YAKOBI SIMVOLI VA UNING AMALIY TADBIQLARI HAQIDA

Sharipov Ozod Odilovich
Navoiy davlar universiteti magistranti,
e-mail: *ozodsharipov1023@gmail.com*

Annotatsiya: *Ushbu maqolada Eyler mezoni va Yakobi simvolining amaliy tadbiq etish jarayonidagi qiyinchiliklar va ularni bartaraf etish yo'llari ko'rib chiqilgan. Eyler mezoniga asoslangan holda kvadratik chegirmalar va nochegirmalarni aniqlashning nazariy jihatlari bayon etilgan. Shuningdek Yakobi simvolining asosiy xossalari, uni hisoblashda qulayligi, ba'zi bir kamchiliklari va Gauss lemmasi asosida olingan natijalar keng muhokama qilinadi.*

Kalit so'zlar: *Eyler mezoni, Yakobi simvoli, kvadratik chegirma, kvadratik nochegirma, Gauss lemmasi, tub sonlar, modulli arifmetika.*

Eyler mezoni va Yakobi simvoli nazariy matematikaning muhim qismlaridan biri bo'lib, ularning amaliy tadbiqi raqamli texnologiyalar, shifrlash algoritmlari va primal arifmetikada keng qo'llaniladi. Eyler mezoni va Yakobi simvoli yuqori darajadagi hisoblashlar va tahlillarni talab qiladigan zamonaviy matematik va texnologik jarayonlar uchun muhim ahamiyat kasb etadi.

1-teorema (Eyler mezoni). Agar a son p modul bo'yicha kvadratik chegirma bo'lsa, u holda

$$a^{\frac{p-1}{2}} \equiv 1(\text{mod p}) \qquad (1)$$

taqqoslama, a son p modul bo'yicha nochegirma bo'lganda esa,

$$a^{\frac{p-1}{2}} \equiv -1(\text{mod p}) \qquad (2)$$

taqqoslama o'rinli bo'ladi.

Isbot. Ferma teoremasiga ko'ra

$$a^{p-1} \equiv 1(mod\ p),\ \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0\ (mod\ p).$$

Ikkinchi taqqoslamalarning chap tomonidagi ko'paytuvchilardan bittasigina p ga bo'linadi. Bu ikkita ko'paytuvchilar bir vaqtda p ga bo'linmaydi, aks holda, ularning ayirmasi 2 ham p ga bo'linadigan bo'lar edi, lekin p toq tub son bo'lganligi uchun $(2, p) = 1$.

Shu sababli (1) va (2) taqqoslamalarining bittasigina bajariladi. Haqiqatdan, bunday holda har bir a kvadratik chegirma uchun x ning $(x, p) = 1$ shartini qanoatlantiradigan shunday qiymat mavjudki, bu qiymat uchun

$$a \equiv x^2\ (\text{mod } p) \qquad (3)$$

taqqoslama bajariladi. Bundan esa $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}}$ (mod p) yoki

$$a^{\frac{p-1}{2}} \equiv x^{p-1}\ (\text{mod p}) \equiv 1(\text{mod p})$$

kelib chiqadi, demak, a son (1) taqqoslamani qanoatlantiradi. Shu bilan birga, (1) taqqoslamaning barcha yechimlari kvadratik chegirmalardan iborat, chunki taqqoslama $\frac{p-1}{2}$ darajali bo'lganligi uchun $\frac{p-1}{2}$ dan ortiq yechimga ega bo'lmaydi. Shuning uchun kvadrat nochegirmalar (2) taqqoslamani qanoatlantiradi.

Lejandr simvolini hisoblashda suratini tub ko'paytuvchilarga ajratish eng katta qiyinchilik tug'diradi, surat yetarlicha katta bo'lgan holda ko'paytuvchilarga ajratish masalasi amalda bajarilmay qolishi mumkin. Maxraj toq tarkibli son bo'lgan holda Lejandr simvoli Yakobi simvoli deyiladi. Undan ko'paytuvchilarga ajratishdan qutilish uchun foydalaniladi. [17]

Tarif. Faraz qilaylik $P = p_1 p_2 \dots p_s$ berilgan bo'lsin. Bunda p_i toq tub sonlar bo'lib, ularning orasida tenglari ham bo'lishi mumkin. Yakobi simvoli $\left(\frac{a}{b}\right)$ quyidagi

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_s}\right)$$

tenglik bilan aniqlanadi, bunda $\left(\frac{a}{p_1}\right)$ (i=1, …, s) -Lejandr simvolidir.

