O‘zbekiston Respublikasi Ta’limni rivojlantirish respublika ilmiy-metodik markazi

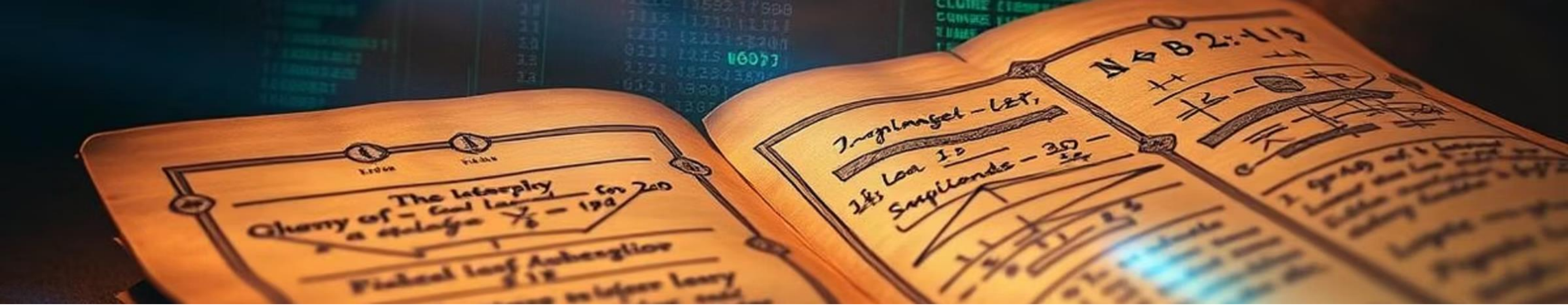
“OXIRGI 2 TA RAQAMNI TOPISH: KLASSIK MAVZUGA KREATIV YONDASHUV”

Kalandarova Maftuna Abdug‘offor qizi
Toshkent shahri Yunusobod tumani
220-sonli umumiy o‘rta ta’lim maktabining
matematika o‘qituvchisi

Mavzuga kirish:

Oxirgi raqamlarni topish kundalik hayotimizda PIN kodlar, bank tizimlari, raqamli xavfsizlikda qo‘llaniladi.

Bu mavzu orqali murakkab darajali sonlarning oxirgi 2ta raqamini topish usullarini o‘rganamiz.



Tarixiy ma’lumot

Oxirgi raqamlarni topish muammosi qadimdan mavjud bo‘lib, asosan arifmetik modullar bilan bog‘liq masalalar sifatida Eronlik matematik Muhammad ibn Muso al-Xorazmiy davrida muhokama qilingan.
Ammo zamonaviy shaklda bu masala XVIII–XIX asrlarda, Yevropalik matematiklar Leonhard Eyler va Pierre de Ferma tomonidan modul arifmetikasiga oid teoremalar orqali shakllangan.
Ayniqsa Fermaning kichik teoremasi va Eyler teoremasi bu yo‘ldagi muhim qadam bo‘lgan.

Oddiy Misol

Misol: $7^4 = 2401$
Oxirgi 2 raqam: 01
Shunchaki sonni hisoblab, oxirgi 2 raqamni yozamiz.

Murakkablik

Misol: 7^{1234} kabi katta darajalarni hisoblash imkonsiz.
Shuning uchun matematik teoremalar yordamga keladi.

Oxirgi 2 ta topish asoslari:

Eyler teoremasi:

Ta’rif:
Agar a va n musbat sonlar bo‘lib, ular o‘zaro tub bo‘lsa (ya’ni eng katta umumiy bo‘luvchisi 1 bo‘lsa), n ixtiyoriy son u holda:

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

Bu yerda $\varphi(n)$ — Eyler funksiyasi bo‘lib, n ga nisbatan o‘zaro tub sonlar sonini bildiradi.

Fermaning kichik teoremasi:

Ta’rif:
Agar p — tub son va a — butun son bo‘lib, a va p o‘zaro tub bo‘lsa (ya’ni p a ga bo‘linmasa), u holda:

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

Bu teorema modul arifmetikasida katta darajalarni tub modul bo‘yicha soddalashtirishda ishlatiladi.

1

Eyler va Ferma teoremalari:

Ferma teoremasi

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

1) a va p ōzaro tub son.
2) p tub son

M: $2^{7-1} \equiv 1 \pmod{7}$

$64 \equiv 1 \pmod{7}$

M: $4^{5-1} \equiv 1 \pmod{5}$

$4^{4} \equiv 1 \pmod{5}$

2

Eyler teoremasi:

$$\boxed{a^{\varphi(n)} = 1 \pmod{n}}$$

n – ixtiyoriy

a va n ōzaro tub son:

φ(n) – Eyler funksiyasi:

M: $\varphi(100)$ $100 = 2^2 \cdot 5^2$

$$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) =$$

$$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

M: $\varphi(24)$ $24 = 2^3 \cdot 3$

$$\varphi(24) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) =$$

$$= 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$$

1 24
5 24
7 24
11 24
13 24
17 24
19 24
23 24

$\varphi(n) \rightarrow$ n sonidan kichik va n soni bilan ōzaro tub sonlar juftliklari soni:

Modul arifmetikasi mod n:
sonni n ga bo‘lgandagi qoldiq.

