EYLER VA FERMA TEOREMASI

Zaxiriddinova Shahlo Zaxiriddin qizi
Shahrisabz davlat pedagogika instituti
Matematika va ta'limda axborot
texnologiyasi kafedrasi o'qituvchisi
Axmedova Yulduz Baxodirovna
Shahrisabz davlat pedagogika
instituti „Matematika va informatika''
yo'nalishi 2-bosqich talabasi

Anotatsiya

Ushbu maqolada sonlar nazariyasining eng muhim teoremalari — Ferma kichik teoremasi va Eller teoremasining nazariy asoslari va amaliy ahamiyati keng yoritilgan. Har ikki teorema modulli arifmetikaning muhim qismini tashkil qiladi va tub sonlar bilan bog‘liq ko‘plab masalalarni soddalashtirishda muhim vosita bo‘lib xizmat qiladi. Maqolada avvalo har bir teoremaning mazmuni, matematik ifodalanishi va isboti tushuntirilgan. Keyin esa ularning o‘zaro bog‘liqligi, farqlari va umumlashtirilgan shakllari ko‘rib chiqilgan.

Shuningdek, maqolada Ferma va Eller teoremalari asosida modulli tenglamalar va sonlar ustida bajariladigan arifmetik amallarni soddalashtirish yo‘llari amaliy misollar bilan izohlangan. Ayniqsa, ushbu teoremalarning kriptografiya sohasida, xususan RSA algoritmida qanday qo‘llanilishi keng yoritilgan. Maqola ushbu matematik nazariy bilimlarning raqamli xavfsizlik, axborot texnologiyalari va zamonaviy algoritmik tizimlar uchun qanday ahamiyat kasb etishini ko‘rsatadi. Bu orqali talabalar, o‘qituvchilar va tadqiqotchilar sonlar nazariyasini chuqurroq o‘rganishlari hamda uni amaliyotda qo‘llash imkoniyatiga ega bo‘ladilar.

Annotation

This article presents a comprehensive exploration of two key theorems in number theory: Fermat's Little Theorem and Euler's Theorem. Both theorems are essential tools in modular arithmetic and play a significant role in simplifying complex operations involving prime numbers and integer relations. The article begins by explaining the core concepts, mathematical formulations, and proofs of each theorem. Their connections, differences, and generalizations are then discussed in detail.

Furthermore, the article examines practical applications of these theorems through illustrative problem-solving examples involving modular equations and arithmetic operations. Special attention is given to their role in the field of cryptography, particularly within the RSA encryption algorithm, which forms the

backbone of modern digital security. The paper highlights how these theoretical concepts extend far beyond pure mathematics and are actively used in real-world applications such as secure communication and data protection. The article serves as a valuable resource for students, educators, and researchers aiming to deepen their understanding of number theory and its practical utility.

Kalit so‘zlar: Ferma kichik teoremasi, Eller teoremasi, sonlar nazariyasi, modulli arifmetika, tub son, kriptografiya, RSA algoritmi, matematik isbot, modulli tenglama, raqamli xavfsizlik

Keywords: Fermat's Little Theorem, Euler’s Theorem, number theory, modular arithmetic, prime number, cryptography, RSA algorithm, mathematical proof, modular equation, digital security

Kirish

Matematikaning eng qadimiy va chuqur yo‘nalishlaridan biri bo‘lgan sonlar nazariyasi — butun sonlar xossalarini o‘rganishga yo‘naltirilgan bo‘lib, u zamonaviy matematik tarmoqlar, ayniqsa kriptografiya, raqamli xavfsizlik, va kompyuter fanlari asoslarini tashkil etadi. Sonlar nazariyasida muhim o‘rin egallagan teoremalardan ikkitasi — bu Ferma kichik teoremasi va Eller teoremasidir. Ular modulli arifmetikaning asosiy tamoyillarini belgilab beradi va tub sonlar bilan ishlashda matematik amallarni soddalashtirishda keng qo‘llaniladi.

