Eyler funksiyasi. Eyler va Ferma teoremalari.

Chegirmalarning keltirilgan sistemasidagi elementlar sonini aniqlash uchun *Eyler funksiyasi* deb ataluvchi $\varphi(m)$ funksiyadan foydalaniladi.

$m-$ ixtiyoriy musbat son bo`lsin, $m$ dan katta bo`lmagan va m bilan o`zaro tub bo`lgan bo`lgan musbat sonlar sonini $\varphi(m)$ bilan belgilanadi.

TA`RIF. Agar quyidagi ikkita shart bajarilsa, $\varphi(m)$ sonli funksiya Eyler funksiyasi deyiladi:

1. $\varphi(1)=1$
2. $\varphi(m)$ funksiya m dan kichik va m bilan o`zaro tub bolgan musbat sonlar soni.

1-TEOREMA. $\varphi(m)$ ta $(m>1)$ sonlarning ixtiyoriy to`plami, ya`ni m bilan o`zaro tub va $m$ modul` bo`yicha ixtiyoriy ikkitasi taqqoslanmaydigan sonlar to`plami m modul` bo`yicha chegirmalarning keltirilgan sistemasi bo`ladi.

2-TEOREMA. a butun son m bilan o`zaro tub va $b_1, b_2, \dots, b_{\varphi(m)}-m$ modul` bo`yicha chegirmalarning keltirilgan sistemasi bo`lsin, u holda

$$ab_1, ab_2, \dots, ab_{\varphi(m)}$$

ham m modul bo`yicha chegirmalarning keltirilgan sistemasi bo`ladi.

ISBOTI. 1-teoremaga ko`ra,

$$ab_1, ab_2, \dots, ab_{\varphi(m)}$$

sonlar to`plamidagi ixtiyoriy ikkitasi $m$ modul` bo`yicha taqqoslanmasligini ko`rsatish kifoya. Haqiqatan, agar

$$ab_i = ab_k (modm) \quad i \neq k$$

bo`lsa, $(a,m)=1$ bo`lgani uchun

$$b_i = b_k (modm)$$

bo`ladi. Bunday bo`lishi mumkin emas, chunki b_i, b_k lar m modul` bo`yicha chegirmalarning turli sinflariga tegishli.

**TA`RIF.** Natural sonlar to`plamida aniqlangan f funksiya uchun $(m,n)=1$ bo`lganda

$$f(m\cdot n)=f(m)\cdot f(n)$$

tenglik bajarilsa, u holda f funksiya multiplikativ funksiya deyiladi.

TEOREMA. Eyler funksiyasi multiplikativ funksiyadir.

TEOREMA. Eyler funksiyasi multiplikativ funksiyadir.

ISBOTI. a va b o`zaro tub bo`lgan musbat butun sonlar bo`lsin. $a \cdot b$ dan kichik bo`lgan barcha manfiymas sonlar to`plami M ni qaraylik. M dagi har bir sonni, qoldiqli bo`lish teoremasiga asosan, yagona tarzda

$$b \cdot q + r \qquad \left(r \in \{0,1, \dots, b-1\},\ q \in \{0,1,2, \dots, a-1\}\right)$$

ko'rinishda ifodalash mumkin.

$bq + r$ son a bilan o`zaro tub bo`lishi uchun $(b, r) = 1$ bo`lishi zarur va yetarli. Bunday $r$ sonlar soni $\varphi(b)$ ta bo`ladi. r_1 $-$shunday sonlarning biri bo`lsin. U holda

$$r_1,\ b + r_1,\ 2b + r_1,\ \dots,\ b(a-1) + r_1$$

sonlar ketma-ketligi a modul bo`yicha chegirmalarning to`la sistemasini tashkil etadi. Shuning uchun, bu sonlar orasida a bilan o`zaro tub bo`lgan sonlar $\varphi(a)$ ta bo`ladi. Shunday qilib, har bir $r_1$ songa ($b$ bilan o`zaro tub bo`lgan) $bq + r_1$ ko`rinishdagi a bilan o`zaro tub sonlar va demak, ab bilan ham o`zaro tub bo`lgan $\varphi(a)$ ta son mos keladi. Shuning uchun, ab bilan o`zaro tub bo`lgan sonlar soni $\varphi(a) \cdot \varphi(b)$, ya`ni

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

bo`ladi.

