6-§. Ikkinchi darajali taqqoslamalar va Lejandr simvoli.

1. **Ikkinchi darajali taqqoslamalar va ularning ikki noma'lumli ikkinchi darajali aniqmas tenglamalar bilan bog'liqligi.** Ikkinchi darajali taqqoslamaning umumiy ko'rinishi

$$Ax^2 + Bx + C \equiv 0 \pmod{M} \qquad (1)$$

dan iborat. Bu ushbu ikki noma'lumli aniqmas tenglama

$$Ax^2 + Bx + C = My \qquad (2)$$

ga teng kuchli. (1) ko'rinishdagi taqqoslamani yechishga ikkinchi darajali ikki noma'lumli aniqmas tenglamaning umumiy holi

$$ax^2+2bxy+cy^2+2dx+2ey+f=0$$

ham keltiriladi. Buni yechish esa o'z navbatida Pell tenglamasi $x^2-ay^2=c$ ning yechimi bilan ham bog'liqdir.

2. Ikki hadli taqqoslamaga keltirish. (1) ni hamma vaqt

$$x^2 \equiv a(\mathrm{mod}\, m) \qquad (3)$$

ko'rinishga keltirish mumkin. Buni quyidagicha amalga oshiriladi. (1) ning ikkala tomonini 4A ga ko'paytiramiz (modulini ham)

$$4A^2x^2+4ABx+4AC\equiv 0(\mathrm{mod}\, 4AM). \qquad (4)$$

(4) dan

$$(2Ax+B)^2 \equiv B^2-4AC(\mathrm{mod}\, 4AM).$$

Bu yerda $y=2Ax+B,\quad D=B^2-4AC$ deb olsak, $y^2\equiv D(mod 4AM)$ hosil bo'ladi.

Agar (3) taqqoslamada *(a,m)=1* bo'lib, u yechimga ega bo'lsa, *a* ga *m* moduli bo'yicha *kvadratik chegirma*, agar yechimga ega bo'lmasa, *kvadratik chegirma emas* deyiladi. Shuningdek, agar $x^n \equiv a(\mathrm{mod}\, m), (a,m)=1$ taqqoslama yechimga ega bo'lsa, *a* ga *n – darajali chegirma*, aks holda esa *a* ga *m* moduli bo'yicha *n-darajali chegirma emas* deb ataladi.

(3) taqqoslamani yechish umumiy holda

1) $x^2\equiv a(\mathrm{mod}\, p),\quad p>2;$ 2) $x^2\equiv a(\mathrm{mod}\, p^\alpha),\ \alpha>1;$ 3) $x^2\equiv a(\mathrm{mod}\, 2^\alpha),\quad \alpha>1.$

taqqoslamalarni yechishga keltiriladi.

3. Yechimlari soni.Tanlash yo'li bilan yechimlarini topish. Kvadratik chegirmalar soni. Ushbu

$$x^2\equiv a(\mathrm{mod}\, p), \qquad p>2 \qquad (5)$$

taqqoslama berilgan bo'lsin. Agar $p\backslash a$ bo'lsa, trivial hol bo'ladi, ya'ni $x\equiv 0(\mathrm{mod}\, p)$. Shuning uchun ham $x\equiv x_1(\mathrm{mod}\, p)$ deb hisoblaymiz. Tushunarliki, agar $x\equiv x_1(\mathrm{mod}\, p)$ (5) ning yechimi bo'lsa, $x\equiv -x_1(\mathrm{mod}\, p)$ ham (5) ning yechimi bo'ladi. $x\equiv -x_1(modp)$ dan $2x_1\equiv 0\ (\mathrm{mod}\, p)$va $ð>2\Rightarrow x_1\equiv 0(\mathrm{mod}\, p)$ kelib chiqadi, u holda $(a,\ p)=1$ ga ziddir. Shunday qilib (5) yechimga ega bo'lsa, u 2 ta har xil yechimga ega bo'lar ekan. (5) yechimlarini tanlash usuli bilan topish jarayoni umumiy holga nisbatan ancha sodda. Bu yerda biz p moduli chegirmalarning keltirilgan sistemasini absolyut qiymati jihatidan eng kichik sistema ko'rinishda yozib olib,

$$\pm 1,\ \pm 2,\ \ldots,\ \pm\frac{p-1}{2} \qquad (6)$$

musbat va manfiy chegirmalarning (5) ni qanoatlantirish yoki qanoatlantirmasligini bir vaqtda tekshirishimiz mumkin. Shuning uchun ham (5) da *x* ning o'rniga

$$1, 2, 3, \ldots, \frac{p-1}{2}$$

larni qo'yib tekshirish yetarli. Bunda chap tomonda:

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \qquad (7)$$

hosil bo'ladi. Bulardan birortasi, masalan k^2 soni a bilan $modp$ bo'yicha taqqoslanuvchi bo'lsa, u holda $x \equiv \pm k(\bmod p)$ ga ega bo'lamiz. Shu bilan birga faqat $a(\bmod p)$bo'yicha (7) da birorta son bilan taqqoslanuvchi bo'lgan (5) ko'rinishdagi taqqoslamalargina yechimga ega. Boshqacha so'z bilan aytganda (7) da $\bmod p$ bo'yicha kvadratik chegirmalar yozilgan. Ularning barchasi har xil sinflarga tegishli. Haqiqatan ham, agar

$1 \le k < l \le \frac{p-1}{2}$ bo'lib, $k^2 \equiv l^2(\bmod p)$ bo'lsa, u holda (5) 4 ta $x \equiv \pm k$ âà $x \equiv \pm l \ (\bmod p)$ yechimga ega bo'ladi. Buning bo'lishi mumkin emas. Shunday qilib, *modp* bo'yicha kvadratik chegirmalar soni $\frac{p-1}{2}$ ga teng va shuning uchun ham kvadratik chegirma emaslar son soni ham $\frac{p-1}{2}$ ga teng bo'ladi.

4. Eyler kriteriyasi. (5) ning yechimga ega yoki ega emasligini aniqlash uchun Eyler tomonidan taklif etilgan ushbu kriteriyadan foydalanish qulay: Agar a oni $modp$ bo'yicha kvadratik chegirma bo'lsa, $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$ bo'ladi. Agar a soni *modp* bo'yicha kvadratik chegirma bo'lmasa, u holda $a^{\frac{p-1}{2}} \equiv -1(\bmod p)$ bo'ladi. Haqiqatdan ham, agar $(a, p) = 1$va$(a, 2) = 1$ bo'lsa, $a^{p-1} \equiv 1(\bmod p)$ bo'ladi (Ferma teoremasi). Bundan $a^{p-1} - 1 \equiv 0(\bmod p)$ yoki $\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(\bmod p)$.

Bu yerda bu qavslarning hech bo'lmasa birortasi *p* ga bo'linishi kerak. Ularning ikkalasi bir vaqtda *p* ga bo'linmaydi, aks holda ularning ayirmasi 2 ga ham *p* ga bo'linar edi, lekin $p>2$

Agar a kvadratik chegirma bo'lsa,

$$a^{\frac{p-1}{2}} \equiv 1(\bmod p) \qquad (8)$$

bajariladi. Bu yerdan agar $a(\bmod p)$bo'yicha kvadratik chegirma emas bo'lsa, u holda

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p \qquad \text{bajariladi.}$$

5. Lejandr simvoli va uning xossalari. a sonining $p$moduli bo'yicha kvadratik chegirma yoki chegirma emasligini aniqlashda Eyler kriteriyasidan foydalanish p katta bo'lsa, uncha ham qulay emas. Shuning uchun Lejandr simvoli $\left(\frac{a}{p}\right)$ qo'llaniladi. U quyidagicha aniqlanadi:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ agar } a \text{ soni mod } p \text{ bo'yicha kvadratik chegirma bo'lsa;} \\ -1, \text{agar } a \text{ soni mod } p \text{ bo'yicha kvadratik chegirma bo'lmasa.} \end{cases}$$

Lejandr simvoli ta'rifidan va Eyler kriteriyasidan

$$\grave{a}^{\frac{p-1}{2}} \equiv \left(\frac{\grave{a}}{\eth}\right) \pmod p \qquad (9)$$

kelib chiqadi. Lejandr simvoli quyidagi xossalarga ega.

1^0. Agar $a \equiv a_1 \pmod p$ bo'lsa, $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$ bo'ladi. Bundan $\left(\frac{a}{p}\right) = \left(\frac{a+pt}{p}\right),\ t \in Z.$

2^0. $\left(\frac{1}{\eth}\right) = 1,$ 3^0. $\left(\frac{-1}{p}\right) = (-1)^{\frac{\eth-1}{2}},$ 4^0. $\left(\frac{\grave{a}\cdot b}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right),$ 5^0. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$

6^0. $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$

Lejandr simvolining qiymatini shu xossalardan foydalanib hisoblash mumkin. 6^0 – xossaga kvadratik chegirmalarning o'zgalik qonuni deyiladi.

292. Berilgan taqqoslamalarni ikkihadli taqqoslama ko'rinishiga keltirib, keyin yeching: 1) $2x^2+4x-1\equiv 0 \pmod 5$; 2) $3x^2+2x\equiv 1 \pmod 7$; 3) $2x^2-2x-1\equiv 0 \pmod 7$; 4) $3x^2-x\equiv 0 \pmod 5$; 5) $3x^2+7x+8\equiv 0 \pmod{17}$; 6) $3x^2+4x+7\equiv 0 \pmod{31}$; 7) $4x^2-11x-3\equiv 0 \pmod{13}$; 8) $x^2-5x+6\equiv 0 \pmod{24}$.