Ta'rifga ko'ra, Lejandr simvoli $\left(\frac{a}{p}\right)$ Yakobi simvolining xususiy holi bo'lib, undan $P = p$ bo'lganda kelib chiqadi. Shunday qilib, tub modul $P = p$ uchun

$$x^2 \equiv a \pmod{p}$$

taqqoslama yechimga ega bo'lmasa, (-1) ga teng bo'ladi. Shu bilan birga, Yakobi simvoli $\left(\frac{a}{p}\right)$ tarkibiy modul uchun $x^2 \equiv a \pmod{p}$ taqqoslama yechimga ega bo'lmasa ham (+1) ga teng bo'lishi mumkin.

Masalan, $x^2 \equiv 2 \pmod{15}$ taqqoslama yechimga ega emas, lekin Yakobi simvoli

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1)^3 = +1$$

ga teng bo'ladi.

Yakobi simvolining xossalari Lejandr simvolining xossalariga o'xshash bo'lib, bu xossalarni o'rganishda har gal p orqali ixtiyoriy toq sonni belgilab, $\left(\frac{a}{p}\right)$ Yakobi simvolida $(a, p) = 1$ deb olamiz.

1-xossa. Agar $a \equiv a_1 \pmod{p}$ bo'lsa, u holda

$$\left(\frac{a}{b}\right) = \left(\frac{a_1}{p}\right).$$

Isbot. Haqiqatdan, Yakobi simvolining ta'rifiga va Lejandr simvolining 1-xossasiga ko'ra

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_s}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\dots\left(\frac{a_1}{p_s}\right) = \left(\frac{a_1}{p}\right).$$

chunki a son p modul bo'yicha a_1 bilan taqqoslanuvchi bo'lsa, u holda u p sonning bo'luvchilari p_1, p_2, …, p_s modullar bilan ham taqqoslanuvchi bo'ladi.

[17] Isroilov, M.I., Soliyeev, A.S. (2003). *Sonlar Nazariyasi*. Toshkent: Fan nashriyoti.

2-xossa. $\left(\frac{1}{p}\right) = 1$

Isbot. Haqiqatdan,

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_s}\right) = 1.$$

3-xossa. $(\frac{1}{p}) =(-1)^{\frac{p-1}{2}}$

$$\left(\frac{-1}{p}\right)= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\dots\left(\frac{-1}{p_s}\right) = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_s-1}{2}}. \quad (4)$$

Lekin,

$$\frac{p-1}{2} = \frac{p_1p_2\dots p_s-1}{2} =\frac{\left(1+2\cdot\frac{p_1-1}{2}\right)\left(1+2\cdot\frac{p_2-1}{2}\right)\dots\left(1+2\cdot\frac{p_s-1}{2}\right)-1}{2}$$
$$= \frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_s-1}{2}+2N \qquad (5)$$

(4) va (5) dan

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

kelib chiqadi.

4-xossa. $\left(\frac{a_1a_2\dots a_n}{p}\right) =\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \dots \left(\frac{a_n}{p}\right)$

Isbot. Haqiqatdan,

$\left(\frac{a_1a_2\dots a_n}{p}\right) =\left(\frac{a_1a_2\dots a_n}{p_1}\right)\dots\left(\frac{a_1a_2\dots a_n}{p_s}\right) =\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \dots \left(\frac{a_n}{p}\right) \dots\left(\frac{a_1}{p_s}\right)\left(\frac{a_2}{p_s}\right)\dots\left(\frac{a_n}{p_s}\right) = = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)$ ... $\left(\frac{a_n}{p}\right)$ $t$englik o'rinli.

Xususiy holda, $\left(\frac{ab^2}{p}\right)= \left(\frac{a}{p}\right)$ bo'ladi.

5-xossa. $\left(\frac{2}{p}\right) =(-1)^{\frac{p^2-1}{8}}$

Isbot. Haqiqatdan, Yakobi simvolining ta'rifi va Lejandr simvolining 5-xossasidan

$$\left(\frac{2}{p}\right) =\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right) \dots\left(\frac{2}{p_s}\right)= (-1)^{\frac{{p_1}^2-1}{8}+\frac{{p_2}^2-1}{8}+\frac{{p_s}^2-1}{8}} \qquad (6)$$

hosil bo'ladi.

