УДК 519.217.2

Неповнота арифметики і теорія діофантових множин

Анатолій Гупал[1], Микита Гупал[2]

[1] член-кореспондент НАН України, д. ф.- н., професор, Інститут кібернетики імені В.М. Глушкова НАН України, проспект Академіка Глушкова, 40, 03187, Київ-187, e-mail: gupalantol@gmail.com
[2] к. ф.-м. н., Інститут кібернетики імені В.М. Глушкова НАН України, проспект Академіка Глушкова, 40, 03187, Київ-187, e-mail: gupalantol@gmail.com

Аналіз діофантових множин показав, що всі рекурсивно перелічені множини є діофантовими. На основі класичних результатів у теорії рекурсивних функцій наведено простий варіант теореми про неповноту арифметики: існує поліном, який не має цілих позитивних рішень, і для якого не можна довести відсутність позитивних коренів.

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

Вступ. Доведення теореми Геделя про неповноту арифметики несе в собі цілий ряд допоміжних тверджень і в наш час не є простим [1]. На основі класичних результатів у теорії рекурсивних функцій і діофантових множин надано достатньо просте доведення неповноти арифметики, яке зовсім відрізняється від конструкції Геделя.

У 1971 році було отримано видатний результат про нерозв'язність 10-ї проблеми Гільберта. Було показано, що не існує алгоритму, який за наданим поліномом розпізнає існування коренів поліному в цілих числах [2].

Основний технічний результат, отриманий при доказі нерозв'язності 10-ї проблеми Гільберта – це теорема про співпадіння класу діофантових множин та класу рекурсивно перелічених множин. Було отримано наступний несподіваний результат: можна явно вказати поліном від багатьох змінних з цілими коефіцієнтами такий, що множина всіх позитивних значень, яких він приймає при цілочисленних значеннях змінних, є в точності множина простих чисел.

1.Діофантові множини

Діофантовими рівняннями називаються рівняння виду

$$D(a_1,...,a_n,x_1,...,x_m)=0\,, \tag{1}$$

де D – поліном з цілими коефіцієнтами відносно усіх змінних $a_1,...,a_n,x_1,...,x_m$, які розбито на дві частини: параметри $a_1,...,a_n$ та невідомі

$x_1,...,x_m$. При фіксації значень параметрів отримуються конкретні діофантові рівняння.

При різному виборі значень параметрів одержують рівняння, які мають розв'язки, так і рівняння, які розв'язків не мають. Параметри діофантового рівняння (1) визначають деяку множину M, яка складається з усіх таких наборів значень параметрів $a_1,...,a_n$, для яких існують значення змінних $x_1,...,x_m$, які задовольняють рівнянню (1):

$$< a_1,...,a_n > \in \mathrm{M} \Leftrightarrow \exists x_1...x_m[D(a_1,...,a_n,x_1,...,x_m)=0]. \quad (2)$$

Число n – розмірність множини M, а еквівалентність (2) – діофантове представлення множини M. Можна вважати діофантовим представленням не тільки (2), а також і (1).

Необхідно вирішити наступну задачу: нехай є деяка множина, яка складається з n-ок натуральних чисел; потрібно встановити, чи являється ця множина діафантовою і якщо являється, то знайти для неї будь яке діафантове представлення. Іноді діофантовість множини тривіальна, наприклад, очевидна діафантовість множини всіх парних чисел. В інших випадках встановити діафантовість технічно важко, наприклад для простих чисел.

Об'єднання та перетин двох діафантових множин однакової розмірності є діафантовою множиною. Отримано можливість спеціалізувати вид рівнянь у діофантових представленнях множиною натуральних чисел у випадку $n=1$. А саме, рівняння

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

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

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

має розв'язок у невідомих $x_0,...,x_m$. Таким чином, множина натуральних чисел є діафантовою тоді і тільки тоді, коли вона є множиною усіх натуральних значень, які приймає деякий поліном з цілими коефіцієнтами при натуральних значеннях змінних [3].

Важливим засобом встановлення діафантовості є поняття діафантової функції як функції, графік якої є діафантовою множиною. Відповідно діафантовим представленням функції F буде еквівалентність типу

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

де D – поліном з цілими коефіцієнтами.

