TUB SONLARNI HOSIL QILISH USULLARI VA ULARNING TAQSIMOTI

Karimov Abdukodir Abdisalomovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
karimovabduqodir041@gmail.com
Ergasheva Farida Yunus qizi *(TATU)*
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
afarida0630@gmail.com

Annotatsiya: tub sonlar kriptografik tizimlarning eng quyi va asosiy qismini tashkil etganligi va ularning chidamliligini belgilaydigan unsur bo‘lganligi sababli tub sonlarni to‘g’ri tanlash, ularni turli usullar bilan hosil qilish muhim hisoblanadi. Ularning chidamliligini tekshirish uchun esa bir qancha algoritmlarni o‘z ichiga olgan test sinovlarni mavjud. Ushbu maqolada yuqorida sanab o‘tilgan testlar, ularning ishlash tartibi va kriptologik ahamiyati yoritilgan. Hamda tub sonlarning son o‘qida yoyilishi ham ma’lum teoremalar va grafiklar yordamida yoritildi.

Kalit so‘zlar: pseudo-tasodifiy, tub sonlar, Evklid.

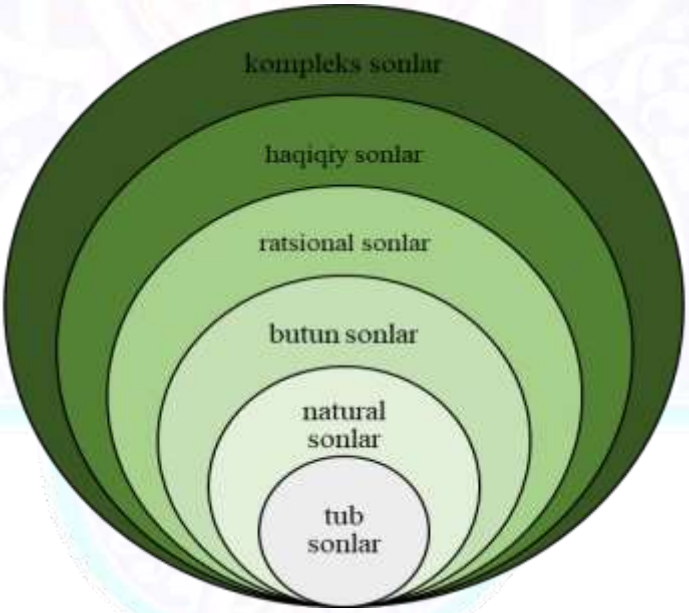
Kirish

Matematikaning asosiy yo‘nalishlaridan biri bo‘lgan, shuningdek kriptografik tizimlarning asosisini tashkil qiladigan sonlar nazariyasi o‘z ichiga ko‘plab sirli va qiziqarli mavzularni qamrab oladi. Ulardan biri tub sonlar va ularning xususiyatlariga oid tadqiqotlardir. Tub sonlar – faqat o‘ziga va 1 ga bo‘linadigan natural sonlar – matematik nazariyaning poydevorlaridan biri bo‘lib, ular nafaqat sof matematik tadqiqotlarda, balki zamonaviy texnologiyalar, kriptografiya, kompyuter xavfsizligi kabi ko‘plab amaliy sohalarda ham katta ahamiyatga ega.

