Natural sonni tub ekanligini aniqlashda tub sonlarga bo`linish alomatlaridan foydalanish.

Nuriddinov J.

Jamiyatning bugungi kundagi taraqqiyot darajasi uchun hos hususiyatlar katta hajmdagi ma'lumotlarni qayta ishlash bo'lib, bu albatta diskret almashtirishning matematik modellarini qanday darajada ishlab chiqilganligiga va hisoblash texnikalarining taraqqiyoti bilan bog'liq. Ta'kidlash joizki, kompyuter tarmoqlari va elektron hujjat almashinuvi texnalogiyalarining rivojlanishi moliya, bank ishlari, savdo-sotiq kabi sohalarda axborot muhofazasining algoritmlarini qo'llashni taqoza qilib, aynan shu sohalarga keng kirib borishiga ham sabab bo'ldi. Ochiq kalitli axborot muhofazasini ta'minlovchi algoritmlarni yaratlishida tub sonlarning xossalaridan foydalaniladi. Biror berilgan sonni tub ko'paytuvchilarga ajratish, uni tub yoki tub emasligini aniqlashga nisbatan murakkab bo'lgan masaladir. Shuning uchun berilgan natural sonni tub yoki tub emasligini aniqlasni samarali usullarini topish bo'yicha tadqiqot olib borish muhim hisoblanadi.

Ma'lumki, birdan farqli natural sonlarni bo`luvchilari soniga qarab ikkita asosiy guruhga, ya'ni tub va murakkab sonlarga ajratishimiz mumkin (lekin 1 soni ikkala guruhga ham mansub emas).

Tub sonlar – faqatgina ikkita bo'luvchiga ega bo'lgan natural sonlardir (birinchi bo'luvchisi 1, ikkinchi bo'luvchisi o'zi bo'ladi). Demak, tub sonlar ketma-ketligi quyidagicha bo`ladi: 2,3,5,7,9,11,13….

Murakkab sonlar – bo'luvchisi ikkitadan ko'p bo'lgan natural sonlardir. Demak, 4,6,8,9,10,12,14,15,… murakkab sonlar ketma-ketligidir.

1soni tub ham murakkab ham emas, chunki uning bo'luvchisi bitta, ya'ni o'zidan iborat.

Tub sonlar jadvalini tuzishning eng oddiy va shu bilan birga eng qadimgi hisoblangan usuli Eratosfen taklif qilgan usuldir. 1954 yil Pragalik injener Miroslav Soukup ham tub sonlar hosil qilishning yana bir jadvallarga asoslangan usulini bergan. U 6 dan katta n sonini 6 ga bo`lganda 0, 2, 3, 4 qoldiqlar hosil bo`lsa, n murakkab son bo`ladi degan fikrga tayanib, 2 va 3 dan farqli tub sonlarni 6n±1 shakldagi sonlar ichidan izlash kerak deb

$n=6km\pm(k+n)$ $(k=1,2,3,\ldots,\ m=0,1,2,3,\ldots,k)$

va

$n=6km\pm(k-n)$ $(k=1,2,3,\ldots,\ m=0,1,2,3,\ldots,k)$

tengliklardan foydalanib jadval tuzgan. Berilgan usul bilan to`liq holda [1] orqali tanishish mumkin.

Tub sonlarni hosil qilishning yana bir usulida 1 bilan birinchi n ta tub sonlarni olib, ular ixtiyoriy yo`l bilan ikki guruhga bo`linadi. Har bir guruh sonlarini ko`paytirib, ikki xil ko`paytma hosil qilinadi va bu ko`paytmalarning yig`indisi yoki ayirmasi tuziladi. Hosil bo`lgan yig`indi yoki ayirma yordamida (n+1)- tub sonning kvadratidan kichik bo`lgan tub sonlar hosil qilinadi [1].

Yuqoridagi usullarni g'oyasidan ko`rinib turibdiki, yetrlicha katta tub sonni topish yoki yetrlicha katta sonni tub yoki tub emasligini aniqlashda bu usullarni samarali deb bo`lmaydi.

