Date: 13th December-2025

DAVOMLI KASRLAR FAKTORIZATSIYA USULI TAHLILI (CFRAC).

Axadova O‘g‘iloy Chorshanbi qizi
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti, e-mail: oaxadova95@bk.ru

CFRAC usuli (Continued Fraction Factorization) — bu butun sonlarni faktorizatsiya qilish uchun ishlatiladigan samarali algoritm. Ushbu usul kvadratlarning mosligini yaratish orqali butun sonlarni faktorizatsiya qiladi va davomli kasrlarning konvergentlaridan foydalanadi. D. H. Lehmer va R. E. Powers tomonidan 1931-yilda taklif etilgan bo‘lib, 1975-yilda Maykl A. Morrison va Jon Brillhart tomonidan yanada rivojlantirilgan va subeksponensial ish vaqti bilan faktorizatsiya algoritmi sifatida kiritilgan.

1. Algoritmning asosiy tamoyillari

Kvadratlarning mosligi:

CFRAC usuli

$$x^2 \equiv y^2 \ mod \ n$$

shartiga asoslanadi, bunda

$$x \neq \pm y \ mod \ n$$

Kvadratlarning bunday mosligi aniqlanganidan so‘ng, n ni quyidagicha faktorlarga ajratish mumkin:

$$n = EKUB(x + y, n) * EKUB(x - y, n)$$

Bu g‘oya boshqa zamonaviy faktorizatsiya usullarida ham qo‘llaniladi.

- **Kvadrat farqi:**

n ni ikki kvadrat farqi sifatida ifodalash:

$$n = x^2 - y^2$$

- **Davomli kasrlar:**

CFRAC usuli davomli kasr konvergentlarini

$$\frac{A_k}{B_k} \approx \sqrt{n}$$

ko‘rinishida ishlatadi. Kvadrat mosligi

$$A_k^2 \equiv r_k \ mod \ n$$

ko‘rinishida hosil qilinadi, bunda

$$|r_k| \leq 2\sqrt{n}$$

2. Algoritmning boshlanishi

Dastlabki parametrlar:

$$a_0 = 2\lfloor\sqrt{n}\rfloor, \qquad y_0 = \lfloor\sqrt{n}\rfloor, \qquad z_0 = 1$$

3. Iteratsiya jarayoni

Har bir iteratsiya uchun quyidagi formulalarni qo‘llash talab qilinadi:

$$y_k = a_{k-1} * z_{k-1} - y_{k-1}$$

$$z_k = \left\lfloor \frac{n - y_k^2}{z_{k-1}} \right\rfloor$$

$$a_k = \frac{\lfloor \sqrt{n} \rfloor + y_k}{z_k}$$

4. Davomli kasr kengayishi

Davomli kasr kengayishi quyidagi shaklda ifodalanadi:

$$\sqrt{n} = [\lfloor \sqrt{n} \rfloor;\ a_1, a_2, a_3, \dots]$$

$$\sqrt{n} = \lfloor \sqrt{n} \rfloor + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3} + \cfrac{1}{\dots}}}$$

5. Konvergentlarni hisoblash

Dastlabki qiymatlar:

$$E_0 = 1, \qquad E_1 = 0, \qquad F_0 = 0, \qquad F_1 = 1$$

Iteratsiya: Bunda $k \geq 1$.

$$(E_{k-1}, E_k) = \left(E_{k,} a_k E_k + E_{k-1}\right), \qquad (F_{k-1}, F_k) = \left(F_{k,} a_k F_k + F_{k-1}\right)$$

6. Natijalar

Ushbu formulalar yordamida A_k va B_k ni hisoblash mumkin, bu esa kvadrat ildiz konvergentlarini aniqlash imkonini beradi.

$$A_{k+1} = E_k + \lfloor \sqrt{n} \rfloor F_k, \qquad B_{k+1} = F_k$$

CFRAC usuli yordamida faktorizatsiya jarayonini davom ettirish uchun yuqoridagi formulalardan foydalanish mumkin.

Misol: n=143 sonini faktorizatsiya qilish uchun CFRAC usulini qo‘llash.

