

$n = p^3$ UCHUN EYLERNING MATRITSALI TEOREMASI

Satniyazova I. Q., Boranbaev O. B.

¹Berdaq nomidagi Qoraqalpogʻ davlat universiteti

Matritsalar nazariyasi va sonlar nazariyasining oʻzaro bogʻliqligi zamonaviy matematikaning qiziqarli yoʻnalishlaridan biri hisoblanadi. Xususan, butun koʻeffitsientli matritsalar uchun klassik Ferma va Eyler teoremlarining analoglarini topish hamda ularning simmetrik funksiyalar bilan aloqasini oʻrganish nazariy va amaliy ahamiyatga ega.

Maʼlumki, butun sonlar uchun Eyler teoremasi $a^{\varphi(n)} \equiv 1 \pmod{n}$ koʻrinishida ifodalanadi. Ushbu gʻoyani matritsalar izi (tr) va Nyuton summolari (s_n) uchun umumlashtirish, ayniqsa, modul $n = p^k$ (tub sonning darajasi) boʻlgan holatlarda murakkab kombinatorik tahlillarni talab etadi. Ilgari oʻtkazilgan tadqiqotlarda ushbu teoremlar asosan $n = p$ (oddiy tub son) holati uchun isbotlangan boʻlsa, ushbu maqolada biz masalani yanada chuqurlashtirib, $n = p^3$ holatini koʻrib chiqamiz.

Maqolaning asosiy maqsadi $n = p^3$ modul boʻyicha matritsaning n -darajali izi va uning Eyler funksiyasi bilan bogʻliq darajasi orasidagi ayirmaning n ga boʻlinishini isbotlashdan iborat. Shuningdek, ushbu bogʻliqlikning fundamental simmetrik funksiyalar orqali ifodalanishi va multinomial koʻeffitsientlarning xossalari tahlil qilinadi. Tadqiqot davomida p toq tub sonlar va $p = 2$ boʻlgan maxsus holatlar uchun alohida algebraik hisoblashlar va lemmalar keltirilgan.

1-teorema. Quyidagi taqqoslash $n = p^3$ modul boʻyicha oʻrinlidir:

$$\text{tr}(A^n) = \text{tr}(A^{n-\varphi(n)}) \pmod{n}.$$

Eyler funksiyasi φ uchun $n = p^3$ boʻlganda $n - \varphi(n) = p^2$ boʻladi. Demak, 1-teorema quyidagi tenglikni tasdiqlaydi:

$$\text{tr}(A^{p^3}) = \text{tr}(A^{p^2}) \pmod{p^3}.$$

Bu fakt simmetrik funksiyalar nazariyasidagi quyidagi teorema ekvivalentdir.

2-teorema. Quyidagi taqqoslash $n = p^3$ modul boʻyicha oʻrinlidir:

$$s_n - s_{n-\varphi(n)} \equiv 0 \pmod{n}.$$

Eslatma. [1] maqolada isbotlangan Ferma matritsali teoremasining analogi (bu yerda $n = p$ - tub son) agar bazaviy simmetrik funksiyalar σ_k orqali ifodalangan koʻphad sifatida qaralsa ($n = p$ holidagi), n ning koʻphad koʻeffitsientlarining ayirmasiga boʻlinishini tasdiqlaydi.

Biroq Eylerning matritsali teoremasi (2-teorema) $n = p^3$ holidagi $s_n - s_{n-\varphi(n)}$ koʻphadining koʻeffitsientlari n ga boʻlinishini tasdiqlamaydi; bu yerda faqat ushbu butun koʻphadning har bir $\sigma \in \mathbb{Q}^r$ nuqtadagi qiymatlari n ga boʻlinishi aytiladi.

