ARIFMETIKANING ASOSIY TEOREMASI VA UNING QO‘LLANILISHI

Nuritdinov Jalolxon Tursunboy o‘g‘li
QDU Matematika kafedrasi o‘qituvchisi
Otajonova Ozoda Doniyorjon qizi
QDU Matematika va informatika yo‘nalishi talabasi

Annotatsiya: *Mazkur maqolada arifmetikaning asosiy teoremasi, ya’ni har qanday natural sonni yagona usulda tub sonlar ko‘paytmasi ko‘rinishida ifodalash mumkinligi isbotlanadi va bu teoremaning nazariy hamda amaliy ahamiyati yoritiladi. Teoremaning asosiy xususiyatlari, uning isboti, tarixiy rivojlanishi va zamonaviy matematikadagi qo‘llanilishlari tahlil qilinadi. Xususan, sonlar nazariyasidagi rollari, kriptografiya va algoritmik hisoblashdagi ahamiyati misollar bilan ko‘rsatiladi.*

Kalit so‘zlar: *Arifmetika, asosiy teorema, tub sonlar, sonlar nazariyasi, faktorizatsiya, kriptografiya, unikal ko‘paytma.*

Аннотация: *В данной статье доказывается основная теорема арифметики, а именно: любое натуральное число можно единственным образом (с точностью до порядка множителей) представить в виде произведения простых чисел. Освещаются теоретическое и практическое значение данной теоремы. Рассматриваются её основные свойства, доказательство, историческое развитие и современные применения в математике. В частности, показана её роль в теории чисел, криптографии и алгоритмических вычислениях с приведением примеров.*

Ключевые слова: *арифметика, основная теорема, простые числа, теория чисел, факторизация, криптография, уникальное разложение.*

Annotation: *This article proves the fundamental theorem of arithmetic, which states that any natural number can be uniquely expressed as a product of prime numbers, and highlights the theoretical and practical significance of this theorem. The main properties of the theorem, its proof, historical development, and applications in modern mathematics are analyzed. In particular, its role in number theory, cryptography, and algorithmic computation is illustrated with examples.*

Keywords: *Arithmetic, fundamental theorem, prime numbers, number theory, factorization, cryptography, unique product.*

Matematikaning eng qadimgi va asosiy bo‘limlaridan biri bo‘lgan arifmetika sonlar bilan bog‘liq eng muhim xossalarni o‘rganadi. Ayniqsa, natural sonlarning tuzilishini chuqur anglash uchun arifmetikaning asosiy teoremasi muhim rol o‘ynaydi. Bu teorema har qanday $n>1$ natural sonni yagona usulda (ko‘paytuvchilarning tartibini hisobga olmaganda) tub sonlar ko‘paytmasi ko‘rinishida yozish mumkinligini bildiradi. Teorema qadim zamonlardan beri matematiklar e’tiborini tortib kelgan va zamonaviy matematikada, xususan, sonlar nazariyasi, hisoblash usullari hamda axborot xavfsizligi sohalarida keng qo‘llanilmoqda.

Bu teorema qadimgi yunon matematiklari tomonidan aniqlangan bo‘lib, birinchi marta Evklid (Euclid) tomonidan miloddan avvalgi III asrda yozilgan "Negizlar" asarida bayon qilingan. Zamonaviy matematikadagi qat’iy isboti esa XIX asrda matematiklar tomonidan ishlab chiqilgan.Ushbu maqolada arifmetikaning asosiy teoremasi isbotlanadi, uning tarixiy taraqqiyoti ko‘rib chiqiladi hamda zamonaviy amaliy masalalarda qanday tatbiq etilishi misollar yordamida tahlil qilinadi.

Teorema. (Arifmetikaning asosiy teoremasi) Birdan katta har kanday natural son yoki tub yoki uni bir xil usul bilan tub sonlar ko‘paytmasi shaklida ifodalash mumkin.

Isbot. 1) Har kanday natural sonni tub sonlar ko‘paytmasi shaklida ifodalash mumkinligini isbotlaylik. n=2 uchun teorema to‘g‘ri, chunki u tub son. Faraz qilaylik $2 \le m < n$ uchun teorema to‘g‘ri bo‘lsin. Teoremani n uchun isbotlaylik.