TEOREMA. Agar $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ bo`lsa, u holda

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_n}\right)$$

bo`ladi.

ISBOTI. $\varphi(m)$ funksiya mul`tiplikativ bo`lgani uchun, bu funksiyani $\varphi(p_k^{\alpha_k})$ uchun hisoblashni bilish kifoya.

p^α dan kichik manfiy bo`lmagan va $p^\alpha$ bilan o`zaro tub bo`lmagan sonlar sonlar soni $p^{\alpha-1}$ ga teng, chunki faqat $kp$, $0 \le k < p^{\alpha-1}$ sonlargina $p^\alpha$ bilan o`zaro tub bo`lmaydi. Shuning uchun $p^\alpha$ dan kichik va $p^\alpha$ bilan o`zaro tub sonlar soni

$$p^{\alpha} - p^{\alpha-1}$$

ta bo`ladi.

$$\varphi(p^{\alpha}) = p^{a}(1 - \frac{1}{p})$$

$m = p_1{}^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}$ va φ multiplikativ bo`lgani uchun

$$\begin{aligned}\varphi(m) = \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdot ... \cdot \varphi\left(p_n^{\alpha_n}\right) \\ = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) ... p_n^{\alpha_n}\left(1 - \frac{1}{p_n}\right) \\ = p_1{}^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_n}\right) \\ = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_n}\right)\end{aligned}$$

EYLER TEOREMASI. Agar *a* butun son m bilan o`zaro tub bo`lsa, u holda

$$a^{\varphi(m)} = 1(modm) \qquad (1)$$

bo`ladi.

ISBOTI. $a_1, a_2, ... , a_{\varphi(m)}$ (2) - m modul bo`yicha chegirmalarning keltirilgan sistemasi bo`lsin, u holda 2-teoremaga ko`ra,

$$aa_1, aa_2, ... , aa_{\varphi(m)} \qquad (3)$$

ham m modul` bo`yicha chegirmalarning keltirilgan sistemasi bo`ladi. Shuning uchun (3) sonlar ko`paytmasi (2) sonlar ko`paytmasi bilan m modul` bo`yicha taqqoslanadi, ya`ni

$$a^{\varphi(m)}a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(m)} \equiv a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(m)}(modm)$$

$a_1 a_2 \cdot ... \cdot a_{\varphi(m)}$ ko`paytma $m$ bilan o`zaro tub, shuning uchun taqqoslamaning xossasiga ko`ra, $a_1 a_2 ... a_{\varphi(m)}$ ga bo`linishi mumkin, demak,

$$a^{\varphi(m)} \equiv 1(modm)$$

bo`ladi.

FERMA TEOREMASI. Agar *a* son p tub songa bo`linmasa, u holda

$$a^{p-1} \equiv 1(modp)$$

taqqoslama o`rinli bo`ladi.

ISBOTI. a son p tub songa bo`linmasa, u holda $(a,p)=1$ bo`ladi. Bundan, Eyler teoremasiga ko`ra, $m=p$ va $\varphi(p)=p-1$ ekanligidan

$$a^{\varphi(p)} \equiv 1(modp)$$

$$a^{p-1} \equiv 1(modp)$$

bo`ladi, yoki $(a,p)=1$ bo`lgani uchun

$$a^{p} \equiv a(modp).$$

Misol 1. Eyler funksiyasini hisoblang: $\varphi(18\cdot 42)$

Yechish: 18 bilan o'zaro tub bo'lgan musbat sonlar: 1, 5, 7, 11, 13, 17. Demak, 18 bilan o'zaro tub bo'lgan musbat sonlar soni 6 ta; 42 bilan o'zaro tub bo'lgan musbat sonlar: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41. Demak, 42 bilan o'zaro tub bo'lgan musbat sonlar soni 12 ta

$\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$ ga asosan $\varphi(18\cdot 42)=\varphi(18)\cdot\varphi(42)=6\cdot 12=72$, ya'ni $\varphi(18\cdot 42)=72$ yechim hosil bo'ladi.

