APPLICATIONS OF THE JACOBIC SYMBOL

Gayniddinov Shaykhislom Tolibjon ugli

Teacher of the Department of Exact Sciences, Namangan State Pedagogical Institute

Annotation: In studying Jacobi symbols, we examine quadratic residues and their properties. The Legendre symbol is used to determine the quadratic relationship between two prime numbers. The Jacobi symbol, on the other hand, is a generalization of the Legendre symbol and is defined for any positive odd number. It is computed as the product of the Legendre symbols corresponding to its prime divisors.Legendre and Jacobi symbols are powerful tools for studying the behavior of integers modulo some number. While the Legendre symbol is based on prime numbers, the Jacobi symbol extends to composite numbers, providing a broader framework for number theory.

Keywords: comparison, modulus, residue class, Legendre symbol, Jacobi symbol.

Аннотатция:В изучении символов Якоби мы рассматриваем квадратичные вычеты и их свойства. Символ Лежандра используется для определения квадратичного соотношения между двумя простыми числами. Символ Якоби, в свою очередь, является обобщением символа Лежандра и определяется для любого положительного нечетного числа. Он вычисляется как произведение символов Лежандра, соответствующих его основным делителям. Символы Лежандра и Якоби являются мощными инструментами для изучения поведения целых чисел по модулю. Символ Лежандра основывается на простых числах, тогда как символ Якоби охватывает и составные числа, что позволяет сделать теорию чисел более всеобъемлющейю

Ключевые слова: сравнение, модуль, класс вычетов, символ Лежандра, символ Якоби.

Annotatsiya: Yakobi simvollarida biz kvadratik qoldiqlar va ularning xossalari to‘grisida o‘rganamiz. Lejandr simvoli ikki tub son orasidagi kvadratik munosabatni aniqlashda ishlatamiz. Yakobi simvoli esa Lejandr simvolining umumlashmasi bo‘lib, har qanday musbat toq son uchun aniqlanadi va uning asosiy bo‘luvchilariga bo‘lingan holda Lejandr simvollari ko‘paytmasi sifatida hisoblanadi. Lejandr va Yakobi simvollari butun sonlar modul bo‘yicha xatti-harakatini o‘rganish uchun kuchli vositalardir. Lejandr simvoli oddiy sonlarga asoslangan bo‘lsa, Yakobi simvoli murakkab sonlarni ham qamrab oladi va bu sonlar nazariyasini yanada keng qamrovli qilishga imkon beradi.

Kalit so‘zlar: taqqoslama, mod, chegirmalar sinfi, Lejandr simvoli, Yakobi simvoli.

KIRISH

Ushbu mavzuda yuqori darajali taqqoslamalarni yechishni o‘rganamiz, ya’ni bizga

$$x^n \equiv a(modm)$$

taqqoslama berilgan bo‘lib, $(a, m) = 1$ bo‘lsin.

1-ta'rif. Agar $x^n \equiv a(modm)$ taqqoslamaning yechimi mavjud bo'lsa, u holda a soniga n-darajali chegirma deyiladi, yechimga ega bo'lmasa a soni n- darajali chegirma bo'lmaydi.

Shuningdek, $n = 2$, $n = 3$ va $n = 4$ bo'lganda chegirmalar mos ravishda kvadratik, kubik va bikvadratik deyiladi.

Dastlab kvadratik bo'lgan hol uchun ko'raylik, bizga

$$x^2 \equiv a(modp) \qquad (1)$$

Kvadratik taqqoslama berilgan bo'lsin, bu yerda p $(p > 2) -$ tub son.

Agar a soni p modul bo'yicha kvadratik chegirma bo'lsa, u holda (1) chegirma kamida bitta yechimga ega. Aytaylik, $x \equiv x_1(modp)$ yechim bo'lsin, u holda $(-x_1)^2 = {x_1}^2$ ekanligidan ushbu $x \equiv -x_1(modp)$ ham yechimi ekankigini ko'rishimiz mumkin.

Kvadrat chegirmaning ikkitadan ko'p yechimi bo'lmaganligi uchun bu yechimlar uning barcha yechimlarini beradi.

Yakobi simvoli. Endi Yakobi simvoli tushunchasini aniqlaymiz.

Yakobi simvoli Lejandr simvolining umumlashmasi hisoblanib, quyidagicha aniqlanadi.

3-ta'rif. Birdan katta P toq son uchun $P = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ bo'lsin, bu yerda $p_1, p_2, \ldots \cdot p_r$ tub sonlar bo'lib, ular orasida o'zaro tenglari bo'lishi ham mumkin.

