

BUTUN SONLI TENGLAMALAR NAZARIYASI VA DIOFANT TENGLAMALARINING AHAMIYATI

Raxmanova Nazokat Abdurazzokovna

Osiyo xalqaro Universiteti

Urganch filiali, matematika yo'nalishi

1-kurs magistratura talabasi

Annotatsiya. Ushbu tezisdagi butun sonli yechimlar nazariyasi va Diofant tenglamalarining asosiy mazmuni hamda ularning matematik va amaliy ahamiyati yoritilgan. Diofant tenglamalari butun sonlarda yechim izlashga qaratilgan tenglamalar bo'lib, sonlar nazariyasining muhim yo'nalishlaridan biri hisoblanadi. Tadqiqotda chiziqli va kvadrat Diofant tenglamalarining asosiy xossalari, ularni yechish usullari hamda Evklid algoritmi va modul arifmetikasining qo'llanilishi tahlil qilindi. Shuningdek, ushbu tenglamalarning kriptografiya va axborot xavfsizligidagi amaliy ahamiyati, xususan RSA tizimi bilan bog'liqligi ko'rib chiqildi. Natijalar Diofant tenglamalarining nafaqat nazariy matematika, balki zamonaviy texnologiyalar rivojida ham muhim o'rin tutishini ko'rsatadi.

Kalit so'zlar: Diofant tenglamalari, butun sonli yechimlar, sonlar nazariyasi, Evklid algoritmi, modul arifmetikasi, kriptografiya, RSA algoritmi, algebra, matematik modellash, axborot xavfsizligi.

Abstract

This thesis discusses the main concepts of the theory of integer solutions and Diophantine equations, as well as their mathematical and practical significance. Diophantine equations are equations focused on finding integer solutions and represent one of the key branches of number theory. The study analyzes the fundamental properties of linear and quadratic Diophantine equations, methods for solving them, and the application of the Euclidean algorithm and modular arithmetic. In addition, the practical importance of these equations in cryptography and information security, particularly their connection

with the RSA system, is examined. The results demonstrate that Diophantine equations play an important role not only in theoretical mathematics but also in the development of modern technologies.

Keywords: Diophantine equations, integer solutions, number theory, Euclidean algorithm, modular arithmetic, cryptography, RSA algorithm, algebra, mathematical modeling, information security.

Kirish

Matematika fanining rivojlanishida sonlar nazariyasi alohida o‘rin egallaydi. Uning muhim bo‘limlaridan biri bo‘lgan Diofant tenglamalari butun sonlarda yechim topish masalalarini o‘rganadi. Ushbu yo‘nalish qadimgi yunon matematigi Diofant nomi bilan bog‘liq bo‘lib, u butun sonli yechimlarni izlashga asoslangan birinchi tizimli yondashuvlardan biri hisoblanadi.

Zamonaviy davrda Diofant tenglamalari nafaqat nazariy matematika, balki axborot texnologiyalari, kriptografiya va kompyuter fanlarida ham keng qo‘llanilmoqda. Ayniqsa, axborot xavfsizligini ta‘minlashda ularning o‘rni katta ahamiyat kasb etadi. Shu sababli ushbu mavzuni o‘rganish dolzarb hisoblanadi.

Asosiy qism

Diofant tenglamalari odatda butun sonlarda yechimga ega bo‘lgan algebraik tenglamalar sifatida qaraladi. Ularning eng sodda ko‘rinishi chiziqli Diofant tenglamalar bo‘lib, ular $ax + by = c$ shaklida ifodalanadi. Bunday tenglamalarning yechim mavjudligi va topilish shartlari eng katta umumiy bo‘luvchi (EKUB) orqali aniqlanadi.

Kvadrat va yuqori darajali Diofant tenglamalari esa ancha murakkab bo‘lib, ularni yechishda turli matematik usullar qo‘llaniladi. Jumladan, parametrik yechimlar, modul arifmetikasi va ba’zi hollarda sonli tahlil usullari ishlatiladi. Evklid algoritmi esa EKUBni tez topish orqali yechimlarni aniqlashda asosiy vosita bo‘lib xizmat qiladi.