Misol 2. $7x\equiv 10(mod\ 4)$ taqqoslamani Eyler teoremasi yordamida yeching.

Yechish: $ax\equiv b(mod\ m)$ taqqoslama (a,m)=1 bo'lsa, u hola uning yechimi $x\equiv b\cdot a^{\varphi(m)-1}(mod\ m)$ formula yordamida topiladi. Haqiqatan ham Eyler teoremasiga ko'ra $a^{\varphi(m)-1}\equiv 1(mod\ m)$. Bundan $a^{\varphi(m)}b\equiv b(mod\ m)$ va $a\cdot a^{\varphi(m)-1}b\equiv b(mod\ m)$ larni hosil qilsak, $x\equiv ba^{\varphi(m)-1}(mod\ m)$ kelib chiqadi.

$7x\equiv 10(mod\ 4)$ dan a=7, b=10, m=4 yechim $x\equiv 10\cdot 7^{\varphi(4)-1}(mod\ 4)$ ni topish uchun $\varphi(4)$ ni aniqlaymiz. $4=2^2$ ekanligidan $\varphi(4)=4\cdot\left(1-\frac{1}{2}\right)=2$ kelib chiqadi. Demak, $x\equiv 10\cdot 7^{2-1}(mod\ 4)$. Agar $10\equiv 2\ (mod\ 4)$, $7\equiv 3\ (mod\ 4)$, $6\equiv 2\ (mod\ 4)$ taqqoslamalaran foydalansak $x\equiv 10\cdot 7^{2-1}(mod\ 4)=2\cdot 3=6\equiv 2\ (mod\ 4)$, ya'ni $x\equiv 2\ (mod\ 4)$ yechimni hosil qilamiz.

Birinchi darjali taqqoslamalar va ularni yechish usullari.

**1-TA`RIF**. Ushbu $ax\equiv b(modm)$ (1) ko`rinishdagi taqqoslama bir noma`lumli birinchi darajali taqqoslama deyiladi. (bu erda a va b-butun sonlar, m-natural son)

**2-TA`RIF**. Agar (1) taqqoslamada $x = x_0$ bo`lganda $ax_0 \equiv b(modm)$ taqqoslama to`g`ri bo`lsa, u holda x_0 son taqqoslamani qanoatlantiradi deyiladi.

**3-TA`RIF**. $m$ modul` bo`yicha taqqoslamaning yechimlar soni deb, bu taqqoslamaning m modul` bo`yicha chegirmalarning to`liq sistemadagi yechimlar soniga aytiladi.

Agar *a* son (1) taqqoslamani qanoatlantirsa u holda m modul` bo`yicha *a* bilan taqqoslanuvchi $\forall\, b$ son ham bu taqqoslamani qanoatlantiradi, bunday 2 ta yechim bitta deb qaraladi.

Misol. $5x \equiv 3(mod6),\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\ \ x = 3(mod6)\ \ x_0 = 3 + 6t,\ \ \forall t \in \mathbb{Z}\ \ x_0 = 9,\ 15,\ \ldots$ sonlar ham bu taqqoslamani qanoatlantiradi.

TEOREMA. Agar $(a, m) = 1$ bo`lsa, u holda (1) taqqoslama yagona yechimga ega bo`ladi.

