2-§. Indekslar va ularning tadbiqlar

Boshlang'ich ildizlarning asosiy xossalari sonlar nazariyasiga logarifm tushunchasiga o'xshash yangi tushuncha, indekslar tushunchasini kiritish imkoniyatini beradi. Faraz etaylik g soni p tub moduli bo'yicha boshlag'ich ildiz bo'lsin. U holda

$$g^0,\ g^1,\ g^2,\ \ldots,\ g^{p-1} \tag{1}$$

sonlari p moduli bo'yicha chegirmalarning to'la sistemasini tashkil etadi. Agar a, $(a,p)=1$ bo'lsa, u $mod p$ bo'yicha (1) sistemadagi birorta $g^{\gamma_1}, 0\le\gamma_1\le p-1$ son bilan taqqoslanuvchi bo'lishi kerak, ya'ni

$$a\equiv g^{\gamma_1}\left(\operatorname{mod} p\right),\qquad 0\le\gamma_1\le p-1 \tag{2}$$

Agar $(a,p)=1$ bo'lsa,

$$a\equiv g^{\gamma}\left(\operatorname{mod} p\right),\quad \gamma\ge 0 \tag{3}$$

(3) shartni qanoatlantiruvchi γ soniga a sonining $p$moduli bo'yicha g asosga ko'ra indeksi deyiladi va $ind_g a$ ko'rinishda yoziladi. Demak, (3) dan

$$a\equiv g^{ind\, a}\left(\operatorname{mod} p\right)\ . \tag{4}$$

Ta'rifdan a bilan $mod p$ bo'yicha taqqoslanuvchi barcha sonlar (4) da birta indeksga ega:

$$0, 1, 2,\ \ldots\ , p-2 \tag{5}$$

Umuman har bir a soni (5) sistemada bitta indeksga ega. Lekin bir asosdan ikkinchi asosga o'tilsa, indekslar umuman aytganda o'zgaradi. Ikkinchi tomondan esa berilgan g asosga ko'ra a soni cheksiz ko'p indekslar γ ga ega. (1) va (2) dan bular manfiy bo'lmagan butun sonlar bo'lib,

$g^{\gamma}\equiv g^{\gamma_1}\left(\operatorname{mod} p\right)$ shartni qanoatlantirishi kerak. Bu yerda g soni p modul bo'yicha boshlang'ich ildiz bo'lganligi sababli, u p-1 ko'rsatkichga tegishli. U holda ko'rsatkichga qarashli sonlarning xossalariga asosan yuqoridagi taqqoslama o'rinli bo'lishi uchun $\gamma\equiv\gamma_1\left(\operatorname{mod} p-1\right)$ bo'lishi kerak. Demak, r moduli bo'yicha p bilan o'zaro tub har bir chegirmalar sinfiga p-1 bo'yicha chegirmalarning biror sinfidagi manfiy bo'lmagan chegirmalardan iborat indekslar to'plami mos keladi va aksincha: $ind\, a\equiv ind\, b\left(\operatorname{mod} p-1\right)$ âãàðãà $a\equiv b\left(\operatorname{mod} p\right)$ bo'lsa (4) ga asosan

$$\gamma\equiv ind\, a\left(\operatorname{mod} p-1\right) \tag{5}$$

Shuningdek indekslar quyidagi xossalarga ega:

1) ko'paytma $a\cdot b\cdot\cdots l$ ning indeksi p-1 moduli bo'yicha shu sonlar indekslari yig'indisi bilan taqqoslanuvchidir, ya'ni

$$ind\left(a\cdot b\cdot\ldots\cdot l\right)\equiv ind\, a+ind\, b+\ldots ind\, l\left(\operatorname{mod} p-1\right). \tag{6}$$

2) $ind\, a^n\equiv n\, ind\, a\left(\operatorname{mod} p-1\right)$.

