TUB VA MURAKKAB SONLAR.

Surxondaryo viloyati Jarqo'rg'on tumani

35-son umumiy o'rta ta'lim maktabining Matematika fani o'qituvchisi

Xudjamkulova Oysora Xushbakovna

Annotatsiya: Ushbu maqolada Tub va murakkab sonlar, ularning bir-biridan farqlari hamda xossalari haqida ma'lumotlar quyidagi teoremalar yordamida isbotlab berilgan.

Kalit so'zlar: Tub sonlar, murakkab sonlar, natural sonlar, ko'paytirish, sonlar nazariyasi, bo'linuvchi, teorema.

Tub son — birdan katta natural son bo'lib, ikkita natural bo'luvchiga ega: 1 va o'zi. Tub sonlarni xossalarini o'rganuvchi fan Sonlar nazariyasi deb ataladi.

Murakkab sonlar - uchta va undan ortiq bo'luvchiga ega bo'lgan natural sonlarga murakkab sonlar deyiladi. Masalan,eng kichik murakkab son 4 va uning bo'luvchilari 1, 2, 4 dir. Undan keyingi murakkab son 6 , uning bo'livchilari soni 4 ta va ular 1 , 2 , 3 , 6 dir. Murakkab sonlarni doimo tub ko'paytuvchilarga ajratish mumkin. Murakkab sonlar cheksiz ko'p va buning isboti juda oddiy. Chunki 2 dan boshqacha barcha juft sonlar o'ziga , 1 ga va 2 ga karralidir va bu ularning bo'luvchilarini 3 ta va undan ko'p ekanligini va murakkab son ekanligini isbotlaydi.[1]

Faqat ikkita turli bo'luvchiga ega bo'lgan natural son tub son, ikkitadan ko'p turli natural bo'luvchiga ega bo'lgan natural son murakkab son deyiladi.

1.Har qanday natural sonning kamida 2 ta bo`luvchisi bor: 1 soni va asonining o`zi.

M: 3, 5, 17 sonlari tub son, chunki ularning 1 va o`zidan boshqa bo`luvchilari yo`q. –12. tub son emas, uning 1 va 12 dan boshqa bo`luvchilari ham bor, ular 2, 3, 4, 6 sonlari, M: 6 -murakkab son, uning to‘rtta bo`luvchisi bor. Ular: 1, 2, 3, 6, 0 sonining bo`luvchilari cheksiz ko`p, 1 ning faqat 1 ta bo`luvchisi bor, shuning uchun bu 0 va 1 ni tub sonlarga ham murakkab sonlarga ham kiritilmaydi.

Shunday qilib, nomanfiy butun sonlar to‘plami 4 ta sinfga ajraladi. N_0 = {0}U{l}U{tub sonlar}U{murakkab sonlar}[2]

Tub sonlar quyidagi xossalarga ega:

1°. Agar r tub soni 1 dan farqli birorta n soniga bo‘linsa, r=n bo‘ladi.

Isbot: haqiqatdan ham r $\neq n$ bo‘lsa, r sonining 3 ta turli bo‘luvchisi bor bo‘ladi: 1, r, n. Bu esa shartga zid, demak, r-tub son bo‘la olmaydi.

2°. Agap r va q turli tub sonlar bo‘lsa, r tub son q tub songa bo‘linmaydi.

Isbot: r tub son bo‘lgani uchun u faqat 1 ga va r ga bo‘linadi. $q \neq r$ va g ≠1 (q -tub son, 1 tub son emas) bo‘lgani uchun

3° Agar a va b natural sonlar ko’paytmasi r tub songa bo`linsa, bu sonlardan biri r ga bo’linadi.

Isbot: Faraz qilaylik , u holda r -tub son bo`lgani uchun ularning 1 dan boshqa umumiy bo`luvchisi yo`q *abr* => *b r*.

