Publisher:
Fast support and result LLC

STDF

Science technology & Digital Finance

VOLUME|3 ISSUE|5
NOVEMBER|2025

ISSN:2992-9199

VOLUME | 3 ISSUE | 5 NOVEMBER | 2025

ТОМ | 3 ВЫПУСК | 5 НОЯБРЬ | 2025

JILD | 3 SON | 5 NOYABR | 2025

Davriy nashrning rasmiy nomi: "Science technology & Digital finance" O`zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 17.08.2023 sanada berilgan №116083 guvohnomasi bilan ro`yxatdan o`tgan.

Jurnal asoschilari: "Fast support and result" nashriyoti.

Xalqaro indeksi: ISSN 2992-9199.

Science technology & Digital finance
journal homepage: https://bestjournalup.com/index.php/stdf

CHEGIRMALAR SINFLARI. EYLER VA FERMA TEOREMALARI

Ibrohimov Javohir Bahrom o'g'li
O'zbekiston Milliy universiteti Jizzax filiali assistenti.
Ergashova Dilshoda, Aliasqarova Nodirabegim, Mavlonova Sevara
O'zbekiston Milliy universiteti Jizzax filiali Amaliy matematika talabalari.

Annotatsiya

Ushbu maqolada modulli arifmetika tushunchalarining asosiy tamoyillari bayon etilgan. Xususan, m modul bo'yicha chegirmalar sinflari, ularning to'la va keltirilgan sistemalari, Eyler va Ferma teoremalari, shuningdek modulli ko'paytirish va qo'shish amallarining algebraik xususiyatlari yoritiladi. Chegirmalarning uchta turi — eng kichik manfiy bo'lmagan, eng kichik manfiy va absolyut qiymati eng kichik sistemalari misollar orqali tushuntiriladi. Keltirilgan sistemaning Eyler funksiyasi bilan bog'liqligi va multiplikativ gruppa hosil qilishi ko'rsatiladi. Maqolada, shuningdek, taqqoslamalarni yechish bo'yicha turli misollar, murakkab sonlar uchun psevdotub sonlar xossalari va Eyler teoremasining qo'llanishi namoyish etilgan. Berilgan misollar yordamida modulli arifmetikaning amaliy qo'llanishlari oson tushunarli tarzda ochib berilgan.

Annotation

This article outlines the basic principles of modular arithmetic concepts. In particular, the classes of deductions on module m, their full and quoted systems, Euler and farm theorems, as well as the algebraic properties of modular multiplication and addition actions are illuminated. Three types of deductions — the smallest non-negative, the smallest negative, and the smallest systems of absolute value-are explained by examples.his article outlines the basic principles of modular arithmetic concepts. In particular, the classes of deductions on module m, their full and quoted systems, Euler and farm theorems, as well as the algebraic properties of modular multiplication and addition actions are illuminated. Three types of deductions — the smallest non-negative, the smallest negative, and the smallest systems of absolute value-are explained by examples. The connection of the given system with the Euler function and the formation of a multiplicative group are shown. The paper also demonstrated various examples of solving comparisons, the pseudotube number property for complex numbers, and the application of Euler's theorem. With the help of the given examples, the practical applications of modular arithmetic are revealed in an easy-to-understand way.

Аннотация

В этой статье излагаются основные принципы понятий модульной арифметики. В частности, будут рассмотрены классы вычетов по модулю M, их полные и приведенные системы, теоремы Эйлера и ферма, а также алгебраические свойства операций умножения и сложения по модулю. Три типа дисконтирования — наименьшая неотрицательная, наименьшая отрицательная и наименьшая системы абсолютного значения-объясняются на примерах. этой статье излагаются основные принципы понятий модульной арифметики. В частности, будут рассмотрены классы вычетов по модулю M, их полные и приведенные системы, теоремы Эйлера и ферма, а также алгебраические свойства операций умножения и сложения по модулю. Три типа дисконтирования — наименьшая неотрицательная, наименьшая отрицательная и наименьшая системы абсолютного значения-объясняются на примерах.

Показано, что представленная система связана с функцией Эйлера и образует мультипликативную группу. В статье также представлены различные примеры решения сравнений, свойства псевдотрубных чисел для комплексных чисел и применение теоремы Эйлера. На приведенных примерах легко для понимания раскрыты практические применения модульной арифметики.