Tub sonlarni aniqlash va ularning xossalarini o‘rganish asrlar davomida matematiklar hamda kriptograflar uchun muhim vazifa bo‘lib kelgan. Tub sonlarning taqsimoti haqida ilk nazariyalarni qadimgi yunon matematiklari, jumladan, Evklid ilgari surgan. Bugungi kunda esa bu soha o‘zida ko‘plab algoritmik yondashuvlar va zamonaviy tadqiqotlarni mujassam etadi. Tub sonlarni hosil qilishning bir qancha usullari mavjud bo’lib, ularning qatoriga **tasodifiy ravishda tub sonlarni generatsiya qilish**ni ham kiritish to‘g’ri bo‘ladi. Birinchi bosqichda tasodifiy ravishda kerakli uzunlikdagi son tanlanadi. Bu son odatda 2^n bit uzunlikka ega bo‘ladi, masalan, 2048 bitli yoki 1024 bitli. Tasodifiy raqam generatorlari yordamida kompyuterda yuqori sifatli tasodifiy raqamlar yaratish mumkin. Ular **Pseudo-random number generators (PRNGs)**: Masalan, Mersenne Twister yoki Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) kabi algoritmlar yordamida tasodifiy sonlar generatsiya qilinadi. **True random number generators (TRNGs)**: Faqat haqiqiy

tasodifiylikka asoslangan generatorlar, masalan, kvant kompyuterlaridan foydalanish mumkin. Bizga ma’lumki, 2 lik sanoq sistemasidagi son 0 bilan tugasa, u son juft bo‘ladi. Toq sonlarni juft sonlarga nisbatan tub bo‘lish ehtimolligi yuqoriroqligi sababli generatordan chiqqan sonni oxiri 0 raqami bilan tugasa, uni 1 ga almashtirib qo’yish maqsadga muvofiq bo‘ladi. Keyingi bosqichda, tasodifiy tanlangan sonning tub yoki bo‘linuvchanligini aniqlash uchun tublikka tekshirish testlaridan foydalaniladi. Bu testlar ehtimoollikka asoslangan testlar yoki deterministik testlar bo‘lishi mumkin. Agar test jarayonida tub son aniqlansa, u 2048-bitli yoki kerakli uzunlikdagi tub son sifatida qaytariladi. Bu tub sonlar, asosan, kriptografiya tizimlarida kalitlarni yaratish uchun ishlatiladi (masalan, RSA algoritmida). 2048-bitli tub sonlar odatda maxfiy kalitlarni yaratishda ishlatiladi va bu kalitlar orqali ma'lumotlarni shifrlash va deshifrlashning imkoni mavjud.

Tub sonlarning kriptografiyadagi ahamiyati ular yordamida shifrlash va rasshifrovkalash jarayonlarini amalga oshirish orqali axborot xavfsizligini ta'minlash mumkinligi, katta sonlarni tezda faktorlashning qiyinligini ta'minlab, shifrlash va ma'lumotlarni himoya qilishni xavfsiz va samarali qilganligi va boshqa bir qator faktorlarga asoslanib o‘lchanadi. Tub sonlar haqida gapirishdan oldin uning ta’rifiga e’tibor qaratamiz. Tub son deb faqat o’ziga va 1 ga bo’linadigan natural sonlarga aytiladi *(2,3,5,7,11,13…).* Tub sonlar natural sonlar to‘plamining qism to‘plami hisoblanadi (1-rasm).



1-rasm.Sonlar diagrammasi.