4°, 1 dan katta istalgan natural sonning *hech* bo`lmaganda 1 ta tub bo`luvchisi bor.[3]

Isbot: Teskarisini faraz qilaylik, 1 dan katta, birorta ham tub bo`luvchisi yo`q natural sonlar mavjud bo`lsin. Bunday sonlar to`plamini A bilan belgilasak, unda eng kichik son mavjud bo`ladi, chunki natural sonlar to`plami quyidan chegaralangan. Eng kichik element a bo‘lsin. a>1 bo‘lgani uchun u yoki tub, yoki murakkab son bo‘lishi kerak. a - tub son bo‘la olmaydi, chunki *a(A* va farazga ko`ra a ning tub bo‘luvchisi yo`q. a -murakkab son bo‘lsa, u o`zidan va 1 dan farqli biror *b* natural bo`luvchiga ega bo`lar edi. *b(A*, chunki *b*<*a*. Demak, b ning biror r tub bo`luvchisi bor, u holda tranzitiv lik xossasiga ko`ra, bu farazimizga zid. Demak 1 dan katta barcha natural sonlar hech bo‘lmaganda 1 ta tub bo‘luvchiga ega.

5°. a murakkab sonning eng kichik tub bo`luvchisi – dan katta emas.

Isbot: a -murakkab son, r -uning eng kichik– tub bo`luvchisi bo`lsin. U holda a = bp bo`ladi. Bundan kelib chiqadiki *r* ( *b*, aks holda b ning tub bo`luvcxilari r dan kichik bo’lib, a soni r dan kichik tub bo`luvchiga ega bo`lib qolar edi. *r* (*b* , tengsiz likning ikkala qismini r ga ko`paytiramiz. r^2 (*b* = a ni hosil qilamiz, Bundan $r^2 \geq$ a *va r(* ga ega bo‘lamiz. Bu xossadan sonning tub yoki murakkabligini tekshirishda, sonni tub ko‘paytuvcxilarga ajratishda foydalaniladi. Masalan: 137 sonini olay lik 121<137<144 ya’ni 11^2<137<12^2 bundan 11 < < 12. Demak, 137 soni 12 dan kichik tub sonlarga boëlinmasa, tub son boëladi. 137 soni 2, 3, 5, 7, 11 sonlarining birortasiga ham bo`linmaydi. Demak, 137 -tub son. 2, Eratosfen g‘alviri. Tub sonlar jadvalini tuzishning qulay usulini eramizdan avvalgi III asrda Aleksandriyada yashagan grek matematigi va astronomi aniqlagani uchun uni Eratosfen g‘alviri deb ataladi. Bu usulga ko‘ra 2 dan biror n natural songacha bo`lgan barcha natural sonlar yozib chiqiladi. So‘ng 2 dan boshqa barcha 2 ga karrali sonlar o`chiriladi, bunda 2 dan boshqa barcha juft sonlar, ya`ni har ikkinchi son o`chiriladi. 2 dan keyin o`chirilmay qolgan 1 - son 3, endi 3 dan tashqari barcha 3 ga karrali sonlarni o`chiramiz, bunda 3 dan boshlab har 3 -son o`chiriladi, ba`zi sonlar 2 martadan o`chiriladi. 3 dan keyin o`chirilmay qolgan son 5 bo`lgani uchun 5 dan tashqari barcha 5 ga karrali, ya’ni Har 5 -sonni o`chiramiz. Shu taxlit l dan katta bo`lmagan o`chirilmay qolgan songacha davom etgiriladi. Natijada n gacha bo`lgan barcha tub sonlar qatoriga ega bo`lamiz. Masalan n = 40 bo`lsin. Quyidagi qatorga ega bo`lamiz.

1	2	3	4	5	6	7	8	9	
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39

1 dan 40 gacha bo`lgan tub sonlar quyidagilardan iborat:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

Tub sonlar to`plamining cheksiz ekanligi eramizdan avvalgi III asrda Aleksandriyada yashagan grek matematigi Evklid tomonidan

isbot qilingan.