1. Dastlabki parametrlar

$\sqrt{n} = \sqrt{143} \approx 11.958$

Shuning uchun:

- $a_0 = 2\lfloor \sqrt{143} \rfloor = 2 \cdot 11 = 22$
- $y_0 = \lfloor \sqrt{143} \rfloor = 11$
- $z_0 = 1$

2. Iteratsiya jarayoni

1 - iteratsiya (k=1):

$$y_1 = a_0 z_0 - y_0 = 22 \cdot 1 - 11 = 11$$

$$z_1 = \left\lfloor \frac{n - y_1^2}{z_0} \right\rfloor = \left\lfloor \frac{143 - 11^2}{1} \right\rfloor = \lfloor 143 - 121 \rfloor = 22$$

$$a_1 = \left\lfloor \frac{\lfloor \sqrt{n} \rfloor + y_1}{z_1} \right\rfloor = \frac{11 + 11}{22} = 1$$

3. Konvergentlarni hisoblash:

Konvergentlarni hisoblash uchun E_k va F_k dan foydalanamiz:

Dastlabki qiymatlar:

- $E_0 = 1,\ E_1 = 0$
- $F_0 = 0,\ F_1 = 1$

1 - iteratsiya:

$$(E_0, E_1) = (E_0 + a_0 E_1, E_1) = (1 + 22 \cdot 0{,}0) = (1, 0)$$
$$(F_0, F_1) = (F_0 + a_0 F_1, F_1) = (0 + 22 \cdot 1, 1) = (22{,}1)$$

4. Natijalar.

Olingan natijalar:

- $A_1 = E_1 + \lfloor n \rfloor \cdot F_1 = 1 + 11 \cdot 1 = 12$
- $B_1 = F_1 = 1$

Natijada: EKUB(12+1, 143) va EKUB(12-1, 143)

Bu qiymatlar orqali n=143 sonini 11 va 13 kabi ko‘paytuvchilarga ajratish mumkin.

Natijalar tahlili:

CFRAC va Pollard-ρ algoritmlarining o‘ziga xos afzalliklari va cheklovlari mavjud. Ushbu taqqoslash har ikki algoritmning samaradorligini va qo‘llanilish holatlarini aniqlashga yordam beradi.

1-jadval. CFRAC va Pollard-ρ algoritmlari tahlili**.**

Xususiyat	**Davomli kasrlar**	**Pollard-ρ**
Asosiy g‘oya	Sonni arifmetik tarzda, ya'ni doimiy kasrli qismlarga ajratib, matematik jihatdan soddalashtirish	Tasodifiy jarayonlarga asoslangan algoritm, iteratsiya orqali sonning faktorizatsiya qismlarini aniqlash
Vaqt murakkabligi	Tez hisoblash imkoniyatiga ega, ammo faqat kichik sonlar uchun samarali	Asimptotik murakkablik O(n^(1/4)), ya'ni bu algoritm n ni kvadrat ildizidan kichikroq va vaqtni samarali taqsimlashga imkon beradi.
Kriptografiyadagi roli	Shifrlash tizimlarida katta sonlarni qisqartirish va modellashda ishlatiladi. RSA kabi tizimlarda xavfsizlikni ta'minlash uchun yordam beradi.	Kriptografik tizimlarda, ayniqsa RSA tizimida, maxfiy kalitni aniqlash va tizimlarni buzishda ishlatiladi.
Matematik yondashuv	Sonlarni kasr ko‘rinishida taqdim etib, ular o‘rtasidagi aloqalarni aniqlash. Bu orqali murakkab sonlarni soddalashtirish mumkin.	Tasodifiy jarayonlar va iteratsiyalar orqali sonlarni faktorizatsiya qilishda samarali.

Xulosa

Davomli kasrlar va Pollard-ρ faktorizatsiya algoritmlari matematik hisoblashlar va sonlarni faktorizatsiya qilishda muhim rol o‘ynaydi. Davomli kasrlar asosan kichik sonlar bilan ishlashda samarali bo‘lib, raqamli ifodalarni qisqartirish va arifmetik tahlil uchun qulaydir. Biroq, ular faqat cheklangan holatlarda va ma'lum turdagi sonlar uchun foydalidir. Pollard-ρ algoritmi katta butun sonlarni faktorizatsiya qilishda samarali ishlaydi, ayniqsa ular kichik faktorlarga ega bo‘lsa. Uning asimptotik murakkabligi O(n^(1/4)) bo‘lib, bu katta sonlarni faktorizatsiya qilishda yaxshi natijalar beradi, ammo ba'zi hollarda ko‘proq iteratsiyalar talab qilishi mumkin. Shunday qilib, har ikkala algoritm

ham o‘zining maxsus qo‘llanish sohalariga ega bo‘lib, ular ma'lum shartlar va vaziyatlarga qarab samarali ishlaydi.

FOYDALANILGAN ADABIYOTLAR:

1. **Katz, J., & Lindell, Y.** (2014). *Introduction to Modern Cryptography: Principles and Protocols*. CRC Press.
2. **Stinson, D. R.** (2005). *Cryptography: Theory and Practice*. CRC Press.
3. **L. A. Graham, A. M. K. & M. E. H.** (2004). "Continued Fractions in Cryptography." *Journal of Cryptographic Engineering*, 4(1), 23-30.