

А.М. ГУПАЛІнститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: gupalanatol@gmail.com.**О.А. ВАГІС**Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: valexdep135@gmail.com.**НЕПОВНОТА АРИФМЕТИКИ З ПОГЛЯДУ
ТЕОРІЇ ДІОФАНТОВИХ МНОЖИН**

Анотація. Проаналізовано Діофантові множини і показано, що всі рекурсивно перелічені множини є Діофантовими. На основі класичних результатів з теорії рекурсивних функцій наведено простий варіант теореми про неповноту арифметики: існує поліном, який не має цілих додатних розв'язків і для якого не можна довести відсутність додатних коренів.

Ключові слова: Діофантова множина, рекурсивно перелічені множини, неповнота арифметики.

ВСТУП

Загальновідома теорема Геделя про неповноту арифметики являє собою результат про формальну арифметику, в якому теорія обчислюваності та логіка пов'язані між собою. Доведення неповноти має низку допоміжних тверджень і натеper не є простим. На основі класичних результатів з теорії рекурсивних функцій і Діофантових множин надано достатньо просте доведення про неповноту арифметики.

У 1971 р. було отримано визначний результат про нерозв'язність 10-ї проблеми Гільберта, а саме, чи існує алгоритм, який за наданим поліномом $p(x_1, \dots, x_n)$ з цілими коефіцієнтами розпізнає існування розв'язків рівняння $p=0$ у цілих числах. Учений математик Ю.В. Матіясеvич показав, що такого алгоритму не існує [1].

Основний технічний результат, отриманий під час доведення нерозв'язності 10-ї проблеми Гільберта — це теорема про збіг класу Діофантових множин та класу рекурсивно перелічених множин. Про обчислювальні можливості поліномів свідчить такий результат: можна явно вказати поліном від багатьох змінних з цілими коефіцієнтами такий, що множина всіх додатних значень, яких він набуває за цілочислових значень змінних, є в точності множина простих чисел.

ДІОФАНТОВІ МНОЖИНИ

Діофантовими рівняннями називають рівняння вигляду

$$D(a_1, \dots, a_n, x_1, \dots, x_m) = 0, \quad (1)$$

де D — поліном з цілими коефіцієнтами відносно всіх змінних $a_1, \dots, a_n, x_1, \dots, x_m$, які розбито на дві частини: параметри $a_1, \dots, a_n$ та невідомі $x_1, \dots, x_m$. Під час фіксації значень параметрів отримуються конкретні Діофантові рівняння.

У процесі різного вибору значень параметрів одержують рівняння, які мають розв'язки, і рівняння, які розв'язків не мають. Параметри Діофантового рівняння (1) визначають деяку множину $\mathfrak{M}$, яка складається з усіх таких наборів значень параметрів $a_1, \dots, a_n$, для яких існують значення змінних $x_1, \dots, x_m$, які задовольняють рівняння (1):

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Leftrightarrow \exists x_1, \dots, x_m [D(a_1, \dots, a_n, x_1, \dots, x_m) = 0]. \quad (2)$$

Число n — розмірність множини $\mathfrak{M}$, а еквівалентність (2) — Діофантове представлення множини $\mathfrak{M}$.

Потрібно розв'язати таку задачу: нехай є деяка множина, яка складається з n -ок натуральних чисел; треба встановити, чи є ця множина Діофантовою, і якщо так, то знайти для неї будь-яке Діофантове представлення. Іноді діофантовість множини тривіальна, наприклад, очевидна діофантовість множини всіх парних чисел. В інших випадках виявляти діофантовість технічно складно, наприклад для простих чисел.

Об'єднання двох Діофантових множин однакової розмірності є Діофантовою множиною. Дійсно, якщо $D_1(a_1, \dots, a_n, x_1, \dots, x_{m_1}) = 0$ та $D_2(a_1, \dots, a_n, x_1, \dots, x_{m_2}) = 0$ — Діофантові представлення двох множин, то $D_1(a_1, \dots, a_n, x_1, \dots, x_{m_1}) \times D_2(a_1, \dots, a_n, x_1, \dots, x_{m_2}) = 0$ — Діофантове представлення їхнього об'єднання.

Перетин двох Діофантових множин однакової розмірності також Діофантів і визначається рівнянням

$$D_1^2(a_1, \dots, a_n, x_1, \dots, x_{m_1}) + D_2^2(a_1, \dots, a_n, x_1, \dots, x_{m_2}) = 0.$$

Показано, що доповнення множини n -ок натуральних чисел до множини всіх n -ок натуральних чисел не обов'язково є Діофантовою множиною і цей факт зовсім не є тривіальним.

