

TAQQOSLAMA VA UNING XOSSLARI. EYLER VA FERMA TEOREMALARI

Zaxriddinova Shaxlo Zaxriddin qizi

Matematika va ta'limda axborot texnologiyasi kafedra o'qituvchisi

Numonova Hulkar Naim qizi

Shahrisabz Davlat Pedagogika Instituti talabasi

Matematika va Informatika yo'nalishi 2-kurs talabasi

<https://doi.org/10.5281/zenodo.15129050>

Annotatsiya: Ushbu maqolada taqqoslama, uning xossalari, sonning oxirgi ikkita va uchta raqamini topish haqida ma'lumot berilgan. Taqqoslamalar yordamida bir nechta misollar keltirilgan.

Kalit so'zlar. Taqqoslama tushunchasi, teng qoldikli sonlar, taqqoslamaning xossalari, Eyler va Ferma teoremlari.

Абстрактный. В этой статье содержится информация о сравнении, его свойствах и нахождении последних двух и трех цифр числа. Приведено несколько примеров с использованием сравнений.

Ключевые слова. Понятие сравнения, числа с равными остатками, свойства сравнения, теоремы Эйлера и Ферма.

Abstract. This article provides information on the comparison, its properties, and finding the last two and three digits of a number. Several examples are given using comparisons.

Keywords. The concept of comparison, numbers with equal remainders, properties of comparison, Euler's and Fermat's theorems.

Kirish. Hozirgi zamonaviy ta'limda o'quvchilarga matematik teoremlar, tasdiqlar, matematik amallar, ba'zi tengliklar va tengsizliklarni o'rgatish katta ahamiyatga ega. Ko'pchilik o'quvchilar matematik amallardan qoldikli bo'lish amalini bajarishga qiyinchiliklarga duch kelishadi. Qoldikli bo'lishni yechishning bir nechta oson usullari mavjud. Shunday usullardan biri Taqqoslama usuli hisoblanadi. Ma'lumki, qoldikli bo'lish haqidagi teoremlarga asosan har qanday ikkita a , $m > 0$ butun son uchun shunday yagona va r sonlar topiladiki, ushbu

$$a = mq_1 + r \quad (1)$$

tenglik bajariladi, bu yerda $0 \leq r < m$.

Biror butun b butun son uchun

$$b = mq_2 + r \quad (2)$$

tenglik o'rinli bo'lgan b sonni olaylik. (1) va (2) tengliklar a va b sonlarini m ga bo'lganda bir xil qoldiq qolishini bildiradi.

T a' r i f. Agar ikkita butun a va b sonni m natural songa bo'lganda hosil bo'lgan qoldiqlar o'zaro teng bo'lsa, u holda a va b sonlarini m modul bo'yicha *teng qoldikli sonlar*, yoki m modul bo'yicha *taqqoslanuvchi sonlar* deyiladi.

Agar a va b sonni m modul bo'yicha taqqoslansa, u holda quyidagicha belgilanadi:

$$a \equiv b \pmod{m} \quad (3)$$

(3) ni a son b bilan m modul bo'yicha o'zaro taqqoslanadi deb o'qiladi.

Endi (1) dan (2) ni ayiraylik, u holda yoki $a - b \equiv m t \pmod{m}$ yoki

$$a - b \equiv mt \quad (t = q_1 - q_2) \quad (4)$$

tenglik hosil bo'ladi.

Yuqoridagi xulosalarni yakunlab quyidagi xulosalarni chiqarish mumkin:

1. Agar $a \equiv b \pmod{m}$ bo'lsa, u holda $(a - b)$ ayirma m ga qoldiqsiz bo'linadi va aksincha, agar a va b sonlar ayirmasi m ga bo'linsa, u holda $a \equiv b \pmod{m}$ o'rinli bo'ladi.

2. Agar $a = b + mt$ bo'lib b ni m ga b o'lgandagi qoldiq r ga teng bo'lsa, a ni ham m ga bo'lgandagi qoldiq r ga teng bo'ladi. Haqiqatdan, $b = mq_1 + r$ ni $a = b + mt$ ga qo'yamiz. U holda

$$a = mq_1 + r + mt = m(q_1 + t) + r = mq_2 + r$$

ya'ni $a = mq_2 + r$ bo'ladi.