Berilgan P soni bilan o'zaro tub a soni uchun quyidagi tenglik yordamida aniqlangan son *Yakobi* simvoli deyiladi:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right)$$

Lejandr simvolining yuqoridagi xossalaridan foydalanib, Yakobi simvolining xossalarini keltiramiz.

1-xossa.

a) agar $a \equiv a_1(modP)$ bo'lsa, u holda $\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right)$;

b) $\left(\frac{1}{P}\right) = 1$

c) $\left(\frac{-1}{P}\right) = (-1)^{\frac{p-1}{2}}$

d) $\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_k}{P}\right) = \left(\frac{a_1}{P}\right) \cdot \left(\frac{a_2}{P}\right) \cdot \ldots \cdot \left(\frac{a_k}{P}\right)$

e) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$

Isboti.

a) $\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_r}\right)=\left(\frac{a_1}{p_1}\right)\cdot\left(\frac{a_2}{p_2}\right)\cdot\ldots\cdot\left(\frac{a_r}{p_r}\right)=\left(\frac{a_1}{P}\right)$

b) $\left(\frac{1}{P}\right)=\left(\frac{1}{p_1}\right)\cdot\left(\frac{1}{p_2}\right)\cdot\ldots\cdot\left(\frac{1}{p_r}\right)=1$

c) quyidagi tenglikni qaraylik:

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\cdot\left(\frac{-1}{p_2}\right)\cdot\ldots\cdot\left(\frac{-1}{p_r}\right)=(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_r-1}{2}}$$

ammo,

$$\frac{P-1}{2}=\frac{p_1\cdot p_2\cdot\ldots\cdot p_r-1}{2}=$$

$$\frac{\left(1+2\cdot\frac{p_1-1}{2}\right)\cdot\left(1+2\cdot\frac{p_2-1}{2}\right)\cdot\ldots\cdot\left(1+2\cdot\frac{p_r-1}{2}\right)-1}{2}=\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_r-1}{2}+2N$$

ekanligidan $\left(\frac{-1}{P}\right)=(-1)^{\frac{p-1}{2}}$ kelib chiqadi.

d) Ushbu xossa quyidagi tengliklardan kelib chiqadi:

$$\left(\frac{a_1\cdot a_2\cdot\ldots\cdot a_k}{P}\right)=\left(\frac{a_1\cdot a_2\cdot\ldots\cdot a_k}{p_1}\right)\cdot\left(\frac{a_1\cdot a_2\cdot\ldots\cdot a_k}{p_2}\right)\cdot\ldots\cdot\left(\frac{a_1\cdot a_2\cdot\ldots\cdot a_k}{p_r}\right)=$$

$$\left(\frac{a_1}{p_1}\right)\cdot\left(\frac{a_2}{p_1}\right)\cdot\ldots\cdot\left(\frac{a_k}{p_1}\right)\cdot\left(\frac{a_1}{p_2}\right)\cdot\left(\frac{a_2}{p_2}\right)\cdot\ldots\cdot\left(\frac{a_k}{p_2}\right)\cdot\ldots\cdot\left(\frac{a_1}{p_r}\right)\cdot\left(\frac{a_2}{p_r}\right)\cdot\ldots\cdot\left(\frac{a_k}{p_r}\right)=$$

$$\left(\frac{a_1}{P}\right)\cdot\left(\frac{a_2}{P}\right)\cdot\ldots\cdot\left(\frac{a_k}{P}\right)$$

e) ma'lumki, $\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\left(\frac{2}{p_r}\right)=(-1)^{\frac{{p_1}^2-1}{8}+\frac{{p_2}^2-1}{8}+\ldots+\frac{{p_r}^2-1}{8}}$

quyidagi tenglikdan

$$\frac{P^2-1}{8}=\frac{{p_1}^2\cdot{p_2}^2\cdot\ldots\cdot{p_r}^2-1}{8}=$$

$$\frac{\left(1+8\cdot\frac{{p_1}^2-1}{8}\right)\cdot\left(1+8\cdot\frac{{p_2}^2-1}{8}\right)\cdot\ldots\cdot\left(1+8\cdot\frac{{p_r}^2-1}{8}\right)-1}{8}=$$

$$\frac{{p_1}^2-1}{8}+\frac{{p_2}^2-1}{8}+\ldots+\frac{{p_r}^2-1}{8}+2N,$$

xossasi kelib chiqadi.

3-xossa. O'zaro tub P va Q toq sonlar uchun quyidagi tenglik o'rinli:

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) \cdot (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

Isboti. Aytaylik, $P = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ va $Q = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ bo‘lsin.