Berilgan sonning tub yoki tub emasligini aniqlashning bizga ma'lum bo'lgan va keng qo`llaniladigan usullaridan biri, bu berilgan sonni o'sha sonning kvadrat ildiziga teng sondan kichik bo'lgan tub sonlarga bo'linishini tekshirib chiqishdan iboratdir. Agar berilgan son o`zining kvadrat ildiziga teng songacha bo'lgan tub sonlarga bo'linmasa bu son tub son hisoblanadi.

Misol. 127 soni tub yoki tub emasligini bilish uchun uning kvadrat ildizining butun qismi bo`lgan 11 sonini aniqlab olamiz. So`ngra, 127 ni 11 gacha bo'lgan tub sonlarga bo'linish yoki bo'linmasligini ko'rib chiqamiz. Hisoblashlardan ko`rinadiki, 127 soni 2, 3, 5, 7 tub sonlarni birortasiga ham bo'linmaydi. Demak, 127 soni tub ekan.

Berilgan sonni biror tub songa bo`linish yoki bo`linmasligini aniqlashning ikkita usuli bor. Birinchisi berilgan sonni o`sha tub songa bevosita bo`lib ko`rish usuli, ikkinchisi tub sonlarga bo`linish belgilaridan foydalanish usuli. Ikkinchi usul ko`p hollarda maqsadga tez erishish uchun samarali hisoblanadi.

Demak, berilgan sonni tub yoki tub emasligini aniqlashda yuqorida keltirilgan usulni qo'llaganda tub sonlarga bo'linish belgilarini bilish maqsadga tezroq erishishga yordam berishi mumkin ekan. Shuning uchun quyida bir qancha tub sonlarga bo'linish belgilarini keltiramiz.

1) Oxiri 0,2,4,6,8 raqamlar bilan tugagan sonlar 2 ga bo'linadi.
2) Raqamlari yig'indisi 3 ga bo'linadigan sonlar 3 ga bo'linadi.
3) Oxiri 0 va 5 raqamlari bilan tugagan sonlar 5 ga bo'linadi.
4) Berilgan sonni oxirgi raqamini 2ga ko'paytirib, oxirgi raqami o`chirishdan qolgan sondan ayirish natijasida hosil bo'lgan son 7ga bo'linsa berilgan son ham 7 ga bo'linadi. Boshqacha aytganda sondagi o`nlar sonidan birlar xonasidagi raqamning ikkilanganini ayirmasi 7ga bo'linsa berilgan son ham 7 ga bo'linadi.

M: $\underbrace{4\,0}$ 6- berilgan son.

$40-6\times2=28$.

28:7=4.

Demak, 406 ham 7ga bo'linadi: 406:7=58.

5) Berilgan sonni juft o`rindagi raqamlari yig'indisidan toq o'rindagi raqamlari yig'indisini ayirmasi 0 bo'lsa yoki 11 ga bo'linsa berilgan son ham 11 ga bo'linadi.

M: 62425-berilgan son.

(6+4+5)-(2+2)=1.

11 soni 11ga bo'linadi, demak berilgan son ham 11 ga bo'linadi.

62425:11=5675.

6) Berilgan sonning oxirgi raqamini 4ga ko'paytirib, oxirgi raqamni o`chirishdan qolgan songa qo'shish natijasida hosil bo'lgan son 13 ga bo'linsa, berilgan son ham 13ga bo'linadi.

M: $\underbrace{1\,9}$ 5-berilgan son.

$19+5\times4=39$.

39 soni 13 ga bo'linadi, demak 195 ham13ga bo'linadi.

195:13=15.

Agar berilgan son juda katta bo’lsa yuqorida keltirilgan usul qo`llanilsa, oxirgi raqami o`chirishdan qolgan songa oxirgi raqamini 4ga ko’paytirib qo’shishdan hosil bo`lgan son ham katta bo`ladi. Shuning uchun bu usulni keyingi hosil bo`lgan songa qo`llaymiz, so`ngra yana keyingi hosil bo`lgan songa qo`llaymiz va hokazo, jarayonni 13 ga bo`lish oson bo`ladigan son hosil bo`lguncha davriy ravishda qaytaraveramiz.