Biz bu hodisa $\sigma(\mathbb{Q}^r)$ toʻplamining oʻziga xos xususiyati ekanmi, yoki yoʻqmi, yaʼni ushbu toʻplamda aniqlangan har qanday koʻphad uchun, agar uning qiymatlari $\sigma(\mathbb{Q}^r)$ ning barcha nuqtalarida n ga boʻlinsa, u holda uning koʻeffitsientlari ham n ga boʻlinadimi buni bilmaymiz. Shuningdek, qaysi shartlar ostida $\sigma(\mathbb{Q}^r)$ ning M kichik toʻplami uchun koʻphadning barcha qiymatlari n ga boʻlinishi kafolatlanishini (yoki maxsus koʻphad $s_n - s_{n-\varphi(n)}$ uchun bunday boʻlinishni taʼminlaydigan qanday xossalari mavjudligini) aniqlash qiziqarli boʻlar edi.

1- va 2-teoremlarning isboti. p toq son boʻlsin. K koʻeffitsientlar uchun [1] -manbada isbotlangan quyidagi

$$K(\{m_k\}) = (-1)^{n-m} \frac{n}{m} C(\{m_k\}), \quad (*)$$

formulaga koʻra, p^3 modul boʻyicha taqqoslashni olish uchun s_n ifodadagi p^3 ga boʻlinadigan barcha hadlarni eʼtibordan chetda qoldirishimiz mumkin. Shu sababli, faqat shunday hadlar sinfi qoladiki, ular uchun koʻrsatkichlardan kamida bittasi m_k tub son p bilan oʻzaro tub boʻlsin.

Demak, p^3 modul boʻyicha ($n = p^3$ boʻlganda) quyidagi taqqoslash oʻrinlidir:

$$s_n \equiv \sum K(\{m_k\}) \Pi(\{m_k\}),$$

bu yerda barcha koʻrsatkichlar m_k p ga boʻlinadi.

Endi bu hadlarni $\{m_k\}$ sonlarining tub son p darajalariga boʻlinishiga qarab guruhlarga ajratamiz. Birinchi guruh α darajali hadlardan iborat boʻlib, unda kamida bitta a_k uchun $(a_k, p) = 1$ bajariladi. Bu yerda, yuqorida boʻlgani kabi

$n = \sum p^{\alpha+1} u_k a_k$, va n ning p ga boʻlingan qiymatini $\tilde{n} = \frac{n}{p} = \sum p^{\alpha} u_k a_k$ bilan belgilaymiz.

Bunday holding $s_n - s_{n-\varphi(n)}$ dagi hissasi $I + II$ ga teng bo'ladi, bu yerda

$$I = (K(\{p^{\alpha+1}a_k\}) - K(\{p^\alpha a_k\}))\Pi(\{p^{\alpha+1}a_k\}),$$

$$II = K(\{p^\alpha a_k\})(\pi^{\alpha+1} - \pi^\alpha),$$

va bu yerda $\pi = \Pi(\{a_k\}) = \Pi(\{\sigma_k^{a_k}\})$.

Endi I va II hadlarining p tub son darajalari bo'yicha bo'linishini baholaymiz.

1-lemma. Agar $n = p^3$ bo'lsa, u holda II had n ga bo'linadi.

Isboti: (*) formulaga ko'ra aniqlangan son

$$K = \pm \frac{n = p^{\alpha+1}}{m} C(\{m_k = p^\alpha a_k\})$$

$p^{\alpha-1}$ ga bo'linishi ma'lum. Bundan tashqari, $\pi^{\alpha+1} - \pi^\alpha$ ifoda sonli Eyler teoremasiga ko'ra $p^{\alpha+1}$ ga bo'linadi.

Demak, ularning ko'paytmasi $p^{(\alpha-1)+(\alpha+1)} = p^{2\alpha}$ ga bo'linadi; bu esa 1-lemmani isbotlaydi.