ISBOTI. m modul` bo`yicha chegirmalarning to`la sistemasi

$$x_1,\ x_2, \ldots, x_m$$

bo`lsin, u holda

$$ax_1,\ ax_2, \ldots, ax_m \qquad (2)$$

ham chegirmalarning to`la sistemasi bo`lishi ma`lum. Agar (1) da $x$ o`rniga ketma ket (2) dagi chegirmalarni qo`yib ko`rsak, u holda bu taqqoslamaning chap qismi chegirmalarning to`la sistemasidagi barcha qiymatlardan o`tadi. Bu esa bitta va faqat bitta x_i son uchun ax_i sonning b songa tegishli bo`lgan chegirma sinfiga tegishli bo`lishini bildiradi, bunda

$$ax_i \equiv b(modm)$$

bo`ladi. Demak, agar $(a, m) = 1$ bo`lsa, (1) taqqoslama yagona bo`lgan

$x = x_i(modm)$ yoki $x = x_i + mt,\ t \in \mathbb{Z}$

yechimga ega bo`ladi.

TEOREMA. Agar $(a, m) = d > 1$ va b son d ga bo'linmasa, u holda $ax \equiv b(modm)$ taqqoslama yechimga ega bo`lmaydi.

ISBOTI. Faraz qilaylik, $ax \equiv b(modm)$ taqqoslama uchun m modul` bo`yicha x_1 sinf yechim bo`lsin va $x_1 \in \overline{x_1}$ bo`lsin, u holda

$$ax_1 \equiv b(modm) \text{ yoki } ax_1 - b = mt, \quad t \in \mathbb{Z}$$

bo`ladi. $a \vdots d \wedge m \vdots d$ dan $b \vdots d$ kelib chiqadi. Bunday bo`lishi mumkin emas, shartga ko`ra b son d ga bo'linmaydi. Demak, teorema isbotlandi.

TEOREMA. Agar $(a,m) = d > 1$ va b son d ga bo'linsa, u holda $ax \equiv b(modm)$ taqqoslama d ta turli yechimlarga ega bo`ladi. Bu yechim $\frac{m}{d}$ modul` bo`yicha bitta sinfni tashkil qiladi.

ISBOTI. Shartga ko`ra $a, b$ va $m$ sonlar $d$ ga bo`linadi. $a = a_1 d,\ b = b_1 d \ \wedge \ m = m_1 d$ (1) ni d ga bo`lib, unga teng kuchli bo`lgan

$$ax_1 \equiv b_1(modm_1) \qquad (4)$$

taqqoslamaga ega bo`lamiz. Haqiqatan $x = \alpha$ son (4) ni qanoatlantirsa, u holda $a\alpha \equiv b(modm)$ taqqoslamaga ega bo`lamiz, uning ikkala qismini va modulni d ga bo`lib, $a_1\alpha = b_1(modm_1)$ hosil bo`ladi. Demak, α (4) ni qanoatlantiradi.

Aksincha, $x = \beta$ butun son $a_1\beta \equiv b_1(modm_1)$ taqqoslamani qanoatlantirsin. Bu taqqoslamaning ikkala qismini va modulni d ga ko`paytirib, $a\beta \equiv b(modm)$ taqqoslamani hosil qilamiz. Demak, β (1) ni qanoatlantiradi.

Shunday qilib (1) va (4) teng kuchli ekan. (4) dagi $(a, m_1) = 1$, shuning uchun bu taqqoslama

$$x = x_0(modm) \quad \vee \quad x = x_0 + mt,\ (t \in t)$$

yagona echimga ega, bu erda x_0 m modul` bo`yicha manfiymas eng kichik chegirma bo`lsin yoki

$$\ldots\ x_0 - 2m_1,\ x_0 - m_1,\ x_0,\ x_0 + m,\ x_0 + 2m_1, \ldots, x_0 + (d-1)m_1,\ x_0 + d_{m_1},\ x_0 + (d+1)m_1,\ \ldots \qquad (5)$$

(5) dagi har bir chegirma (4) ni qanoatlantiradi va demak, (1) ni ham qanoatlantiradi.