Misol. 1607502-berilgan son bo`lsin.

160750+2×4=160758,

16075+8×4=16107,

1610+7×4=1638,

163+8×4=195,

19+5×4=39.

7) Berilgan sonning oxirgi raqamini 5ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan sondan ayirish natijasida hosil bo’lgan son 0 yoki17 ga bo’linsa berilgan son ham 17 ga bo’linadi.

M: 425-berilgan son.

42-5×5=17.

Demak, 425soni 17ga bo’linadi.

425:17=25.

8) Berilgan sonning oxirgi raqamini 2ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shish natijasida hosil bo’lgan son 19 ga bo’linsa , berilgan son ham 19 ga bo’linadi.

M: 228- berilgan son.

22+2×8=38.

38 soni 19 ga bo’linadi. Demak, 228 ham 19 ga bo’linadi.

228:19=12.

9) Berilgan sonning oxirgi raqamini 7ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shish natijasida hosil bo’lgan son 23 ga bo’linsa berilgan son ham 23 ga bo’linadi.

10) Berilgan sonning oxirgi raqamini 3ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shish natijasida hosil bo’lgan son 29 ga bo’linsa, berilgan son ham 29 ga bo’linadi.

29 dan katta tub sonlarga bo’linish alomatlari ham 13, 17, 19, 23 sonlariga bo`linish alomatlariga o`xshash yo’l bilan amalga oshiriladi. Faqat oxirgi raqamiga ko’paytiriladigan sonlar va ularni qo’shish yoki ayirilishi o’zgaradi. Quyida keyingi tub sonlar uchun oxirgi raqamga ko`paytiriladigan sonlar va oxirgi raqamni o`chirishdan qolgan songa qo’shish yoki ayirish bo`lishligi keltirilgan.

31 uchun: 3ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shamiz.

37 uchun: 11ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan sondan ayiramiz.

41 uchun: 4ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan sondan ayiramiz.

43 uchun:13ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shamiz.

47 uchun: 14ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan sondan ayiramiz.

53 uchun: 16ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shamiz

59 uchun: 6 ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan songa qo’shamiz.

61uchun: 6ga ko’paytirib, oxirgi raqamni o`chirishdan qolgan sondan ayiramiz.

Misollar:1) 59×85=5015sonini 59 ga bo’linishini bilamiz. Endi uni bo`linish belgisi orqali tekshiramiz.

501+5×6=531.

53+1×6=59. Demak, 5015 soni 59 ga bo`linadi.

2) 79608 ni 31 ga bo’linishini isbotlang.

7960-8×3=7936.

793-6×3=775.

77-5×3=62.

6-2×3=0.

Demak, isbot bo`ldi.

Yeterlicha katta sonlarning tub yoki tub emasligini aniqlashning muhim ekanligi va bu kriptologiya hamda kriptoanaliz masalalarini yechishda qanday qo`llanilishi haqidagi ma’lumotlarni [2,3] asarlardan topish mumkin. Bu asarlarda sonlarning tub yoki tub emasligini aniqlashning yanada soddaroq, qulayroq ratsional usulini topish hozirda dolzarb muammolardan biri ekanligi ham ta`kidlangan. Muallif masalani yechish bo`yicha o`zining ko`plab ratsional takliflarini bildirgan.

Adabiyotlar.

1. Yagudayev B.Y. Ajoyib sonlar olamida. ”O`qituvchi”, - T.: -1973, -232 bet.
2. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, “Ўзбекистон маркаси”, 2009 – 434 бет.
3. Акбаров Д.Е., Мухтаров Ф., Сиддиқов А.А. Криптотахлил масалаларига тизимли ёндошув асослари ва уларни ечиш усуллари– Тошкент.: Изд. “ФАН”»., 2014 й. – 189 бет.