Demak $a = mq_2 + r$ bo'lib, a ni m ga bo'lgandagi qoldiq ham r ga teng ekan. Shunday qilib, $a \equiv b \pmod{m}$ taqqoslamani $a - b = mt$ va $a = b + mt$ tengliklar bilan bir xil deyish mumkin. Agar $a = b + mt$ bo'lsa, u holda uni $a \equiv b \pmod{m}$ kabi yozish ham mumkin.

3. Xususiy holda agar a/m bo'lsa, u holda $a \equiv 0 \pmod{m}$ bo'ladi. Bu taqqoslama m soni a ning bo'luvchisi ekanligini bildiradi.

Taqqoslama quyidagi xossalarga ega:

1^o. Taqqoslama ekvivalent binar munasabat.

a) $a \equiv a \pmod{m}$, chunki $a - a = 0$ bo'lib, 0 son m ga bo'linadi. Demak, taqqoslama refleksivlik xossasiga ega.

b) $a \equiv b \pmod{m}$ yoki $a - b = mt$ bo'lsin. Bundan $b - a = m(-t)$ tenglikni yozish mumkin. U holda $b - a \equiv 0 \pmod{m}$ yoki $b \equiv a \pmod{m}$. Demak, taqqoslama simmetriklik xossasiga ega.

c) Agar $a \equiv b \pmod{m}$ va $b \equiv c \pmod{m}$ bo'lsa, u holda $a \equiv c \pmod{m}$ bo'ladi. Haqiqatan, $a = b + mt_1$, $b = c + mt_2$ tengliklarni hadlab qo'shsak, $a - c = mt$ tenglik hosil bo'ladi. Bunda $t = t_1 + t_2$. U holda $a \equiv c \pmod{m}$ bo'ladi. Demak taqqoslama tranzitivlik xossasiga ega. Ekvivalentlik va binar munosabatlari tarifiga ko'ra, taqqoslama ekvivalent binar munosabat ekan.

2^o. Bir xil modulli taqqoslamalarni xadlab qo'shish (ayirish) mumkin.

Haqiqatan ham,

$$a_1 \equiv b_1 \pmod{m},$$

$$a_2 \equiv b_2 \pmod{m},$$

.....

$$a_k \equiv b_k \pmod{m}$$

bo'lsa, u holda ularni

$$a_1 \equiv b_1 + mt_1,$$

$$a_2 \equiv b_2 + mt_2,$$

.....

$$a_k \equiv b_k + mt_k \quad (5)$$

kabi yozish mumkin. Bu tengliklarni hadlab qo'shib (ayirib)

$$a_1 \pm a_2 \pm a_3 \pm \dots \pm a_k = b_1 \pm b_2 \pm b_3 \pm \dots \pm b_k \pm m(t_1 + t_2 + t_3 + \dots + t_k)$$

yoki

$$a_1 \pm a_2 \pm a_3 \pm \dots \pm a_k = b_1 \pm b_2 \pm b_3 \pm \dots \pm b_k \pm mt \quad (6)$$

tenglikka ega bo'lamiz. (4) ni

$$a_1 \pm a_2 \pm a_3 \pm \dots \pm a_k = b_1 \pm b_2 \pm b_3 \pm \dots \pm b_k \pmod{m}$$

ko`rinishda ham yozish mumkin.

3⁰. Bir xil modulli taqqoslamalarni hadlab ko`paytirish mumkin. Haqiqatan, (5) dagi tengliklarni hadlab ko`paytirib,

$$a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_k = b_1 \cdot b_2 \cdot b_3 \cdot \dots \cdot b_k + mA$$

tenglikga ega bo`lamiz. Bunda

$$A = b_1 b_2 b_4 \dots b_k t_2 + b_1 b_3 b_4 \dots b_k t_1 + \dots$$

bo`lib

$$a_1 a_2 a_3 \dots a_k = b_1 b_2 b_3 \dots b_k \pmod{m} \quad (8)$$

taqqoslama o`rinli.