$m_1 = \frac{m}{d}$ modul` bo`yicha (5) dagi hamma sonlar bitta sinfga tegishli, lekin $m = m_1 d$ modul` bo`yicha ular turli sinflarga tegishli bo`ladi, bu sinflarning chegirmalari esa

$$(6) \qquad x_0,\ x_0 + m_1,\ x_0 + 2m_1, \ldots,\ x_0 + (d-2)m_1,\ x_0 + (d-1)m_1$$

Demak, (1) m modul` bo`yicha d ta turli echimga ega bo`ladi:

$$x \equiv x_0(modm),\ \ x \equiv x_0 + m_1(modm)$$

$$x \equiv x_0 + 2m_1(modm), \dots,\ x \equiv x_0 + (d-1)m_1(modm)$$

bu erda x_0 $-$(3) taqqoslamaning yechimi bo`lgan sinfning eng kichik manfiymas chegirmasi.

Misol. $3x \equiv 6(mod9)$

$(3{,}6) = 3$ ∧ 6 ⁝ 3 =2 3 ta yechimga ega.

$$x = 2(mod3)$$

Demak, berilgan taqqoslamaning barcha yechimlari

$$x = 2(mod9),\ \ x = 2 + 3(mod9) \equiv 5(mod9)$$

$$x \equiv 2 + 3 \cdot 2(modm) \equiv 8(mod9)$$

bo`ladi.

TEOREMA. Agar $(a, m) = 1$ bo`lsa, u holda $ax \equiv b(modm)$ taqqoslamaning yechimi $x \equiv ba^{\varphi(m)-1}(modm)$ bo`ladi.

ISBOTI. $(a, m) = 1$ bo`lgani uchun Eyler teoremasiga ko`ra $a^{\varphi(m)} \equiv 1(modm)$. Bundan

$$a^{\varphi(m)} \cdot b = b(modm)$$

$a \cdot a^{\varphi(m)-1} \cdot b = b(modm)$ (3)

Demak, (1) ∧ (3) ni solishtirsak, $x = a^{\varphi(m)-1} \cdot b(modm)$

yechimi ekani ko`rinadi.

Misol. $5x \equiv 3(mod6)$

$(5{,}6) = 1$ bo`lgani uchun $x = 3 \cdot 5^{\varphi(6)-1}(modm) \equiv 3 \cdot 5(modm) \equiv 15 \equiv 3(modm)$.

Sinash usuli. Bu usulning mohiyati shundaki (1) taqqoslamadagi x o`rniga $m$ modulga ko`ra chegirmalarning to`la sistemasidagi barcha chegirmalar ketma-ket qo`yib chiqiladi. Ulardan qaysi biri (1) ni to`g`ri taqqoslamaga aylantirsa, o`cha chegirma qatnashgan sinf yechim hisoblanadi. Lekin koeffitsient yetarlicha katta bo`lganda bu usul qulay emas.

**Koeffitsientlarni o`zgartirish usuli**. Taqqoslamalarning xossalaridan foydalanib, (1) da no'ma`lum oldidagi koeffitsientni va b ni shunday o`zgartirish kerakki, natijada taqqoslamaning o`ng tomonida hosil bo`lgan son $ax$ hadning koeffitsientiga bo`linsin.

MISOL. 1. $7x \equiv 5(mod9)$

$7x \equiv 5 + 9(mod9)$

$7x \equiv 14(mod9)$

$x \equiv 2(mod9)$

2. $17x \equiv 25(mod28)$

$17x + 28x \equiv 25(mod28)$

$45x \equiv 25(mod28)$

$9x \equiv 5(mod28)$

$9x \equiv 5 - 140(mod28)$

$9x \equiv -135(mod28)$

$x \equiv -15(mod28)$

$x \equiv 13(mod28)$

Eyler teoremasidan foydalanish usuli. Ma`lumki, $(a, m) = 1$ bo`lsa, u holda $a^{\varphi(m)} \equiv 1\ (modm)$ taqqoslama o`rinli edi. Shunga ko`ra, $x = a^{\varphi(m)-1} \cdot b(modm)$ bo`ladi.

