V-BOB. BOSHLANG'ICH ILDIZLAR VA INDEKSLAR

1-§.Ko'rsatkichga qarashli sonlar va boshlang'ich ildizlar.

1.Ko'rsatkichga qarashli sonlar va boshlang'ich ildizlar. Agar *(a,m)=1* bo`lib, δ>0

$$a^{\delta} \equiv 1 \pmod{m} \qquad (1)$$

ni qanoatlantiruvchi eng kichik butun son bo'lsa, u holda *a* soni *m* moduli bo'yicha δ *ko'rsatikichga tegishli* deyiladi. Shuni ham ta'kidlash kerakki, agar *(a,m)=d >1* bo'lsa, (1) taqqoslama o'rinli bo'lmaydi, chunki uning o'ng tomoni d ga bo'linmaydi. Ma'lumki, *(a,m)=1* bo'lsa, Eyler teoremasiga ko'ra

$$a^{\varphi(m)} = 1 \pmod{m} \qquad (2)$$

Demak, $0<\delta\leq\varphi(m)$. Agar δ=φ(m) bo'lsa, ya'ni *a* soni *m* moduli bo'yicha *φ(m)* ko'rsatkichga tegishli bo'lsa, *a* va *m* moduli bo'yicha *boshlang'ich ildiz* deyiladi. Agar *m=p* tub son bo'lsa, a soni *p* modul bo'yicha boshlang'ich ildiz bo'lishi uchun u *p-1* ko'rsatkichiga tegishli bo'lishi kerak. *a* sonining *m* moduli bo'yicha tegishli bo'lgan ko'rsatkichini topish uchun quyidagicha yo'l tutish mumkin: $a, a^2, a^3, \ldots$ larni hisoblaymiz, toki birinchi $a^{\delta} \equiv 1 \pmod{m}$ shartni qanoatlantiruvchi δ ni hosil qilgunga qadar.

2. Endi ko'rsatkichga qarashli sonlarning ba'zi xossalarini qaraymiz.

1^0. $a_1 \equiv a \pmod{m}$ bo'lsa, u holda a va a_2 lar m moduli bo'yicha bir xil ko'rsatkichga tegishli bo'ladi.

Demak, agar *a* soni *m* moduli bo'yicha δ ko'rsatkichga tegishli bo'lsa, *a* bilan taqqoslanuvchi sonlar $a+mt$ ning barchasi shu δ ko'rsatkichga tegishli bo'lar ekan.

2^0. Agar *a* soni *m* moduli bo'yicha *δ* ko'rsatkichga tegishli bo'lsa, u holda

$$a^0,\ a,\ a^2,\ \ldots,\ a^{\delta-1} \qquad (3)$$

sonlari *m* moduli bo'yicha o'zaro taqqoslanmaydi. Bu xossadan kelib chiqadiki, agar $\delta=\varphi(m)$ bo'lsa, (3) sistema *m* moduli bo'yicha chegirmalarning keltirilgan sistemasini tashkil qiladi.

3^0. Agar *a* soni *m* moduli bo'yicha δ ko'rsatkichga tegishli bo'lsa, u holda

$$a^{\gamma} \equiv a^{\gamma_1} \pmod{m} \qquad (4)$$

bo'lishi uchun $\gamma \equiv \gamma_1 \pmod{\delta}$ bo'lishi zarur va yetarlidir.

Natija.1). Agar *a* soni *m* moduli bo'yicha *δ* ko'rsatkichga tegishli bo'lib, $a^{\gamma} \equiv 1 (mod m)$

bo'lishi uchun $\gamma \equiv 0(\mathrm{mod}\,\delta)$ bo'lishi zarur va yetarlidir.

2). Agar a soni m moduli bo'yicha δ ko'rsatkichga tegishli bo'lsa, $\delta \setminus \varphi(m)$.

2-natijadan foydalanib, δ ni topish jarayonini biroz soddalashtirish mumkin, ya'ni δ bu $\varphi\,(m)$ ning bo'luvchilari orasida bo'ladi.

3). Agar a soni m moduli bo'yicha δ ko'rsatkichga tegishli bo'lsa, a^k soni $\frac{\delta}{(\delta,k)}$ ko'rsatkichga tegishli bo'ladi. Xususiy holda, agar $(k,\delta) = 1$ bo'lsa, γ=δ, ya'ni $\grave{a}^k$ soni ham δ ko'rsatkichga tegishli bo'ladi.

3. Ko'rsatkichga qarashli sinflarning mavjudligi va ularning soni. Biz bundan ilgari har bir $(a,m)=1$ shartni qanoatlantiruvchida sonining m moduli bo'yicha biror δ $(\delta \setminus \varphi(m))$ko'rsatkichga tegishli ekanligini ko'rdik. Buning teskarisi, ya'ni $\varphi(m)$ ning har bir bo'luvchisi m moduli bo'yicha biror sinfning ko'rsatkichi bo'ladimi? Xususan $\varphi(m)$ soni ham biror sinfning m moduli bo'yicha ko'rsatkichi bo'ladimi? Ya'ni ixtiyoriy m moduli bo'yicha boshlang'ich ildiz mavjudmi? Bu savolga faqat $m=p$ – tub son hamda m maxsus (ba'zi bir ko'rinishdagi butun sonlar uchun) ijobiy javob bor.

Lemma. p-1 sonining bo'luvchisi δ soni p moduli bo'yicha yoki birorta ham sinfning ko'rsatkichi bo'lmaydi yoki $\varphi(\delta)$ ta sinfning ko'rsatkichi bo'ladi.

