4-§. Tub modul bo'yicha n-darajali taqqoslamalar.

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0(modp) \qquad (1)$$

ko'rinishdagi taqqoslamaga tub modul bo'yicha n-darajali taqqolama deyiladi. Bunda p-tub son, $a_0 \not\equiv 0(modp)$, n –butun musbat son, a_i – koeffitsientlar butun sonlar.

Eng avvalo $a_0, a_1, \dots, a_n$ sonlarini p moduli bo'yicha absolyut qiymati jihatidan eng kichik chegirmalar bilan almashtirsak, (1) taqqoslama biroz soddaroq ko'rinishga keladi. Masalan:

$$25x^3 + 17x^2 - 13 \equiv 0(mod11) \qquad (1')$$

ni

$$3x^3 - 5x^2 - 2 \equiv 0(mod11) \qquad (2')$$

ko'rinishda yozish mumkin.

Ikkinchidan (1) ni hamma vaqt bosh hadining koeffitsienti 1 ga teng bo'lgan holga keltirish mumkin, chunki $aa_0 \equiv 0(modp)$ taqqoslama $(a_0, p) = 1$ bo'lgani uchun yagona yechimga ega va (1) ning ikkala tomonini a ga ko'paytirsak, x^n ning koeffitsientini 1 bilan almashtirish mumkin bo'ladi. Masalan: $3a \equiv 1(mod11) \rightarrow a \equiv 4(mod11)$. Shuning uchun ham (2′) ning ikkala tomonini 4 ga ko'paytiramiz, u holda

$$12x^3 - 20x^2 - 8 \equiv 0(mod11) \rightarrow x^3 + 2x^2 + 3 \equiv 0(mod11)\,.$$

Uchinchidan ushbu teorema yordamida berilgan taqqoslamani ancha soddalashtirish mumkin.

1 – teorema. Agar (1) da $n \geq p$ bo'lsa, uni darajasi $p-1$ dan katta bo'lmagan taqqoslama $R(x) \equiv 0(modp)$ taqqoslama bilan almashtirish mumkin. Bunda $R(x)$ ko'phaq $f(x)$ ni $x^p - x$ ga bo'lishdan chiqqan qoldiq.

Amaliyotda $f(x)$ ni $x^p - x$ ga bo'lishi shart emas. Buning uchun x^m ni darajasini *p-1* dan katta bo'lmagan had bilan almashtirish uchun m ni *p-1* ga bo'lamiz. $m = (p-1)k + r$. U holda $x \equiv x^p(modp)$ taqqoslamaning ikki tomonini mos ravishda x^{r-1}, $x^{(p-1)1+r-1}, \dots$

$\dots$, $x^{(p-1)(k-1)+r-1}$ larga ko'paytirsak,

$x^r \equiv x^{(p-1)+r}$, $x^{p-1+r} \equiv x^{2(p-1)+r}, \dots, x^{(p-1)(k-1)+r} \equiv x^{k(p-1)+r} \equiv x^m$

hosil bo'ladi. Bulardan $x^m \equiv x^r$(modp). Bu esa yuqoridagi teoremaning yana bir isbotidir.

Misol. $x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0(mod5)$ taqqoslamani darajasi 4dan katta bo'lmagan taqqoslama bilan almashtiring.

$$x^{4\cdot 2+0} + 2x^{4\cdot 1+3} + x^{4\cdot 1+1} - x^{4\cdot 1} - x + 3 \equiv 0(mod5)$$

$$\rightarrow 1 + 2x^3 + x - x^0 - x + 3 \equiv 0(mod5) \rightarrow 2x^3 + 3 \equiv 0(mod5).$$

2-teorema(yechimlari soni haqida teorema).p-tub moduli bo'yicha n-darajali $(n \leq p-1)$ taqqoslama$n$-tadan ortiq bo'lmagan ildizga ega.

Agarda $a_0 \not\equiv 0(modp)$shartdan voz kechsak bu teoremadan quyidagi natija kelib chiqadi.

Natija. Agar p-tub modul bo'yicha n-darajali taqqoslama n tadan ortiq ildizga ega bo'lsa uning barcha koeffitsientlari p ga bo'linadi.

3-teorema (Vilson teoremasi). Agar p tub son bo'lsa, u holda

$$(p-1)!+1 \equiv 0(mod p) \quad (3)$$

Bu taqqoslama agar p tub son bo'lmasa, bajarilmaydi. Haqiqatdan ham agarda $p = p_1 \cdot d, 1 < d < p,$ bo'lsa $(p-1)!$ soni d ga bo'linadi, u holda $(p-1)!+1$ soni d ga bo'linmaydi, shuning uchun ham p ga bo'linmaydi. Demak, ushbu teskari teorema ham o'rinli ekan.

4-teorema. Agar butun musbat p soni uchun(3) taqqoslama o`rinli bo`lsa, p-tub son bo'ladi.

Shunday qilib Vilson teoremasini tub sonlarni aniqlash kriteriyasi deb qabul qilish mumkin, lekin $(p-1)!+1$ soni katta p lar uchun juda katta son bo'lgani uchun amaliyotda qo'llash noqulay.