293. x ning qanday natural qiymatlarida quyidagi funksiyalar butun qiymat qabul qiladi:

$$1)\ \frac{x^2+2x+7}{55};\quad 2)\ \frac{x^2+3x+1}{25};\quad 3)\ \frac{x^2+3x+5}{15}.$$

294.a).Eyler kriteriyasidan foydalanib, 7 moduli bo'yicha eng kichik musbat chegirmalarning keltirilgan sistemasida qaysi sonlar shu modul bo'yicha kvadratik chegirma bo'ladi.

b). 17 moduli bo'yicha eng kichik musbat kvadratik chegirmalarni aniqlang.

295. Eyler kriteriyasidan foydalanib, quyidagi modullar bo'yicha kvadratik chegirma sinflarini aniqlang: 1) 11; 2) 13; 3) 17.

296. Quyidagi taqqoslamalarni berilgan modul bo’yicha absolyut qiymati jihatidan eng kichik (noldan boshqa) chegirmalarni sinab ko’rish yo’li bilan yeching:
1) $x^2 \equiv 2 \pmod 7$; 2) $x^2 \equiv 4 \pmod 7$; 3) $x^2 \equiv 3 \pmod 7$; 4) $x^2 \equiv 3 \pmod{13}$; 5) $x^2 \equiv 4 \pmod{11}$.

297. Lejandr simvolining qiymatini hisoblang:

1) $\left(\frac{63}{131}\right)$; 2) $\left(\frac{35}{97}\right)$; 3) $\left(\frac{47}{73}\right)$; 4) $\left(\frac{29}{383}\right)$; 5) $\left(\frac{241}{593}\right)$; 6) $\left(\frac{257}{571}\right)$; 7) $\left(\frac{251}{577}\right)$; 8) $\left(\frac{342}{677}\right)$.

298. Lejandr simvolidan foydalanib, quyidagi taqqoslamalardan qaysilari yechimga ega ekanligini aniqlang va yechimlarini toping:

1) $x^2 \equiv 6 \pmod 7$; 2) $x^2 \equiv 3 \pmod{11}$; 3) $x^2 \equiv 12 \pmod{13}$; 4) $x^2 \equiv 3 \pmod{13}$;

5) $x^2 \equiv 5 \pmod{11}$; 6) $x^2 \equiv 13 \pmod{17}$; 7) $x^2 \equiv 7 \pmod{19}$; 8) $x^2 \equiv 5 \pmod{17}$.

299. Berilgan taqqoslamalar yechimga ega bo’ladigan a ning qiymatini toping:

1) $x^2 \equiv a \pmod 5$; 2) $x^2 \equiv a \pmod 7$; 3) $x^2 \equiv a \pmod{11}$;

4) $x^2 \equiv a \pmod{13}$; 5) $x^2 \equiv 5 \pmod 3$.

300. $x^2 + 1 \equiv 0 \pmod p$ taqqoslama modulning $p = 4n + 1, (n = 1,2,3, \dots)$ qiymatida va faqat shundagina yechimga ega ekanligini isbotlang.

301. $(a,b) = 1$ bo’lganda $a^2 + b^2$ ko’rinishdagi sonning kanonnik yoyilmasida faqat $p = 4n + 1, (n = 1,2,3, \dots)$ ko’rinishdagi tub sonlar qatnashishini isbotlang.

302. Ikki ketma-ket butun sonning ko’paytmasining 13 moduli bo’yicha 1 bilan taqqoslanuvchi bo’lmasligini isbotlang.

303. a ning $x(x+1) \equiv a \pmod{13}$ taqqqoslama yechimga ega bo’ladigan barcha qiymatlarini toping.

304. 300-masaladan foydalanib $p = 4n + 1, (n = 1,2,3, \dots)$ ko’rinishdagi tub sonlar sonining cheksiz ko’p ekanligini isbotlang.

305. Tenglamalarni butun sonlarda yeching (quyidagi egri chiziqlarda yotuvchi butun koordinatali nuqtalarni toping): 1) $4x^2 - 5y = 6$; 2) $11y = 5x^2 - 7$;

3) $x^2 - 10x - 11y + 5 = 0$; 4) $x^2 - 21x + 110 = 13y$; 5) $15x^2 - 7y^2 = 9$.

306. Berilgan sonlar kvadratik chegirma(chegirma emas) bo’lgan modullarni toping: 1) $a = 5$; 2) $a = -3$; 3) $a = 3$; 4) $a = 2$; 5) $a = -7$.

307. Berilgan taqqoslamalar yechimga ega bo’lgan barcha toq tub modullarni toping:

1). $x(x+1) \equiv 1 \pmod p$; 2). $x(x-1) \equiv 2 \pmod p$; 3). $x(x-1) \equiv 3 \pmod p$.

308. Lejandr simvolidan foydalanib, quyidagi taqqoslamalar modul $p>2$ ning qiymatiga bog’liq bo’lmagan yechimga ega ekanligini isbotlang:

1) $(x^2-13)(x^2-17)(x^2-221)\equiv 0\left(\operatorname{mod} p\right)$;

2) $(x^2-3)(x^2-5)(x^2-7)(x^2-11)(x^2-1155)\equiv 0\left(\operatorname{mod} p\right)$.