Kalit so'zlar:
Modulli arifmetika, chegirmalar sinfi, to'la sistema, keltirilgan sistema Eyler funksiyasi, Eyler teoremasi, Ferma teoremasi, multiplikativ gruppa.

Key words:
Modular arithmetic, residue class, complete system, reduced system Euler function, Euler's theorem, Fermat's theorem, multiplicative group.

Ключевые слова:
Модульная арифметика, класс вычетов, полная система, система, представленная функция Эйлера, теорема Эйлера, теорема Ферма, мультипликативная группа.

Email: javohir1003@gmail.com

m natural songa bo'linganida bir xil r qoldiq qoladigan barcha butun sonlar to'plami m modul bo'yicha sonlar sinfini tashkil qiladi. Bu sinfning har bir soni umumiy holda $mk+r$, $k\in \mathbf{Z}$ ko'rinishda yoziladi. Barcha sinflar soni m ga teng.

Sinfning ixtiyoriy soni m modul bo'yicha *chegirma* deyiladi (shu sinfning boshqa sonlariga nisbatan).

Har bir sinfdan ixtiyoriy ravishda bittadan olingan sonlar to'plami berilgan m modul bo'yicha *chegirmalarning to'la sinfi* deyiladi.

Odatda chegirmalarning to'la sinfi sifatida berilgan m bo'yicha eng kichik manfiy bo'lmagan chegirmalar, ya'ni 0, 1, 2,..., m - 1 sistema olinadi.

Ba'zan berilgan m modul bo'yicha chegirmalardan absolyut qiymati bo'yicha eng kichik musbat bo'lmagan chegirmalarning to'la sistemasi ham qaraladi: -(m-1), -(m-2),..., -2, -1, 0. m modul bo'yicha absolyut qiymati jihatidan eng kichik chegirmalarning to'la sinfi ham ishlatiladi. Masalan, $m = 7$ bo'lganda bu sistema -3, -2, -1, 0, 1, 2, 3 chegirmalardan iborat bo'ladi; $m = 8$ bo'lganda esa -3, -2, -1, 0, 1, 2, 3, 4 yoki –4, -3, -2, -1, 0, 1, 2, 3 chegirmalardan tashkil topadi.

Chegirmalarning to'la sistemasidan olingan va m modul bilan o'zaro tub bo'lgan chegirmalar m modul bo'yicha chegirmalarning keltirilgan sistemasi deyiladi. Kelitirilgan sistemada chegirmalar soni $\varphi(m)$- Eyler funksiyasining qiymatiga teng.

Chegirmalarning to'la sistemasidagi kabi keltirilgan sistemaning ham uch turi ishlatiladi: *eng kichik musbat chegirmalarning keltirilgan sistemasi, absolyut qiymati bo'yicha eng kichik manfiy chegirmalarning keltirilgan sistemasi va absolyut qiymati bo'yicha eng kichik chegirmalarning keltirilgan sistemasi.*

$x_1, x_2,..., x_s$ butun sonlar sistemasi $s = m$ va $i \neq j$ da $x_i \equiv x_j\ (mod\ m)$ bo'lganda va faqat shu holda m modul bo'yicha chegirmalarning to'la sistemasidan iborat bo'ladi. $(a, m) = 1$ bo'lganda $ax + b$ chiziqli formaning qiymatlari m modul bo'yicha chegirmalarning to'la sistemasidan iborat bo'lishi uchun x qabul qiladigan qiymatlar ham chegirmalarning to'la sistemasidan iborat bo'lishi zarur va yetarlidir.

$x_1, x_2,..., x_s$ butun sonlar sistemasi $s = \varphi(m)$ va $i \neq j$, $(x_i, m) = 1$ da $x_i \equiv x_j\ (mod\ m)$ bo'lganda va faqat shu holda m modul bo'yicha chegirmalarning keltirilgan sistemasidan iborat bo'ladi. $(a, m) = 1$ bo'lganda ax chiziqli formaning qiymatlari m modul bo'yicha chegirmalarning keltirilgan sistemasidan iborat bo'lishi uchun x qabul qiladigan qiymatlar ham chegirmalarning keltirilgan sistemasidan iborat bo'lishi zarur va yetarlidir.