Lekin, $\frac{p^2-1}{8} =\frac{{p_1}^2{p_2}^2\dots {p_s}^2-1}{8} = \frac{\left(1+8\cdot\frac{{p_1}^2-1}{8}\right)\left(1+8\cdot\frac{{p_2}^2-1}{8}\right)\dots\left(1+8\cdot\frac{s^2-1}{8}\right)-1}{8} =\frac{{p_1}^2-1}{8}+\frac{{p_2}^2-1}{8}+\frac{{p_s}^2-1}{8}+2N.$ (7)

Bu yerda 5-xossa (6) va (7) dan kelib chiqadi.

5-teorema. (Kvadratik chegirmalarning o'zarolik qonuni). Faraz qilaylik, P va Q o'zaro tub va toq sonlar bo'lsin. U holda,

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} = \left(\frac{P}{Q}\right) \qquad (8)$$

bo'ladi.

Isbot. Faraz qilaylik, $Q = q_1q_2\dots q_r$ bo'lib, q_i tub sonlar (ular orasida tenglari ham bo'lishi mumkin) bo'lsin. U holda Yakobi simvolining ta'rifi va Lejandr simvolining 4-xossasiga ko'ra,

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{P_1}\right)\left(\frac{Q}{Q_2}\right)\cdots\left(\frac{Q}{P_s}\right)=\prod_{k=1}^{s}\prod_{m=1}^{r}\left(\frac{q_m}{p_k}\right)=(-1)^{\sum_{k=1}^{s}\sum_{m=1}^{r}\frac{p_k-1}{2}\cdot\frac{q_m-1}{2}}\prod_{k=1}^{s}\prod_{m=1}^{r}\left(\frac{p_k}{q_m}\right)=$$

$$(-1)^{\left(\sum_{k=1}^{s}\frac{p_k-1}{2}\right)\left(\sum_{m=1}^{r}\frac{q_m-1}{2}\right)}\cdot\left(\frac{P}{Q}\right) \qquad (9)$$

hosil bo'ladi.

Biz 3-xossaning isboti jarayonida

$$\frac{p-1}{2}=\sum_{k=1}^{s}\frac{p_k-1}{2}+2N,\quad \frac{Q-1}{2}=\sum_{m=1}^{r}\frac{q_m-1}{2}+2N_1 \qquad (10)$$

tengliklarni o'rinli bo'lishini ko'rgan edik. (9) va (10) tengliklardan (6) kelib chiqadi. Tub modullar uchun Yakobi simvolining xossalaridan foydalanib, Lejandr simvolini tezroq hisoblash mumkin.

Endi Yakobi simvoli bo'yicha quyidagi taqqoslamalarning yechimining mavjud yoki mavjud emasligini aniqlaylik:

1. $x^2 \equiv 2 \pmod 3$ (11)

$\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1$

2. $x^2 \equiv 2 \pmod 5$ (12)

$\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1$

3. $x^2 = 2 \pmod{3\cdot5}$ (13)

$\left(\frac{2}{3\cdot5}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)(-1)=1$

Agar e'tibor qilsak $a \not\equiv b \pmod m$ $x^2 \equiv 2 \pmod 3$ va $x^2 \equiv 2 \pmod 5$ taqqoslamalar yechimga ega emas, Lekin $x^2 = 2 \pmod{15}$ yechimga ega, ya'ni,

$a \not\equiv b \pmod{m_1}$, $a \not\equiv b \pmod{m_2}$ $a \equiv b \pmod{m_1m_2}$.

Bu esa taqqoslamalarning xossasiga ziddir. Xatolik qayerda ekanligini aniqlash quyidagi algoritm yordamida amalga oshiriladi:

$$\left(\frac{a}{p_1p_2\dots p_k}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right) \qquad (14)$$

Bu simvollarni navbat bilan hisoblaymiz.

Birinchi $\left(\frac{a}{p_1}\right)$ agar bu simvol 1 ga teng bo'lsa jarayonni davom ettiramiz agar (-1) ga teng bo'lsa, jarayon to'xtatiladi hamda $x^2 \equiv a \pmod{p_1, p_2, \dots, p_k}$ yechimga ega emas. Xuddi shu narsani keying simvollarni hisoblashga qo'llaymiz.

Misol: $x^2 \equiv 2 \pmod{3\cdot15}$

$\left(\frac{2}{3}\right) = -1$ edi, demak taqqoslama yechimga ega emas.

FOYDALANILGAN ADABIYOTLAR:

1. Isroilov, M.I., & Soliyeev, A.S. (2003). *Sonlar Nazariyasi*. Toshkent: Fan nashriyoti.
2. Виноградов, И.М. (1972). *Основы теории чисел*. – М.: Наука.