy tadqiqot ishlari natijasidir:

**Tasdiq.** Biror natural son berilgan bo‘lib, $2 \le n \le \left[\frac{N}{2}\right]$, bu yerda $\left[\frac{N}{2}\right]$ bo‘linmaning butun qismini anglatadi, tengsizlikni qanoatlantiruvchi ixtiyoriy natural n son uchun (N–m)ayirma va m sonlari birdan farqli umumiy bo‘luvchiga ega bo‘lmasa, berilgan N soni tub sonbo‘ladi va aksincha.

Bu tasdiqda keltirilgan shart zaruriylik va yetarlilik shartlari hisoblanadi.Shuning uchun tasdiqni teorema ko‘rinishida quyidagicha ham ifodalash mumkin.

**Teorema.** Biror ixtiyoriy $N=2n+1$ natural son tub bo‘lishi uchun, $2\le m\le n$ tengsizlikni qanoatlantiruvchi ixtiyoriy natural m son va (N–m)-ayirma birdan farqli umumiy bo‘luvchiga ega bo‘lmasligi zarur va yetarlidir.

**Zaruriyligi.** Berilgan $N=2n+1$ natural son tub bo‘lsin. U holda (N–m) va m sonlarining ixtiyoriy ushbu $2\le m\le n$ tengsizlikni qanoatlantiruvchi m larda o‘zaro tubligini (ya’ni birdan farqli umumiy bo‘luvchiga ega emasligini) ko‘rsatiladi.Haqiqatan ham, N soni tub bo‘lsa, bu N=k·m, k=const, ko‘rinishda ifodalanmaydi. Bundan esa N–m=k·m–m tenglik birorta ham m da o‘rinli bo‘lmaydi. Shuning uchun (N–m) - ayirma va tengsizlikni qanoatlantiruvchi m sonlari o‘zaro tubdir.

**XULOSA**

Xulosa o‘rnida shuni aytish mumkinki, $N=2n+1$ soni berilgan bo‘lib, $2\le m\le n$ tengsizlikni qanoatlantiruvchi m lar uchun (N–m) va m sonlari o‘zaro tub bo‘lsa, N soni tub sondir.

Barcha $2\le m\le n$ tengsizlikni qanoatlantiruvchi m lar uchun (N–m) va m sonlari o‘zaro tub bo‘lib, ya’ni (N–m) va m sonlari eng katta umumiy bo‘luvchisi birga teng ((N–m),m)=1 bo‘lganda, $N=2n+1$ tub bo‘lmasin deb faraz qilinadi. U holda N soni biror $q_1,q_2,q_3,q_4...q_l$ sonlari ko‘paytmasi ko‘rinishida ifodalanadi. Shuningdek m soni ham $p_1,p_2,p_3,p_4...p_d$ sonlari ko‘paytmasida ifodalanib, $p_i$ va $q_j$ larni biror juftligida $p_{i_0}=q_{j_0}$ bo‘ladi.Bu degani ((N–m),m)=1 shartga zid. Bu ziddiyat ((N–m),m)=1 bajarilganda $N=2n+1$- tub bo‘lmasin degan farazdan kelib chiqdi. Bundan $N=2n+1$ tub ekanligi kelib chiqadi. Shuning bilan teorema isbotlandi.

2018 yil 7 yanvar kuni yangi tub son aniqlandi. U 23 millionta raqamdan iborat. Matematikada topilgan yangi tub sonni yozish uchun 7 mingta sahifadan iborat kitob kerak bo‘ladi. Bu yangi tub son 23249425 ta raqamdan iborat. Topilgan yangi tub son Marsenn (fransiyalik matematik) sonlariga tegishlidir, ya’ni bunda sonni 2 ning n-darajasi minus 1 ya’ni $2^n-1$ko‘rinishida tasvirlash mumkin.Yangi topilgan tub sonni esa 2 ning 77232917-darajasi minus 1 ya’ni $2^{77232917}-1$ko‘rinishida yozish mumkin. Shu sababli yangi songa M77232917 belgisi berildi. Bu son Marsenn sonlariga kiruvchi 50-son bo‘ldi.

**REFERENCES**


1. Аминов И.Б., Эштемиров С., Суяров А.М.-Мапле муҳитида математик масалаларни ечиш(услубий қўлланма). Самарқанд 2014.156 бет.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд. – М.: Гелиос АРВ, 2002. – с. 480
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2003. – с. 816
4. Ягудаев Б.Й. Ажойиб сонлар оламида. – Т.: ―Ўқитувчи‖, 1973. – 232 бет.
5. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. – Т.: ―Ўзбекистон маркаси‖, 2009. – 434 бет.
6. Акбаров Д.Е., Мухтаров Ф.М, Сиддиқов А.А. Криптотахлил масалаларига тизимли ёндашув асослари ва уларни ечиш усуллари. – Т.: ―Фарғона‖, 2014. – 142 бет.

7. Z.Zaparov, R.Jo‘raqulov – “O‘qitishda tajribalar: Soddalik va qiziqarlilik” ACADEMIC RESEARCH IN EDUCATIONAL SCIENCES VOLUME 2 | ISSUE 2 | 2021, 700-706 betlar.
8. БА Кулматова, ДА Буранова, ЗА Запаров.- Способы защиты от интернет-мошенничества, Научно-методический журнал Academy 2019 г 78-80 ст.
9. З.Запаров., Б.Эгамбердиева «Адаптивная система обучения» Перспективы развития науки и образования в современных экологических условиях с. Соленое займище, 18–19 мая 2017 года. 1054-1056 ст.