$m > 1$ va $(a, m) = 1$ bo'lganda quyidagi taqqoslama o'rinli:

$$a^{\varphi(m)} \equiv 1\ (mod\ m),$$

bu yerda $\varphi(m)$ –Eyler funksiyasi (*Eyler teoremasi*).

p tub son va $(a, p) = 1$ bo'lganda quyidagi taqqoslama o'rinli:

$$a^{p-1} \equiv 1\ (mod\ p)$$ (*Ferma teoremasi*).

a butun sonni o'zida saqlaydigan m bo'yicha chegirmalar sinfini $a\ mod\ m$ bilan belgilaymiz. Demak,

$$a\ mod\ m = a + m\boldsymbol{Z} = \{a + km \mid k \in \boldsymbol{Z}\}.$$

$\boldsymbol{Z}/m\boldsymbol{Z}$ bilan m modul bo'yicha barcha chegirmalar sinflari to'plamini belgilaymiz:

$$\boldsymbol{Z}/m\boldsymbol{Z} = \{0\ mod\ m, 1\ mod\ m,..., (m-1)\ mod\ m\}.$$

Bu to'plamda qo'shish va ko'paytirish amallarini quyidagi tengliklar orqali kiritiladi:

$$a\ mod\ m + b\ mod\ m = (a + b)\ mod\ m,$$
$$(a\ mod\ m) \cdot (b\ mod\ m) = ab\ mod\ m.$$

$(\boldsymbol{Z}/m\boldsymbol{Z}, +)$ – abel gruppasidan, hamda $\boldsymbol{Z}$ gruppaning $m\boldsymbol{Z}$ qism gruppa bo'yicha faktor gruppasidan iborat bo'lib, *m modul bo'yicha chegirmalar sinfining additiv gruppasi deyiladi.*

$(Z/mZ, +, \cdot)$ – birlik elementli kommutativ xalqadan iborat bo'lib, *m modul bo'yicha chegirmalar sinfinig xalqasi deyiladi.*

Agar (a, m) = 1 bo'lsa, a mod m sinf m modul bilan o'zaro tub bo'lgan chegirmalar sinfi deyiladi.

m modul bilan o'zaro tub bo'lgan chegirmalar sinflari to'plami ko'paytirishga *nisbatan* abel gruppasi tashkil etadi va u *m modul bilan o'zaro tub bo'lgan chegirmalar sinflarining multiplikativ gruppasi deyiladi.*

Agar $ab \equiv 1\ (mod\ m)$ bo'lsa, a chegirma b chegirmaga m modul bo'yicha teskari deyiladi.

1-Misol. 10 modul bo'yicha chegirmalar to'la sistemasining uchta turini yozing.

Yechilishi. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 – 10 modul bo'yicha eng kichik manfiy bo'lmagan chegirmalarning to'la sistemasi.

-9, -8, -7, -6, -5, -4, -3, -2, -1, 0 – 10 modul bo'yicha absolyut qiymati jihatidan eng kichik manfiy chegirmalarning to'la sistemasi.

-4, -3, -2, -1, 0, 1, 2, 3, 4, 5 yoki –5, -4, -3, -2, -1, 0, 1, 2, 3, 4 – 10 modul bo'yicha absolyut qiymati jihatidan eng kichik chegirmalarning to'la sistemasi.

2-Misol. 10 modul bo'yicha chegirmalarning keltirilgan sistemasining uchta turini yozing.

Yechilishi. 1, 3, 7, 9 – 10 modul bo'yicha eng kichik manfiy bo'lmagan chegirmalarning keltirilgan sistemasi.

-9, -7, -3, -1 – 10 modul bo'yicha absolyut qiymati jihatidan eng kichik manfiy chegirmalarning keltirilgan sistemasi.

-3, -1, 1, 3 chegirmalar 10 modul bo'yicha absolyut qiymati jihatidan eng kichik chegirmalarning keltirilgan sistemasi.

3-Misol. 20, -4, 22, 18, -1 sonlar qanday modul bo'yicha chegirmalarning to'la sistemasini tashkil etadi?

