JEL Classification: C61 *УДК 330.4*

ПОСЛІДОВНІСНА МОДЕЛЬ БУЛЕВОЇ АЛГЕБРИ ТА ДЕЯКІ ЇЇ ЗАСТОСУВАННЯ

Сенчуков В. Ф.

Пропонується конструктивний підхід до вирішення проблеми впровадження формальної логіки в побудову математичних моделей, пов'язаних з описом дискретних множин. Метою є створення інструментарію, за допомогою якого можна було б на аналітичному рівні (у вигляді єдиної формули) описувати закономірності, яким підкоряються множини дискретних об'єктів.

Витоком усіх понять, на яких будується виклад, є поняття нумерації як функціонального відображення множини натуральних чисел на задану множину (не обов'язково числової природи). Зокрема, числові послідовності з відомим загальним членом є нумерацією множини значень їх елементів. З часів Г. Кантора не було наукових робіт, у яких би розглядався систематичний конструктивний підхід до нумерації елементів дискретних множин.

Метод дослідження ґрунтується на алгебрі логіки Буля – булевій алгебрі, – пропозиційними змінними (висловленнями) якої є послідовності, зокрема – числові. Логічні операції над такими змінними, на відміну від відомих арифметичних операцій, здатні враховувати властивості самих операндів. Це, відповідно, дає можливість зберегти властивості чинників економічного процесу, для опису якого будується математична модель. Шляхи практичного застосування результатів дослідження обумовлені: проблемою управління підприємствами у разі моделювання нелінійних процесів в економіці, як і взагалі нелінійних динамічних процесів; задачами теорії алгоритмів, теорії чисел, дискретної математики, математичного програмування, оптимального розкрою матеріалів, кристалографії і т. ін.

На прикладі теоретико-числової задачі показано ефективність застосування запропонованого алгебро-логічного підходу для вирішення четвертої проблеми списку Едмунда Ландау та встановлення потужності множини простих чисел у многочлені Ейлера. Є припущення, що такий підхід застосовний до вивчення потужності простих чисел у інших формах.

Ключові слова – булева алгебра, логічні операції, многочлен, модель, породна множина, послідовність, просте число.

JEL Classification: C61 *УДК 330.4*

ПОСЛЕДОВАТЕЛЬНОСНАЯ МОДЕЛЬ БУЛЕВОЙ АЛГЕБРЫ И НЕКОТОРЫЕ ЕЕ ПРИМЕНЕНИЯ

Сенчуков В. Ф.

Предлагается конструктивный подход к решению проблемы внедрения формальной логики в построение математических моделей, связанных с описанием дискретных множеств. Целью является создание инструментария, с помощью которого можно было бы на аналитическом уровне (в виде единой формулы) описывать закономерности, которым подчиняются множества дискретных объектов.

Истоком всех понятий, на которых строится изложение, является понятие нумерации как функционального отображение множества натуральных чисел на заданное множество (не обязательно числовой природы). В частности, числовые последовательности с известным общим членом является нумерацией множества значений их элементов. Со времен Г. Кантора не было научных работ, в которых бы рассматривался систематический конструктивный подход к нумерации элементов дискретных множеств.

Метод исследования основывается на алгебре логики Буля - булевой алгебре, – пропозициональными переменными (высказываниями) которой является последовательности, в частности – числовые. Логические операции над такими переменными, в отличие от известных арифметических операций, способны учитывать свойства самих операндов. Это, соответственно, дает возможность сохранить свойства факторов экономического процесса, для описания которого строится математическая модель. Пути практического применения результатов исследования обусловлены проблемой управления предприятиями в случае моделирования нелинейных процессов в экономике, как и вообще нелинейных динамических процессов; задачами теории алгоритмов, теории чисел, дискретной математики, математического

программирования, оптимального раскроя материалов, кристаллографии и т. д.

На примере теоретико-числовой задачи показана эффективность применения предложенного алгебро-логического подхода для решения четвертой проблемы списка Эдмунда Ландау и установления мощности множества простых чисел в многочлене Эйлера. Есть предположение, что такой подход применим к изучению мощности простых чисел в других формах.

Ключевые слова – булева алгебра, логические операции, многочлен, модель, порождающее множество, последовательность, простое число.

