Impact Factor: 9.9 ISSN-L: 2544-980X

Kengaytirilgan Evklid Algoritmining Kriptografiyada Maxfiylik Va Xavfsiz Aloqani Ta’minlashdagi Ahamiyati

Arabboyev Alisher Avazbek o‘g‘li [1]

Annotatsiya: Ushbu maqolada maxfiylikni va xavfsiz aloqani ta’minlashda foydalaniladigan, kriptografik usullarda qo‘llaniladigan kengaytirilgan Evklid algoritmi va uning ahamiyati to‘g‘risida ma’lumot berilgan.

Kalit so‘zlar: kengaytirilgan Evklid algoritmi, kriptografiya, modul, EKUB, chiziqli diofant tenglama.

Kirish

Kengaytirilgan Evklid algoritmi klassik Evklid algoritmining kengaytmasi bo‘lib, u ikkita butun sonning eng katta umumiy bo‘luvchisini (EKUB) hisoblash uchun ishlatiladi. Standart Evklid algoritmi faqat EKUB ni topsada, kengaytirilgan Evklid algoritmi Bezoutning identifikatorini qanoatlantiradigan koeffitsientlarni topadi:

$$ax + by = EKUB(a;b) \qquad (1)$$

Kengaytirilgan Evklid algoritmi sonlar nazariyasida bir qancha amaliy qo‘llanmalarga ega kuchli vositadir. U nafaqat ikkita butun sonning eng katta umumiy bo‘luvchisini (EKUB) hisoblabgina qolmay, balki EKUB ni a va b sonlarining chiziqli birikmasi sifatida ifodalovchi butun son koeffitsientlarini topadi, bu Diofant tenglamalarini yechishda muhim ahamiyatga ega. Kriptografiyada, ayniqsa RSA kabi algoritmlarda kalitlarni yaratish va shifrni ochish jarayonlari uchun zarur bo‘lgan modulli teskarilarni topishga yordam beradi. Kengaytirilgan Evklid algoritmi kriptografiyadagi diofant tenglamalarini yechish, kasrlarni soddalashtirish va kodlashdagi xatolarni tuzatish bilan ikkita butun sonning EKUB ni hisoblash va chiziqli birikmalar uchun butun son koeffitsientlarini topish uchun ishlatiladi.

Algoritmning samaradorligi unga katta sonlarni boshqarish imkonini beradi, bu esa uni zamonaviy hisoblash dasturlari uchun mos qiladi. Umuman olganda, kengaytirilgan Evklid algoritmi murakkab matematik muammolarni hal qilish imkoniyatini oshiradi va shu bilan birga turli amaliy ilovalar uchun fundamental yordam beradi.

Tadqiqot usuli

Qoldiqli bo‘lish amali quydiagi formula ko‘rinishida ifodalangan:

$$a = b * q + r \qquad (2)$$

bu yerda a - bo‘linuvchi son, b - bo‘luvchi, q - butun qism va qolgan r esa $0 \le r < b$ qanoatlantiradi. Evklid algoritimida ushbu bo‘lish amali EKUB (a,b) topilguncha davom etadi. Ikkita $0 < b < a$ butun songa nisbatan bo‘linish algoritmini takroriy qo‘llaymiz, natijada ular nol qoldiq bilan tugaydi:

$$a = bq_1 + r_1,\ 0 < r_1 < b,$$

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2,$$

…

[1] TATU Farg‘ona filiali “Axborot xavfsizligi” kafedrasi assistenti

$$r_{i-2} = r_{i-1}q_i + r_i,\ 0 < r_i < r_{i-1}$$

$$r_{i-1} = r_i q_{i+1}$$

a va b ning eng katta umumiy bo‘luvchisi, bo‘lish jarayonida nolga teng bo‘lmagan oxirgi qoldiqqa teng bo‘ladi.

Kengaytirilgan Evklid algoritmi esa nafaqat ikkita sonning EKUB ni va chiziqli diofant tenglamalarni yechishda va kriptografik usullarda foydalaniladigan modulli teskarilarni topish imkoniyatini beradi. Ya’ni, a*x+b*y=d tenlamadan a va b sonlarining EKUB(a;b) = d bo‘lsa yoki d ga karrali son bo‘lsa, x va y ni topish mumkin bo‘ladi.

