FERMA TEOREMASI YORDAMIDA BA‘ZI MASALALARNI YECHISH.

Amirov Abdurasul Kamolovich
abdurasulamirov2@gmail.com,
Shahrisabz davlat pedagogika instituti o‘qituvchisi.
https://doi.org/10.5281/zenodo.8026181

ARTICLE INFO

Qabul qilindi: 05-June 2023 yil
Ma’qullandi: 08-June 2023 yil
Nashr qilindi: 12-June 2023 yil

KEY WORDS

Taqqoslama, Eyler funksiyasi, Fermaning kichik teoremasi, o’zaro tub son.

ABSTRACT

Ushbu maqolaning asosiy maqsadi o‘rta maktab, akademik litseylardagi olimpiadaga qiziquvchi o‘quvchilarga sonlar nazariyasi bo‘limidan ba‘zi murakkab masalalarni sodda usullar bilan yechishni o‘rgatishdan iborat.

Ta’rif. Agar a va b butun sonlarni m natural songa bo`lganda bir xil qoldiq chiqsa, a va b sonlar m modul bo‘yicha taqqoslanadi deb aytiladi va $a \equiv b\,(\mathrm{mod}\ m)$ kabi belgilanadi. Ushbu maqolada taqqoslamaning ba‘zi xossalarini keltiramiz:

1 – xossa: Agar a va b sonlari m modul bo’yicha taqqoslansa, u holda a – b ayirma m natural songa qoldiqsiz bo‘linadi. Ya‘ni,

$a = mk + r,\ b = mn + r$ bo’lsa,

$$a - b = mk - mn + 0,\quad a - b = m(k - n).$$

2 – xossa: Har biri c soni bilan taqqoslanadigan a va b sonlari bir – biri bilan ham taqqoslanadi. Ya‘ni

$a \equiv c\ (\mathrm{mod}\ m)$ $b \equiv c\ (\mathrm{mod}\ m)$ bo‘lsa, u holda $a \equiv b\ (\mathrm{mod}\ m)$.

3 – xossa: Modullari bir xil bo`lgan taqqoslamalarni hadma – had qo‘shish mumkin. Ya‘ni,

$a \equiv b\ (\mathrm{mod}\ m)$ va $c \equiv d\ (\mathrm{mod}\ m)$ bo‘lsa, u holda $a + c \equiv b + d\ (\mathrm{mod}\ m)$ o‘rinli bo‘ladi.

Natija: Taqqoslamaning biror hadini bir tomonidan ikkinchi tomoniga qarama – qarshi ishora bilan olib o‘tish mumkin.Ya‘ni,

$$a + c \equiv b\ (\mathrm{mod}\ m) \Rightarrow a \equiv b - c\ (\mathrm{mod}\ m)$$

4 – xossa: Taqqoslamaning ixtiyoriy tomoniga uning moduliga karrali bo‘lgan sonni qo‘shish mumkin.Ya‘ni,

$$a \equiv b\ (\mathrm{mod}\ m) \Rightarrow a + mk \equiv b\ (\mathrm{mod}\ m) \text{ va } a \equiv b + mn(\mathrm{mod}\ m)$$

5 – xossa: Bir xil modulli taqqoslamalarni hadma – had ko‘paytirish mumkin. Ya‘ni, $a \equiv b\ (\mathrm{mod}\ m)$ va $c \equiv d\ (\mathrm{mod}\ m)$ bo‘lsa, u holda $a * c \equiv b * d\ (\mathrm{mod}\ m)$ o‘rinli bo‘ladi.

Natija: Taqqoslamani darajaga oshirish mumkin. $a^n \equiv b^n\ (\mathrm{mod}\ m)$

6 – xossa: Taqqoslamaning har ikkala qismini biror butun songa ko‘paytirish mumkin.

$$a \equiv b\ (\mathrm{mod}\ m) \Rightarrow a * k \equiv b * k\ (\mathrm{mod}\ m)\quad k \in Z$$

7 – xossa: Taqqoslamaning har ikkala qismini va modulini biror natural songa

ko‘paytirish mumkin.

$$a \equiv b\ (\mathrm{mod}\ m) \Rightarrow a * n \equiv b * n\ (\mathrm{mod}\ m * n) \quad n \in N$$

8 – xossa: Taqqoslamaning har ikkala qismini ularning umumiy bo‘luvchilariga bo‘lish mumkin.

$$a * n \equiv b * n\ (\mathrm{mod}\ m) \Rightarrow a \equiv b\ (\mathrm{mod}\ m)$$

9 - xossa: Agar a va b soni $m_1, m_2, \dots m_k$ sonlari bilan taqqoslansa, u holda ular EKUK bo‘yicha ham taqqoslanadi.