Misol. $3x \equiv 7(mod11)$

$$x \equiv 3^{\varphi(11)-1} \cdot 7(mod11) \qquad \varphi(11) = 10$$

$$x \equiv 3^9 \cdot 7(mod11) \equiv (3^3)^3 \cdot 7 \equiv 5^3 \cdot 7 \equiv 4 \cdot 7 \equiv$$

$$28 \equiv 6(mod11)$$

Taqqoslamaning moduli yetarlicha katta bo`lsa, quidagi usul ancha qulaydir.

Uzluksiz kasrlardan foydalanish usuli.

$$ax \equiv b(modm)$$

taqqoslama berilgan bo`lib, $(a,m)=1 \wedge a>0$ bo`lsin. $\frac{m}{a}$ kasrni uzluksiz kasrlarga yoyib, uning munosib kasrlarini $\frac{P_k}{Q_k}$ $(k=\overline{1,n})$ kabi belgilaymiz, bunda

$P_n=m \wedge Q_n=a$ bo`ladi, u holda

$$P_nQ_{n-1}-P_{n-1}Q_n=(-1)^n$$

tenglikni

$$mQ_{n-1}-aP_{n-1}=(-1)^n$$

ko`rinishda yozish mumkin, yoki

$aP_{n-1}\equiv(-1)^n+mQ_{n-1}$ dan

$aP_{n-1}\equiv(-1)^{n-1}(modm)$ (2)

(2) ni $(-1)^{n-1}\cdot b$ ga ko`paytirib,

$(-1)^{n-1}\cdot b\cdot aP_{n-1}\equiv b(modm)$ (3)

(1) va (3) ni solishtirib

$$x\equiv(-1)^{n-1}b\cdot P_{n-1}(modm)$$

ni hosil qilamiz. Bu erda P_{n-1} son $\frac{m}{a}$ kasrning $(n-1)-$ munosib kasrning suratidan iborat.

(1) taqqoslama yagona yechimga ega bo`lgani uchun (3) yechim (1) ning yagona yechimi bo`ladi.

MISOL. $68x\equiv164(mod212)$

$$(68,164)=4,\ \ 212/4$$

$$17x\equiv41(mod53),\ \ (17,53)=1$$

$$P_{k-1}=25\quad n=3,\ \ n-1=2$$

$$x_0\equiv(-1)^2\cdot25\cdot41(mod53)\equiv18(mod53)$$

$$x\equiv18,\ 71,\ 124,\ 177(mod212)$$

Ljandr simvoli va uning xossalari.

Ushbu $x^2 \equiv a\ (mod\ p)$, $(a;p) = -1$ taqqoslamaning moduli yetarlicha katta bo'lganda Eyler kriteriysidan foydalaninsh unchalik qulay emas. Bunda hollarda Lejandr simvoli deb ataluvchi va $\left(\frac{a}{p}\right)$ kabi atluvchi simvoldan foydalaniladi.

Ta'rif. Quyidagi shatrlarniqanoatlantiruvchi $\left(\frac{a}{p}\right)$ simvol *Lejandr simvoli* deyiladi:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & agar\ \ a\ \ son\ \ p\ \ toq\ tub\ modul\ bo'yichakvadratik\ chegirma\ bo'lsa; \\ -1, & agar\ \ a\ son\ \ p\ \ toq\ tub\ modul\ bo'yichakvadratik\ chegirmamas\ bo'lsa. \end{cases}$$

$\left(\frac{a}{p}\right)$ simvol a sondan p bo'yicha tuzlgan *Lejandr simvoli* deb taladi, bu yerda a Lejandr simbolining *surati*, *p* esa Lejandr simvolining *maxraji* deyiladi.