Misol: 12345 mod 100 = 45

Shunday qilib, oxirgi 2 raqam = son mod 100 ekan.

Misol: $7^{45} \bmod 100$
$\varphi(100) = 40 \rightarrow 7^{40} \equiv 1 \pmod{100}$
$45 = 40\times1 + 5 \rightarrow 7^{45} \equiv 7^5 \pmod{100}$
$7^5 = 16807 \rightarrow 16807 \bmod 100 = 07$

Kreativ Yondashuv: Binariy eksponentatsiya

Katta darajali sonlarning oxirgi 2ta raqamini topishda faqat klassik formulalarga tayanmasdan, algoritmik va struktural yondashuvlardan foydalanish bu mavzuga "kreativ yondashuv"dir. Ayniqsa, binar (ikkiyuzli) eksponentatsiya algoritmi murakkab sonlarni juda tez hisoblash imkonini beradi.

Asosiy g‘oya: Katta darajalarni mod orqali bosqichma-bosqich hisoblash.

Masalan: 21^13 ni topamiz → 21^13 = 21^8 * 21^4 * 21^1

21^1 = 21

21^2 = 441 → mod 100 = 41

21^4 = (21^2)^2 = 41^2 = 1681 → mod 100 = 81

21^8 = (21^4)^2 = 81^2 = 6561 → mod 100 = 61

21^13 mod 100 = (21 * 81*61) mod 100 = 103761 → mod 100 = 61

Nima uchun bu kreativ? Katta sonlar ustida ishlashda matematik soddalashtirishlar yetarli emas. Kompyuter algoritmlari bilan uyg‘unlashadi. Real vaqtli hisob-kitobda tezlikni ta’minlaydi. Kod yozishga ham mos: pow(a, b, mod) funksiyasi aynan shu g‘oyaga asoslanadi. Bu yondashuv nafaqat sonni "quruq hisoblash"ni, balki uni strukturali tarzda tahlil qilishni o‘rgatadi.

1

Eyler va Ferma teoremalari.

1. 13^7 sonni 7 ga bo'lgandagi qoldiqni toping.

$13^7 = x \pmod 7$

$a = 13$
$p = 7$

Ferma: $13^{7-1} = 1 \pmod 7$

$13^6 = 1 \pmod 7$

$\cancel{13^6} \cdot 13 = x \pmod 7$

$x = 6$

2

2. $7^{7^{77}}$ sonning oxirgi ikki raqamini toping.

$7^{7^{77}} = x \pmod{100}$

$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40.$

1) $7^{40} = 1 \pmod{100}$

2) $7^{77} = y \pmod{40}$

$\varphi(40) = 40 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 16$

$7^{16} = 1 \pmod{40}$

$7^{13} = y \pmod{40} \to (7^2)^6 \cdot 7 = (49)^6 \cdot 7 = 9^6 \cdot 7 = (9^2)^3 \cdot 7 = 81^3 \cdot 7 \Rightarrow 1 \cdot 7 = 7.$

$\boxed{y = 7}$

$7^7 = x \pmod{100}$

$x = 43$

$7^4 = 2401$
$7^6 = \ldots 49$
$7^7 = \ldots 43$

Sonning oxirgi 2ta raqami.

1°

$$\boxed{51^{8} = \ldots 01}$$

$$21^{2} = \ldots 41$$

$$81^{82} = \ldots 61$$

2°

$$2^n \Rightarrow 2^{10} = 1024$$

$$\boxed{24^n = \begin{cases} 24, & n-\text{toq} \\ 76, & n-\text{juft} \end{cases}}$$