JEL Classification: C61 *УДК 330.4*

A SEQUENTIAL MODEL OF A BOOLE ALGEBRA AND SOME ITS APPLICATIONS

V. Senchukov

The general problem is that since the time of G. Cantor there have been no scientific papers in which a systematically constructive approach to the numbering of elements of discrete sets would be considered. The proposed article is one of the author's works, which covers issues related to the analytical description of objects of a discrete type. The source of all concepts on which the exposition is based is the notion of numbering as a functional mapping of the set of natural numbers onto a given set (not necessarily a numerical nature). In particular, numerical sequences with a known common term are the numbering of the set of values of their elements.

We consider an algebra-logical approach to the description of phenomena and processes of a different nature. The method of investigation is based on Boolean algebra, the propositional variables (statements) of which are sequences, in particular - numerical ones. Logical operations on such variables, unlike known arithmetic operations, are able to take into account the properties of the operands themselves. This, accordingly, makes it possible to preserve the properties of factors of the economic process, for the description of which a mathematical model is constructed.

The aim of the research is the combination of traditional methods of constructing mathematical models with an algebra-logical approach based on the introduction into their construction of a sequential model of Boolean algebra.

Expressive results are obtained concerning questions related to the study of the cardinality of a set of primes in polynomials (this is of great importance in cryptography).

Ways of practical application of the results are due to: the problem of enterprise management in the case of modeling non-linear processes in the economy, as well as in general non-linear dynamic processes; problems of the theory of algorithms, number theory, discrete mathematics, mathematical programming, optimal cutting of materials, crystallography, etc.

Keywords: Boolean algebra, logical operations, polynomial, model, generating set, sequence, prime number.

Під впливом і у світлі ідей, які привели до створення теорії R-функцій [1], розроблено конструктивні засоби, що дозволяють побудувати формулу для функції, що описує дискретну множину, елементи якої мають певні властивості. (Засоби називають конструктивними, якщо в них відразу задається правило (конструкція), за яким функцію, що визначається, можна обчислити.)

Запропонований алгебро-логічний підхід до вивчення властивостей послідовностей є оригінальним, тому ні у вітчизняній, ні зарубіжній науковій літературі немає робіт, які б висвітлювали порушені питання.

Побудову послідовнісної моделі алгебри Буля – алгебри логіки з алфавітом $B_2 = \{0, 1\}$ – почнемо з нестрогого, в описовому плані, ключового поняття.

Логічні операції над послідовностями. Під **логічними операціями над послідовностями** будемо розуміти операції, в результаті виконання яких одержуються послідовності, складені з тих чи інших елементів вихідних послідовностей.

Добре відомі арифметичні операції над послідовностями $(+, -, \times, :)$ зводяться до їх виконання над елементами заданих послідовностей – операндів, при цьому вихідні послідовності немовби "губляться".

Якщо ж йдеться про логічні операції, то результівна послідовність ніби "вбирає" в себе певні властивості операндів. *Наприклад,* яка послідовність буде об'єднанням послідовностей непарних ($x = 2n - 1$) і парних ($y = 2n$) чисел? Ґрунтуючись на суто інтуїтивних міркуваннях, відповідаємо: послідовність натуральних чисел ($z = n$).

Але як формальним шляхом отримати такий результат? У зв'язку з цим виникає проблема створення конструктивних засобів, за допомогою яких можна було б за відомими аналітичними зображеннями заданих послідовностей отримати формулу результату логічної операції над ними.

Як відомо, за допомогою R-функцій, які побудовані на стику математичної логіки, класичних методів прикладної математики та методів кібернетики, єдиним аналітичним виразом можливо описати різні континуальні множини. Звуження R-функцій на дискретні множини не дає такої можливості, оскільки якісні градації "додатність" і "від'ємність" розглядаються на незліченних множинах і не торкаються кожного індивідуума-точки.

Вихідними множинами у цьому викладі є дискретні числові множини, зокрема множина натуральних чисел.

У математичних моделях задач економічного змісту здебільше змінні приймають невід'ємні дійсні значення або невід'ємні цілі значення (наприклад, у задачах цілочислового математичного програмування).