Misol. $\left(\frac{7}{19}\right) = \mathbf{1}$, chunki Eyler kriteriysiga asosan, $7^{\frac{19-1}{2}} \equiv 1\ (mod\ 19)$ bo'lgani uchun 7 son 19 modul bo'yicha vadratik chegirmadir. 5 son 17 modul bo'yicha kvadratik chegirmamas bo'lganligidan $\left(\frac{5}{17}\right) = -1$ bo'ladi.

Ma'lumki, $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$, $a^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ ekanligiga qarab, a kvadratik chegirma yoki kvadratik chegirmamas bo'ladi. Demak, Ljandr simvoli va Eyler kriteriylariga asosan, quyidagini yoza olamiz:

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

Endi Lejandr simvolining quyidagi ba'zi bir xossalarini o'rib chiqamiz:

1-xossa. $a \equiv a_1(mod\ p) => \left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$. (2)

Haqiqatan, bitta sinfning elementlari berilgan modul bo'yicha yo kvadratik chegirma, yoki kvadratik chegirmamas bo'ladi. Bunga asosan, (1) ning to'g'rilii kelib chiqadi. Bu xossadan foydalanib, har qanday $k \in Z$ uhun quyidagini yoza olamiz: $\left(\frac{a}{p}\right) = \left(\frac{kp+a_1}{p}\right)$, $\left(\frac{kp+a_1}{p}\right) = \left(\frac{a_1}{p}\right)$ bo'lgani uchun $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$ bo'ladi.

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

Haqiqatan, $x^2 \equiv 1 \ (mod\ p)$ taqqoslama doimo yechimga ega bo'lib, $x \equiv \pm 1 \ (mod\ p)$ uning yehimidir.

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

(1) taqqoslamaga asosan quyidagini yoza olamiz:

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \ (mod\ p)$ (3).

Lekin $\left(\frac{-1}{p}\right)$ va $(-1)^{\frac{p-1}{2}}$ larning qiymati ± 1 dan farqli emas. Shu bilan bir vaqtda p toq tub son bo'lgani uchun 1 va -1 lar shu modul bo'yicha taqqoslanuvchi bo'la olmaydi. Demak, $\left(\frac{-1}{p}\right)$ va $(-1)^{\frac{p-1}{2}}$ lar bir vaqtda 1 ga yoki -1 ga teng bo'ladi.

4-xossa. $\left(\frac{a\cdot b}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Isboti. (1) taqqoslaamaga asosan quyidagini yozish mumkin: $\left(\frac{a\cdot b}{p}\right) \equiv (a\cdot b)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}} \cdot (b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \ (mod\ p)$ yoki $\left(\frac{a\cdot b}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \ (mod\ p)$. $(a)^{\frac{p-1}{2}} \cdot (b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \ (mod\ p)$ taqqoslamaning ikkala qismi a va b lar p modul bo'yicha kvadratik chegirma yoki kvadratik chegirmamas bo'lsa, 1 ga, a va b larning biri p modul bo'yicha kvadratik chegirma, ikkinchisi esa kvadratik chegirmamas bo'lsa, -1 ga teng. Shuning uchun $\left(\frac{a\cdot b}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ tenglikni yosa olamiz. Bu xossadan quyidagi natijalar kelib chiqadi:

1-natija. $\left(\frac{a^2}{p}\right) \equiv 1$, $\left(\frac{a\cdot b^2}{p}\right) \equiv \left(\frac{a}{p}\right)$.

2-natija. Juft sondagi kvadratik chegirmalar yoki kvadratik chegirmamaslar ko'paytmasi doimo kvadratik chegirma bo'ladi. Toq sondagi kvadratik chegirmamaslar ko'paytmasi yana kvadratik chegirmamas bo'ladi.