10 - xossa: Agar d soni m sonining bo‘luvchisi bo’lib $a \equiv b\ (\mathrm{mod}\ m)$ bo`lsa, u holda $a \equiv b\ (\mathrm{mod}\ d)$ o‘rinli bo‘ladi.

$$a \equiv b\ (\mathrm{mod}\ m) \Rightarrow a \cdot k \equiv b \cdot k\ (\mathrm{mod}\ m) \quad k \in Z$$

Ta’rif. Musbat sonlar ustida aniqlangan, hamda a soniga $1,2,3,4, \dots, a-1$ sonlar ichida a bilan o‘zaro tub bo‘lgan sonlar sonini mos qo‘yuvchi funksiya **Eyler funksiyasi** deyiladi va φ(a) kabi belgilanadi.

Teorema (Eyler teoremasi). O‘zaro tub bo‘lgan va $(m > 1)$ sonlari uchun quyidagi munosabat o‘rinli: $a^{\varphi(m)} \equiv 1(\mathrm{mod}m)$.

Agar Eyler teoremasida m soni o‘rniga biror p tub olinsa, u holda $a^{p-1} \equiv 1(\mathrm{mod}m)$ tenglikka kelamiz. [1],[2]

Ushbu tenglikning ikkala tomonini a ga ko‘paytirsak, $a^p \equiv a(\mathrm{mod}m)$ tenglikka ega bo‘lamiz. Bu tenglik **Fermaning kichik teoremasi** deyiladi.

Taqqoslamaning xossalaridan hamda Eyler va Ferma teoremalaridan foydalanib quyidagi masalalarni yechamiz.

1-masala: Ixtiyoriy $k = 0,1,2 \dots$ sonlar uchun $2^{2^{6k+2}} + 3$ sonining 19 ga qoldiqsiz bo‘linishini isbotlang.

Isbot: Bizga ma‘lumki $2^6 = 64 \equiv 1(\mathrm{mod}\ 9)$ o‘rinli. Taqqoslamaning xossalaridan foydalanib quyidagi amallarni bajaramiz. $k = 0,1,2 \dots$ uchun $2^6 = 64 \equiv 1(\mathrm{mod}\ 9)$ ni darajaga oshirib $2^{6k} \equiv 1(\mathrm{mod}\ 9)$ va taqqoslamaning hadlarini 2 ga ko‘paytirib $2^{6k+1} \equiv 2(\mathrm{mod}\ 9)$ ni hosil qilamiz.

$2^{6k+1} \equiv 2(\mathrm{mod}\ 9)$ taqqoslamaning hadlarini va modulini 2 ga ko‘paytirib$2^{6k+2} \equiv 2^2(\mathrm{mod}\ 18)$ ni hosil qilamiz va $2^{6k+2} = 18 \cdot t + 2^2$ ga ega bo‘lamiz. t – butun son.

Ferma teoremasiga ko‘ra $2^{18} \equiv 1(\mathrm{mod}\ 19)$ taqqoslama o‘rinli, taqqoslamani $t = 0,1,2 \dots$ darajaga oshirib $2^{18t} \equiv 1(\mathrm{mod}\ 19)$ hosil qilamiz. Shuningdek $2^{2^{6k+2}} = 2^{18 \cdot t+2^2} \equiv 2^4(\mathrm{mod}\ 19)$ taqqoslamaning ikkala tomoniga 3 sonini qo‘shib, $2^{2^{6k+2}} + 3 \equiv 2^4 + 3 \equiv 0(\mathrm{mod}19)$. Demak ixtiyoriy $k = 0,1,2, \dots$ sonlar uchun $2^{2^{6k+2}} + 3$ soni 19 ga qoldiqsiz bo‘linadi.