Agar m - tub bo‘lsa teorema to‘g‘ri. Agar murakkab bo‘lsa $\exists\, n_1, n_2 \in N$ $1 \le n_1 \le n$ $2 \le n_2 < n$ bo‘lib, $m=n_1 \cdot n_2$ tenglik o‘ringa ega. Teorema n_1, n_2 lar uchun to‘g‘ri, ya’ni, $n_1=p_1 p_2 \dots p_s$ $n_2 = p_{s+1} \dots p_k$, bundan

$$n=p_1 p_2 \dots p_k \qquad (1)$$

bu yerda $p_1, p_2, \dots$ - tub sonlar.

Demak, har kanday n>1 son yo tub yoki uni tub ko‘paytuvchilarga yoyish mumkin ekan.

2) Endi yagonaligini isbotlaylik.Faraz kilaylik n>1 natural son (1) dan farqli

$$n=q_1 q_2 \dots q_m \qquad (2)$$

tub sonlar ko‘paytmasi shaklida ifoladangan bo‘lsin.

(1) va (2) dan

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_m \qquad (3)$$

kelib chiqadi. (3) ning chap tomoni p_1 - tub songa bo‘linganligi sababli O‘ng tomoni xam p_1 larga bo‘linishi kerak. Ma’lumki, ko‘paytma biror tub songa bo‘linsa, ko‘paytuvchilardan birortasi shu tub songa bo‘linadi. Masalan, $q_1 \mid p_1$, p_1 va q_1 lar har xil tub sonlardir. Bundan $p_1=q_1$ kelib chiqadi.

Xuddi shuningdek, m>k bo‘lsa $p_2=q_2 \dots p_k = q_k$ ekanligini isbotlash mumkin. Buni e’tiborga olsak (3) dan $q_{k+1} \dots q_m = 1$, bu esa bo‘lishi mumkin emas.

Demak, m>k tengsizlik o‘rinli emas. Xuddi shuningdek k>m tengsizlikning ham o‘rinli emasligi ko‘rsatish mumkin.

Demak, m=k bo‘lib, $p_1=q_1 \dots p_k=q_m$. Teorema isbotlandi.

Misol. n=900 $n=2\times 2\times 3\times 3\times 5\times 5$ n- natural sonning (1) yoyilmasida ba’zi tub sonlar o‘zaro teng b’lishi mumkin. Shuning uchun (1) ni umumiy xolda

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h} \qquad (4)$$

ko‘rinishda ifodalanadi.

$p_1 p_2 \dots p_s$ - tub sonlar o‘sish tartibida joylashgan (4) ni n - natural sonning kanonik ko‘rinishi deyiladi.

Misol. $1176=2^3\times 3\times 7^2$, $136125=5^5\times 11^2$, $900=2^2\times 3^2\times 5^2$

Arifmetikaning asosiy teoremasidan kuyidagi natijalar kelib chiqadi.

1-natija. Agar $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ko‘rinishga ega bo‘lsa uning barcha bo‘luvchilari $c = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ ko‘rinishda bo‘ladi. $(0 \le \beta_i \le \alpha_i,\ i = \overline{1,k})$

Misol. 75=3 × 52 bo‘lsa 1,3,5, 3 × 5, 5 × 5, 3 × 52

2-natija. Aytaylik $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ va $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ ko‘rinishga ega bo‘lsin. U holda

$(a,b) = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_m^{\lambda_m}\ \lambda_i = \min\{\alpha_i, \beta_i\} i = \overline{1,m}\ [a,b] = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_m^{\lambda_m}\ \lambda_k = \max\{\alpha_k \beta_k\} k = \overline{1,m}$

Misol. (900,1176) = $2^2 \cdot 3$ =12; (900; 1176) =$2^3 \cdot 3^2 \cdot 5^2 \cdot 7^2$.

Algebra va sonlar nazariyasida son funksiyalaridan τ(n), σ(n), φ(a), [a], {a} larni ko‘rsatish mumkin.

1. τ(n) -n natural sonning barcha natural bo‘luvchilari soni, agar $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ bulsa , τ(n)=(α_1 +1) (α_2 +1) ... (α_k+1) bo‘ladi.