4⁰. Modulni o`zgartirmagan holda taqqoslamaning ikkala qismini bir xil butun songa ko`paytirish mumkin.

Haqiqatan, $a \equiv b \pmod{m}$ taqqoslamani $k \equiv k \pmod{m}$ taqqoslama bilan hadlab ko`paytirish natijasida  $ak \equiv bk \pmod{m}$  ga ega bo`lamiz.

5⁰. Agar $x \equiv y \pmod{m}$ bo`lsa, u holda ixtiyoriy butun koeffitsiyentli  $f(x)$  va  $f(y)$  ko`phadlar uchun $f(x) \equiv f(y) \pmod{m}$, ya`ni

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n = a_0 y^n + a_1 y^{n-1} + \dots + a_n \pmod{m} \quad (a_i \in \mathbb{Z})$$

6⁰. Agar bir vaqtda $a_i \equiv b_i \pmod{m} \quad (1 \neq 1, n)$ va $x \equiv y \pmod{m}$ taqqoslamalar o`rinli bo`lsa, u holda

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n = b_0 y^n + b_1 y^{n-1} + \dots + b_n \pmod{m}$$

taqqoslama o`rinli bo`ladi.

Taqqoslamani darajaga nisbatan qo`llash mumkin emas. Masalan,  $3 \equiv 8 \pmod{5}$  uchun  $2^3 \not\equiv 2^8 \pmod{5}$  bo`ladi. Chunki $2^3 \equiv 3 \pmod{5}$ va $2^8 \equiv 1 \pmod{5}$, ammo $1 \equiv 3 \pmod{5}$.

7⁰. Taqqoslamaning ikkala qismini modul bilan o`zaro tub bo`lgan ko`paytuvchiga qisqartirish mumkin.

$$ad \equiv bd \pmod{m} \quad (11)$$

bo`lib,  $(d; m) = 1$  bo`lsin. (11) taqqoslama $(ad - bd)/m$ munosabatga teng kuchli. U holda $(a - b)d/m$ dan $(d; m) = 1$ bo`lgani  $(a - b)/m$  yoki  $a \equiv b \pmod{m}$  bo`ladi.

Agar $(m; d) = k$ bo`lib,  $k > 1$  bo`lsa, u holda bu xossa o`rinli emas.

M i s o l. $5 \cdot 4 \equiv 7 \cdot 5 \pmod{15}$, $(5; 15) = 5 \neq 1$ bo`lgani uchun bu taqqoslamaning xar ikkala tamoni 5 ga bo`lib, $4 \equiv 7 \pmod{15}$, $(5; 15) = 5 \neq 1$ bo`lgani uchun bu taqqoslamaning xar ikkala tomonini 5 ga bo`lib, $4 \equiv 7 \pmod{15}$ xulosaga kelamiz

8⁰. Taqqoslamaning ikkala qismini va modulini bir xil butun musbat songa ko`paytirish, taqqoslamaning ikkala qismi va modul umumiy ko`paytuvchiga ega bo`lsa, u holda bu taqqoslamaning ikkala qismi va modulini umumiy ko`paytuvchiga bo`lish mumkin.

9⁰. Agar taqqoslama bir necha modul bo`yicha o`rinli bo`lsa, u holda bu taqqoslama shu modullarning eng kichik umumiy karralisi bo`yicha ham o`rinli bo`ladi.

10⁰. Agar taqqoslama biror m modul bo`yicha o`rinli bo`lsa, u holda shu taqqoslama modulning ixtiyoriy bo`luvchisi bo`yicha ham o`rinli bo`ladi.

Haqiqatan, agar $a \equiv b \pmod{m}$ yoki $a - b = mt$ bo`lib  $m = m_1 d$  bo`lsa, u holda $a - b = m_1 dt$ deyish mumkin. Bundan $a - b = m_1 (dt)$ bo`ladi. Demak, $a \equiv b \pmod{m_1}$ ekan.