2-masala. Barcha haqiqiy musbat n butun sonlar uchun quyidagi $a_n = 2^{2 \cdot n+1} - 2^{n+1} + 1$ va $b_n = 2^{2 \cdot n+1} + 2^{n+1} + 1$ sonlardan qaysilari 5 ga qoldiqsiz bo‘linadi?

Yechish: Ixtiyoriy musbat butun sonni $n = 4 \cdot k$, $n = 4 \cdot k + 1$, $n = 4 \cdot k + 2$, va $n = 4 \cdot k + 3$ $k = 0,1,2, \dots$ ko‘rinishda yozish mumkin ekanligidan quyidagi 4 ta holni qarab chiqamiz. Bunda $2^4 \equiv 1(\mathrm{mod}5)$ taqqoslamani darajaga oshirib $2^{4 \cdot k} \equiv 2^{8 \cdot k} \equiv 1(\mathrm{mod}5)$ taqqoslamaga kelamiz va shundan foydalanamiz.

1-hol: $n = 4 \cdot k$ bo‘lsin. $k = 0,1,2, \dots$

$a_n = 2^{2 \cdot n+1} - 2^{n+1} + 1 = 2^{8 \cdot k+1} - 2^{4 \cdot k+1} + 1 \equiv 2 - 2 + 1 \equiv 1(\mathrm{mod}5)$

$b_n = 2^{2 \cdot n+1} + 2^{n+1} + 1 = 2^{8 \cdot k+1} + 2^{4 \cdot k+1} + 1 \equiv 2 + 2 + 1 \equiv 0(\mathrm{mod}5)$.

2-hol: $n = 4 \cdot k + 1$ bo‘lsin. $k = 0,1,2, \ldots$

$a_n = 2^{2 \cdot n+1} - 2^{n+1} + 1 = 2^{8 \cdot k+3} - 2^{4 \cdot k+2} + 1 \equiv 8 - 4 + 1 \equiv 0(\mathrm{mod}5)$

$b_n = 2^{2 \cdot n+1} + 2^{n+1} + 1 = 2^{8 \cdot k+3} + 2^{4 \cdot k+2} + 1 \equiv 8 + 4 + 1 \equiv 3(\mathrm{mod}5).$

3-hol: $n = 4 \cdot k + 2$ bo‘lsin. $k = 0,1,2, \ldots$

$a_n = 2^{2 \cdot n+1} - 2^{n+1} + 1 = 2^{8 \cdot k+5} - 2^{4 \cdot k+3} + 1 \equiv 32 - 8 + 1 \equiv 0(\mathrm{mod}5)$

$b_n = 2^{2 \cdot n+1} + 2^{n+1} + 1 = 2^{8 \cdot k+5} + 2^{4 \cdot k+3} + 1 \equiv 32 + 8 + 1 \equiv 1(\mathrm{mod}5).$

4-hol: $n = 4 \cdot k + 3$ bo‘lsin $k = 0,1,2, \ldots$

$a_n = 2^{2 \cdot n+1} - 2^{n+1} + 1 = 2^{8 \cdot k+7} - 2^{4 \cdot k+4} + 1 \equiv 128 - 16 + 1 \equiv 3(\mathrm{mod}5)$

$b_n = 2^{2 \cdot n+1} + 2^{n+1} + 1 = 2^{8 \cdot k+7} + 2^{4 \cdot k+4} + 1 \equiv 128 + 16 + 1 \equiv 0(\mathrm{mod}5).$

Demak a_n soni $n = 4 \cdot k + 1$ va $n = 4 \cdot k + 2$ bo‘lgan holda, b_n soni esa $n = 4 \cdot k$ va $n = 4 \cdot k + 3$ bo‘lgan holda 5 ga qoldiqsiz bo‘linadi. a_n va b_n sonlarining ikkalasi bir vaqtda 5 ga qoldiqsiz bo‘linmaydi.

3-masala: $20^{15} - 1$ sonining $11 * 13 * 61$ ko‘paytmaga bo‘linishini isbotlang.

Isbot: 11, 31 va 61 sonlarni tub sonlar bo‘lganligi uchun, $20^{15} - 1$ sonini 11,13 va 61 sonlarining har biriga bo‘linishini isbotlash yetarli.