Yevklid teoremasi: Tub sonlar to‘plami cheksizdir. Isbot: tub sonlar to`plami chekli deb faraz qilay lik. U holda *R* = {r_1, r_2,...r_n} tub sonlar to‘plamiga ega bo‘lamiz. a = r_1, r_2,...r_{n+1} sonni hosil qilaylik.

a soni tub emas, chunki u a_1, a_2,...a_n tub sonlarning hammasidan katta va barcha tub sonlar to`plami R ga kirmaydi. a soni murakkab ham bo`la olmaydi, chunki 4° ga ko‘ra barcha murakkab sonlarning kamida 1 ta tub bo`luvchisi boëlishi kerak, bu tub bo`luvchi r_1, r_2,...r_n tub sonlarning biri bo`lishi kerak, lekin a soni bu tub sondarning birortasiga ham bo`linmaydi, (ularning har biriga boëlganda 1 qoldiq chiqadi). Demak, R to’plamga kirmaydigan 1 ta bo`lsa ham tub son bor ekan. Bu qarama - qarsxilik farazimiz noto`g`riligini ko`rsatadi. Demak, tub sonlar to`plami cheksiz ekan. Matematikada ko`pincha sonni ko`paytuvcxilarga ajratish, yoki uning bo`luvcxilarini topish masalasiga duch kelamiz. Shu o`rinda quyidagi teoremani bilib qo`yish foydalidir. Bu teoremani natural sonlar arifmetikasining asosiy teoremasi deyilady va quyidagicha ifodalanadi:

Teorema. Har bir murakkab son yagona usul bilan tub sonlar ko`paytmasiga ajratiladi.

Isboti: Teoremada sonning tub sonlar ko`paytmasiga ajratishning mumkinligi va bunday ko`paytmaning yagonaligi haqida gapiriladi. Bu tasdiqlarni alohida isbot qilamiz. Tasdiqlarning birinchisini teskarisini faraz qilish yo`li bilan isbot qilallik:

Faraz qilamiz, tub sonlar ko`paytmasi shaklida yozib bo`lmaydigan murakkab sonlar mavjud. Ularning to`plamini A bilan, to`plamning eng kichik elementini a bilan belgilaymiz. a- murakkab son va u tub ko‘paytuvcxilarga ajralmaydi. a murakkab son bo`lgani uchun uning o`zidan kichik murakkab bo`luvchilari bor: $a_1a_2$ bo`lsin. a_1<a, a_2<a bo`lgani uchun $a_1a_2$ sonlari A to`plamga kirmaydi, demak ular yoki tub sonlar ko‘paytmasiga ajraladi. a_1=p_1...r_n a_2=q_1...q_n bo‘lsin, u holda

$a=p_1...p_nq_i...q_n$ shaklda tub ko`paytuvcilarga ajraladi va bu farazimizga zid. Demak, tub sonlar ko`paytmasiga ajralmaydigan murakkab son boëlishi mumkin emas.

