Дубовенко Марина,
студентка V курсу, спеціальність «Математика та економіка».
Науковий керівник – ***Дідківська Т. В.,***
кандидат фізико-математичних наук, доцент

ПРО ОДИН МЕТОД РОЗВ'ЯЗУВАННЯ ДІОФАНТОВИХ РІВНЯНЬ

Рівняння виду $ax+by=c$, де a,b,c – цілі числа, а x,y– змінні, $x,y\in Z$, називають діофантовим рівнянням першого степеня з двома змінними. Для розв'язання рівняння застосовують наступні теореми [2, с. 84–88].

Теорема 1. *Якщо* a *і* b *– взаємно прості числа, то для будь якого цілого* c *, рівняння* $ax+by=c$ *має хоча б один розв'язок в цілих числах.*

Теорема 2. *Якщо* a *і* b *мають спільний натуральний дільник* $d\neq1$*, а ціле число* c *не ділиться на* d*, то рівняння* $ax+by=c$ *не має розв'язків в цілих числах.*

Теорема 3. *Якщо* a *і* b *взаємно прості числа, то рівняння* $ax+by=c$ *має нескінченну кількість розв'язків, які знаходять за формулами* $x=x_0+bk$, $y=y_0-ak$*, де* $(x_0;y_0)$ *– будь який цілий розв'язок даного рівняння,* $k\in Z$.

Частіше всього такі рівняння розв'язуються методом розсіювання. Розглянемо, як розв'язувати лінійні діофантові рівняння за допомогою порівнянь. Перетворимо лінійне рівняння

$$ax+by=c,\ a>0, b>0, (a,b)=1,\ ax=c+b(-y)$$

Використаємо критерій порівняності: для того, щоб числа були порівняні за модулем, необхідно і досить, щоб вони відрізнялися на число кратне модулю. Тоді одержимо порівняння $ax\equiv c(\mathrm{mod}\, b)$, розв'язки якого збігаються з розв'язками даного рівняння.

Нехай x_0 – деякий розв'язок порівняння, тоді відповідь для порівняння буде мати наступний вигляд: $x\equiv x_0(\mathrm{mod}\, b)$ або $x=x_0+bt$.

Невідоме x для діофантового рівняння визначено. Знайдемо y.

$$ax+by=c$$
$$by=c-ax$$
$$by=c-a(x_0+bt)=c-ax_0-abt$$
$$y=\frac{c-ax_0}{b}-at$$
$$y=\frac{ax_0+by_0-ax_0}{b}-at=y_0-at$$

Отже, маємо загальний розв'язок даного рівняння $ax+by=c$

$$\begin{cases} x=x_0+bt \\ y=y_0-at \end{cases};\quad t\in Z$$

Одержане порівняння, після перетворення діофантового рівняння можна розв'язувати різними способами

I. Спосіб рівносильних перетворень [1, с. 177-178].

Можна виконати з порівнянням такі операції:

- домножити, або поділити обидві частини порівняння на число, взаємнопросте з модулем;
- додати до однієї частини порівняння число кратне модулю;
- замінити коефіцієнти найменшими лишками і звести порівняння до вигляду $x \equiv x_0 (\bmod m)$.

II. Спосіб випробовування чисел ПСЛ [2, с. 85].

Взявши від кожного класу по одному лишку, дістанемо так звану повну систему лишків за модулем m. Найчастіше за повну систему лишків беруть найменші невід'ємні лишки, або абсолютно найменші лишки. Безпосередньо підстановкою в порівняння чисел ПСЛ визначають частинний розв'язок.

III. Метод Ейлера [2, с. 85–84].

Нехай треба розв'язати конгруенцію $ax \equiv b (\bmod m)$, якщо $(a, m) = 1$. Помножимо дану конгруенцію на $a^{\varphi(m)-1}$, дістанемо еквівалентну конгруенцію:

$$a^{\varphi(m)} \cdot x \equiv ba^{\varphi(m)-1} (\bmod m)$$

Але за теоремою Ейлера, при $(a, m) = 1$ $a^{\varphi(m)} \equiv 1 (\bmod m)$, отже будемо мати наступний розв'язок порівняння:

$$x \equiv b \cdot a^{\varphi(m)-1} (\bmod m)$$

Одержану відповідь потрібно перетворити, замінивши найменшим лишком

Завдання. Розв'язжіть діофантове рівняння виду $ax + by = c$ шляхом зведення до лінійного порівняння $ax \equiv c (\bmod b)$ [3, с. 10-11].

Приклад. $43x + 37y = 21$

(43,37)=1$\Rightarrow$ існує розв'зок рівняння

$$43x = 21 + 37(-y)$$

За необхідною і достатньою умовою порівняності чисел за модулем маємо:

$$43x \equiv 21 (\bmod 37) \text{ або } 6x \equiv 21 (\bmod 37)$$

Розв'яжемо методом Ейлера.

Якщо $ax \equiv b (\bmod m)$, $(a, m) = 1$, то $x \equiv ba^{\varphi(m)-1} (\bmod 37)$

$$x \equiv 21 \cdot 6^{\varphi(37)-1} (\bmod 37)$$

$$x \equiv 21 \cdot 6^{36-1} (\bmod 37)$$

$$x \equiv 21 \cdot 6^{35} (\bmod 37)$$

Виконаємо перетворення: $x \equiv 21 \cdot 6^{35} \equiv 21 \cdot 6^2 \cdot 6^{33} \equiv 21 \cdot 36 \cdot 6^{33} \equiv 21 \cdot (-1) \cdot 6 \cdot 6^{32} \equiv$

$$\equiv -21 \cdot 6 \cdot (6^2)^{16} \equiv -126 \cdot (36)^{16} \equiv -126 \cdot (-1)^{16} \equiv -126 \equiv 22 (\bmod 37$$

Маємо $x = 22 + 37t$, $t \in Z$

Підставимо отримане x в рівняння, і знайдемо y:

$$y = -25 - 43t, t \in Z$$

Загальний розв'язок буде: $\begin{cases} x = 22 + 37t \\ y = -25 - 43t \end{cases}$, $t \in Z$

Перевірка: $43(22 + 37t) + 37(-25 - 43t) = 946 + 1591t - 925 - 1591t = 21$

Відповідь: $\begin{cases} x = 22 + 37t \\ y = -25 - 43t \end{cases}$, $t \in Z$

Література

1. Завало С. Т. Алгебра і теорія чисел / Завало С. Т., Костарчук В. М., Хацет Б. І. – К. : Вища школа, 1976. – Ч. 2. – 384с.
2. Бородін О. І. Теорія чисел / Бородін О. І. – К. : Радянська школа, 1960. – 244с.
3. Сверчевська І. А. Алгебра і теорія чисел : метод. вказівки та завданя для сам. роботи студ. фізико-математ. відділень ун-в. – Ч. 2. – Житомир : Вид-во ЖДУ ім. І. Франка, 2010. – 14 с.