Yechilishi. 5 modul bo'yicha berilgan sonlar mos ravishda 0, 1, 2, 3, 4 sonlar bilan taqqoslanadi, shuning uchun izlanayotgan modul 5 ga teng.

4-Misol. $3^1, 3^2, 3^3, 3^4, 3^5, 3^6$ sonlar sistemasi 7 modul bo'yicha chegirmalarning keltirilgan sistemasini tashkil eitishini ko'rsating.

Yechilishi. Berilgan sonlardan eng kichik musbat chegirmalarni tuzamiz:

3, 2, 6, 4, 5, 1, chunki $3^2 \equiv 2$ (mod 7), $3^3 \equiv 6$ (mod 7), $3^4 \equiv 4$ (mod7), $3^5 \equiv 5$ (mod 7), $3^6 \equiv 1$ (mod 7).

5-Misol. 383^{175} ni 45 ga bo'lganda hosil bo'ladigan qoldiqni toping.

Yechilishi. $383 \equiv 23$ (mod 45) bo'lganligi uchun $383^{175} \equiv 23^{175}$ (mod 45). Endi $\varphi(45) = 24$ va (23, 45) = 1 dan Eyler teoremasiga ko'ra:

$23^{24} \equiv 1$ (mod 45) ni hosil qilamiz. Demak,

$23^{175} = 23^{24\bullet 7+7} = (23^{24})^7 \cdot 23^7 \equiv 1^7 \cdot 23^7$ (mod 45).

Shu taxlitda davom etib, $23^7 = (23^2)^3 \cdot 23 \equiv 34^3 \cdot 23 = 34^2 \cdot 34 \cdot 23 \equiv 1156 \cdot 782 \equiv 31 \cdot 17 = 527 \equiv 32$ (mod 45) ni hosil qilamiz.

Shunday qilib, $383^{175} \equiv 32$ (mod 45). Izlanayotgan qoldiq 32 dan iborat.

6-Misol. x ning har qanday butun qiymatida $x^7 \equiv x$ (mod 42) taqqoslamani to'g'riligini ko'rsating.

Yechilishi. Ferma teoremasiga ko'ra, $x^7 \equiv x$ (mod 7). Endi $x^7 \equiv x$ (mod 2 va 3) ekanligini isbot qilamiz, buning uchun 2 va 3 modullar bo'yicha chegirmalarning to'la sistemasini, y'ani 0, 1, 2 sonlarni sinash yetarli.

7-Misol. Butun sonning 100-darajasini 125 ga bo'lganda hosil bo'ladigan qoldiqni toping.

Yechilishi. Agar (a, 5) = 1 bo'lsa, u holda Eyler teoremasiga ko'ra:

$a^{\varphi(125)} = a^{100} \equiv 1$ (mod 125).

Agarda (a, 5) = 5 bo'lsa, u holda $a^{100} \equiv 0$ (mod 125).

Demak, agar (a, 5) = 1 bo'lsa, u holda izlanayotgan qoldiq 1 ga teng. Agarda (a, 5) = 5 bo'lsa, u holda a^{125} soni 125 ga bo'linadi.

8-Misol. $2^{\varphi(m)-1}$ ni toq m soniga bo'linganida hosil bo'ladigan qoldiqni toping.

Yechilishi. $2^{\varphi(m)-1} \equiv r \; (mod\; m)$, $0 \le r < m$ bo'lsin. U holda $2^{\varphi(m)} \equiv 2r \equiv 1 \; (mod\; m)$ yoki $r = \frac{1+mq}{2}$, bu yerda $q \in \mathbf{Z}$. $0 \le r < m$ shartni $q = 1$ da yagona $\frac{1+mq}{2}$ qiymat qanoatlantiradi, bu yerdan r = $\frac{1+m}{2}$ ni hosil qilamiz.

9-Misol. 341 soni uchun $2^{341} \equiv 2$ (mod 341) taqqoslamaning o'rinli ekanligini ko'rsating.

Yechilishi. 341 – murakkab son, 341 = 11· 31. $2^5 \equiv 1$ (mod 31) va $2^{10} \equiv 1$ (mod 31) taqqoslamalar o'rinli ekanligini osongina tekshirish mumkin.