Ikkinchi tasdiqni isbotlaymiz, ya`ni murakkab sonning tub sonlar koëpaytmasi ko`rinishida yagona usul bilan yozish mumkin. Faraz qilay lik, turlicha tub sonlar ko'paytmasiga ajraladigan murakkab sonlar mavjud, ularning to`plami A va eng kichik elementi a bo`lsin. Farazga ko'ra $a=r_1...r_m$ va $a=q_1...q_k$. Teng liklarning o`ng tomonlarini tenglaymiz: $p_1...p_m= q_1...q_k$. Bu teng likning chap qismi $p_i$ ga boëlinadi, demak o`ng qismi ham boëëlinishi kerak, tub sonlar bo`lgani uchun, ularning biri, masalan, ga bo`linadi, tub sonlar xossasiga ko`ra bo`ladi. Teng likning ikkala qismini p_1 ga bo`lsak, soniga ega bo`lamiz, bo`lgani uchun s>a va u A to'plamga tegshpli bo`lmaydi, demak u tub sonlar ko`paytmasi shaklida yagona usul bilan yoziladi. Demak, yoyilmalar tarkibiga ko`ra bir xil va faqat ko`paytuvcxilar tartibi bilangina farq qilishi mumkin. U holda ham bir xil sonlardan iborat bo'ladi. Bu esa, . farazimizga zid. Demak istalgan murakkab son faqat bir xil usul bilan tub sonlar ko`paytmasiga ajratiladi va turli ko'paytmalar mavjud bo`lsa, ular faqat ko`paytuvcxilar tartibi bilan farq qiladi. Bunday ko`paytmada odatda sonning tub bo`luvchilari o`sib borish tartibida, bir xil ko'paytuvcxilarni esa, daraja ko'rinishida yoziladi. Ko'paytmaning bu shaklini sonning kanonik yoyilmasi deyiladi. a sonining kanonik yoyilmasi shaklida bo'ladi, bu erda $p1<p_2<...<p_n$. Masalan, 150=2x3x5x5 bo'lsa, kanonik yoyilmasi $2xZx5^2$ ko'rinishida, 2000 soni uchun esa, $200=2^3x5^2$ ko'rinishida bo'ladi. Faqat ikkita turli bo`luvchiga ega bo`lgan natural son tub son, ikkitadan ko`p turli natural bo`luvchiga ega bo`lgan natural son murakkab son deyiladi. Izoh. p tub son 1 dan farqli bo`lib, faqat 1 va p ga bo`linadi. m murakkab sonning 1 va m bo`luvchilardan farqli kamida yana bitta bo`luvchisi mavjud. 1 soni esa na tub , na murakkab son hisoblanadi. Tub va murakkab sonlarning ba'zi xossalarini ko'rib chiqamiz. 1. $a > 1$ murakkab sonning 1 dan farqli eng kichik natural bo'luvchisi p bo'lsa, u holda p tub son bo'ladi. Haqiqatdan, aks holda p biror q $(1 < q < p)$ bo'luvchiga ega bo'lib, $p\ q \wedge a\ q \Rightarrow a\ q$ va $q < p$ bo'lar edi. Bu esa p ning eng kichik bo'luvchi ekaniga ziddir. 2. Har qanday natural a va p tub soni yo o'zaro tub, yoki a son p ga bo'linadi. 3. Agar ab ko'paytma biror p tub songa bo'linsa, u holda ko'paytuvchilardan kamida bittasi p ga bo'linadi, ya'ni ($\forall a$, $b \epsilon N$) (ab p) ⇒ (a p ∨ b p). Misol. 2,3,5,7,11,13 –tub sonlar , 4,6,8,9,10,12 – murakkab sonlar. Teorema. a natural sonning eng kichik tub bo'luvchisi $\sqrt{a}$ dan katta emas. Isboti. Faraz qilaylik $p1$ tub son a ning eng kichik bo'luvchisi bo'lsin. U holda $a = p1 \cdot a1$ bo'lib, $a \geq p1$ bo'ladi. Bundan $a = p1a1 \geq p1$ 2 yoki $p1 \leq \sqrt{a}$ Teorema. Tub sonlar to'plami cheksizdir. Isbot. Faraz qilaylik tub sonlar soni chekli bo'lib, ular o'sish tartibida joylashgan $p1$, $p2$, … , pn ko'rinishdagi tub sonlardan iborat bo'lsin. $Qn = p1 \cdot p2 \cdot \ldots \cdot pn + 1$ sonni olamiz. Bu sonning eng kichik bo'luvchisini pm desak, u albatta tub son bo'ladi (tub sonlarning 1-xossasi) va u pi larning birontasiga ham teng bo'lmaydi. pm son pi $(i = 1, n)$ tub sonlarning birortasiga ham teng bo'la olmaydi, aks holda Qn va $p1 \cdot p2 \cdot \ldots \cdot pn$ larning pm ga bo'linishidan 1 ning ham pm ga bo'linishi kelib chiqar edi. Bu esa mumkin emas. Demak, farazimiz noto'g'ri ekan. Qn tub son bo'lsa, u holda $Qn > pi$ $(i = \overline{1,n})$ va yangi tub son hosil bo'ladi. Bu holda ham farazimiz noto'g'ri. Demak, tub sonlarning soni cheksiz, ya'ni tub sonlar to'plami cheksizdir. Ta'rif. 1 dan farqli umumiy bo'luvchilarga ega bo'lmagan ikkita natural son o'zaro tub sonlar deyiladi. Ta'rif. Agar noldan farqli a va b butun sonlar uchun a=bq tenglikni qanoatlantiradigan q butun son mavjud bo'lsa, u holda a son b songa qoldiqsiz bo'linadi (bo'linadi) yoki b son a sonni bo'ladi deyiladi hamda b | a kabi yoziladi. a=bq tenglikdagi a son bo`linuvchi yoki b soniga karrali son, b son a sonining bo`luvchisi, q son esa bo`linma deb yuritiladi. Ravshanki, ikkita son umumiy bo`luvchiga ega bo`lsa, u holda ularning yig`indisi, ayirmasi va karralilari ham shu bo`luvchiga ega. x, y va z butun sonlar bo'lsa, u holda quyidagi sodda xossalar o`rinli: (a) x | x (refleksivlik xossasi); (b) Agar x | y va y | z bo`lsa , u holda x | z (tranzitivlik xossasi); (c) Agar x | y va y ( 0 bo`lsa , u holda |x| (|y|; (d) Agar x | y va x | z bo'lsa , u holda barcha butun ((, sonlar uchun x | ((y z (; (e) Agar x | y va x | y ± z bo'lsa , u holda x | z; (f) Agar x | y va y | x bo'lsa , u holda |x|=|y|; (g) x | y (|x| | |y|; Izoh. Shuni aytish joizki, oxirgi (g) xossa bo`linish bilan bog`liq mulohazalarni butun sonlar uchun emas, balki natural sonlar uchun yuritishga imkon yaratadi. 2 ga karrali butun sonlar (ya'ni 2 k , k Z (, ko`rinishdagi sonlar) juft, 2 ga karrali bo'lmagan butun sonlar (ya'ni 2 k +1 , k Z ( , ko'rinishdagi sonlar) esa toq sonlar deb yuritiladi. Bunda quyidagilar o`rinli: a) Ikkita toq sonlarning yig`indisi va ayirmasi juft, ko□paytmasi esa toq son bo`ladi. b) Ikkita juft sonlarning yig`indisi , ayirmasi va ko`paytmasi juft son bo`ladi. Teorema. Agar $a = p1\ \alpha 1 \cdot p2\ \alpha 2 \cdot \ldots \cdot pn\ \alpha n$ bo'lsa, u holda a sonning barcha natural bo'luvchilari soni $\tau(a)$ quyidagi formula bilan aniqlanadi: $\tau(a) = (\alpha 1 + 1) \cdot (\alpha 2 + 1) \cdot \ldots \cdot (\alpha n + 1)$. Teorema. $a = p1\ \alpha 1 \cdot p2\ \alpha 2 \cdot \ldots \cdot pn\ \alpha n$ sonning barcha natural bo'luvchilari yig'indisi $\sigma(a)$ quyidagi formula orqali aniqlanadi: $\sigma(a) = p1\ \alpha 1{+}1\ {-}1\ p1{-}1 \cdot p2\ \alpha 2{+}1\ {-}1\ p2{-}1 \cdot \ldots \cdot pn\ \alpha n{+}1{-}1\ pn{-}1$. Teorema. $a = p1\ \alpha 1 \cdot p2\ \alpha 2 \cdot \ldots \cdot pn\ \alpha n$ sonning undan katta bo'lmagan va u bilan o'zaro tub sonlar soni $\varphi(a)$ quyidagi formula orqali aniqlanadi: $\varphi(a) = a\ (1 - 1\ p1\ )\ (1 - 1\ p2\ ) \cdot \ldots \cdot (1 - 1\ pn\ )$. Misollardan namunalar: 1-misol. Berilgan 1321 sonining tub yoki murakkab ekanligini aniqlang. Yechish. Berilgan a natural sonining tub yoki murakkab ekanligini aniqlash uchun $\surd a$ songacha bo'lgan tub sonlarga berilgan sonning bo'linishi yoki bo'linmasligi aniqlanadi. Agar berilgan a son $\surd a$ gacha bo'lgan birorta ham tub songa bo'linmasa, u holda a tub son bo'ladi. Demak, $\surd 1321 \approx 36$ ni topamiz. 36 gacha bo'lgan tub sonlar 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 ga berilgan 1321 sonni bo'linishini tekshiramiz. 2 ga bo'linmaydi, chunki 1321 toq son; 3 ga bo'linmaydi, chunki 1+3+2+1=7/3; 5 ga bo'linmaydi, chunki 1321 ning oxirgi raqami 1; 1321:7≈188; 1321:11≈120; 1321:13≈101; 1321:17≈77; 1321:19≈69; 1321:23≈54; 1321:29≈45; 1321:31≈42 Demak, 1321 36 gacha bo'lgan tub sonlarga bo'linmaydi. U tub son. 2-misol. Berilgan $a = 126$ sonining natural bo'linuvchilari soni va yig'indisini, undan kata bo'lmagan va u bilan o'zaro tub sonlar sonini toping. Yechish. Berilgan a sonining natural bo'luvchilari soni $\tau(a)$ va natural bo'luvchilari yig'indisini $\sigma(a)$, a dan kata bo'lmagan u bilan o'zaro tub sonlar soni $\varphi(a)$ jarni aniqlash uchun a sonining tub ko'paytuvchilarga kanonik yoyilmasini topamiz. Agar $a = p1\ \alpha 1 \cdot p2\ \alpha 2 \cdot \ldots \cdot pn\ \alpha n$ bo'lsa, u holda $\tau(a) = (\alpha 1 + 1) \cdot (\alpha 2 + 1) \cdot \ldots \cdot (\alpha n + 1)$; $\sigma(a) = p1$