Tub sonlarni generatsiya qilish usullari

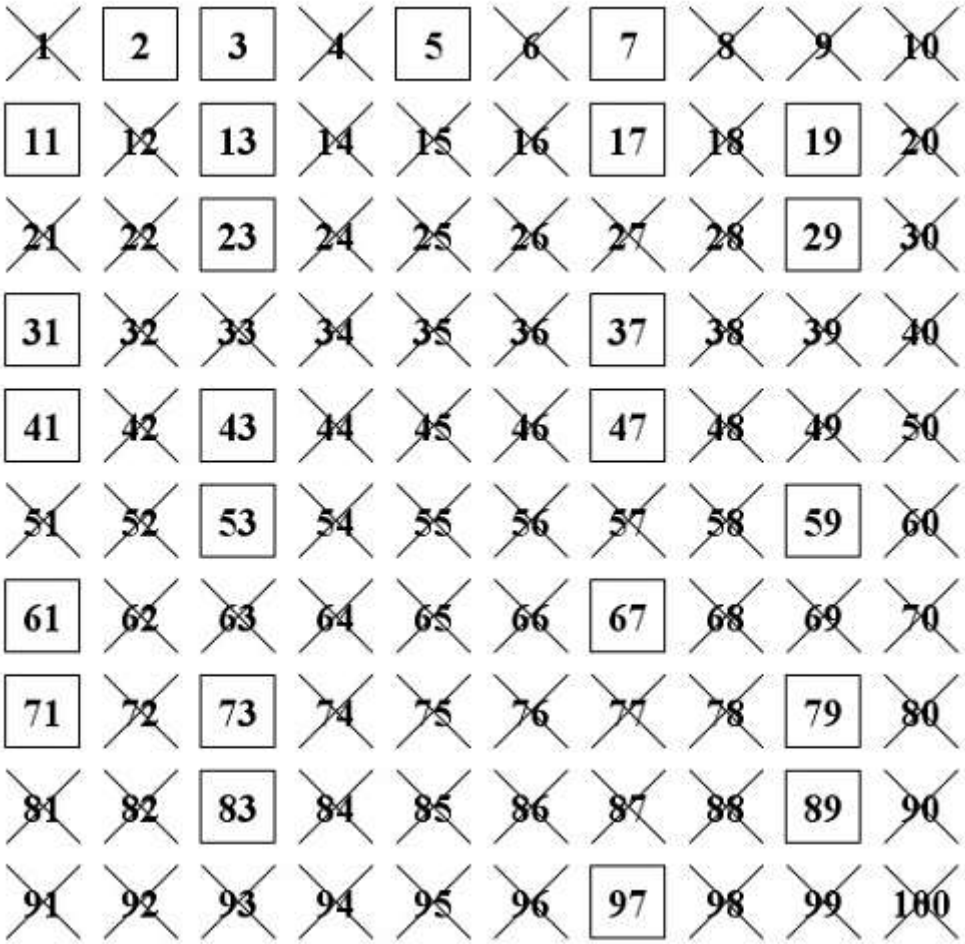
Sonni tublikka tekshirish ma’lum intervaldagi sonlarni orasidan tub sonlarni ajratib olish imkonini beradi. Tublikka tekshirishning bir qancha usullari mavjud bo’lib

eng mashxurlari Eratasfen g'alvir usuli hisoblanadi. Eratosthenesning Sieve usuli quyidagi qadamlardan iborat:

1. 1dan *N* gacha bo'lgan sonlar yozib chiqiladi.

2. 1 tub bo'lmaganligi uchun ro'yxatga 2 dan boshlab qaraladi va 2 tub bo'lganligi uchun unga karrali bo'lgan barcha sonlar o'chirib chiqiladi.

3. Keyingi son 3, u ham tub bo'lganligi uchun 3 ga karrali bo'lgan barcha sonlar o'chirib chiqiladi va shu tartibda barcha tub sonlar olinadi va ularga karralilari o'chirib chiqilsa, yangi hosil bo'lgan ro'yxatimizda faqatgina tub sonlar qoladi(2-rasm).



2-rasm. Eratosthenesning Sieve usuli orqali hosil qilingan 1 dan 100 gacha bo'lgan tub sonlar ro'yxati.

Bu usulning eng katta kamchiligi sifatida uni katta sonlar uchun qo'llab ko'rish juda ko'p vaqt olishi ko'riladi. Masalan, 768723209327231 sonini tublikka tekshirish yuqorida keltirilgan usul bilan amalga oshirilsa, 1 dan to shu songacha davom ettirishim va undan sonlarni o'chirib chiqishim kerak bo'ladi. Bunga ko'p vaqt sarflamaslik uchun esa, tub soonlarni hosil qiluvchi bir qancha formulalar mavjud:

1. $6\times n+1$ va $6\times n-1$ $n\in N$;
2. $n!\pm 1$ $n\in N$;
3. $2^{2^n}+1$ $n\in N$ orqali tub sonlarni hosil qilish mumkin.