Ferma kichik teoremasi XVII asrda Pyer Ferma tomonidan ilgari surilgan bo‘lib, u orqali har qanday tub son bilan ishlovchi modulli tenglamalarni samarali tarzda yechish mumkin. Bu teorema sonlar ustida bajariladigan murakkab arifmetik amallarni yengillashtiradi va matematik mantiqni chuqur tushunishga xizmat qiladi. Eller teoremasi esa Ferma teoremasining umumlashtirilgan shakli bo‘lib, u faqat tub sonlar emas, balki har qanday musbat butun sonlar bilan o‘zaro tub bo‘lgan sonlar orasidagi munosabatni modulli shaklda ifodalash imkonini beradi. Bu esa modulli arifmetikaning qo‘llanish doirasini yanada kengaytiradi.

Ushbu teoremalar zamonaviy texnologiyalar, ayniqsa axborot xavfsizligi sohasida muhim ahamiyat kasb etadi. Aynan ular asosida qurilgan RSA shifrlash algoritmi internetdagi ko‘plab maxfiy muloqot va ma’lumot almashuvni himoyalashda foydalaniladi. Shunday ekan, Ferma va Eller teoremalari nafaqat nazariy, balki amaliy jihatdan ham nihoyatda muhim hisoblanadi.

Ushbu maqolada aynan shu teoremalar chuqur tahlil qilinadi, ularning matematik mazmuni, formulalari, isbotlari va amaliy misollardagi qo‘llanilish usullari ko‘rib chiqiladi. Shuningdek, ular yordamida qanday qilib modulli tenglamalar yechilishi va katta sonlar ustida tez hisob-kitoblar olib borilishi mumkinligi izohlanadi. Bu nafaqat matematikani chuqurroq anglashga yordam beradi, balki ularni real hayotda, texnologiyada qo‘llash imkoniyatini ham ochib beradi.

Introduction

Number theory, one of the oldest and most profound branches of mathematics, is primarily focused on the properties and relationships of integers. It forms the theoretical foundation for various modern mathematical disciplines, particularly cryptography, digital security, and computer science. Among the many theorems that play a crucial role in number theory, two stand out for their fundamental significance — Fermat's Little Theorem and Euler's Theorem. These theorems establish key principles of modular arithmetic and are widely used to simplify operations involving prime numbers.

Fermat's Little Theorem, proposed in the 17th century by Pierre de Fermat, provides an efficient way to solve modular equations involving prime numbers. It allows complex arithmetic operations to be reduced in modular systems and enhances understanding of mathematical logic. Euler's Theorem, considered a generalization of Fermat's, extends these principles to any pair of relatively prime positive integers, making it applicable in a broader range of problems within modular arithmetic.

Both theorems have immense importance not only in theoretical mathematics but also in practical applications, especially in information security. They form the mathematical basis for the RSA encryption algorithm, which is one of the most widely used systems to ensure secure communication over the internet. As such, understanding these theorems is crucial for both mathematicians and computer scientists alike.

This article aims to explore these two theorems in depth, examining their mathematical structure, proofs, and practical use through real examples. It also highlights how they enable efficient computation with large numbers and the solution of modular equations — serving not only to deepen one's mathematical insight but also to connect theory with real-world technological applications.

Asosiy qism

Ferma kichik teoremasi va Eller teoremasi sonlar nazariyasining eng muhim teoremalari qatoriga kiradi. Ular modulli arifmetika, tub sonlar va algoritmlarda keng qo‘llaniladi. Quyida har bir teorema alohida ko‘rib chiqilib, ularning o‘ziga xosliklari, formulalari, isbotlari va amaliy qo‘llanilishi haqida batafsil ma’lumot beriladi.