Masalan. n=900 900=$2^2 \cdot 3^2 \cdot 5^2$, m =75=$3 \cdot 5^2$, τ(900)=(2+1)(2+i)(2+1)=27 , τ (75)= (1+1)(2+1)=6

2. $\sigma(n)$ - n natural sonning barcha natural bo‘luvchilari yigindisi.

$$\sigma(n) = \frac{p_1^{\alpha_{n+1}} - 1 \cdot}{p_1 - 1} \cdot \frac{p_2^{\alpha_{2+1}} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_k^{\alpha_{kn+1}} - 1}{p_k - 1}$$

Masalan. $\sigma(75) = \frac{3^2 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} = \frac{3 \cdot 124}{2 \cdot 4} = 124$

3. [a] - a ning butun qismi; n ≤ a ‹ n+1, n∈ Z, [a]=n

Masalan. {2,75}=0,75 {-2,75}=-2,75 - (-3) =0,25

4. {a}- a ning kasr qismi; a=[a]+{a} {a}=a-[a]

Masalan. {2,75}=0,75 {-2,75}=-2,75 - (-3) =0,25

Sonning butun qismi quyidagi tatbiqlarga ega. n! tarkibida p tub son k_p daraja bilan qatnashadi.

$$k_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

Misol. 10! = 1× 2 × 3 ×22 × 5×2×3×7×23×32×2×5=1×28 × 34 × 52 × 7

$$\alpha_2 = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 5 + 2 + 1 = 8$$

$$\alpha_3 = \left[\frac{10}{3}\right] + \left[\frac{10}{4}\right] = 4\ \alpha_5 = \left[\frac{10}{5}\right] = 2; 7 = \left[\frac{10}{7}\right] = 1$$

1) 10! da k_5=2 =2 2) 50! k ta nollar tugaydi. $k = \left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] = 10 + 2 = 12$

(5)) φ(n) -n dan katta bo‘lmagan n bilan o‘zaro tub bo‘lgan natural sonlar soni. f(1)=1 deb qabul qilamiz.

Natural sonlar to‘plamida aniqlangan f(n) funksiyani mulptiplikativ deyiladi, agar 1) f(1)=1 bo‘lsa va 2) o‘zaro tub bo‘lgan n va m lar uchun f(n,m)=f(n)×f(m) o‘ringa ega bo‘lsa.

Arifmetikaning asosiy teoremasi quyidagi sohalarda keng qo‘llaniladi:

- Sonlar nazariyasi: eng sodda arifmetik masalalarni yechishda foydalaniladi.

• Algebra: ko‘paytuvchilarga ajratish, eng katta umumiy bo‘luvchi (EKUB) va eng kichik umumiy karrali (EKUK) ni topishda.

• Kriptografiya: ayniqsa, RSA algoritmi kabi zamonaviy shifrlash texnologiyalarida tub sonlarga ajratish muhim rol o‘ynaydi.

• Kompyuter fanlari: algoritmlarning samaradorligini oshirishda va optimallashtirishda qo‘llaniladi.