2.Мови опису діофантових множин

Мова $Я_0 = \{+, \times, =, \exists\ \}$, 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 $a = \{a_1, ..., a_k\}$, $x = \{x_1, ..., x_m\}$. Тоді можна охарактеризувати діофантові множини як ті і тільки ті множини, які можна виразити мовою $Я_0$. Однак можливості мови $Я_0$ обмежені і на ній не можна висловити багато цікавих з теоретико-числової точки зору множин. Наприклад, множина простих чисел виражається формулою

$$p > 1 \& \forall y \le p \forall z \le p[yz \ne p \vee y = 1 \vee z = 1],$$

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

Ю.В. Матіясевич вивчив мови $Я_1 - Я_5$ з наростаючою можливістю кожної наступної мови. У сукупності вони містять символи +, $\times, \uparrow$ (оператор зведення у ступінь), =, $\ne$, >, $\ge$, | (операція поділу), обмежений квантор загальності $\forall_{\le}$. (mod), &, $\vee$, $\exists$, а також деякі функції . Технічно складними виявилися докази діофантовості функції двох аргументів b^C та обмеженого квантора загальності. На основі діафантовості функції b^C отримано діафантовість біноміальних коефіцієнтів і факторіалу та виписано діафантове представлення простих чисел в іншому виді: $\Pr ime(a) \Leftrightarrow a > 1 \& GCD(a, (a-1)!) = 1$, де GCD – найбільший загальний дільник позитивних цілих чисел.

Матіясевич довів рівнооб'ємність мов $Я_0$ і $Я_5$, тобто будь-яка множина, що виражається однією мовою, виражається також і в іншій мові. З цього негайно слідує діофантовість множини всіх простих чисел. З іншого боку, у теорії рекурсивних функцій встановлено, що клас множин, описаних мовою $Я_5$, збігається з класом рекурсивно перелічених (р.п.) множин. Таким чином, з рівнооб'ємності мов $Я_0$ та $Я_5$ доведено, що класс діофантових множин співпадає з классом р. п. множин. Одним з класичних результатів в теорії рекурсивних функцій є теорема про існування р.п. множини, для якої не існує засобу, що дозволяє за скінчене число кроків розпізнати присутність або відсутність довільного числа у цій множині. Цей результат разом з діафантовістю р.п. множин дає негативний розв'язок 10-ї проблеми Гільберта [1].

Відомо у 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 [4]. Множина $K = \{x | x \in W_x\}$ – рекурсивно перелічена (р. п.), вона є областю визначеності деякої обчислюваної функції.

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

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

Це можна зробити в результаті діофантовості р. п. множини K. В формулі (5) діафантів предикат $\exists y_1, ..., \exists y_m (p(a, y_1, ..., y_m) = 0)$ є формальним аналогом предиката $x \in K$, і це є ключовим результатом у теорії. В конструкції Геделя були присутні квантор загальності та логічна операція «ні», які у теорії фіофантових множин не використовуються [1].

Розглянемо функцію, яка визначається наступним чином

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

Якщо би існувала вирішальна 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 про неповноту арифметики. Оскільки діафантові множини є р. п., всі рівняння $p(x_1, ..., x_k)$=0, які мають розв'язки у цілих числах, можна рекурсивно перелічити.

Непереліченими лишаються твердження про відсутність рішень для рівнянь

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

Якщо припустити, що для деякої несуперечливої системи аксіом можна довести усі факти виду (6), це означало би існування алгоритму, який перелічує теореми (6). Оскільки будь-які докази є скінченими, всі вони утворюють рекурсивно перелічену множину [4]. Тобто цей алгоритм перелічує доповнення до множини поліномів, які мають позитивні розв'язки. Відома теорема Поста [4] говорить про те, що множина A є рекурсивною (розв'язною) тоді і тільки тоді, коли множини A та $\overline{A}$ є р. п. Тобто отримуємо розв'язність множини поліномів, які мають позитивні корені (в такому випадку множина поліномів (6) є теж розв'язною). Таким чином маємо суперечність з негативним рішенням 10-ї проблеми Гільберта.

Теорема 3. Для будь-якої несуперечної теорії, яка містить арифметику, існує поліном, який не має цілих позитивних рішень, 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 у теорії рекурсивних функцій можна привести простий варіант теореми про неповноту арифметики: існує поліном, який не має цілих позитивних рішень, і для якого не можна довести відсутність натуральних коренів.

Література

[1] *Мендельсон Э.* Введение в математическую логику. — М.: Наука, 1971. – 320 с.
[2] *Матиясевич Ю.В.* Диофантовы множества. Успехи математических наук. 1971. т.22. Вып.5.С.185 – 222.
[3] *Матиясевич Ю.В.* Десятая проблема Гильберта. – М.: Наука, 1993. – 224 с.
[4] *Катленд Н.* Вычислимость. Введение в теорию рекурсивных функций: Пер. с англ. – М.: Мир, 1983. – 256 с.

–

Incompleteness of arithmetic and the Diophantine sets theory

Anatolii Hupal, Mykyta Hupal

Analysis of Diophantine sets showed that all recursively enumerated sets are Diophantine. Based on the 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

Отримано 30.03.23