11⁰. Taqqoslamaning bir qismi va modulining eng katta umumiy bo`luvchisi bilan uning ikkinchi qismi va modulining eng katta umumiy bo`luvchisi o`zaro teng bo`ladi. Haqiqatan, $a \equiv$

$b \pmod{m}$ dan $a = b + mt$ yoki $a - mt = b$ tengliklarni yozish mumkin. $(a; m) = d$ va $(b; m) = d_1$ bo'lsin. Aytaylik, $a = da_1$ va $m = dm_1$ bo'lsin.

$a_1 d - m_1 dt = b$ ning chap qismi d ga bo'linganidan b ham d ga bo'linadi. d son b va m sonlarning umumiy bo'luvchisi ekan va

$$d_1 / d \quad (12)$$

$b = db_1$ bo'lsin. U holda $a = b_1 d_1 + m_2 d_1 t$ tenglikdan a/d_1 va d_1 son a va m sonlarning umumiy bo'luvchisi bo'lgani uchun

$$d_1 / d \quad (13)$$

bo'ladi. (12) va (13) larga ko'ra $d_1 = d$ bo'ladi.

Eyler funksiyasi

$$\varphi(a) = a(1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_n)$$

Eyler funksiyasi a sonidan kichik va a soni bilan o'zaro tub sonlar soni.

Eyler teoremasi: $m > 1$ va $(a; m) = 1$ bo'lganda quyidagi taqqoslama o'rinli:

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

Bu yerda $\varphi(m)$ – Eyler funksiyasi

Misol: 3^{4n+2} ning oxirgi raqamini toping.

$$3^{4n+2} = (3^2)^{2n+1} = 9^{2n+1}$$

$$3 \equiv 3 \pmod{10}$$

$$9 \equiv 9 \pmod{10}$$

$$9 \equiv -1 \pmod{10}$$

$$9^{2n+1} \equiv 9 \pmod{10}$$

Javob: 9

Ferma teoremasi

p tub son va $(a; p) = 1$ bo'lganda quyidagi taqqoslama o'rinli

$$a^{p-1} \equiv 1 \pmod{p}$$

Misol: p tub son bo'lsa, $a^p + a(p-1)! \equiv 0 \pmod{p}$ bo'lishini isbotlang.

$$a^p + a(p-1)! = a^p + a(p-1)! + a - a = a((p-1)! + 1) + a^p - a$$

Vilson teoremasiga ko'ra, $(p-1)! + 1 \equiv 0 \pmod{p}$ ga qoldiqsiz bo'linadi.

$a^p - a$ sonini qoldiqsiz bo'linishini isbotlash yetarli.

$$p=2 \quad a^2 - a = a(a-1)$$

$$p=3 \quad a^3 - a = a(a-1)(a+1)$$

$$p=5 \quad a^5 - a = a(a^4 - 1) = a(a-1)(a+1)(a^2 + 1)$$

$$p=7 \quad a(a^6 - 1) = a(a^3 - 1)(a^3 + 1) = a(a-1)(a+1)(a^2 + a + 1)(a^2 - a + 1)$$

$$p=n-1 \quad a(a^{n-2} - 1) \text{ soni } n-1 \text{ ga qoldiqsiz bo'linadi}$$

$$p=n \quad a(a^{n-1} - 1) \text{ soni } n \text{ ga qoldiqsiz bo'linadi, bunda } n \text{ tub son.}$$

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Sharipova, M. P., & Latipova, S. S. (2024). Taqqoslamalar. Eyler funksiyasi. Yangi O'zbekiston talabalari axborotnomasi, 2(2), 23–33.
2. Averbux, K. Ya. (2004). Obshchaya teoriya termina. Ivanovo.

3. Litovchenko, V. I. Klassifikatsiya i sistematizatsiya terminov. Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta im. Akademika M. F. Reshetnyova, 156–159.
4. Madrakhimov, I. S., & Abdullayev, S. (2022). Yuklama. Galaxy International Interdisciplinary Research Journal, 10(12), 1754–1760.
5. Taqqoslamalarni yechish. Arxiv.uz

INNOVATIVE
ACADEMY