(Bu lemmani boshqacha qilib quyidagicha aytish mumkin. Agar p moduli bo'yicha δ ko'rsatkichga tegishli biror sinf mavjud bo'lsa, (bu yerda $\delta \mid p$-1), u holda shunday sinflar soni$\varphi(\delta)$ bo'ladi).

Agar p moduli bo'yicha δ ko'rsatkichga tegishli sinflar soninni ψ(δ) bilan belgilasak, lemmani

$$\psi(\delta) = \begin{cases} 0 \\ \varphi(\delta) \end{cases}$$

ko'rinishda yozish mumkin. Bu agar δ ko'rsatkichga tegishli sonlar mavjud bo'lsa, mod p bo'yicha ularning soni $p-1$ga tengligini bildiradi. Lekin berilgan δ uchun p modul bo'yicha shu ko'rsatkichga tegishli son mavjud yoki mavjud emasligiga javob bermaydi. Bunga ushbu teorema javob beradi.

Teorema (Gauss). p tub modul bo'yicha p-1 ning har bir bo'luvchisi δ uchun shu δ ko'rsatkichga tegishli bo'lgan $\varphi(\delta)$ ta sinf mavjud. Xususan p moduli bo'yicha $\varphi(p-1)$ ta boshlang'ich ildiz mavjud.

Umuman boshlang'ich ildizlar $m = 2, 4, p^\alpha$ và $2p^\alpha$ modullari bo'yichagina mavjud. Bu yerda $p>2$ tub son va α≥1. I.M.Vinogradov p tub son bo'lsa, u holda $2^{2^{\hat{e}}}\sqrt{p}\ln p$ dan katta bo'lmagan boshlang'ich ildiz mavjud ekanligini isbotlagan, bu yerda κ soni p-1 ning har xil bo'luvchilari sonidir. Boshlang'ich ildizni topishning effektiv usuli esa hozirgacha topilgan emas. Qarab chiqilganlardan agar

$$g^{\frac{p-1}{\delta_1}} \not\equiv 1, \quad g^{\frac{p-1}{\delta_2}} \not\equiv 1, \; \dots, \; g^{\frac{p-1}{\delta_k}} \not\equiv 1$$

bo'lsa, u holda g ning p moduli bo'yicha boshlang'ich ildiz bo'lishi kelib chiqadi. Boshlang'ich ildizlarni aniqlashning ikkinchi bir usuli bu, agar p moduli bo'yicha boshlang'ich ildizlardan birortasi (yaxshisi eng kichigi) g ma'lum bo'lsa, qolgan barchasini $g^k(modp)$ ning eng kichik musbat chegirmasi sifatida aniqlash mumkin. Bunda $(k, p-1) = 1$ va $1 < k < p-1$.

309. 1) 2 soni 7 moduli bo'yicha tegishli bo'lgan daraja ko'rsatkichini toping.

2) 3 soni m=7 moduli bo'yicha tegishli bo'lgan daraja ko'rsatkichini toping.

3) 5 ning m=7 moduli bo'yicha qanday ko'rsatkichga tegishli ekenligini aniqlang.

310. Tanlash usuli bilan m moduli bo'yicha 2 dan $m-1$ gacha sonlar orasidan m bilan o'zaro tublari tegishli bo'lgan daraja ko'rsatkichlarini toping:

1). $m = 5$; 2). $m = 7$; 3). $m = 8$; 4). $m = 10$; 5) $m = 11$; 6). $m = 9$.

311. m moduli bo'yicha $m-1$ soni tegishli bo'lgan daraja ko'rsatkichini aniqlang.

312. Quyidagi modullar bo'yicha barcha boshlang'ich ildizlarni toping:

1). $p = 7$; 2) $p = 11$; 3). $p = 13$; 4). $p = 17$.

313. Quyidagi modullar bo'yicha barcha boshlang'ich ildizlarning sonini va eng kichik boshlang'ich ildizni toping:

1). $p = 19$; 2) $p = 23$; 3). $p = 31$; 4). $p = 37$; 5). $p = 43$; 6). 53.

314. Quyidagi modullarning har biri bo'yicha eng kichik boshlang'ich ildizni bilgan holda barcha boshlang'ich ildizlarni toping:

1). $p = 19$; 2) $p = 23$; 3). $p = 31$.

315. 6 moduli bo'yicha boshlang'ich ildizlarning barcha sinflarini toping.

316. $2, 2^2, 2^3, \dots, 2^{10}$ sonlarining 11 moduli bo'yicha chegirmalarning keltirilgan sistemasini tashkil etishini isbotlang.

317. $2^{2^n} + 1, (n = 1,2,\dots)$ sonining tub bo'luvchilari $k \cdot 2^{n+1} + 1$ ko'rinishda bo'lishini isbotlang.

318. $\varphi(a^m - 1) \equiv 0(modm)$ ekanligini isbotlang. Bunda $a > 1$.

319. 8 moduli bo'yicha boshlang'ich ildizlarning mavjud emasligini isbotlang.

320. Quyidagi taqqoslamalar yechimga ega bo'ladigan b ning barcha qiymatlarini toping. 1). $5^x \equiv b(mod9)$, 2). $4^x \equiv b(mod9)$, 3). $a^x \equiv b(modm)$ taqqoslama yechimga ega bo'lmaydigan b ning barcha qiymatlarini sonini toping. Bunda $(a, m) = 1$.