Отримано можливість спеціалізувати вид рівнянь у Діофантових представленнях множиною натуральних чисел (тобто у випадку $n = 1$). Неважко зрозуміти, що рівняння

$$D(a, x_1, \dots, x_m) = 0 \quad (3)$$

має розв'язок у невідомих $x_1, \dots, x_m$ тоді і тільки тоді, коли рівняння

$$(x_0 + 1)(1 - D^2(x_0, \dots, x_m)) - 1 = a \quad (4)$$

має розв'язок у невідомих $x_0, \dots, x_m$. Дійсно, з довільного розв'язання рівняння (3) можна отримати розв'язок (4) для $x_0 = a$. З іншого боку, співмножник $(1 - D^2(x_0, \dots, x_m))$ повинен бути додатним, а це можливо лише, якщо $D(x_0, \dots, x_m) = 0$. У цьому випадку з (4) випливає, що $x_0 = a$, і це означає, що (3) також виконується.

Таким чином, множина натуральних чисел є Діофантовою тоді і тільки тоді, коли вона є множиною усіх натуральних значень, які набуває деякий поліном з цілими коефіцієнтами за натуральних значень змінних.

ЛОГІЧНА ТЕРМІНОЛОГІЯ

Часто натомість мови множин зручніше використовувати мову властивостей та відношень (предикатів) між числами. Властивість P натуральних чисел є Діофантовою властивістю, якщо діофантовою є множина всіх чисел, які мають властивість P , відповідно еквівалентність вигляду

$$P(a) \Leftrightarrow \exists x_1, \dots, x_m [D(a, x_1, \dots, x_m) = 0]$$

називається Діофантовим представленням властивості P .

Аналогічно відношення R між n натуральними числами називається Діофантовим відношенням, якщо Діофантовою є множина n -ок натуральних чисел, які містяться у відношенні R ; відповідно еквівалентність вигляду

$$R(a_1, \dots, a_n) \Leftrightarrow \exists x_1, \dots, x_m [D(a_1, \dots, a_n, x_1, \dots, x_m) = 0]$$

називається Діофантовим представленням відношення R .

Об'єднанню множин за цією термінологією відповідає побудова нової властивості (відношення) за допомогою логічної операції «або» (диз'юнкція). Інакше кажучи, якщо R_1 та R_2 — два Діофантові відношення (або властивості), то відношення R (властивість) таке, що для всіх $a_1, \dots, a_n$ виконується $R(a_1, \dots, a_n) \Leftrightarrow R_1(a_1, \dots, a_n) \vee R_2(a_1, \dots, a_n)$, також є Діофантовим.

Аналогічно перетину множин відповідає логічна операція «і» (кон'юнкція). Еквівалентність типу $R(a_1, \dots, a_n) \Leftrightarrow R_1(a_1, \dots, a_n) \& R_2(a_1, \dots, a_n)$ також розглядається як загальне Діофантове представлення відношення R , якщо діофантовість R_1 та R_2 вже була встановлена.

Важливим засобом встановлення діофантовості є поняття Діофантової функції як функції, графік якої є Діофантовою множиною. Відповідно Діофантовим представленням функції F буде еквівалентність типу

$$a = F(b_1, \dots, b_n) \Leftrightarrow \exists x_1, \dots, x_m [D(a, b_1, \dots, b_n, x_1, \dots, x_m) = 0],$$

де D — поліном з цілими коефіцієнтами.

ПРИКЛАДИ ДІОФАНТОВИХ МНОЖИН, ВІДНОШЕНЬ І ФУНКЦІЙ

Наведемо декілька простих прикладів: діофантовість нерівностей $\leq$ та $<$

$$a \leq b \Leftrightarrow \exists x [a + x = b], \quad a < b \Leftrightarrow \exists x [a + x + 1 = b].$$

Діофантовість множини всіх парних чисел: $\exists x [a = 2x]$. Діофантовість відношення ділення $a | b \Leftrightarrow \exists x [ax = b]$ дає змогу дати загальне представлення діофантовості функції $\text{rem}(b, c)$ — залишок від ділення b на c : $a = \text{rem}(b, c) \Leftrightarrow a < c \& c | b - a$.