Ferma teoremasiga asosan $2^{10} \equiv 1$ (mod 11). 11 va 13 sonlar o'zaro tub bo'lganligi uchun bu yerdan $2^{10} \equiv 1$ (mod 11·31) kelib chiqadi, ya'ni $2^{10} \equiv 1$ (mod 341). Demak, $2^{340} \equiv 1$ (mod 341) va $2^{341} \equiv 2$ (mod 341) taqqoslamalar o'rinli.

Foydalanilgan adabiyotlar ro'yxati:

1. Кострикин А.И. Введение в алгебру. М., 1977, 495 стр.
2. Курош А.Г. Олий алгебра курси. Тошкент, 1972.
3. Фаддеев Д.К. Лекции по алгебре. М., Наука, 1984, 415 ст.

4. Гельфанд И.М. Чизикли алгебрадан лекциялар. Тошкент, 1966.
5. Боревич Э.И. Определители и матрицы. – М., Наука, 1975, 253 ст.
6. Фаддеев Д.К., Фаддеева В.Н. Вычислительные методы линейной алгебры. М., Наука, 1964, 388 с.
7. Baxtiyor P. et al. BA'ZI BIR MUHIM XOSMAS INTEGRALLARNI HISOBLASHDA FRULLANI FORMULASIDAN FOYDALANISH //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 363-367.
8. Po'latov B., Ibrohimov J. BA'ZI RATSIONAL FUNKSIYALARNI INTEGRALLASHDA OSTRAGRADSKIY USULIDAN FOYDALANISH //Talqin va tadqiqotlar. – 2023. – Т. 1. – С. 21.
9. Bahrom o'g'li I. J. OCHIQ CHIZIQLI QAVARIQ TO 'PLAMDA POLINOMIAL QAVARIQLIKNING YETARLI SHARTI //International Journal of Contemporary Scientific and Technical Research. – 2022. – Т. 1. – №. 2. – С. 363-5.
10. Xurramov Y., Polatov B., Ibrohimov J. Kophadning keltirilmaslik alomati //Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar. – 2022. – Т. 1. – №. 1. – С. 399-401.
11. Xurramov Y., Polatov B., Ibrohimov J. Kophadning keltirilmaslik alomati //Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar. – 2022. – Т. 1. – №. 1. – С. 399-401.
12. Пулатов Б. и др. Darajali geometriyaning oddiy differensial tenglamalarda qo 'llanilishi //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 2. – С. 266-269.
13. Полатов Б., Хуррамов Ё., Иброхимов Д. Matematika darslarida muammoli oqitish texnologiyasidan foydalanish //Современные инновационные исследования актуальные проблемы и развитие тенденции: решения и перспективы. – 2022. – Т. 1. – №. 1. – С. 401-404.
14. Javohir I. et al. XEVISAYD USULI YORDAMIDA RATSIONAL FUNKSIYALARNI INTEGRALLASH //International Journal of Contemporary Scientific and Technical Research. – 2023. – Т. 416. – С. 418.
15. Polatov B., Xurramov Y., Ibrohimov J. Murakkab funksiyalardan olingan aniq integralni taqribiy hisoblash //Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar. – 2022. – Т. 1. – №. 1.
16. Javohir I. B.. o 'g 'li, & Muxammadiyev, GJ. o 'g 'li.(2023). AYRIM IRRATSIONAL KO 'RINISHDAGI INTEGRALLARNI EYLER ALMASHTIRISHLARI YORDAMIDA RATSIONALLASHTIRISH //Educational Research in Universal Sciences. – Т. 2. – №. 2. – С. 237-241.
17. Бозоров А. Р. и др. ИНТЕГРИРОВАНИЕ РАЦИОНАЛЬНЫХ ФУНКЦИЙ ПО СХЕМЕ ГОРНЕРА //ДОСТИЖЕНИЯ ВУЗОВСКОЙ НАУКИ. – 2023. – Т. 2023. – С. 13-16.
18. Sobirovich P. B. Darajali Geometriyani Algebraik Tenglamalarda Qo 'Llab Asimptotik Yechimlarini Topish. – 2022.
19. Nuraliyev T. et al. MATRISANING XOS SON VA XOS VEKTORLARNI TOPISH //Science technology&Digital finance. – 2024. – Т. 2. – №. 4. – С. 62-71.