Amaliy jihatdan Diofant tenglamalari kriptografiyada muhim o‘rin tutadi. Masalan, RSA shifrlash tizimi katta tub sonlar va modul hisoblashlarga asoslangan bo‘lib, uning matematik poydevorida sonlar nazariyasi va butun sonli yechimlar g‘oyalari yotadi. Bu esa ma’lumotlarni himoyalash va xavfsiz uzatishda muhim ahamiyatga ega.

Diofant tenglamalarini chuqur o‘rganishda muhim yo‘nalishlardan biri bu tenglamalarning yechimlar fazosini tahlil qilishdir. Ba’zi hollarda yechimlar ma’lum bir qonuniyat asosida tartiblanadi va ular geometrik ko‘rinishda nuqtalar to‘plami sifatida tasvirlanishi mumkin. Bu yondashuv algebraik geometriyaning boshlang‘ich tushunchalari bilan bog‘liq hisoblanadi.

Zamonaviy tadqiqotlarda Diofant masalalarini yechish uchun raqamli (numerik) usullar ham keng qo‘llanilmoqda. Bu usullar yordamida aniq yechim topish qiyin bo‘lgan hollarda yaqinlashgan yechimlar hisoblanadi. Ayniqsa katta sonlar ishtirok etgan tenglamalarda bu yondashuv samarali hisoblanadi.

Diofant tenglamalarining yana bir qiziqarli yo‘nalishi — eksponentsial Diofant tenglamalaridir. Bunday tenglamalarda noma’lumlar daraja ko‘rinishida qatnashadi (masalan, $a^x + b^y = c^z$). Bu turdagi masalalar juda murakkab bo‘lib, ularning ko‘pi faqat maxsus hollarda yechiladi yoki umuman yechimga ega emasligi isbotlanadi.

Tarixiy jihatdan qaralganda, Diofant tenglamalarining rivojlanishi Fermatning oxirgi teoremasi kabi mashhur muammolar bilan chambarchas bog‘liq. Bu muammo yuz yillar davomida yechilmagan va faqat zamonaviy matematika usullari yordamida isbotlangan. Bu esa Diofant tipidagi masalalarning qanchalik chuqur va murakkab ekanligini ko‘rsatadi. Diofant tenglamalari kodlash va xatolarni aniqlash nazariyasida ham qo‘llaniladi. Ma’lumot uzatish jarayonida yuz berishi mumkin bo‘lgan xatolarni aniqlash va tuzatish uchun butun sonli strukturalar asosida ishlaydigan algoritmlar ishlab chiqiladi.

Amaliy tomondan yana bir muhim jihat — Diofant tenglamalari sun’iy intellekt va mashinaviy o‘rganishda optimallashtirish masalalarini yechishda ishlatiladi. Ba’zi model parametrlarini butun sonlarda tanlash zarur bo‘lganda Diofant yondashuvi qo‘l keladi.

Shuningdek, Diofant tenglamalari algoritmlar nazariyasi, kodlash nazariyasi va kompyuter modellashtirishda ham qo'llaniladi. Ular yordamida murakkab tizimlarning matematik modellari tuziladi va optimallashtirish masalalari hal qilinadi.

Bundan tashqari, Diofant tenglamalari informatika, algoritmlar nazariyasi va matematik modellashtirishda ham qo'llaniladi. Ular optimallashtirish masalalarini yechishda, kodlash nazariyasida hamda xavfsiz aloqa tizimlarini yaratishda muhim rol o'ynaydi. Bu esa ularning amaliy ahamiyati juda keng ekanligini ko'rsatadi.

Umuman olganda, Diofant tenglamalari nazariy matematika bilan amaliy sohalar o'rtasidagi muhim bog'lovchi bo'g'in bo'lib, zamonaviy ilm-fan va texnologiyalarning rivojlanishida katta ahamiyatga ega.

Adabiyotlar ro'yxati

1. Hardy G.H., Wright E.M. *An Introduction to the Theory of Numbers*. Oxford University Press.
2. Burton D.M. *Elementary Number Theory*. McGraw-Hill Education.
3. Rosen K.H. *Discrete Mathematics and Its Applications*. McGraw-Hill.
4. Koblitz N. *A Course in Number Theory and Cryptography*. Springer.
5. Apostol T.M. *Introduction to Analytic Number Theory*. Springer.
6. O'zbekiston Respublikasi oliy ta'lim muassasalari uchun "Sonlar nazariyasi" o'quv qo'llanmalari.