Bizga ma‘lumki $2^5 \equiv -1(\mathrm{mod}11)$ va $10 \equiv -1(\mathrm{mod}11)$ taqqoslamalarni bir xil darajaga oshirib $2^5 \equiv -1(\mathrm{mod}11)$ va $10^5 \equiv -1(\mathrm{mod}11)$ larni hosil qilamiz. $2^5 \equiv -1(\mathrm{mod}11)$ va $10^5 \equiv -1(\mathrm{mod}11)$ taqqoslamalarni ko‘paytirib $20^5 \equiv 1(\mathrm{mod}11)$ ni darajaga oshirib $20^{15} \equiv 1(\mathrm{mod}11)$ hosil qilamiz. Bundan $20^5 - 1 \equiv 0(\mathrm{mod}11)$ taqqoslamaga ega bo‘lamiz.

Endi $20 \equiv -11(\mathrm{mod}31)$ taqqoslamani darajaga oshirib $20^2 \equiv 121 \equiv -3(\mathrm{mod}31)$ va $20^3 \equiv (-11) * (-3) \equiv 33 \equiv 2(\mathrm{mod}31)$ ni hosil qilamiz. $20^3 \equiv 2(\mathrm{mod}31)$ taqqoslamani darajaga oshiramiz va $20^{15} \equiv 2^5 \equiv 1(\mathrm{mod}31)$ bundan $20^{15} - 1 \equiv 0(\mathrm{mod}31)$ taqqoslamaga ega bo‘lamiz.

Bizga ma‘lumki $3^4 \equiv 20(\mathrm{mod}61)$ taqqoslamani darajaga oshirib $3^{60} \equiv 20^{15}(\mathrm{mod}61)$ taqqoslamaga ega bo‘lamiz. Fermaning kichik teoremasiga ko‘ra $EKUB(3: 61) = 1$ ekanidan $3^{60} \equiv 1(\mathrm{mod}61)$ taqqoslama o‘rinli bundan $3^{60} \equiv 20^{15} \equiv 1(\mathrm{mod}61)$ demak $20^{15} - 1 \equiv 0(\mathrm{mod}61)$.

4-masala: $2^{70} + 3^{70}$ yig‘indining 13 ga qoldiqsiz bo‘linishini isbotlang.

Isbot: Ferma teoremasidan bizga ma‘lumki $2^{12} \equiv 1(\mathrm{mod}\ 13)$ o‘rinli, taqqoslamani darajaga oshirib $2^{60} \equiv 1(\mathrm{mod}\ 13)$ ni hosil qilamiz.

$2^5 \equiv 6(\mathrm{mod}\ 13)$ taqqoslamadan $2^{10} \equiv 36(\mathrm{mod}\ 13)$ni hosil qilamiz.

$2^{60} \equiv 1(\mathrm{mod}\ 13)$ va $2^{10} \equiv 36(\mathrm{mod}\ 13)$ taqqoslamalarni hadma – had ko‘paytirib $2^{70} \equiv 36(\mathrm{mod}\ 13)$ taqqoslamani hosil qilamiz. Endi

$3^3 \equiv 1(\mathrm{mod}\ 13)$ taqqoslamani darajaga ko‘tarib $3^{69} \equiv 1(\mathrm{mod}\ 13)$ ga ega bo‘lamiz. Hadlarini 3 ga ko‘paytirib $3^{70} \equiv 1(\mathrm{mod}\ 13)$ ni hosil qilamiz. $2^{70} \equiv 36(\mathrm{mod}\ 13)$ va $3^{70} \equiv 1(\mathrm{mod}\ 13)$ taqqoslamalarni hadma – had qo‘shib $2^{70} + 3^{70} \equiv 36 + 3 \equiv 0(\mathrm{mod}\ 13)$ni hosil qilamiz. Demak $2^{70} + 3^{70}$ yig‘indi 13 ga qoldiqsiz bo‘linadi.

Foydalanilgan adabiyotlar:

1. Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev, F.H.Haydarov “ALGEBRA VA SONLAR NAZARIYASI”, Toshkent – 2019

2. A. S. Yunusov, S. I. Afonina, M. A. Berdiqulov, D. I. Yunusova. “QIZIQARLI MATEMATIKA VA OLIMPIADA MASALALARI”, „O‘qituvchi” nashriyoti. Toshkent – 2007z