ETHIOPIAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 02, February-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

[1]*Jo'raxonov Asadillo Hasanboy ugli*

juraxonovasadillo@gmail.com

[2]*Husanov To'xtamurod Dilshod ugli*

husanovtoxtamurod850@gmail.com

[3]*G`ayniddinov Shayxislom Tolibjon ugli*

[1,2]*Namangan State Pedagogical Institute, student of the 2nd stage of Mathematics and Informatics*
[2]*Namangan State Pedagogical Institute, teacher of the Exact Sciences Department*

LEGEND AND JACOBIC SYMBOLS

Annotation: In studying Legendre and 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.

INTRODUCTION

In this topic, we will learn how to solve higher-degree congruences, specifically those in the form of $x^n \equiv a(\mathrm{mod} m)$, where $\gcd(a, m) = 1$.

Definition 1. If the congruence $x^n \equiv a(\mathrm{mod} m)$ has a solution, then a is called an n-th power residue. If there is no solution, a is not an n-th power residue.

Additionally, when $n = 2, n = 3$ and $n = 4$ these residues are called quadratic, cubic, and biquadratic, respectively.

Let us first consider the case where $n = 2$. For the quadratic congruence:

$$x^2 \equiv a(\mathrm{mod} p) \qquad (1)$$

where p is a prime number greater than 2, if a is a quadratic residue modulo p, then the congruence has at least one solution. If $x \equiv x_1(\mathrm{mod} p)$ is a solution, then $(-x_1)^2 = x_1^2$, so $x \equiv -x_1(\mathrm{mod} p)$ is also a solution. Since there can be no more than two solutions to a quadratic congruence, these two solutions are all the solutions to the congruence.

Legendre Symbol. Given a number a that is not divisible by p, we define the Legendre symbol for a as follows:

Definition 2. For all values of a that are not divisible by p, the Legendre symbol is defined by:

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

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 02, February-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

This can be written as:

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

Property 1. The following properties hold for the Legendre symbol:

if $a \equiv a_1 (\mathrm{mod} p)$, then $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$[1-9].

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

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

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

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

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

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

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

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

Example 1. Solve the congruence $x^2 \equiv 595 (\mathrm{mod} 431)$.

Solution: According to the properties:

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

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

Thus, we find:

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

Answer: The congruence $x^2 \equiv 595 (\mathrm{mod} 431)$ has no solution[10-14].

Example 2. $x^2 \equiv 219 (\mathrm{mod} 383)$

Solution: 1 - According to the properties, the following holds:

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

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

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 02, February-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

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

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

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

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

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

Answer: The equation $x^2\equiv 219(\mathrm{mod}383)$ has 2 solutions[15-18].

Jacobi Symbol: Now, we define the concept of the Jacobi symbol, which is a generalization of the Legendre symbol and is defined as follows:

3rd Definition: For a large odd prime $=p_1\cdot p_2\cdot\ldots\cdot p_r$, where $p_1,p_2,\ldots,p_r$ are prime numbers, the Jacobi symbol for a number a, which is coprime with P, is defined as:

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

Using the properties of the Legendre symbol, we derive the properties of the Jacobi symbol.

2-xossa.

a) if $a\equiv a_1(\mathrm{mod}P)$, then: $\left(\frac{a}{P}\right)=\left(\frac{a_1}{P}\right)$;

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

Proof:

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) Consider the following equality:

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

But:

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

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

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

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 02, February-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

d) This property follows from the following equalities:

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

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

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

e) It is known that: $\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\left(\frac{2}{p_r}\right)=(-1)^{\frac{{p_1}^2-1}{8}+\frac{{p_2}^2-1}{8}+\ldots+\frac{{p_r}^2-1}{8}}$

Using the following equality:

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

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

the property is obtained.

Property 3: For two odd coprime integers P and Q, the following equality holds:

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

Proof: Let $P=p_1\cdot p_2\cdot\ldots\cdot p_r$ and $Q=q_1\cdot q_2\cdot\ldots\cdot q_s$ Then:

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

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

As stated in Property 2(c),

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

This completes the proof of the property.

Example 3: Compute $\left(\frac{319}{403}\right)$.

Solution: Using Property 1, we have the following:

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

From these, we find:

$$\left(\frac{319}{403}\right)=\left(\frac{403}{319}\right)\cdot(-1)^{\frac{319-1}{2}\cdot\frac{403-1}{2}}=-\left(\frac{403}{319}\right)=-\left(\frac{84}{319}\right)=-\left(\frac{2^2\cdot3\cdot7}{319}\right)=-\left(\frac{2^2}{319}\right)\left(\frac{3}{319}\right)\left(\frac{7}{319}\right)=-1\cdot(-1)\cdot(-1)=-1.$$

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 02, February-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

Answer: -1.