На основі діофантовості rem можна дати загальне Діофантове представлення функції $b \text{ div } c$ — ціла частина від ділення b на c :

$$a = b \text{ div } c \Leftrightarrow ac + \text{rem}(b, c) = b$$

та загальне Діофантове представлення тримісного відношення порівняння за додатним модулем $a = b \pmod{c} = \text{rem}(a, c) = \text{rem}(b, c)$. Функція $b \text{ div } c$ відіграє важливу роль у встановленні діофантовості функції піднесення до степеня b^c .

Отримано загальне Діофантове представлення функції GCD — найбільший загальний дільник додатних цілих чисел:

$$a = GCD(b, c) \Leftrightarrow bc > 0 \& a | b \& \exists x y [a = bx - cy].$$

МОВИ ОПИСУ ДІОФАНТОВИХ МНОЖИН

Мова $\mathcal{Y}_0 = \{+, \times, =, \exists\}$, де $\exists$ — квантор існування дає змогу записати будь-який поліном $p(a, x)$ та робити висновки у вигляді $\exists x p(a, x) = 0$, де $a = \{a_1, \dots, a_k\}$, $x = \{x_1, \dots, x_m\}$. Тоді можна охарактеризувати Діофантові множини як такі і тільки такі, які можна виразити мовою $\mathcal{Y}_0$. Однак можливості мови $\mathcal{Y}_0$ обмежені і на ній не можна висловити багато цікавих з теоретико-числової точки зору множин. Наприклад, множина простих чисел виражається формою

$$p > 1 \& \forall y \leq p \forall z \leq p [yz \neq p \vee y = 1 \vee z = 1],$$

до якої входить обмежений квантор загальності $\forall_{\leq}$.

Ю.В. Матіясевиц вивчив мови $\mathcal{Y}_1 - \mathcal{Y}_5$, при чому можливості кожної наступної мови збільшувалися. У сукупності вони містять символи $+$, $\times$, $\uparrow$ (оператор піднесення до степеня), $=$, $\neq$, $>$, $\geq$, $|$ (операція поділу), обмежений квантор загальності $\forall_{\leq}$ (mod), $\&$, $\vee$, $\exists$, а також деякі функції. Мова $\mathcal{Y}_5$ отримується додаванням обмеженого квантора загальності $\mathcal{Y}_5 = \mathcal{Y}_4 \cup \{\forall_{\leq}\}$.

Технічно складними виявилися доведення діофантовості функції двох аргументів b^c та обмеженого квантора загальності. На основі діофантовості функції b^c отримано діофантовість біноміальних коефіцієнтів і факторіала та записано Діофантове представлення простих чисел в іншому вигляді

$$\text{Prime}(a) \Leftrightarrow a > 1 \ \& \ GCD(a, (a-1)!) = 1.$$

Матіясевич довів рівнооб'ємність мов $\mathcal{Y}_0$ і $\mathcal{Y}_5$, тобто будь-яка множина, що виражається однією мовою, виражається також і в іншій мові. З цього випливає діофантовість множини всіх простих чисел.

З іншого боку, у теорії рекурсивних функцій встановлено, що клас множин, описаних мовою $\mathcal{Y}_5$, збігається з класом рекурсивно перелічених (р.п.) множин. Таким чином, з рівнооб'ємності мов $\mathcal{Y}_0$ та $\mathcal{Y}_5$ доведено, що клас Діофантових множин збігається з класом р.п. множин. Одним з класичних результатів у теорії рекурсивних функцій є теорема про існування р.п. множини (наведена далі), для якої не існує засобу, що дає змогу за скінченну кількість кроків розпізнати наявність або відсутності довільного числа у цій множині. Цей результат разом з діофантовістю р.п. множин дає від'ємний розв'язок 10-ї проблеми Гільберта [1].

ТЕРМІНОЛОГІЯ З ТЕОРІЇ РЕКУРСИВНИХ ФУНКЦІЙ

Надамо деякі необхідні відомості з теорії рекурсивних функцій. Далі без обмеження загальності розглянемо випадок однопараметричних Діофантових множин.

Нехай $p(x, y_1, \dots, y_m)$ — поліном з цілими коефіцієнтами. Тоді предикат (відношення) $M(x)$, який задається формулою

$$M(x) = \exists y_1, \dots, \exists y_m (p(x, y_1, \dots, y_m) = 0),$$

називається Діофантовим предикатом, область визначення кванторів $\exists y_1, \dots, \exists y_m$ є множиною натуральних чисел.

Теорема 1. Діофантові предикати є частково розв'язними.