Shuningdek $ind\,1\equiv 0\ \left(\operatorname{mod} p-1\right),\quad ind\, g\equiv 1\left(\operatorname{mod} p-1\right).$

Indekslar jadvali. Indekslar jadvalini tuzish p tub modul bo'yicha berilgan songa ko'ra uning indeksi va aksincha, berilgan indeksga ko'ra shu sonni topish imkoniyatini beradi. Bunda asos sifatida p modul bo'yicha boshlang'ich ildizlardan birortasi olinadi. Umuman indekslar jadvalini tub bo'lmagan boshlang'ich ildizlar mavjud bo'lgan m modul bo'yicha tuzish ham mumkin.

Indekslarning taqqoslamalarni yechishga tadbiqlari.

a) Ikki hadli taqqoslamalarni yechish. Ikki hadli bir noma'lumli tenglamaning umumiy ko'rinishi

$$ax^n \equiv b \pmod m \tag{7}$$

Ma'lumki, murakkab m modul bo'yicha taqqoslamani tub modul bo'yicha taqqoslamani yechishga keltirish mumkin. Shuning uchun ham $m=p$ bo'lgan holni

$$ax^n \equiv b \pmod p, \qquad p \nmid a \tag{8}$$

qaraymiz. $p>2$ deb olamiz. $p=2$ bo'lsa, 0 va 1 chegirmalarni sinab ko'rish yo'li bilan yechish mumkin. (8) dan $ind a+n ind x \equiv ind b (mod p-1)$ yoki bundan

$$n ind x = ind b - ind a \ (mod p-1). \tag{9}$$

Demak,1) $(n, p-1)=1$ bo'lsa, u holda (9) va demak (8) ham yagona yechimga ega;

2) $(n, p-1)= d>1$ bo'lib, $d|ind b-ind a$ bo'lsa, (9) va demak (8) ham d ta yechimga ega;

3) $(n,p-1)=d>1$ bo'lib, $d\nmid ind b-ind a$ bo'lsa, (9) va demak (8) ham yechimga ega emas.

b). $$x^n \equiv a \pmod p \tag{10}$$

taqqoslamaning yechimga ega bo'lish sharti. Bu taqqoslamani indekslasak,

$$n\, ind\, x \equiv ind\, a \pmod{p-1}. \tag{11}$$

Bu yerda $(n, \ p-1)=d$ bo'lsa, (11) ning yechimga ega bo'lishi uchun

$$ind\, a \equiv 0 \pmod d \tag{12}$$

shartning bajarilishi zarur va yetarlidir. (12) shartni p va d ga bog'liq holda ifodalaymiz.

(12) ning ikkala tomonini va modulini $\frac{p-1}{d}$ ga ko'paytiramiz, u holda

$\frac{p-1}{d} ind\, a \equiv 0 \pmod{p-1}$ yoki $ind\, a^{\frac{p-1}{d}} \equiv 0 \pmod{p-1}$. Bundan esa

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p \tag{13}$$

Shunday qilib (10) ning yechimga ega bo'lishi uchun (13) shartning bajarilishi zarur va yetarlidir.

в) *Ko'rsatkichli taqqoslamalarni yechish.*

$$a^x \equiv b \pmod p\,. \tag{14}$$

(14) dan $x \, ind\, a \equiv ind\, b \pmod{p-1}$. Bu taqqoslamani esa osongina yechish mumkin.

321. Indekslar jadvalini tuzing: 1). 2 asosga ko'ra 29 moduli boyicha; 2). 5 asosga ko'ra 23 moduli boyicha.

322. 11 moduli bo'yicha indekslar jadvalini tuzing.

323. Quyidagi taqqoslamalardan δ ko'rsatkichni aniqlang:

1) $5^{\delta} \equiv 1(mod7)$; 2) $5^{\delta} \equiv 1(mod11)$; 3) $8^{\delta} \equiv 1(mod13)$;
4) $12^{\delta} \equiv 1(mod17)$; 5) $24^{\delta} \equiv 1(mod31)$; 6) $10^{\delta} \equiv 1(mod13)$
7) $27^{\delta} \equiv 1(mod17)$; 8) $18^{\delta} \equiv 1(mod11)$; 9) $23^{\delta} \equiv 1(mod41)$.

