УДК: 511.1

Мороз Д. В., здобувач вищої освіти,
Луценко А. В., доктор філософії з математики,
в. о. зав. кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ПРО ЛІНІЙНІ ДІОФАНТОВІ РІВНЯННЯ ТА МЕТОДИ ЇХ РОЗВ'ЯЗУВАННЯ

Анотація. Лінійні діофантові рівняння мають важливе значення в теорії чисел і застосовуються в криптографії та теорії алгоритмів. Основні методи їх розв'язання включають алгоритм Евкліда, використання тотожності Безу, метод перебору та метод підбору цілих розв'язків. Ці підходи дають змогу знаходити як одиничні, так і всі можливі розв'язки в межах існуючих систем рівнянь.

Ключові слова: лінійні діофантові рівняння, теорія чисел, алгоритм Евкліда, криптографія.

Актуальність. Діофант – одна з ключових постатей в історії математики, хоча точні дані про його життя невідомі. Він відомий завдяки своїй праці «Арифметика», що містить 189 задач, з яких до нас дійшли 7 книг із 13. Діофант розв'язував невизначені рівняння, шукаючи лише додатні цілі та раціональні числа, відкидаючи ірраціональні розв'язки як «неможливі». Діофантові рівняння – це алгебраїчні рівняння з цілими коефіцієнтами, де шукають цілі або раціональні розв'язки. Проблема розв'язування таких рівнянь була включена до списку проблем Гільберта, і в 1970 році Юрій Матіясевич довів її алгоритмічну нерозв'язність.

Мета. Мета роботи полягає в дослідженні лінійних діофантових рівнянь і методів їх розв'язування. Це включає аналіз умов існування розв'язків, вивчення основних алгоритмів, як-от метод Евкліда, та знаходження загальних рішень через параметризацію. Окрема увага приділяється практичному застосуванню діофантових рівнянь у різних галузях математики та науки.

1. Означення лінійного діофантового рівняння.

Рівняння виду:

$$ax + by = c \tag{1}$$

називається лінійним діофантовим рівнянням з двома невідомими, якщо a, b, c – цілі числа, $a \neq 0,\ b \neq 0,\ c \neq 0$.

До виду лінійних діофантових рівнянь з двома невідомими можна звести рівняння виду:

$$px + qy = g, \tag{2}$$

якщо $p,\ q,\ g$ – звичайні дроби, $p \neq 0, q \neq 0, g \neq 0$.

Для цього достатньо: записати всі коефіцієнти звичайними дробами і помножити ліву та праву частини рівняння на спільний знаменник, тобто помножити на найменше спільне кратне коефіцієнтів $\text{НСК}(p, q, g)$.

Умови існування розв'язків лінійних діофантових рівнянь виду $ax + by = c$ визначаються так:

– Основна умова існування розв'язків: рівняння має цілі розв'язки тоді і тільки тоді, коли найбільший спільний дільник *(НСД)* чисел a і b ділить c. Тобто існують цілі числа x і y, якщо НСД(a, b) є дільником c.

– Алгоритм Евкліда: для перевірки умови існування розв'язку можна використовувати алгоритм Евкліда для знаходження *НСД* чисел a і b.

– Якщо НСД$(\boldsymbol{a}, \boldsymbol{b})$ не ділить c: якщо ця умова не виконується, то рівняння не має цілих розв'язків.

2. Методи розв'язування.

1. Алгоритм Евкліда

Використовується для знаходження найбільшого спільного дільника (НСД) чисел a і b у рівнянні виду $ax + by = c$. Якщо *НСД* числа a і b ділить число c, рівняння має розв'язок. За допомогою розширеного алгоритму Евкліда можна знайти конкретні значення x і y.

2. Метод розширеного алгоритму Евкліда

Цей метод розвиває алгоритм Евкліда та дає змогу знайти конкретні розв'язки x_0 і y_0 у рівнянні $ax + by =$ НСД(a, b), а також узагальнені розв'язки для випадку, коли $c \neq$ НСД(a, b).

3. Метод узагальнених розв'язків

Якщо базовий розв'язок x_0 і y_0 знайдено для рівняння $ax + by = c$, то всі інші розв'язки можна отримати за допомогою формул:

$$x = x_0 + \frac{b}{\text{НСД}(a,b)} \cdot t, \qquad y = y_0 + \frac{a}{\text{НСД}(a,b)} \cdot t, \tag{3}$$

де t – довільне ціле число.

4. Метод пошуку часткових розв'язків

Якщо рівняння не має розв'язку безпосередньо, можна спробувати знайти часткові розв'язки для спрощених випадків і потім комбінувати їх для отримання загального розв'язку.

5. Геометричний підхід

Лінійне діофантове рівняння $ax + by = c$ можна інтерпретувати як лінію на площині з цілими координатами. Пошук розв'язків іноді зводиться до знаходження точок на цій прямій, де x і y є цілими числами.

6. Метод підбору

У випадку невеликих чисел можна вручну перебирати можливі значення змінних, шукаючи відповідні комбінації.

7. Модульний метод

Застосовується, якщо рівняння можна спростити до вигляду модулів. Це може спростити пошук цілих розв'язків у рівняннях типу $a \equiv c(mod\ b)$.

8. Метод обмеження та відсічення (Branch and Bound)

Застосовується для знаходження цілих розв'язків в обмежених діапазонах, що особливо корисно за великих коефіцієнтів.

Ці методи можуть комбінуватися або використовуватися залежно від складності рівняння й його коефіцієнтів.

Лінійні діофантові рівняння мають широке практичне застосування в криптографії, комбінаториці, теорії чисел та оптимізаційних задачах. Наприклад, їх ви-

користовують у створенні алгоритмів шифрування, розробці схем розподілу ресурсів та у задачах планування. Одним із відомих прикладів є криптографічний метод RSA, який базується на властивостях цілих розв'язків.

Висновки. Методи розв'язування лінійних діофантових рівнянь, як-от алгоритм Евкліда і тотожність Безу, забезпечують фундаментальні підходи до пошуку цілих розв'язків. Їх універсальність дає змогу успішно вирішувати задачі в різних математичних та прикладних сферах.

Список використаних джерел

1. Батирбаєв М. Х. Лінійні діофантові рівняння. Курс лекцій: навч. посіб. Київ: Наука, 2020. 120 с.
2. Чистяков А. В. Методи розв'язування лінійних діофантових рівнянь: навч. посіб. Київ: Наука і техніка, 2015. 85 с.
3. Нівен І., Зукерман Г., Монтгомері Х. Л. Вступ до теорії чисел: навч. посіб. Київ: Наукова думка, 1981. 520 с.
4. Еліотт П. Д. Т. А. Діофантові рівняння та їх застосування у теорії чисел: навч. посіб. Львів: Математичні дослідження, 2018. 95 с.
5. LeVeque W. J. Fundamentals of Number Theory: навч. посіб. Київ: Освіта, 1977. 290 с.