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right) \cdot \left(\frac{Q}{p_2}\right) \cdot \ldots \cdot \left(\frac{Q}{p_r}\right) = \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{q_j}{p_i}\right) =$$

$$(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}} \cdot \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right) = (-1)^{\left(\sum_{i=1}^{r}\frac{p_i-1}{2}\right)\cdot\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)} \left(\frac{P}{Q}\right)$$

2-xossaning c) qismidagi kabi

$$\frac{P-1}{2} = \sum_{i=1}^{r}\frac{p_i-1}{2} + 2N_1, \frac{Q-1}{2} = \sum_{j=1}^{s}\frac{q_j-1}{2} + 2N_2,$$

Ekanligidan xossaning isboti kelib chiqadi.

3-misol. $\left(\frac{319}{403}\right)$ ni toping.

Yechish: 1-xossaga ko‘ra quyidagilar o‘rinli:

1. $\left(\frac{2^2}{319}\right) = 1$
2. $\left(\frac{3}{319}\right) = \left(\frac{319}{3}\right) \cdot (-1)^{\frac{3-1}{2}\cdot\frac{319-1}{2}} = -\left(\frac{319}{3}\right) = -\left(\frac{1}{3}\right) = -1$
3. $\left(\frac{7}{319}\right) = \left(\frac{319}{7}\right) \cdot (-1)^{\frac{319-1}{2}\cdot\frac{7-1}{2}} = -\left(\frac{319}{7}\right) = -\left(\frac{2^2}{7}\right) = -1$

Demak, bulardan quyidagini topamiz:

$$\left(\frac{319}{403}\right) = \left(\frac{403}{319}\right) \cdot (-1)^{\frac{319-1}{2}\cdot\frac{403-1}{2}} = -\left(\frac{403}{319}\right) = -\left(\frac{84}{319}\right) = -\left(\frac{2^2\cdot 3\cdot 7}{319}\right) = -\left(\frac{2^2}{319}\right)\left(\frac{3}{319}\right)\left(\frac{7}{319}\right) = -1 \cdot (-1) \cdot (-1) = -1.$$

Javob: -1.

XULOSA VA TAKLIFLAR

Lejandr va Yakobi simvollari sonlar nazariyasining muhim tushunchalari bo‘lib, ular kvadratik qoldiqlar va bir qator arifmetik xossalarni o‘rganishda muhim ahamiyat kasb etadi. Ushbu simvollar yordamida arifmetik masalalarni yechish ancha sodda va samarali bo‘lishi ta’minlanadi. Lejandr simvoli asosida Yakobi simvoli kiritilgani esa ushbu tushunchani kengaytirib, undan katta bo‘linuvchilar uchun foydalanish imkonini yaratdi. Bu esa, o‘z navbatida, algoritmik hisoblashlar uchun qulaylik yaratadi va zamonaviy kriptografiya tizimlarida keng qo‘llaniladi.Shuningdek, Lejandr va Yakobi simvollarini qo‘llash orqali sonlar nazariyasining boshqa yo‘nalishlarida, masalan, elliptik

egri chiziqlar nazariyasida yoki kriptografik algoritmlarni mustahkamlashda yangi imkoniyatlar ochilishi mumkin.

References

1. Polvanov, R. R. (2023). HOLDING PROBLEM FOR SECOND-ORDER GRONWALL BOUNDARY CONTROLS. RESEARCH AND EDUCATION, 2(12), 62-67.

2. Tolibjon o'g, S. G. A. (2022). CHAOS-EVAUSION PROBLEM IN CLOSED SIMPLE GRAPHS FOR MIXED BOUNDARY CONTROLS.

3.Jumayev M.E., “Practical on Mathematics Teaching Methods-Tashkent.: Teacher, 2004.

4. Qahramon o‘g, O. K. I., Hasanboy o‘g, J. R. A., & Hasanboy o‘g, X. J. R. (2024). METHODS FOR CALCULATING SOME LIMITS WITH THE HELP OF A DEFINITE INTEGRAL. JOURNAL OF THEORY, MATHEMATICS AND PHYSICS, 3(6), 23-27.

5.Umirzaqova, Kamola Oripjanovna. "PERIODIC GIBBS MEASURES FOR HARD-CORE MODEL." Scientific Bulletin of Namangan State University 2.3 (2020): 67-73.

6.A. Sadullayev, Kh. Mansurov and others, Collection of examples and problems from the course of mathematical analysis I, T., Uzbekistan 1993.