Buning uchun quyidagi farqni ko'rib chiqamiz:

$$K(\{p^{\alpha+1}a_k\}) - K(\{p^\alpha a_k\}) = \frac{n}{m} (C(\{p^{\alpha+1}a_k\}) - C(\{p^\alpha a_k\})).$$

bu yerda birinchi ko'paytuvchi $\frac{n}{m} = p^{\alpha-1} = p^2$, ikkinchi ko'paytuvchi esa multinomial koeffitsientlarning ayirmasi

bo'lib, 2-teoreмага ko'ra p^2 ga bo'linadi. Shu sababli, $n = p^3$ holda ko'paytmaning p^3 ga bo'linishini isbotlash uchun maxraj $m = \sum p^\alpha a_k$ sonining p^2 ga bo'linmasligini tekshirish kifoya.

Bu holni oson tavsiflash mumkin, chunki

$$m = \sum p^\alpha a_k \leq n = \sum p^{\alpha+1} u_k = p^2.$$

Demak, m ning p^2 ga bo'linishi ($m \neq 0$ bo'lgani, chunki $(a_k, p) = 1$ bo'lgan kamida bitta k mavjud) faqat $m = p^2$ bo'lgandagina mumkin. Ammo shartga ko'ra $m = n$, bundan esa qaralayotgan hol kelib chiqmaydi.

Shunday qilib, I ham p^3 ga bo'linadi va natijada 1- va 2-teoremlarning isboti yakunlanadi.

Shunday qilib, $p^\alpha \sum a_k = p^\alpha \sum (u_k a_k)$, demak, $\sum (u_k - 1)a_k = 0$. Bundan kelib chiqadiki, faqat bitta koeffitsient a_k noldan farqli bo'lishi mumkin; u uchun esa $u_k = 1$ bo'ladi. Shuning uchun $p^\alpha a_k = p^2$ va $p^{\alpha+1} a_k = p^3$. Natijada $K(\{p^{\alpha+1}a_k\}) = K(\{p^\alpha a_k\}) = 1$. Demak, o'rganilayotgan I ko'phadi p^3 ga bo'linadi va shu bilan 2-teorema p toq tub sonlar uchun isbotlanadi.

1- va 2-teoremlarning $p = 2$ uchun ham to'g'riligini deyarli xuddi shunday yo'l bilan isbotlash mumkin; farq faqat shundaki, ayrim hadlarda (bu yerda daraja m toq bo'lganda) quyidagi ayirma

$$C(\{p^{\alpha+1}a_k\}) - C(\{p^\alpha a_k\})$$

o'rniga aynan shu multinomial koeffitsientlarning yig'indisi paydo bo'ladi. Bu yig'indi hamon $p^2 = 4$ ga bo'linadi; buni, masalan, $s_8 - s_4$ ayirma hadlari juda ko'p bo'lmagan quyidagi aniq formula orqali ko'rish mumkin

$$\begin{aligned} s_8 - s_4 = & \sigma_1^8 - 8\sigma_1^7\sigma_2 + 8\sigma_1^6\sigma_2^2 - 8\sigma_1^5\sigma_2^3 + 8\sigma_1^4\sigma_2^4 - 8\sigma_1^3\sigma_2^5 + 8\sigma_1^2\sigma_2^6 - 8\sigma_1\sigma_2^7 + \sigma_2^8 \\ & + 20\sigma_1^4\sigma_2^2 - 32\sigma_1^3\sigma_2^3 - 16\sigma_1^2\sigma_2^3 + 24\sigma_1^2\sigma_2^4 + 12\sigma_1^2\sigma_2^5 + 24\sigma_1\sigma_2^2\sigma_3 \\ & - 16\sigma_1\sigma_2\sigma_5 - 16\sigma_1\sigma_3\sigma_4 + 2\sigma_2^4 - 8\sigma_2^2\sigma_4 - 8\sigma_2\sigma_3^2 + 8\sigma_2\sigma_6 + 8\sigma_3\sigma_5 + 4\sigma_4^2. \end{aligned}$$

Modul 8 bo'yicha quyidagi taqqoslash o'rinni:

$$s_8 \equiv \sigma_1^8 + 20\sigma_1^4\sigma_2^2 + 12\sigma_1^2\sigma_3^2 + 2\sigma_2^4 + 4\sigma_4^2 \pmod{8}.$$