Ferma kichik teoremasi

Ferma va Eller teoremalari o‘rtasidagi bog‘liqlik

Ferma teoremasi — maxsus holat, ya’ni tub son bo‘lganidagi holat, Eller teoremasi esa umumiyroq, ya’ni har qanday musbat butun son bo‘lishi mumkin. Har ikki teorema modulli arifmetika asosida ishlaydi va bir-birini to‘ldiradi.

Amaliy qo‘llanishi

Ferma va Eller teoremalari zamonaviy kriptografik algoritmlar asosida qo‘llaniladi. Ayniqsa, RSA algoritmida ochiq kalitni yaratish va yopiq kalitni topish uchun aynan ushbu teoremalardan foydalaniladi.

RSA algoritmida:
Ikki katta tub son va tanlanadi.
, va hisoblanadi.
Shunda maxfiy kalitni topishda dan foydalaniladi.
Shuningdek, bu teoremalar modulli darajali hisoblash, raqamli imzolar, ma’lumotlarni shifrlash va raqamli xavfsizlikni ta’minlashda keng qo‘llaniladi
Yechiladigan masalalar turlari
Ferma va Eller teoremalari asosida quyidagi turdagi masalalar yechiladi:
1. Modulli darajalar hisoblash:
2. O‘zaro tub sonlar aniqlash
3. Raqamli shifrlash va deshifrlash masalalari
4. Modular tenglamalar yechimi
5. Kriptografik kalitlarni aniqlash

Main part
Farm small theorem and Eller's theorem are numbers
among the most important theorems of his theory.
They are wide in modular arithmetic, prime numbers and algorithms
applied. Below, each theorem is considered separately,
their identities, formulas, proofs and practical
details of the application will be given.
Farm small theorem
Relation between farm and Eller theorems
The farm theorem is a special case, i.e. one that is prime
the case, while Eller's theorem is more general, i.e. any
can be a positive integer. Both theorems are modular
it works on the basis of arithmetic and complements each other.
Practical application
Farm and Eller theorems-modern cryptographic algorithms
applied on the basis. Especially open in the RSA algorithm
this is exactly what you need to create a key and find a closed key
theorems are used.
In the RSA algorithm:
Two large prime numbers and are selected.
, and is.
Then when finding the secret key, dan is used.
Also, these theorems are modular level computing, numerical
signatures, data encryption and digital security
widely used in supply

Types of issues to be solved

Based on the farm and Eller theorems, the following types of issues are undo:

1. Modular levels calculation:
2. Determination of mutual prime numbers
3. Digital encryption and decryption issues
4. Modular equation solutions
5. Cryptographic key recognition

Foydalanilgan adabiyotlar

1. Turaev D. T. – Diskret matematika va matematik mantiq. Toshkent: “Fan va texnologiya”, 2015.
2. Rasulov A. A. – Sonlar nazariyasiga kirish. Toshkent: O‘zbekiston Milliy Universiteti, 2007.
3. Kadyrov B. va boshqalar – Kriptografiya asoslari. Toshkent: Iqtisodiyot, 2018.
4. https://en.wikipedia.org/wiki/Fermat%27s_little_theorem
5. https://en.wikipedia.org/wiki/Euler%27s_theorem_(mathematics)
6. Rosen K. H. – Discrete Mathematics and Its Applications, 7th Edition, McGraw-Hill, 2012.

References

1. Turaev D. T. – Discrete Mathematics and Mathematical Logic. Tashkent: “Fan va texnologiya”, 2015.
2. Rasulov A. A. – Introduction to Number Theory. Tashkent: National University of Uzbekistan, 2007.
3. Kadyrov B. et al. – Foundations of Cryptography. Tashkent: Iqtisodiyot, 2018.
4. https://en.wikipedia.org/wiki/Fermat%27s_little_theorem
5. https://en.wikipedia.org/wiki/Euler%27s_theorem_(mathematics)
6. Rosen K. H. – Discrete Mathematics and Its Applications, 7th Edition, McGraw-Hill, 2012.