Bu kengaytirilgan usul ko‘pincha modulli teskari sonni topishda, ya’ni a*x≡1(mod m) tengligini qanoatlantiradigan x ni topishda ham qo‘llaniladi.

Natijalar

Kengaytirilgan Evklid algoritimi yordamida quyida berilgan misolni yechishni tahlil qilamiz:

a = 3587 va b = 1819 sonlarini EKUB(a;b) ni toping:

3587 = 1819*1 + 1768

1819 = 1768*1 + 51

1768 = 51*34 + 34

51 = 34*1 + **17**

34 = 17*2 + 0

Natija EKUB(3587; 1819) = **17**.

Ushbu natijadan foydalangan holda quyidagi chiziqli diofant tenglamani yechishni ko‘rib chiqamiz:

1819x + 3587y = 17

biz yuqorida EKUB ni hisoblashda quyidagi ifodalarni hisoblaganmiz:

1768 = 3587 – 1819*1

51 = 1819 – 1768*1

34 = 1768 – 51*34

17 = 51 – 34*1

Endi bizdagi oxirgi natija topilgan qatordan boshlab, har bir qoldiqdan foydalangan holda, o‘rniga qo‘yish orqali x va y qiymatlarini topamiz.

17 = 51 – 34*1 = 51 – (1768 – 51*34)*1 = 51*35 – 1768*1

17 = (1819 – 1768*1)*35 – 1768*1 = 1819*35 – 1768*36

17 = 1819*35 – (3587 – 1819*1)*36 = 1819***71** – 3587***36**

Demak, natija **x = 71** va **y = -36** ga teng ekanligi kelib chiqdi.

Kengaytirilgan Evklid algoritmidan foydalangan holda hisoblanadigan yana bir amal, kriptografik usullarda keng qo‘llaniladigan modulli teskarini topish amalidan ham foydalanamiz. Misol uchun bizga *8 mod 13* bo‘yicha teskarisini, ya’ni x*8 ≡ 1 mod 13 topishimiz kerak bo‘lsin. EKUB (8;13) = 1, ekanligini aniqlab olamiz:

13 = 8*1 + 5

8 = 5*1 +3

5 = 3*1 + 2

3 = 2*1 +1

$$2 = 1*1 + 1$$

$$1 = 1*1 + 0$$

Endi, hosil bo‘lgan qoldiqlardan foydalangan holda modulli teskarini topamiz:

$$1 = 3 - 2*1$$

$$1 = 3 – (5 – 3*1)*1 = 3*2 – 5*1$$

$$1 = (8 – 5*1)*2 – 5*1 = 8*2 – 5*3$$

$$1 = 8*2 – (13 – 8*1)*3 = 8*\mathbf{5} – 13*3$$

Demak, natija **x = 5** ga teng bo‘ldi.

Muhokama

Kengaytirilgan Evklid algoritmi kriptografiyada, ayniqsa asimmetrik shifrlash tizimlarida, modular arifmetika, modular teskari qiymatlar va chiziqli diofant tenglamalar yechimini topishda muhim rol o‘ynaydi. Shuningdek, RSA, Elliptik egri chiziq (ECC) va boshqa kriptografik tizimlar uchun zaruriy vosita bo‘lib, tizimlarning xavfsizligini ta’minlashda samarali ishlaydi.

Xulosa

Kengaytirilgan Evklid algoritmi Evklid algoritmining kengaytmasi bo‘lib, u ikkita butun sonning EKUB ni va EKUB ni butun sonlarning chiziqli birikmasi sifatida ko‘rsatish usulini ham beradi. Uning ish sohasi kriptografiya va hisoblash matematikasi kabi sohalarda juda keng va dolzarbdir, shuning uchun u matematik nazariya va uning ilovalarida juda muhim mavzu hisoblanadi.

Foydalanilgan adabiyotlar

1. M.Aripov, A.S. Matyakubov Axborotlarni himoyalash usullari, 2014.
2. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.
3. Eknoyan, G. (2015). *The Euclidean Algorithm: An Introduction*.
4. Stinson, D. R. (2006). *Cryptography: Theory and Practice*. CRC Press.