Shu bilan bir vaqtda,

$$s_4 = \sigma_1^4 - 4\sigma_1^3\sigma_2 + 4\sigma_1^2\sigma_3 - 4\sigma_1\sigma_2^2 + 2\sigma_2^2.$$

Demak, modul 8 bo'yicha quyidagi taqqoslash kelib chiqadi:

$$\begin{aligned} s_8 - s_4 = & \sigma_1^4(\sigma_1^4 - 1) + 4\sigma_1^3(\sigma_2 + 1) + 2\sigma_2^2(\sigma_2^2 - 1) \\ & + 4\sigma_1^2\sigma_2(\sigma_1^2\sigma_2 + 1) + 4\sigma_1\sigma_3(3\sigma_1\sigma_3 - 1). \end{aligned}$$

Ushbu besh hadning har biri 8 ga bo'linadi, bu esa $p = 2$ holda ham 1- va 2-teoremlarning to'g'riligini isbotlaydi.

ADABIYOTLAR

1. Арнольд В. И. Динамика Ферма, арифметика матриц, конечная окружность и конечная плоскость Лобачевского // Функцион. анализ и его прилож. 2004. Т. 38. №1. С. 1-15.
2. Arnold Problems. Heidelberg-Berlin-N. Y: Phasis-Springer, 2004. P. 157-162.

3. Girard A. Sur des decouvertes nouvelles en algebre. Amsterdam, 1629.
4. Newton I. Arithmetica universalis. Cambridge, 1707.

Euler's matrix theorem for $n = p^3$

Abstract. The article investigates analogues of Euler's theorem for matrix traces and symmetric functions modulo $n = p^3$, where p is a prime number. The main result proves the validity of the congruence $\text{tr}(A^n) \equiv \text{tr}(A^{n-\varphi(n)}) \pmod{n}$. Furthermore, the equivalence in the theory of symmetric functions and the divisibility properties of polynomial coefficients are analyzed using Newton's sums and multinomial coefficients. The proofs cover cases for both odd primes p and the specific case of $p = 2$.

Key words: Matrix trace, Euler's theorem, symmetric functions, congruences, Newton sums.

Матричная теорема эйлера для $n = p^3$

Аннотация. В статье исследуются аналоги теоремы Эйлера для следов матриц и симметрических функций по модулю $n = p^3$, где p — простое число. В качестве основного результата доказана справедливость сравнения $\text{tr}(A^n) \equiv \text{tr}(A^{n-\varphi(n)}) \pmod{n}$. Также с использованием формул Ньютона и мультиномиальных коэффициентов проанализированы эквивалентности в теории симметрических функций и свойства делимости коэффициентов многочленов. Доказательства представлены как для нечетных простых чисел p , так и для случая $p = 2$.

Ключевые слова: След матрицы, теорема Эйлера, симметрические функции, сравнения, суммы Ньютона.

$n = p^3$ uchun eylerning matritalsali teoremasi

Annotatsiya. Maqolada $n = p^3$ (bu yerda p - tub son) modul bo'yicha matritalarning izlari va simmetrik funksiyalar uchun Eyler teoremasining analoglari tadqiq etilgan. Asosiy natija sifatida $\text{tr}(A^n) \equiv \text{tr}(A^{n-\varphi(n)}) \pmod{n}$ taqqoslamasining o'rinli ekanligi isbotlangan. Shuningdek, Nyuton formulalari va multinomial koeffitsientlar yordamida simmetrik funksiyalar nazariyasidagi ekvivalentliklar hamda ko'phad koeffitsientlarining bo'linish xususiyatlari tahlil qilingan. Isbotlashda p toq tub son va $p = 2$ holatlari alohida ko'rib chiqilgan.

Kalit so'zlar: Matritsa izi, Eyler teoremasi, simmetrik funksiyalar, taqqoslashlar, Nyuton summalari.