M: 2^n

M: $2^{2038} = (2^{10})^{203} \cdot 2^8 =$

$$= (1024)^{203} \cdot 2^8 = \ldots 24 \cdot \ldots 56 = \ldots 44$$

M: $\boxed{3^n} \Rightarrow 3^{830} = (3^4)^{207} \cdot 3^2 =$

$$= 81^{207} \cdot 9 = \ldots 61 \cdot 9 = \ldots 49$$

M: $\boxed{4^n}$ $4^{2025} = (2^2)^{2025} = 2^{4050} =$

$$= (2^{10})^{405} = (1024)^{405} = \ldots 24$$

M: 5^n M: $5^{526} = \ldots 25$

$$5^{555555} = \ldots 25$$

M: $6^n \Rightarrow 2^n \cdot 3^n$

M. $6^{214} = (2 \cdot 3)^{214} = 2^{214} \cdot 3^{214} \Rightarrow$

1-ish: $2^{214} = (2^{10})^{21} \cdot 2^4 = (1024)^{21} \cdot 16 =$

$$= \ldots 24 \cdot 16 = \ldots 84$$

2-ish: $3^{214} = (3^4)^{53} \cdot 3^2 = 81^{53} \cdot 9 =$

$$= \ldots 41 \cdot 9 = \ldots 69$$

$$\Rightarrow \ldots 84 \cdot \ldots 69 = \ldots 96$$

javob: 96

M: $7^{289} = (7^4)^{72} \cdot 7 = (2401)^{72} \cdot 7 =$

$= ...01 \cdot 7 = ...07$

M: $8^{344} = (2^3)^{344} = 2^{1032} = (2^{10})^{103} \cdot 2^2 =$

$= (1024)^{103} \cdot 4 = ...24 \cdot 4 = ...96$

M: $9^{271} = (3^2)^{271} = 3^{542} = (3^4)^{135} \cdot 3^2 =$

$= (81)^{135} \cdot 9 = ...01 \cdot 9 = ...09$

M: $\boxed{10^n} = ...00$

M: $10^{270} = ...00 \quad 10^{501} = ...00$

M: $11^{103} = ...31$

M: $12^{57} = (2^2 \cdot 3)^{57} = 2^{114} \cdot 3^{57} \Rightarrow$

1-ish: $2^{114} = (2^{10})^{11} \cdot 2^4 = (1024)^{11} \cdot 16 =$

$= ...24 \cdot 16 = ...84$

2-ish: $3^{57} = (3^4)^{14} \cdot 3 = 81^{14} \cdot 3 =$

$= ...21 \cdot 3 = ...63$

javob: $...84 \cdot ...63 = ...92$

M: $13^{15} = (13^4)^3 \cdot 13^3 = (...61)^3 \cdot ...97 =$

$= ...81 \cdot ...97 = ...57$

M: $14^{1414} = (2 \cdot 7)^{1414} = 2^{1414} \cdot 7^{1414}$

M: $257^{237} = 57^{237} = (57^4)^{59} \cdot 57 =$

$= (...01)^{59} \cdot 57 = ...01 \cdot 57 = ...57$

M: $2024^{2025} = ...24^{25} = ...24$

M: $12^{5^{2025}} = ...12^{25} = (2^2 \cdot 3)^{25} =$

$\langle$ 1-ish: $5^{2025} = ...25$ $\rangle$

$= 2^{50} \cdot 3^{25} = (2^{10})^5 \cdot (3^4)^6 \cdot 3 =$

$= (1024)^5 \cdot 81^6 \cdot 3 =$

$= ...24 \cdot ...81 \cdot 3 = ...32$

M: $222^{222^{222}} = 22^{84}$

1-ish: $222^{222} = 22^{222} = 2^{222} \cdot 11^{222} =$

$= (2^{10})^{22} \cdot 2^2 \cdot ...21 = (1024)^{22} \cdot 4 \cdot ...21 =$

$= ...76 \cdot 4 \cdot ...21 = ...84$

2-ish: $22^{84} = 2^{84} \cdot 11^{84} =$

$= (2^{10})^8 \cdot 2^4 \cdot ...41 = ...76 \cdot 16 \cdot ...41 =$

$= ...56$

javob: 56

M: $33^{259} = 3^{259} \cdot 11^{259} =$

$= (3^4)^{64} \cdot 3^3 \cdot ...91 = 81^{64} \cdot 27 \cdot ...91 =$

$= ...21 \cdot 27 \cdot ...91 = ...97$

$$\begin{array}{r|l} 259 & 4 \\ \hline -24 & 64 \\ 19 & \\ 16 & \\ \hline 3 & \end{array}$$

Oxirgi 2 ta raqam

1.	651^{84} ning oxirgi 2 ta raqamini toping.
2.	1001^{845} ning oxirgi 2 ta raqamini toping.
3.	11^{581} ning oxirgi 2 ta raqamini toping.
4.	2^{65} ning oxirgi 2 ta raqamini toping.
5.	2^{1001} ning oxirgi 2 ta raqamini toping.
6.	3^{62} ning oxirgi 2 ta raqamini toping.
7.	3^{100} ning oxirgi 2 ta raqamini toping.
8.	4^{44} ning oxirgi 2 ta raqamini toping.

9.	4^{612} ning oxirgi 2 ta raqamini toping.
10.	5^{54} ning oxirgi 2 ta raqamini toping.
11.	5^{555} ning oxirgi 2 ta raqamini toping.
12.	7^{65} ning oxirgi 2 ta raqamini toping.
13.	7^{98} ning oxirgi 2 ta raqamini toping.
14.	8^{62} ning oxirgi 2 ta raqamini toping.
15.	9^{99} ning oxirgi 2 ta raqamini toping.
16.	10^{54} ning oxirgi 2 ta raqamini toping.
17.	12^{50} ning oxirgi 2 ta raqamini toping.

E’TIBORINGIZ UCHUN RAHMAT!