$\alpha 1+1 -1\ p1-1 \cdot p2\ \alpha 2+1 -1\ p2-1 \cdot \ldots \cdot pn\ \alpha n+1-1\ pn-1$; $\varphi(a) = a\ (1 - 1\ p1\ )\ (1 - 1\ p2\ ) \cdot \ldots \cdot (1 - 1\ pn\ )$ bo'ladi. $a = 126$ ning tub ko'paytuvchilarga kanonik yoyilmasi 126 = 2 1 · 3 2 · 7 1 ko'rinishda ekan. U holda a) $\tau(126)$ = (1 + 1)(2 + 1)(1 + 1) = 2 · 3 · 2 = 12. Demak, 126 ning natural bo'luvchilari 12 ta. Haqiqatdan ham ular: 1, 2, 3, 6, 7, 9, 14, 18, 21, 42, 63, 126. b) $\sigma(126)$ = 2 2−1 2−1 · 3 3−1 3−1 · 7 2−1 7−1 = 312 Haqiqatdan ham 1+2+3+6+7+9+14+18+21+42+63+126=312 c) $\varphi(126) = 126 \cdot (1 - 1\ 2\ )\ (1 - 1\ 3\ )\ (1 - 1\ 7\ ) = 36$. Demak, 126 dan katta bo'lmagan, u bilan o'zaro tub sonlar soni 36 ta. 3-misol. 23! ni tub ko'paytuvchilarga kanonik yoyilmasini toping. Yechish. Berilgan n! sonning tub ko'paytuvchilarga yoyilmasini topish uchun, n dan katta bo'lmagan tub sonlar qanday daraja bilan kanonik yoyilmada qatnashishini topamiz. 23 dan katta bo'lmagan tub sonlar 2, 3, 5, 7, 11, 13, 17, 19, 23 2 ning 23! ning kanonik yoyilmasidagi darajasini topamiz.[4]