Arifmetikaning asosiy teoremasi matematikada juda muhim o‘ringa ega bo‘lib, har qanday natural sonning noyob ko‘rinishda tub sonlarga ajratilishini ta'minlaydi. Bu teorema nafaqat nazariy jihatdan, balki amaliy masalalarda ham katta ahamiyat kasb etadi. Uning asosida ko‘plab algoritmlar, kriptografik tizimlar va matematik modellar quriladi. Shuning uchun ushbu teoremaning mazmuni va mohiyatini chuqur o‘rganish har bir matematik uchun zarurdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. R.N. Nazarov, B.T. Toshqulov, A.D. Do‘sumbetov. Algebra va sonlar nazariyasi. II k. – T. O‘qitvchi, 1995.-272 b.
2. Л.Я.Куликов. Алгебра и теории чисел. М.:Вксшая школа, 1979.-559 с.
3. Nuritdinov, J., & Muhammadjonova, N. (2024). TARTIB AKSIOMALARINING GEOMETRIK TASDIQLARNI ASOSLASHDA QO‘LLANILISHI. University Research Base, 835–838. Retrieved from https://scholar.kokanduni.uz/index.php/rb/article/view/737
4. Sh, M. M., & Nuritdinov, J. T. (2020). MINKOVSKIY YIG ‘INDISINI VA AYIRMASINI HISOBLASHGA DOIR BA ‘ZI QONUNIYATLAR HAQIDA. Matematika Instituti Byulleteni Bulletin of the Institute of Mathematics Бюллетень Института, (3), 49-59.
5. Nuritdinov, J. (2024). TO‘G‘RI CHIZQDAGI KESMALARNING MINKOVSKIY AYIRMASI. University Research Base, 830–834. Retrieved from https://scholar.kokanduni.uz/index.php/rb/article/view/736
6. Nuritdinov, J., & Sharifjonova, M. (2024). LOBACHEVSKIY GEOMETRIYASINING BA’ZI MASALALARI TAHLILI. University Research Base, 869–874. Retrieved from https://scholar.kokanduni.uz/index.php/rb/article/view/745
7. Жалолхон Нуритдинов Турсунбой ўғли. (2023). ТЕКИСЛИКДА БЕРИЛГАН ЭЛЛИПСЛАР МИНКОВСКИЙ АЙИРМАСИ. QO‘QON UNIVERSITETI XABARNOMASI, 1(1), 105–113. https://doi.org/10.54613/ku.v1i1.312
8. Nuritdinov J.T. (2023). YARIM TEKISLIKLAR MINKOVSKIY AYIRMASI. QO‘QON UNIVERSITETI XABARNOMASI, 1(1), 38–40. https://doi.org/10.54613/ku.v1i1.281
9. Mamatov , M., Nuritdinov, J., & Esonov, E. (2021). Differential games of fractional order with distributed parameters. International Scientific Technical Journal "Problems of Control and Informatics", 66(4), 38–47. https://doi.org/10.34229/1028-0979-2021-4-4
10. Mamatov, M. S., & Nuritdinov, J. T. (2020). About some rules for calculating the Minkovsky sum and difference. Bulletin of the Institute of Mathematics, 3, 49-59.

11. Маматов, М. Ш., & Нуритдинов, Ж. Т. (2020). О некоторых геометрических свойствах разности и суммы Минковского. In Колмогоровские чтения. Общие проблемы управления и их приложения (ОПУ–2020) (pp. 69-72).

12. Nuritdinov, J., Khaydarov, I., Turdaliyev, S., & Djuraev, I. (2025, October). Application of Minkowski difference to optimal control tasks. In AIP Conference Proceedings (Vol. 3377, No. 1, p. 030001). AIP Publishing LLC.

13. Jalolxon Nuritdinov Tursunboy ugli (2020). Determining the Minkowski Difference and Sum of Some Sets. Solid State Technology, 2235-2240.

14. Nuritdinov, J., Kakharov, S., & Tashxodjayev, A. (2024, November). Application of Minkowski operator in artificial intelligence tasks. In AIP Conference Proceedings (Vol. 3244, No. 1). AIP Publishing.

15. Nuritdinov, J. T., & Nematov, B. B. (2024). NEW METHODS FOR DETERMINING WHETHER A SUFFICIENTLY LARGE NATURAL NUMBER IS PRIME OR COMPOSITE. International journal of medical sciences, 4(11), 177-181.

16. Tursunboy o'g'li, N. J. (2025). SONNING BUTUN VA KASR QISMINING AHAMIYATI. Научный Фокус, 3(29), 264-270.

17. Nuritdinov, J. T. (2022). About the Minkowski difference of squares on a plane. Differential Geometry-Dynamical Systems, 24.

18. Axadjon o'g'li, A. A., & Tursunboy o'g'li, N. J. (2023). SANOATNING YAIMGA TA'SIRINI BAHOLASH. Qo 'qon universiteti xabarnomasi, 290-293.

19. Tursunboy o'g'li, Nuritdinov Jalolxon. "TALABALARGA TEKISLIKDA KVADRATNING KANONIK TENGLAMASI VA UNING XOSSALARI MAVZUSINI O 'QITISHDA ZAMONAVIY TEXNOLOGIYALARDAN FOYDALANISH." MODELS AND METHODS FOR INCREASING THE EFFICIENCY OF INNOVATIVE RESEARCH 4.43 (2025): 187-194.

20. Nuritdinov, J., & Nosirov, H. (2025). TURLI SANOQ SISTEMALARIDA AMALLAR BAJARISH VA BIR SANOQ SISTEMASIDAN BOSHQA SANOQ SISTEMASIGA O'TISHNING TURLI USULLARI. ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ, 81(2), 85-90.