Із відомих означень поняття числової послідовності приймемо таке. **Числовою послідовністю** (**ч/п**) елементів даної множини M називається визначена на множині натуральних чисел $\mathbf{N}$ функція $x = f(n)$, область значень $\operatorname{rng} f$ якої належить розглядуваній множині: $\operatorname{rng} f \subseteq M$, тобто, мовою відображень, $f: \mathbf{N} \to M$. Упорядкована пара $x_n = (n, x)$ – **елемент**, або **член** ч/п $x = f(n)$: x_n ∊ x, де ∊ – символ належності; $f(n)$ – **загальний член** ч/п. Множину $\operatorname{rng} f$ – підмножину M – назвемо **породною множиною** (для) ч/п $x = f(n)$.

Якщо $x = f(n) - const \ \forall n \in \mathbf{N}$, то ч/п називають **стаціонарною**

Послідовність, породна множина якої – порожня множина, називається **порожньою** і позначається через $s_{\varnothing}$ (від лат. *sequence* – послідовність).

Нехай $\nu: \mathbf{N} \to \mathbf{N}$ – деяка зростаюча ч/п: $\nu(n+1) - \nu(n) > 0$. Композиція $y = x(\nu(n))$, або $y = x \circ \nu$ – суперпозиція двох компонент, – називається **підпослідовністю** ч/п x: y ⊏ x, де ⊏ – символ включення.

Відносно послідовності y ч/п $\nu = \nu(n)$ назвемо **нумератором** y в x і позначимо через ν_y. Зрозуміло, що в граничних випадках: $\nu_y = n$ і $\nu_y = s_\varnothing$, отримуємо відповідно: $y = x$ і $y = s_\varnothing$.

Поряд з нумератором однією з характеристик підпослідовності y є **індикатор** μ_y – двозначний предикат, значення якого для кожного її члена визначається булевим алфавітом $B_2 = \{0, 1\}$:

$$(\mu_y)_n = \begin{cases} 1, & \text{якщо } x_n \in y \\ 0, & \text{якщо } x_n \bar{\in} y \end{cases}. \tag{1}$$

де $\in$ ($\bar{\in}$) – знак належності (неналежності).

Індикатори підпослідовностей даної ч/п x є нескінченними булевими векторами:

$$\mu_{s_\varnothing} = (0,\ 0,\ \dots\ ,0,\ \dots),\ \mu_x = (1,\ 1,\ \dots,\ 1,\ \dots).$$

Із наведених означень випливає, що між підпослідовностями та їх нумераторами і індикаторами існує взаємно однозначна відповідність (бієкція): $y \leftrightarrow \nu_y$, $y \leftrightarrow \mu_y$.

Приклад. Нехай універсум $s_\circ$, з породною множиною $\mathbf{N}$, такий:

$$s_\circ = (1,\ 1,\ 2,\ 2,\ 3,\ 3,\ \dots,\ [(n+1)/2],\dots\ ),$$

де $[\cdot]$ – ціла частина числа (Антьє).

Опишемо підпослідовність універсума $s_\circ(n)$: $x = f(n) = s_\circ(\nu_x(n))$, елементи якої визначаються нумератором $\nu_x = (1,\ 4,\ 7,\ 10,\ \dots, 3n-2,\ \dots)$.

Розв'язання. Складаємо композицію $x = s_\circ \circ \nu$, для чого у вираз загального члена універсума замість n підставляємо $\nu_x(n)$:

$$x = s_\circ \circ \nu = \left[\frac{\nu_x(n)+1}{2}\right] = \left[\frac{(3n-2)+1}{2}\right].$$

Остаточно, з урахуванням, що цілий доданок можна виносити за символ цілої частини, отримуємо:

$$x = f(n) = \left[\frac{2n + (n-1)}{2}\right] = n + \left[\frac{n-1}{2}\right].$$

Індикатор μ_x послідовності x має вигляд:

$$\mu_x = (1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ \ldots).$$

В теоретико-числових дослідженнях часто в якості універсума $s_\circ$ виступає послідовність натуральних чисел: $s_\circ = s_\circ(n) = n$, і тоді універсум нумераторів $\nu_\circ(n) = n$ співпадає з основною послідовністю.

Звичайно розглядаються підпослідовності деякої фіксованої ч/п, яка називається **основною,** або **універсальною** (**універсумом**), і позначається через $s_\circ$. Універсум нумераторів – послідовність натуральних чисел ($\nu_\circ(n) = n$), індикаторів – стаціонарна ч/п ($\mu_\circ(n) = 1$).

Перейдемо до формалізації наведеного вище описового означення (дефініції) логічних операцій над ч/п [2; 3].

Щоб відрізняти такі операції від операцій алгебри множин і алгебри логіки, для них використовуються інші символи.

