IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
**Volume 21 Issue 2 May 2026**

# TUB VA MURAKKAB MODULLI TAQQOSLAMALAR VA ULARNI YECHISH USULLARI

**O‘ralova Maqsuda Izzatilla qizi**
Samarqand Davlat Pedagogika instituti assistenti

**Norboyev Nuriddin Parda o‘g‘li**
Samarqand Davlat Pedagogika instituti talabasi
DOI: https://doi.org/10.5281/zenodo.20100178

**Annotatsiya:** Ushbu maqolada modulli arifmetikaning muhim bo‘limi hisoblangan tub va murakkab modulli taqqoslamalar nazariyasi yoritilgan. Taqqoslamalarning asosiy xossalari, tub modullar uchun yechimlar, murakkab modullar uchun yechish usullari, xususan, Xitoy qoldiqlar teoremasi va Eyler teoremasi asosida yechim topish usullari keng bayon qilingan. Shuningdek, amaliy misollar orqali nazariy bilimlar mustahkamlangan.

**Kalit so‘zlar**: modulli arifmetika, taqqoslama, tub son, murakkab modul, Eyler funksiyasi, Xitoy qoldiqlar teoremasi.

## Kirish

Modulli arifmetika sonlar nazariyasining muhim bo‘limlaridan biri bo‘lib, u matematika, kriptografiya, informatika va boshqa ko‘plab sohalarda keng qo‘llaniladi. Taqqoslamalar tushunchasi esa modulli arifmetikaning asosini tashkil etadi.

Agar $a$ va $b$ sonlar $m$ modul bo‘yicha bir xil qoldiq bersa, u holda quyidagicha yoziladi:

$$a \equiv b (mod m)$$

Mazkur maqolada taqqoslamalar ikki asosiy turga ajratilib o‘rganiladi:

**Tub modulli taqqoslamalar**

**Murakkab modulli taqqoslamalar**

1. Tub modulli taqqoslamalar

1.1. Ta’rif

Agar modul $p$ tub son bo‘lsa, u holda taqqoslama tub modulli taqqoslama deyiladi.

Masalan:

$$x \equiv 3 (mod 7)$$

Bu yerda 7 — tub son.

1.2. Asosiy xossalar

1. **Refleksivlik xossasi**

Har qanday son o‘ziga o‘zi taqqoslanadi: $a \equiv a (mod\ m)$ chunki $a - a = 0$ va $m$ soni 0 ni bo‘ladi.

2. **Simmetriklik xossasi**

Agar $a \equiv b (mod\ m)$ bo‘lsa, u holda $b \equiv a (mod\ m)$ ham bo‘ladi.

3. **Tranzitivlik xossasi**

Agar $a \equiv b (mod\ m)$ va $b \equiv c (mod\ m)$ bo‘lsa, u holda $a \equiv c (mod\ m$ bo‘ladi.

4. **Qo‘shish xossasi**

Agar $a \equiv b (mod\ m)$ va $c \equiv d (mod\ m)$ bo‘lsa, u holda $a + c \equiv b + d (mod m)$

5. **Ayirish xossasi**

Agar $a \equiv b (mod\ m)$ va $c \equiv d (mod\ m)$ bo‘lsa, u holda $a - c \equiv b - d (mod m)$

6. **Ko‘paytirish xossasi**

Agar $a\equiv b(mod\ m)$ va $c\equiv d(mod\ m)$ bo‘lsa, u holda $ac\equiv bd(modm)$

***Tub modulli taqqoslamalar quyidagi muhim xossalarga ega***:

**1.Yagona yechim mavjudligi**

Agar $p$ tub son va $a\neq 0(modp)$ bo‘lsa, u holda $ax\equiv b(modp)$

**2.Teskari element mavjudligi**

Har qanday $a\neq 0(modp)$ uchun shunday $a^{-1}$ mavjudki , $aa^{-1}\equiv 1(modp)$

1.3. Fermatning kichik teoremasi

Agar $p$ tub son va $a$ son $p$ ga karrali bo‘lmasa, u holda, $a^{p-1}\equiv(modp)$

Bu teorema tub modulli taqqoslamalarni yechishda muhim ahamiyatga ega.