Sonlarni tublikka tekshirish usullari. Miller-Rabin tublikka tekshirish testi.

Bu algoritm sonning tub yoki tub emasligini taxmin qilishda ishlatiladi. Agar son tub bo'lsa, test uni tub sifatida tasdiqlaydi, lekin agar son tub bo'lmasa, u yuqori ehtimollik bilan kompozit(bo'linuvchan son) deb topiladi. Tasodifiy hosil qilingan *n-1* sonini $2^s \times d$ shaklida yozib olish kerak bo‘ladi.bu yerda d son toq bo‘lishi kerak. Misol uchun *n=25* bo‘lsa, *25-1*=$2^3 \times 3$, *s=3* va *d=3*.

Endi tasodifiy a soni *[2;n-2]* oralig’idan tanlab olinadi.keyingi qadamda esa $x=a^d modn$ hisoblanadi. Natija esa *x=1* yoki *x=n-1* bo‘lgandagina tub son deb qabul qilinadi. Agar $x^2 modn = n-1$ bo‘lsa, natija tub deb taxmin qilinadi va bu jarayon s-1 marta takrorlanadi. Agar yuqoridagi shartlar bajarilmasa son tub deb topilmaydi.

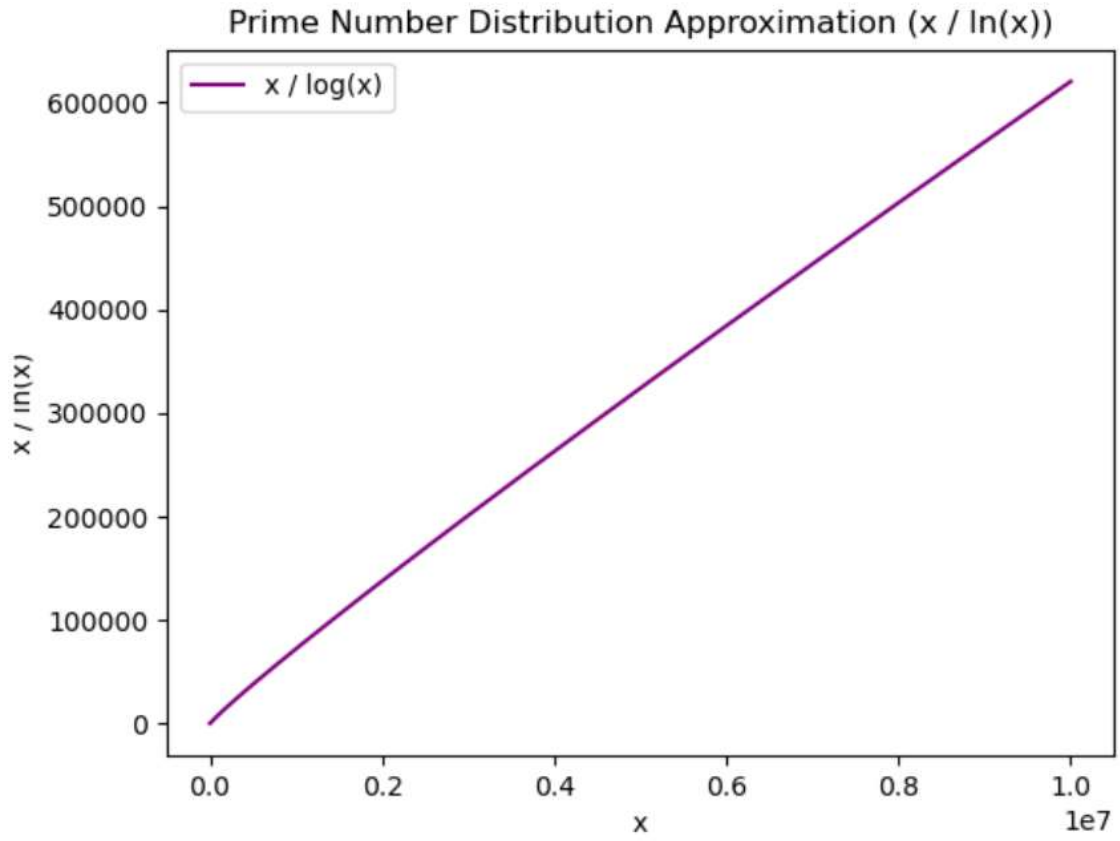
Ferma tublikka tekshirish testi.