Xulosa: Buning uchun 23 ni 2 ga bo'lamiz. Bo'linma 2 dan kichik son bo'lguncha bu jarayonni davom ettiramiz: 23=2·11+1 11=2·5+1 5=2·2+1 2=2·1+0 Demak, 2 ning kanonik yoyilmadan darajasi 11+5+2+1=19. 3 ning darajasini topamiz: 23=3·7+2 7=3·2+1, 3 ning darajasi 7+2=9. 5 ning darajasini topamiz: 23=5·4+3, 5 ning darajasi 4. 7 ning darajasi 3 23=7·3+2. 11 ning darajasi 2 23=11·2+1. 13 ning darajasi 1 23=13·1+10. Huddi shunday 17, 19, 23 larning ham yoyilmadagi darajalari 1 ga teng. Demak, 23! = 2 19 · 3 9 · 5 4 · 7 3 · 112 · 13 · 17 · 19 · 23.

Foydalanilgan adabiyotlar:

1.Г. Гальперин, «Просто о простых числах», «Квант», № 4, 1987[1]

2 «Алгоритмические проблемы теории чисел» Wayback Machine saytida arxivlandi (2005-01-13)., глава из книги «Введение в криптографию» под редакцией В. В. Ященко[2]

3.О. Н. Василенко, «Теоретико-числовые алгоритмы в криптографии» [3]

4.А. В. Черемушкин, «Лекции по арифметическим алгоритмам в криптографии»[4]