Нехай x, y, z – ч/п, які належать множині підпослідовностей деякого універсума $s_\circ$; $\nu_x = a(n)$, $\nu_y = b(n)$, $\nu_z = c(n)$ – відповідні нумератори; $rng\, a = A$, $rng\, b = B$, $rng\, c = C$ – породні множини нумераторів, елементами яких є натуральні числа.

Логічною сумою (**s-об'єднанням $\sqcup$**) двох послідовностей x, y називається ч/п z, породна множина нумератора якої є об'єднанням породних множин нумераторів вихідних послідовностей:

$$z = x \sqcup y \ \rightleftharpoons\ C = A \cup B. \tag{2}$$

Логічним добутком (**s-перетином $\sqcap$**) двох послідовностей x, y називається ч/п z, породна множина нумератора якої є перетином (перерізом) породних множин нумераторів вихідних послідовностей:

$$z = x \sqcap y \ \rightleftharpoons \ C = A \bigcap B. \qquad (3)$$

Логічною різницею (s**-різницею** $\llcorner$) двох послідовностей x, y називається ч/п z, породна множина нумератора якої є різницею породних множин нумераторів вихідних послідовностей:

$$z = x \llcorner y \ \rightleftharpoons \ C = A \setminus B. \qquad (4)$$

Різниця $z = s_{\circ} \llcorner x$ називається s**-доповненням** послідовності x і позначається через $\urcorner x$:

$$z = \urcorner x \ \rightleftharpoons \ C = \mathbf{N} \setminus A = A^{'}. \qquad (5)$$

Формалізовані логічні операції об'єднуються загальною назвою – s**-операції.**

Нехай $M(s)$ – множина ч/п, яка є замкненою щодо композицій, $M(\nu)$ – множина нумераторів ч/п, а $M(rng\,\nu)$ – відповідна сукупність породних множин нумераторів, $M(\mu)$ – множина індикаторів числових послідовностей із $M(s)$.

Теорема. Множина послідовностей $M(s)$ з визначеними на ній s-операціями є булевою алгеброю:

$$A_s = (M(s);\ \sqcup, \sqcap, \urcorner). \qquad (6)$$

Доведення. Кожній послідовності із множини $M(s)$, замкненій відносно композицій, відповідає породна множина нумератора. Згідно означень (2) – (5) логічних операцій над ч/п алгебра A_s і алгебра породних множин нумераторів:

$$A_{rng\,\nu} = (M(rng\,\nu);\ \cup, \bigcap, ^{'}), \qquad (7)$$

ізоморфні; це і означає, що алгебра A_S – булева алгебра.

Алгебра A_S називається **булевою алгеброю послідовностей**, або коротко – s**-алгеброю.**

Завдяки бієкції між множинами $M(s)$, $M(\nu)$, $M(rng\,\nu)$, $M(\mu)$ і однотипності операцій робимо висновок про ізоморфність усіх відповідних алгебр.

У плані прикладних досліджень можливості пропонованої моделі досить великі, оскільки з точки зору алгебри природа елементів, з яких складені послідовності, цілковито "байдужа". Це можуть бути підприємства, показники ефективності їхньої роботи та інші чинники.

Теоретико-числові дослідження на засадах s-алгебри торкаються питання потужності множини простих чисел у многочленах, що є важливим із точки зору криптографії – науки про математичні методи забезпечення конфіденційності , цілісності й автентичності інформації.

Щодо простих чисел, досі існує багато відкритих питань, найбільш відомі з яких були перелічені Едмундом Ландау на П'ятому Міжнародному математичному конгресі, який відбувся в 1912 році в Кембриджському університеті. У своєму виступі він запропонував список проблем теорії чисел, аналогічний до списку Гільберта. Жодна з чотирьох задач списку Ландау досі повністю не розв'язана.

Одна з проблем, четверта, така: чи є нескінченною множина простих чисел вигляду x^2+1, де x – натуральне число?

Більш загальну постановку задачі знаходимо в роботах Вацлава Серпінського [4; 5]: чи існують многочлени, які для натуральних значень змінної дають нескінченну множину простих чисел? Існують многочлени першого степеня, наприклад, двочлен $2x+1$, що містить серед своїх значень усі прості числа, але невідомо жодного многочлена степеня, більшого від одиниці, який містив би зліченну множину простих чисел. Узагальненням четвертої проблеми Едмунда Ландау є припущення: для кожного натурального k існує нескінченно багато простих чисел вигляду x^2+k, де x – натуральне число.