276. Quyidagi taqqoslamalarning avval darajasini pasaytirib keyin yeching.

a). $6x^{10} - 12x + 1 \equiv 0(mod 5)$,

b). $x^5 - 2x^3 + x^2 - 2 \equiv 0(mod 3)$,

c).$x^5 - 7x^4 + 9x^2 - x + 13 \equiv 0(mod 3)$,

d). .$x^7 - x^6 + 5x^2 - 3 \equiv 0(mod 5)$,

e). $x^5 + x^4 + x^3 - x^2 - 2 \equiv 0(mod 5)$,

f). $x^7 - 6 \equiv 0(mod 5)$,

g). $x^8 + 2x^7 + x^5 - x + 3 \equiv 0(mod 5)$,

h). $6x^4 + 17x^2 - 16 \equiv 0(mod 3)$,

i). $4x^7 - 2x^3 + 8 \equiv 0(mod 5)$,

j). $3x^7 - 2x^6 + 2x^2 + 13 \equiv 0(mod 5)$.

277. Quyidagi taqqoslamalarni berilgan modul bo'yicha ko'paytuvchilarga ajrating.

a). $x^3 + 4x^2 - 3 \equiv 0(mod 5)$,

b). $x^4 + x^3 - x^2 + x - 2 \equiv 0(mod 5)$,

c). $x^4 + x + 4 \equiv 0(mod 11)$,

d). $x^2 + 2x + 2 \equiv 0(mod 5)$,

e). $3x^3 - 1 \equiv 0(mod 5)$,

f). $2x^4 + x^3 - 3x^2 + 2x - 2 \equiv 0(mod 11)$,

g). $x^4 - 7x^3 + 13x^2 + 21x + 23 \equiv 0(mod 7)$,

h). $2x^4 + x^3 - 3x^2 + 2x - 2 \equiv 0(mod 5)$,

i). $2x^3 + 5x^2 - 2x - 3 \equiv 0(mod 7)$,

j). $x^4 - 2x^2 + x + 4 \equiv 0(mod 7)$.

278. Quyidagi taqqoslamalarning 1-teoremadan foydalanib, darajasini pasaytiring va yechimlarini toping:

a). $8x^{20} - 15x^{19} + 7x^{18} + 28x^{17} - 4x^{16} + 30x^{15} + 10x^{6} - 4x^{3} + 23x^{2} - 21x - 11 \equiv 0(mod13)$,

b). $x^{10} + x^{8} + x^{7} - x^{4} - x^{2} + 4x - 3 \equiv 0(mod7)$,

c). $x^{101} + 3x^{15} + x^{11} - 3x^{5} + 9x^{2} + 10x - 5 \equiv 0(mod11)$,

d). $2x^{35} - 17x^{15} + 13x^{8} - 3x^{5} + 12x + 5 \equiv 0(mod11)$,

e). $x^{12} - 2x^{7} + x^{3} + 1 \equiv 0(mod5)$.

279. Quyidagi teoremani isbotlang: $f(x) = x^{n} + \sum_{i=1}^{n} a_i x^{n-i}$va $n < p$ bo'lsin. $f(x) \equiv 0(modp)$ taqqoslamaning n ta yechimga ega bo'lishi uchun $x^{p} - x$ ni $f(x)$ ga bolishdan chiqqan qoldiqning barcha koeffitsientlarining p ga bo'linishi zarur va yetarli.

280. Agar $a \not\equiv 0(mod7)$ va $b \not\equiv 0(mod7)$ bo'lsa, $x^{3} + ax + b \equiv 0(mod7)$ taqqoslamaning uchta yechimga ega bo'lmasligini isbotlang.

281. Tub modul bo'yicha taqqoslama $x^{n} \equiv a(modp)$ ning $(a,p) = 1$ va $n < p$ bo'lganda n ta yechimga ega bo'lishining zaruriy va yetarli shartini toping.

282.280-misolda topilgan shartdan foydalanib, quyida berilgan $x^{n} \equiv a(modp)$ ko'rinishdagi taqqoslamalarning n ta yechimga ega yoki yechimga ega emas ekanligini aniqlang va yechimga ega bo'lsa ularni toping.

a). $x^{3} \equiv 1(mod7)$;

b). $x^{2} \equiv 2(mod5)$;

c). $x^{5} \equiv 10(mod11)$;

d). $x^{4} \equiv 1(mod11)$;

e). $x^{6} \equiv 3(mod7)$;

f). $x^{4} \equiv 3(mod13)$.

283. Agar $p -$ tub son bo'lsa, $(p-2)! \equiv 1(modp)$ ekanligini ko'rsating.

284. p va $p + 2$ sonlarining "egizak" tub sonlar bo'lishi uchun $4[(p-1)! + 1] + p \equiv 0\ (modp(p+2))$ shartning bajarilishi yetarli va zarur ekanligini (Klement teoremasini) isbotlang.

285. Vilson teoremasidan foydalanib p soni $p = 4n + 1$ ko'rinishdagi tub son bo'lganda $(2n)!$ sonining $x^{2} \equiv -1(modp)$ taqqoslamani qanoatlantirishini isbotlang.

286. p tub son bo'lganda quyidagi taqqoslamalarning o'rinli ekanligini isbotlang:
a). $a^{p} + a(p-1)! \equiv 0(modp)$; b). $a^{p}(p-1)! + a \equiv 0(modp)$.

287. Leybnits teoremasi "$p > 2$ sonining tub son bo'lishi uchun $(p-2)! - 1 \equiv 0(modp)$ shartning bajarilishi zarur va yetarli" ekanini isbotlang.

288. 279-misoldagi teoremani quyidagi taqqoslamalarni yechishga qo'llang:

a). $x^{2} + 2x + 2 \equiv 0(mod5)$, b). $3x^{3} - 4x^{2} - 2x - 4 \equiv 0(mod7)$.