CONCLUSION AND SUGGESTIONS

The Legendre and Jacobi symbols are essential concepts in number theory, playing a significant role in studying quadratic residues and various arithmetic properties. These symbols simplify and make solving arithmetic problems more efficient. The introduction of the Jacobi symbol as an extension of the Legendre symbol allows its application to larger divisors, enabling broader usage. This, in turn, facilitates algorithmic calculations and finds extensive application in modern cryptographic systems. Moreover, applying the Legendre and Jacobi symbols opens new possibilities in other areas of number theory, such as the theory of elliptic curves or strengthening cryptographic algorithms.

List of References:

1. G.Xudoyberganov, A. Vorisov va boshqalar. Matematik analizdan ma’ruzalar I, T., 2010.
2. A. G`oziyev, I. Isroilov, M. Yaxshiboyev, Matematik analizdan misol va masalalar I, Toshkent, 2012.
3. Jumayev M.E., “Matematika o’qitish metodikasidan praktikum-Toshkent.: O‘qituvchi, 2004.
4. Qahramon o‘g, O. K. I., Hasanboy o‘g, J. R. A., & Hasanboy o‘g, X. J. R. (2024). ANIQ INTEGRAL YORDAMIDA BA’ZI BIR LIMITLARNI HISOBLASH METODLARI. 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.
7. Polvanov, R. R. (2023). IKKINCHI TARTIBLI GRONUOLL CHEGARALANISHLI BOSHQARUVLAR UCHUN TUTISH MASALASI. RESEARCH AND EDUCATION, 2(12), 62-67.
8. Xolmuradov, F. M. (2024). DIFFERENTSIAL TENGLAMALAR FANINI OQITISHDA KONPETENSIYAVIY VA ADAPTIV YONDASHUVLARDAN FOYDALANISH METOKASI. Научный Фокус, 1(11), 172-178.
9. Tolibjon o'g, S. G. A. (2022). BOSHQARUVLAR ARALASH CHEGARALANISHLI BO'LGAN HOL UCHUN YOPIQ SODDA GRAFLARDA QUVISH-QOCHISH MASALASI.
10. Xo‘jamqulov, R. (2024). Matematika fanini o ‘rganishda Maple platformasidan foydalanish imkoniyatlari va amaliy jihatlari. Universal xalqaro ilmiy jurnal, 1(12), 335-338.
11. Холмурадов, Ф. М., Умрзаков, Ш. К., & Мамадалиев, У. Х. (2024). ЎҚУВЧИЛАРДА АБСТРАКТ ТАФАККУРНИ ШАКЛЛАНТИРИШ МЕТОДИКАСИНИ ТАКОМИЛЛАШТИРИШ. Научный Фокус, 1(11), 457-462.
12. Xolmuradov, F. M., Tillabayev, I. N., & Sobitov, R. A. (2024). Geografiya mutaxassisligi uchun Oliy matematika fanini oqitishda matematik modellarning tadbiqlari. PEDAGOG, 7(3), 99-105.
13. SHAIKHISLAM, G., & Solovev, T. M. (2024). Mining informational and analytical bulletin (scientific and technical journal).
14. Shaikhislam, T., Musakhanova, S. T., & Ch, K. B. (2015). The methods of the active concrete items production from industrial waste. Наука и техника Казахстана, (1-2), 124-130.

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 02, February-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

15. Xo‘jamqulov, R., & Ibrohimjonova, M. (2024). Taqqoslamalar va qoldiqli bo ‘lish bilan bo ‘g ‘liq muammolarni hal qilishda Xitoy Qoldiqlar Teoremasi. Universal xalqaro ilmiy jurnal, 1(12), 428-431.
16. Xo‘Jamqulov, R. (2024). Chiziqli algebra fani masalalarini C# va C++ dasturlash tillarida yechish. Universal xalqaro ilmiy jurnal, 1(12), 318-321.
17. Xo‘jamqulov, R., & Abdullayeva, S. (2024). Diofant tenglamalar. Chiziqli Diofant tenglamalarni Evklid algoritmi yordamida yechish metodlari. Universal xalqaro ilmiy jurnal, 1(12), 509-513.
18. Xolmuradov, F. M., & Sobitov, R. A. (2024). APPLICATIONS OF HIGHER MATHEMATICS IN THE FIELDS OF GEOGRAPHY. Galaxy International Interdisciplinary Research Journal, 12(3), 685-691.