Fermaning kichik teoremasining asosiy g‘oyasi shundan iboratki, agar *p* tub son bo'lsa, har qanday a soni uchun $a^{p-1} \equiv 1 \bmod p$ bo‘lishi kerak, bu yerda *a* va *p* sonlari o‘zaro tublik shartini qanoatlantirishi lozim. Bu algoritmni ishlatish jarayonida *a* ning bir nechta qiymatidan foydalanilsa, *p* sonning tub ekanligining ehtimoli yuqori bo‘ladi.

Tub sonlarning son o‘qidagi taqsimoti.

Bizga ma’lumki sonlar cheksizlikka intiladi. Bundan kelib chiqadiki, tub sonlar ham cheksiz davomiylikka egadir. Agar tub sonlar cheksiz davom etsa, ular son o‘qida qanday taqsimlanadi degan savol paydo bo‘lishi tabiiy. Bu savolga Gaussning tub sonlar teoremasi javob beradi. *N* gacha bo’lgan tub sonlar soni, ya’ni $\pi(N)$ asimptotik ravishda quyidagicha o‘sadi [1]:

$\pi(N) \sim \frac{N}{\ln N}$ yoki $\pi(N) \sim \lim_{N\to\infty} \frac{N}{\ln N}$ *N*-natural son.



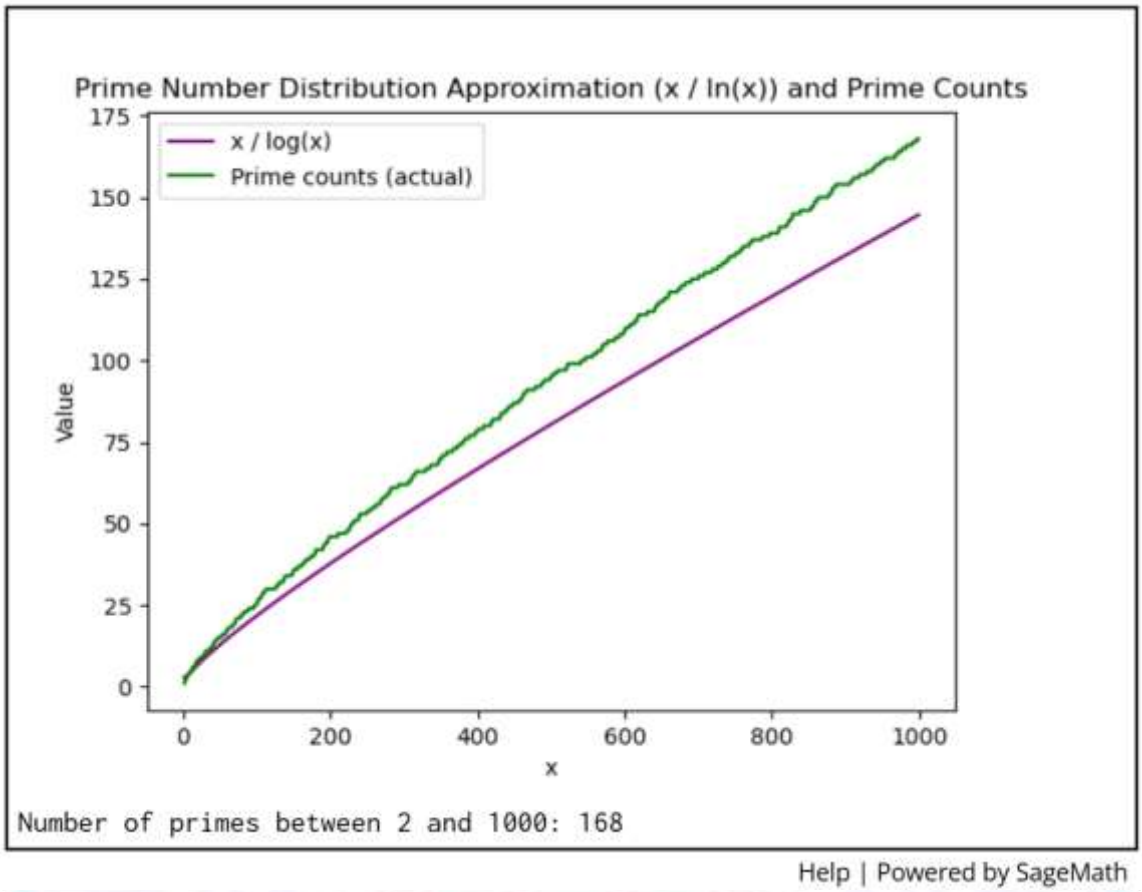
3-rasm. Gaussning tub sonlar teoremasi orqali $\pi(N)$ ning asimptotik ravishda o‘sishi.

