APPLICATIONS OF THE LEGENDARY SYMBOL

Gayniddinov Shaykhislom Tolibjon ugli

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

Annotation: In studying Legendre 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.

Аннотатция:В изучении символов Лежандра 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.

Annotatsiya: Lejandr simvollarida biz kvadratik qoldiqlar va ularning xossalari to‘grisida o‘rganamiz. Lejandr simvoli ikki tub son orasidagi kvadratik munosabatni aniqlashda ishlatamiz. Lejandr 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.

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.

Lejandr simvoli. p ga bo‘linmaydigan a son berilgan bo‘lsin.

2-ta’rif. p bo‘linmaydigan barcha a lar uchun quyidagicha aniqlangan songa *Lejandr* simvoli deyiladi:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, agar\ a\ \ kvadratik\ chegirma\ bo‘lsa \\ -1, aks\ holda. \end{cases}$$

ifodani quyidagicha yozish mumkin:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(modp) \qquad (2)$$

1-xossa. Lejandr simvoli uchun quyidagilar o‘rinli,

a) agar $a \equiv a_1(modp)$ bo‘lsa, u holda $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$;

b) $\left(\frac{a^2}{p}\right) = 1$

c) $\left(\frac{1}{p}\right) = 1$

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

e) $\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right)$

f) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

g) $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$

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

i) $\left(\frac{P}{q}\right) = \left(\frac{q}{P}\right) \cdot (-1)^{\frac{P-1}{2}\cdot\frac{q-1}{2}} \qquad (P,q) = 1$

1-misol. $x^2 \equiv 595(mod431)$

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

1) $\left(\frac{5}{431}\right) = \left(\frac{431}{5}\right) \cdot (-1)^{\frac{431-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{431}{5}\right) = \left(\frac{1}{5}\right) = 1$

2) $\left(\frac{7}{431}\right) = \left(\frac{431}{7}\right) \cdot (-1)^{\frac{431-1}{2}\cdot\frac{7-1}{2}} = -\left(\frac{431}{7}\right) = -\left(\frac{2^2}{7}\right) = -1$

3) $\left(\frac{17}{431}\right) = \left(\frac{431}{17}\right) \cdot (-1)^{\frac{431-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{431}{17}\right) = \left(\frac{2\cdot3}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = 1$

$\left(\frac{2}{17}\right) = 1, \qquad \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) \cdot (-1)^{\frac{17-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = 1$

Demak, bulardan quyidagini topamiz:

$\left(\frac{595}{431}\right) = \left(\frac{5\cdot7\cdot17}{431}\right) = \left(\frac{5}{431}\right) \cdot \left(\frac{7}{431}\right) \cdot \left(\frac{17}{431}\right) = 1 \cdot (-1) \cdot 1 = -1$

Javob: $x^2 \equiv 595(mod431)$ taqqoslma yechimga ega emas.

2-misol. $x^2 \equiv 219(mod383)$

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

1) $\left(\frac{41}{219}\right) = \left(\frac{219}{41}\right) \cdot (-1)^{\frac{219-1}{2}\cdot\frac{41-1}{2}} = \left(\frac{219}{41}\right) = \left(\frac{14}{41}\right) = \left(\frac{2\cdot7}{41}\right) = \left(\frac{2}{41}\right) \cdot \left(\frac{7}{41}\right) = -1$

$\left(\frac{2}{41}\right) = (-1)^{\frac{41^2-1}{8}} = 1,$

$$\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) \cdot (-1)^{\frac{7-1}{2}\cdot\frac{41-1}{2}} = \left(\frac{41}{7}\right) = \left(\frac{2\cdot3}{7}\right) = \left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right)$$

$$= (-1)^{\frac{7^2-1}{8}} \cdot \left(\frac{7}{3}\right) \cdot (-1)^{\frac{7-1}{2}\cdot\frac{41-1}{2}} = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

2) $\left(\frac{2^2}{219}\right) = 1$

$\left(\frac{219}{383}\right) = \left(\frac{383}{219}\right) \cdot (-1)^{\frac{383-1}{2}\cdot\frac{219-1}{2}} = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{41\cdot2^2}{219}\right) =$

$-\left(\frac{41}{219}\right) \cdot \left(\frac{2^2}{219}\right) = -(-1) \cdot 1 = 1$

Javob: $x^2 \equiv 219(mod383)$ taqqoslama 2 ta yechimga ega bo‘ladi.

CONCLUSIONS AND SUGGESTIONS

Legendary and Jacobi symbols are important concepts in number theory, which are of great importance in the study of quadratic residues and a number of arithmetic properties. Using these symbols, solving arithmetic problems is much simpler and more efficient. The introduction of the Jacobi symbol based on the Legendary symbol expanded this concept and made it possible to use it for large divisors. This, in turn, creates convenience for algorithmic calculations and is widely used in modern cryptographic systems. Also, the use of Legendary and Jacobi symbols can open up new opportunities in other areas of number theory, for example, in the theory of elliptic curves or in strengthening cryptographic algorithms.

References

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

2. Tolibjon o'g, S. G. A. (2022). THE CHAOS-EVAULATION PROBLEM IN CLOSED SIMPLE GRAPHS FOR THE CASE OF MIXED 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.