1.4. Misol

Quyidagi taqqoslamani yeching:

$$3x\equiv 4(mod 7)$$

Yechish: 3 ning modul 7 bo‘yicha teskarisini topamiz: $3\cdot 5=15\equiv 1(mod\ 7)$

Demak: $x\equiv 5\cdot 4=20\equiv 6(mod\ 7)$

Javob:

$$x\equiv 6(mod 7)$$

**2. Murakkab modulli taqqoslamalar**

**2.1. Ta’rif**

Agar modul $m$ murakkab son bo‘lsa, ya’ni: $m=ab\ \ (a,b>1)$

Masalan:

$$x\equiv 5(mod 12)$$

**2.2. Yechim mavjudligi sharti**

Taqqoslama:

$$ax\equiv b(modm)$$

yechimga ega bo‘lishi uchun $EKUB(a,m)/b$ bo‘lishi kerak.

2.3. Eyler teoremasi

Agar $EKUB(a,m)=1$ bo‘lsa, u holda: $a^{\varphi(m)}\equiv 1(mod\ m)$

bu yerda $\varphi(m)$ — Eyler funksiyasi.

2.4. Misol Taqqaslamaning xossalaridan foydalanib yechimni toping.

$6x\equiv 8(mod 14)$ $EKUB(6,14)=2$

$2\mid 8\rightarrow$ yechim mavjud.

Tenglamani 2 ga qisqartiramiz:

$$3x\equiv 4(mod 7)$$

Oldingi misolga o‘xshash:

$$x\equiv 6(mod 7)$$

Demak umumiy yechim: $x=6+7k$

**3. Xitoy qoldiqlar teoremasi**

3.1**. Teorema**

Agar modullar o‘zaro tub bo‘lsa, $\begin{cases}x\equiv a_1(modm_1)\\ x\equiv a_2(modm_2)\end{cases}$ u holda yagona yechim mavjud.

Bu yechim $x\equiv a(modm_1m_2)$ ko’rinishda bo’ladi.

3.2. Misol . Taqqoslamani yeching.

$$\begin{cases}x\equiv 1(mod 3)\\ x\equiv 2(mod 5)\end{cases}$$

Yechish: $x=3k+1$ Ikkinchi tenglamaga qo‘yamiz:

$3k+1\equiv(mod 5)$

$3k\equiv 1(mod 5)$

$k\equiv 2(mod 5)$

$k=5t+2$
$x=3(5t+2)+1=15t+7$

Javob: $x\equiv 7(mod 15)$

4. Amaliy qo‘llanilish

Tub va murakkab modulli taqqoslamalar quyidagi sohalarda keng qo‘llaniladi:
Kriptografiya (RSA algoritmi)
Kompyuter arifmetikasi
Kodlash nazariyasi
Diskret matematika
Algoritmlar nazariyasi

**Xulosa**

Mazkur maqolada tub va murakkab modulli taqqoslamalar nazariyasi chuqur tahlil qilindi. Tub modullar uchun taqqoslamalar nisbatan sodda bo‘lib, teskari elementlar orqali oson yechiladi. Murakkab modullar uchun esa qo‘shimcha usullar — Eyler teoremasi va Xitoy qoldiqlar teoremasi muhim rol o‘ynaydi.

Ushbu nazariyalar zamonaviy matematika va axborot texnologiyalarining ajralmas qismi hisoblanadi.

**Foydalanilgan adabiyotlar**

1. Hardy G.H., Wright E.M. — An Introduction to the Theory of Numbers
2. Kurosh A.G. — Algebra kursi
3. Vinogradov I.M. — Sonlar nazariyasi asoslari
4. Niven I., Zuckerman H. — An Introduction to Number Theory