Ma’lum oraliqdagi tub sonlar sonini aniqlash.

Tub sonlar cheksiz davom etishiga qaramay oraliqning ortgani sari uning ma’lum intervaldagi soni kamayib ketaveradi. Ya’ni tub sonlarning orasidagi masofa ortib ketadi. Tushunarliroq qilib aytganda, N kattalashsa, tub sonlar sonining o‘sish sur’ati kamayadi. Gauss va Chebyshev tub sonlar taqsimotining umumiy xususiyatlarini keltirib chiqargan, va bu formulalar a dan b gacha bo‘lgan oraliqdagi tub sonlar sonini taxminiy hisoblash uchun ham ishlatiladi:

a dan b gacha bo’lgan oraliqdagi sonlarni ichida taxminiy tub sonlar sonini aniqlash:

$$\pi(b) - \pi(b) \sim \left(\frac{b}{\ln b} - \frac{a}{\ln a}\right)$$



4-rasm. Tub sonlar taqsimoti.

Foydalanilgan adabiyotlar:

1. Koukoulopoulos, D. (2019). The distribution of prime numbers (Vol. 203). American Mathematical Soc.
2. Blum, L., Blum, M., & Shub, M. (1986). A simple unpredictable pseudo-random number generator. *SIAM Journal on computing*, *15*(2), 364-383.
3. Bhattacharjee, K., & Das, S. (2022). A search for good pseudo-random number generators: Survey and empirical studies. *Computer Science Review*, *45*, 100471.
4. Obaid, T. S. (2020). Study a public key in RSA algorithm. *European Journal of Engineering and Technology Research*, *5*(4), 395-398.
5. Ezz-Eldien, A., Ezz, M., Alsirhani, A., Mostafa, A. M., Alomari, A., Alserhani, F., & Alshahrani, M. M. (2024). Computational challenges and solutions: Prime number generation for enhanced data security. *PloS one*, *19*(11), e0311782.
6. Пер. с англ. / Под ред. и с предисл. В. Н. Чубарикова. - М.: УРСС: Книжный дом “ЛИБРОКОМ ”, 2011.-664 с
7. Joye, M., Paillier, P., & Vaudenay, S. (2000). Efficient generation of prime numbers. In Cryptographic Hardware and Embedded Systems—CHES 2000: Second International Workshop Worcester, MA, USA, August 17–18, 2000 Proceedings 2 (pp. 340-354). Springer Berlin Heidelberg.