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

Biz bu xossani isbot qilib o'tirmasdan undan amaliy mashg'ulotlarda foydalnishning a'zi bir tomonlarin ko'rsatib o'tamiz.

a) $p \equiv 8m \pm 1$ shakldagi tub son bo'lsin. U holda

$$\frac{p^2-1}{8}=\frac{(8m\pm 1)^2-1}{8}=8m^2\pm 2m\equiv 0\ (mod\ 2)$$

Bo'lgani uchun $\left(\frac{2}{p}\right)\equiv 1.$

b) $p\equiv 8m\pm 3$ shakldagi tub son bo'lsa,

$$\frac{p^2-1}{8}=\frac{(8m\pm 3)^2-1}{8}=8m^2\pm 6m+1\equiv 1\ (mod\ 2)$$

bo'adi. Demak, $p\equiv 8m\pm 3$ shakldagi tub son bo'lsa, 2 son p modul boyicha kvadratik chegirmamas bo'lad, ya'ni $\left(\frac{2}{p}\right)\equiv -1.$

6-xossa. O'zarolik qonuni.

Agar p va q lar har xil toq tub son bo'lsa,

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \qquad (4)$$

tenglik o'rinli bo'ladi.

Bu xossani ham isbot qilmasan uning amaliy mashg'ulotlardaqo'llanishini ko'rsatmiz. Buning uchun (4) ning har ikkaa qismini $\left(\frac{p}{q}\right)$ ga ko'paytiramiz:

$$\left(\frac{q}{p}\right)\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right), \qquad (5)$$

bu yerda $\left(\frac{p}{q}\right)^2=1.$

(5) tenglikka asosan, p va q larning kamida bittasi 4m+1 shakldagi son bo'lsa, $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=1$ bo'lib, $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ hosil boladi.

Agar p va q larning har biri 4m+3 shaklagi tub son bo'lsa,u holda (-1) ning darajasi toq son bo'lib, $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$ bo'ladi.

Misol. $x^2\equiv 426(mod\ 491)$ taqqoslama yechimga egami?

Bu savolga javob berish uchun $\left(\frac{426}{491}\right)$ Lejandr simvolini tuzamiz. $426=2\cdot 3\cdot 71$ shakldagi son bo'lgani uchun 4- xossaga asosan quyidagicha yozamiz:

$$\left(\frac{426}{491}\right)\equiv\left(\frac{2}{491}\right)\cdot\left(\frac{3}{491}\right)\cdot\left(\frac{71}{491}\right).$$

1. $\left(\frac{2}{491}\right) \equiv -1$, chunki $491 \equiv 3\ (mod\ 8)$.
2. $\left(\frac{3}{491}\right) \equiv -\left(\frac{491}{3}\right) \equiv -\left(\frac{2}{3}\right) \equiv -(-1) = 1$, chunki $491 \equiv 3\ (mod\ 4)$ va $3 \equiv 3\ (mod\ 4)$ hamda $3 \equiv 3\ (mod\ 8)$.
3. $\left(\frac{71}{491}\right) \equiv -\left(\frac{491}{71}\right) \equiv -\left(\frac{65}{71}\right) \equiv -\left(\frac{5}{71}\right) \cdot \left(\frac{13}{71}\right) \equiv -\left(\frac{71}{5}\right) \cdot \left(\frac{71}{13}\right) \equiv -\left(\frac{1}{5}\right) \cdot \left(\frac{6}{13}\right) \equiv -\left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) \equiv -(-1)\left(\frac{13}{3}\right) \equiv 1 \cdot \left(\frac{1}{3}\right) \equiv 1$, chunki $491 \equiv 3 (mod\ 4)$, $71 \equiv 3\ (mod\ 4)$, $491 \equiv 65\ (mod\ 71), 5 \equiv 1\ (mod\ 4)$, $13 \equiv 5\ (mod\ 8)$.

Demak, $\left(\frac{426}{491}\right) \equiv (-1) \cdot 1 \cdot 1 = -1$, $\left(\frac{426}{491}\right) \equiv -1$, bo’lgan uchun berilgan taqqoslama yechimga ega emas.