5 ЛІНІЙНІ ДІОФАНТОВІ РІВНЯННЯ

Нехай $a, b, c \in \mathbb{Z}$. Нас цікавлять розв'язки (x, y) рівняння $ax + by = c$.

Якщо $a = b = 0$, то при $c = 0$ розв'язок довільний, а при $c \neq 0$ розв'язків немає.

Якщо $b = 0$, $a \neq 0$, отримуємо рівняння $ax = c$. Якщо $a \mid c$, то $x = \frac{c}{a}$, y – довільний; інакше розв'язків немає.

Позначимо $d = \gcd(a, b)$. Помітимо, що $d \mid a$, $d \mid b$, тому d має ділити вираз $ax + by$ при всіх x, y. Отже, якщо d не ділить c, то розв'язків немає.

Нехай тепер $d \mid c$. Запишемо $a = da_1$, $b = db_1$, $c = dc_1$; тоді обидві частини нашого рівняння можна поділити на d і прийти до еквівалентного рівняння $ax_1 + by_1 = c_1$, для якого вже $\gcd(a_1, b_1) = 1$, оскільки

$$d = \gcd(a, b) = \gcd(da_1, db_1) = d \gcd(a_1, b_1).$$

Тому тепер можна вважати, що $\gcd(a, b) = 1$. Ми знаємо, що є лінійне представлення НСД: $au_0 + bv_0 = 1$. Помножуючи на c обидві частини, одержуємо, що $a(u_0c) + b(v_0c) = c$. Позначимо $x_0 = u_0c$, $y_0 = v_0c$. Ми отримали, що у нашого рівняння є розв'язок (x_0, y_0). Як знайти всі розв'язки?

Нехай (x, y) – деякий розв'язок рівняння $ax + by = c$. Віднімаючи $ax_0 + by_0 = c$ з цієї рівності, отримуємо $a(x - x_0) + b(y - y_0) = 0$, звідки $a(x - x_0) = b(y_0 - y)$. Отже, $b \mid a(x - x_0)$; але $a \perp b$, тому $b \mid x - x_0$. Запишемо $x - x_0 = bt$; тоді $abt = b(y_0 - y)$, звідки $y_0 - y = at$. Отримали, що довільний розв'язок (x, y) нашого рівняння виглядає так: $x = x_0 + bt$, $y = y_0 - at$. Отже, якщо (x_0, y_0) – деякий один розв'язок рівняння $ax + by = c$, то всі його розв'язки мають вигляд $(x_0 + bt, y_0 - at)$ або $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ для $t \in \mathbb{Z}$. Навпаки, пряма підстановка показує, що $(x_0 + bt, y_0 - at)$ дійсно є розв'язком нашого рівняння.

Таким чином, запишемо *алгоритм розв'язання* лінійного діофантового рівняння $ax + by = c$:

1) За допомогою алгоритму Евкліда знаходимо найбільший спільний дільник $d = \gcd(a, b)$ і перевіряємо, чи $d \mid c$. Якщо $d \nmid c$, то рівняння розв'язків не має.

2) Якщо $d \mid c$, то за допомогою алгоритму Евкліда знаходимо зображення $d = au_0 + bv_0$ і частковий розв'язок $x_0 = u_0 \frac{c}{d}$, $y_0 = v_0 \frac{c}{d}$.

3) Знаходимо загальний розв'язок

$$x = x_0 + bt,\ y = y_0 - at \text{ або } x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t \text{ для } t \in \mathbb{Z}.$$

Теорема 1 (критерій можливості розв’язання лінійного діофантова рівняння від декількох змінних) Нехай $a_1, a_2, ..., a_n, c \in \mathbb{Z}$. Лінійне рівняння $a_1x_1 + a_2x_2 + ... + a_nx_n = c$ розв’язанне в цілих числах тоді і тільки тоді, коли $c \mid \gcd(a_1, a_2, ..., a_n)$.

Доведення.

Очевидно, що якщо це рівняння розв’язанне, то кожний доданок в лівій частині ділиться на $\gcd(a_1, a_2, ..., a_n)$, тому і c на нього ділиться. Доведемо тепер, що якщо c ділиться на $d = \gcd(a_1, a_2, ..., a_n)$, то рівняння розв’язується.

З нашого аналізу лінійного діофантова рівняння від двох змінних випливає, що цей критерій вірний для $n = 2$. Це буде базою для індукції по n. Нехай тепер $n \geq 3$. Розглянемо наступне рівняння: $\gcd(a_1, a_2)y_1 + a_3y_3 ... + a_ny_n = c$. Це лінійне діофантове рівняння від $n-1$ змінних $y_1, y_3, ..., y_n$. За припущенням індукції воно розв’язанне тоді і тільки тоді, коли його права частина, c, ділиться на $\gcd(\gcd(a_1, a_2), a_3, ..., a_n) = \gcd(a_1, a_2, a_3, ..., a_n) = d$. У нас за умовою $d \mid c$, тому нове рівняння має розв’язок $(y_1, y_3, ..., y_n)$. Побудуємо тепер розв’язок нашого початкового рівняння. Подивимося на ще одне допоміжне рівняння $a_1x_1 + a_2x_2 = \gcd(a_1, a_2)y_1$ з невідомими x_1, x_2. Права частина ділиться на НСД його коефіцієнтів, тому воно розв’язанне. Отже, ми знайшли x_1, x_2; покладемо тепер $x_3 = y_3, ..., x_n = y_n$. Тоді

$$a_1x_1 + a_2x_2 + ... + a_nx_n = \gcd(a_1, a_2)y_1 + a_3x_3 ... + a_nx_n =$$
$$= \gcd(a_1, a_2)y_1 + a_3y_3 ... + a_ny_n = c,$$

тому $(x_1, x_2, ..., x_n)$ – розв’язок вихідного рівняння.