Доведення. Предикат $p(x, y_1, \dots, y_m) = 0$ є розв'язним, оскільки він перевіряється підстановкою у поліном значень змінних x та $y_1, \dots, y_m$. Існує теорема [2], яка показує, що предикат вигляду

$$M(x) = \exists y_1, \dots, \exists y_m (p(x, y_1, \dots, y_m) = 0)$$

є частково розв'язним.

Зрозуміло, що з числа частково розв'язних предикатів Діофантовими є ті, які можна представити у відносно простому вигляді. Багато часу було невідомо про існування нерозв'язних Діофантових предикатів. Ця проблема пов'язана з 10-ю проблемою Гільберта. Саме тому визначним досягненням виявився доведений Матіясевичем у 1971 р. результат.

Теорема 2. Кожний частково розв'язний предикат є Діофантовим предикатом.

Відомо з теорії рекурсивних функцій, що проблема $x \in W_x$ є нерозв'язною, де W_x — область визначення часткової обчислюваної функції ϕ_x , яка виконується програмою P_x з індексом x . Ця програма завершує роботу на вході x . Програма P_x складається зі скінченного набору команд, які можна закодувати натуральним числом.

Характеристична функція цієї проблеми, яка задається формулою,

$$f(x) = \begin{cases} 1, & \text{якщо } x \in W_x, \\ 0, & \text{якщо } x \notin W_x, \end{cases}$$

не є обчислюваною функцією. У протилежному випадку за допомогою діагонального методу будується обчислювана функція $g(x)$, яка відрізняється від

будь-якої обчислюваної функції [2]:

$$g(x) = \begin{cases} 1, & \text{якщо } x \notin W_x, \\ \text{не визначена,} & \text{якщо } x \in W_x. \end{cases}$$

Означення 1. Нехай A — підмножина множини натуральних чисел N . Характеристичною функцією A є функція

$$C_A(x) = \begin{cases} 1, & \text{якщо } x \in A, \\ 0, & \text{якщо } x \notin A. \end{cases}$$

Тоді множина A називається рекурсивною, якщо C_A — обчислювана функція або, якщо предикат $x \in A$ є розв'язним.

Таким чином, множина $K = \{x | x \in W_x\}$ не є рекурсивною. Для $K = \{x | x \in W_x\}$ не існує програми, яка дає змогу за скінченну кількість кроків розпізнати наявність або відсутність довільного числа $n = 0, 1, 2, \dots$ у цій множині.

Хоча предикат $x \in W_x$ і має необчислювану характеристичну функцію, проте наступна функція, яка пов'язана з цією проблемою, є обчислюваною

$$f(x) = \begin{cases} 1, & \text{якщо } x \in W_x, \\ \text{не визначена,} & \text{якщо } x \notin W_x. \end{cases}$$

Якщо вважати, що одиницею кодується відповідь «так», то будь-який алгоритм, який обчислює f , є процедурою, яка дає відповідь «так», коли $x \in W_x$, але продовжує роботу нескінченно, якщо твердження $x \in W_x$ не виконується. Таку процедуру називають частково розв'язною процедурою для проблеми $x \in W_x$, та до того ж вважають, що ця проблема або цей предикат є частково розв'язним.

Означення 2. Предикат $M(x)$ називається частково розв'язним, якщо функція

$$f(x) = \begin{cases} 1, & \text{якщо } M(x) \text{ істинний,} \\ \text{не визначена,} & \text{якщо } M(x) \text{ хибний,} \end{cases}$$

обчислювана. Ця функція називається частковою характеристичною функцією $M(x)$.

Означення 3. Нехай A — підмножина множини N . Тоді множина A є рекурсивно переліченою, якщо функція f , яка задається формулою

$$f(x) = \begin{cases} 1, & \text{якщо } x \in A, \\ \text{не визначена,} & \text{якщо } x \notin A. \end{cases}$$

обчислювана (або, якщо предикат $x \in A$ є частково розв'язним).

Показано, що множина A є р.п. тоді і тільки тоді, коли вона є областю визначеності обчислюваної функції [2].

Установити р.п. будь-якої множини буває значно легше, ніж виявити діофантовість цієї множини. Наприклад, звичайно, що множина простих чисел є р.п., але зовсім не очевидно, що вона є Діофантовою. Ця р.п. множина виявилась множиною додатних значень деякого многочлена (він має 26 змінних [3]). Це твердження вважали дуже неправдоподібним доти, поки Матіасевич не довів свою теорему.