324. Indekslashdan foydalanib p tub moduli bo'yicha 2 dan p-1 gacha bo'lgan sonlar tegishli bo'lgan ko'rsatkichlarni toping:

1) $p = 5$; 2) $p = 7$; 3) $p = 11$.

325. Indekslashdan foydalanib, quyidagi sonlarning 59 moduli bo'yicha boshlang'ich ildiz bo'lish bo'lmasligini aniqlang:

1) 2; 2) 3; 3) 6; 4) 8; 5) 12; 6) 13; 7) 14; 8) 19.

326. Quyidagi modullar bo'yicha boyicha barcha boshlang'ich ildizlarni toping: 1) $p = 17$; 2) $p = 19$; 3) $p = 23$.

327. Birinchi darajali taqqoslamalarni indekslardan foydalanib yeching:

1) $7x \equiv 23(mod17)$; 2) $39x \equiv 84(mod97)$;
3) $125x \equiv 7(mod79)$; 4) $37x \equiv 25(mod89)$;
5) $4x \equiv 13(mod37)$; 6) $37x \equiv 5(mod221)$;
7) $47x \equiv 13(mod667)$; 8) $228x \equiv 317(mod1517)$.

328. Ko'rsatkichli taqqoslamalarni indekslardan foydalanib, yeching:

1) $2^{x} \equiv 7(mod67)$; 2) $13^{x} \equiv 12(mod47)$;
3) $16^{x} \equiv 11(mod53)$; 4) $52^{x} \equiv 38(mod61)$;
5) $12^{x} \equiv 17(mod31)$; 6) $20^{x} \equiv 21(mod41)$.

329.Ikki hadli taqqoslamalarni indekslardan foydalanib yeching:

1) $37x^{15} \equiv 62(mod73)$; 2) $5x^{4} \equiv 3(mod11)$;
3) $2x^{8} \equiv 5(mod13)$; 4) $2x^{3} \equiv 17(mod41)$;
5) $27x^{5} \equiv 25(mod31)$; 6) $11x^{3} \equiv 6(mod79)$;
7) $23x^{3} \equiv 15(mod73)$; 8) $8x^{26} \equiv 37(mod41)$;
9) $37x^{8} \equiv 59(mod61)$; 10) $18x^{8} \equiv 6(mod13)$.

330.Ikki hadli taqqoslamalarni indekslardan foydalanib yeching:

1) $x^{12} \equiv 37(mod41)$; 2) $x^{55} \equiv 17(mod97)$;
3) $x^{35} \equiv 17(mod67)$; 4) $x^{30} \equiv 46(mod73)$;
5) $x^{8} \equiv 23(mod41)$; 6) $x^{5} \equiv 74(mod71)$;
7) $x^{27} \equiv 39(mod43)$; 8) $x^{8} \equiv 29(mod13)$;
9) $x^{2} \equiv 59(mod67)$; 10) $x^{2} \equiv 59(mod83)$;

$$11)\ x^2 \equiv 32 (mod 43); \qquad 12)\ x^2 \equiv -17 (mod 53);$$
$$13)\ x^2 \equiv -28 (mod 67); \quad 14)\ x^2 \equiv 56 (mod 41).$$

331. Eyler kriteriyasi va indekslardan foydalanib quyidagi sonlar 15, 16, 17, 18, 19, 20 dan qaysilari berilgan modul bo'yicha kvadratik chegirma bo'lishini aniqlang: 1) 23 moduli bo'yicha; 2) 29 moduli bo'yicha; 3) 41 moduli bo'yicha; 4) 73 moduli bo'yicha; 5) 97 moduli bo'yicha.

332. Berilgan modul bo'yicha indekslarning bir sistemasidan ikkinchi bir sistemasiga o'tish formulasini keltirib chiqaring.

333. a ning qanday butun qiymatlarida quyidagi munosabatlar o'rinli:

$$1)\ 3a^2 - 5 \vdots 7; \quad 2)\ 7a^2 + 13 \vdots 23; \quad 3)\ 13a^2 - 11 \vdots 29.$$