Приклад 1 Знайти загальний розв’язок лінійного діофантового рівняння $15x - 39y = 55$.

Розв’язання.

$\gcd(15, 39) = 3$, але $3 \nmid 55$. Тому дане рівняння розв’язків не має.

Відповідь: рівняння розв’язків не має.

Приклад 2 Знайти загальний розв’язок лінійного діофантового рівняння $187x - 143y = 77$.

Розв’язання.

1) Шукаємо найбільший спільний дільник чисел 187 і –143:

$$187 = -1 \cdot (-143) + 44,$$
$$-143 = -4 \cdot 44 + 33,$$
$$44 = 1 \cdot 33 + 11,$$
$$33 = 3 \cdot 11 + 0.$$

Отже, $\gcd(187, -143) = 11$. Оскільки $77 \vdots 11$, то розв’язки існують.

2) Шукаємо зображення числа 11 як лінійної комбінації чисел 187 і –143:

$$11=44-1\cdot 33=44-1\cdot\left(-143+4\cdot 44\right)=-3\cdot 44-1\cdot\left(-143\right)=$$
$$=-3\cdot\left(187+1\cdot\left(-143\right)\right)-1\cdot\left(-143\right)=-3\cdot 187-4\cdot\left(-143\right).$$

Тоді

$$7\cdot\left(-3\right)\cdot 187+7\cdot\left(-4\right)\cdot\left(-143\right)=7\cdot 11=77$$

і пара $\left(7\cdot\left(-3\right),\,7\cdot\left(-4\right)\right)=\left(-21,\,-28\right)$ є частковим розв'язком рівняння.

3) Загальний розв'язок має вигляд

$x=-21-143t$, $y=-28-187t$ або $x=-21-13t$, $y=-28-17t$, $t\in\mathbb{Z}$.

Відповідь: $x=-21-13t$, $y=-28-17t$, $t\in\mathbb{Z}$.

Інколи на розв'язки лінійного діофантового рівняння накладають додаткові обмеження. Наприклад, задача про видачу касиром суми c, якщо в касі є лише банкноти номіналів a і b, зводиться до розв'язування лінійного діофантового рівняння $ax+by=c$ за природного обмеження $x\ge 0$, $y\ge 0$.

Приклад 3 Знайти всі натуральні розв'язки рівняння $5x+7y=116$.

Розв'язання.

Оскільки $\gcd\left(5,\,7\right)=1$ і $1=5-2\cdot 2=5-2\cdot\left(7-1\cdot 5\right)=3\cdot 5-2\cdot 7$, то частковим розв'язком рівняння буде, наприклад, пара $\left(3\cdot 116,\,-2\cdot 116\right)=\left(348,\,-232\right)$, а загальний розв'язок матиме вигляд $x=348+7t$, $y=-232-5t$, $t\in\mathbb{Z}$. Щоб розв'язки були натуральними, мають виконуватись нерівності $348+7t>0$ і $-232-5t>0$. Звідси $-\frac{348}{7}<t<-\frac{232}{5}$. З того, що $t\in\mathbb{Z}$, то $t\in\left\{-49,\,-48,\,-47\right\}$, а натуральні розв'язки рівняння вичерпуються парами (19, 3), (12, 8), (5, 13).

Відповідь: (19, 3), (12, 8), (5, 13).

Приклад 4 Розв'язати в цілих числах рівняння: $4x-6y+11z=7$.

Розв'язання.

Поділивши з остачею –6 на 4, отримаємо: $-6=4\cdot\left(-2\right)+2$. Представимо вихідне рівняння у вигляді:

$$4\left(x-2y\right)+2y+11z=7.$$

Після заміни $x'=x-2y$ це рівняння запишеться наступним чином:

$$4x'+2y+11z=7.$$

Далі, $11=5\cdot 2+1$, тому перетворимо останнє рівняння:

$$4x'+2\left(y+5z\right)+z=7$$

і ввівши заміну $y'=y+5z$, отримаємо

$$4x'+2y'+z=7.$$

З останнього рівняння $z=7-4x'-2y'$ для довільних $x',\,y'\in\mathbb{Z}$. Отже,

$$y=y'-5z=y'-5\left(7-4x'-2y'\right)=-35+20x'+11y',$$
$$x=x'+2y=x'+2\left(-35+20x'+11y'\right)=-70+41x'+22y'.$$

Відповідь: $x = -70 + 41x' + 22y'$, $y = -35 + 20x' + 11y'$, $z = 7 - 4x' - 2y'$, $x', y' \in \mathbb{Z}$.