НЕПОВНОТА АРИФМЕТИКИ І ДІОФАНТОВІ МНОЖИНИ

Зрозуміло, що Діофантова множина є рекурсивно переліченою, і тому всі рекурсивно перелічені множини з теореми Матіасевича є Діофантовими.

Оскільки предикат $x \in K$ частково розв'язний, множина $K = \{x | x \in W_x\}$ рекурсивно перелічена. Множина K є областю визначеності р.п. множини W_i деякої обчислюваної функції ϕ_i .

Виберемо тепер поліном $p(a, y_1, \dots, y_m)$ такий, що

$$a \in W_a \Leftrightarrow \exists y_1, \dots, \exists y_m (p(a, y_1, \dots, y_m) = 0). \quad (5)$$

Це можна зробити в результаті діофантовості р.п. множини K . У формулі (5) Діофантів предикат $\exists y_1, \dots, \exists y_m (p(a, y_1, \dots, y_m) = 0)$ є формальним аналогом предиката $x \in K$, і це є ключовим результатом Матіясевича. У конструкції Геделя для отримання формального аналога предиката $x \in K$ присвячена суттєва частина доведення Геделя [4].

Розглянемо функцію, яка визначається у такий спосіб:

$$F(a) = \begin{cases} 1, & \text{якщо } \exists y_1, \dots, \exists y_m (p(a, y_1, \dots, y_m) = 0), \\ 0 & \text{у протилежному випадку.} \end{cases}$$

Якщо би існувала розв'язувальна процедура для 10-ї проблеми Гільберта, то можна було ефективно обчислити значення функції F , тобто проблема $a \in W_a$ була би розв'язною, але це неможливо.

З теорії Діофантових множин випливає простий варіант теореми Геделя про неповноту арифметики. Оскільки Діофантові множини є р.п., всі рівняння $p(x_1, \dots, x_k) = 0$, які мають розв'язки у цілих числах, можна рекурсивно перелічити.

Непереліченими залишаються твердження про відсутність розв'язків для рівнянь

$$\forall x_1, \dots, \forall x_k p(x_1, \dots, x_k) \neq 0. \quad (6)$$

Якщо припустити, що для деякої несуперечливої системи аксіом можна довести всі факти вигляду (6), це означало би існування алгоритму, який перелічує теореми (6). Оскільки будь-які докази є скінченними, всі вони утворюють рекурсивно перелічену множину [2]. Тобто цей алгоритм перелічує доповнення до множини поліномів, які мають додатні розв'язки. Згідно з відомою теоремою [2] множина A є рекурсивною (розв'язною) тоді і тільки тоді, коли множини A та A^c є р.п. Отже, отримуємо розв'язність множини поліномів, які мають додатні корені (в такому випадку множина поліномів (6) є теж розв'язною). Таким чином маємо суперечність з від'ємним розв'язком 10-ї проблеми Гільберта.

Теорема 3. Для будь-якої несуперечної теорії, яка містить арифметику, існує поліном, який не має цілих додатних розв'язків і для якого не можна довести відсутність натуральних коренів.

ВИСНОВКИ

Аналіз Діофантових множин показав, що всі рекурсивно перелічені множини є Діофантовими. На основі класичних результатів з теорії рекурсивних функцій можна привести простий варіант теореми про неповноту арифметики: існує поліном, який не має цілих додатних розв'язків і для якого не можна довести відсутність натуральних коренів.

СПИСОК ЛІТЕРАТУРИ

1. Матіясевич Ю.В. Діофантові множества. *Успехи математических наук*. 1971. Т. 22. Вып. 5. С. 185–222.
2. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. Москва: Мир, 1983. 256 с.
3. Матіясевич Ю.В. Десятая проблема Гильберта. Москва: Наука, 1993. 224 с.
4. Мендельсон Э. Введение в математическую логику. Москва: Наука, 1971. 320 с.

A.M. Gupal, O.A. Vagis

INCOMPLETENESS OF ARITHMETIC FROM THE POINT OF VIEW OF DIOPHANTINE SET THEORY

Abstract. Analysis of Diophantine sets showed that all recursively enumerated sets are Diophantine. Based on classical results in the theory of computable functions, a simple version of the theorem on the incompleteness of arithmetic can be given: there is a polynomial that does not have positive integer solutions, and for which it is impossible to prove the absence of positive roots.

Keywords: Diophantine set, recursively enumerated sets, incompleteness of arithmetic.

Надійшла до редакції 27.02.2023