Ще в першій половині XIX століття займались питанням: які із арифметичних прогресій включають нескінченну множину простих чисел.

Якщо є арифметична прогресія з першим членом a і різницею r, тобто прогресія:

$$a,\ a+r,\ a+2r,\ a+3r,\ \ldots,\ \text{або}\ a+kr,\ \text{де}\ k=0,1,2,\ldots,$$

і якщо натуральні числа a і r мають спільний дільник $d=(a,r)>1$, то всі члени прогресії діляться на d. Отже, всі її члени, крім, можливо, першого, складені числа. Виникає природне питання, а який стан справ у разі коли $d=1$?

Знаний французький математик Лежен-Діріхле довів [6], що кожна арифметична прогресія $a+kr$ $(k=0,1,2,...)$, де k і r – взаємно прості числа, містить нескінченну множину простих чисел, але її доведення не є елементарним. Елементарне доведення теореми можна знайти у книзі Е. Троста [7].

У роботі В. Серпінського [4] відзначається, що не було б легше довести, що в кожній арифметичній прогресії, перший член і різниця якої суть взаємно прості числа, є принаймні одне просте число. Із цього твердження легко було б вивести теорему Лежен-Діріхле. Наведемо відповідний фрагмент із книги В. Серпінського, названий автором **теоремою Серпінського** (*про арифметичні прогресії*):

"Доведемо, що з теореми (А):

в кожній арифметичній прогресії, перший член і різниця якої – взаємно прості числа, існує (щонайменше) одне просте число,

випливає теорема Лежен-Діріхле:

в кожній арифметичній прогресії, перший член і різниця якої – взаємно прості числа, існує нескінченна множина простих чисел.

Нехай

$$a,\ a+r,\ a+2r,\ \dots \qquad (1)$$

буде арифметичною прогресією, яка задовольняє умови кожної з названих теорем.

Кожна з прогресій

$$a+kr,(a+kr)+r,\ (a+kr)+2r,\dots \text{ або } (a+kr)+mr, \qquad (2)$$

де $m=0,1,2,\dots$ і k – фіксоване натуральне число, яке задовольняє умову кожної з цих теорем. В кожній із арифметичних прогресій (2) на підставі теореми (А) є просте число, більше за k, оскільки перший член кожної з цих прогресій більший від k.

Прогресію (2) ми отримаємо з прогресії (1), пропускаючи k перших її членів. Отже, в прогресії (1) є просте число, більше від k, де k – довільне натуральне число; отже, простих чисел у ній нескінченна множина"

Вирішення четвертої проблеми списку Ландау потребує розв'язання невизначених (діофантових) рівнянь другого степеня з двома змінними x, y параболічного типу [8]:

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0, \tag{8}$$

де A, B, C, D, E, F – сталі (коефіцієнти при невідомих), $B^2 - 4AC = 0$.

Для розв'язання рівняння (8) скористаємося вирішувачем, створеним відомим в Аргентині та за її межами інженером – електронником Даріо Алехандро Альперном (1969 р. н.) [9]. Згідно з алгоритмом, за яким невідомі x і y можуть бути тільки цілими числами, позначено: $g = \text{gcd}(A, C)$ – найбільший спільний дільник A і C, $a = A/g$, $b = B/g$, $c = C/g \geq 0$ (знак $\sqrt{c}$ визначається знаком дробу B/A); тоді $b^2/4 = ac$.

Відповідні розв'язки описуються співвідношеннями:

$$\begin{aligned} x &= \sqrt{c}g(\sqrt{a}E - \sqrt{c}D)t^2 - (E + 2\sqrt{c}gu_i)t - \frac{\sqrt{c}gu_i^2 + Eu_i + \sqrt{c}F}{\sqrt{c}D - \sqrt{a}E}, \\ y &= \sqrt{a}g(\sqrt{c}D - \sqrt{a}E)t^2 + (D + 2\sqrt{a}gu_i)t + \frac{\sqrt{a}gu_i^2 + Du_i + \sqrt{a}F}{\sqrt{c}D - \sqrt{a}E}, \end{aligned} \tag{9}$$

де t – будь-яке ціле додатне число (параметр);

u_i – скінченний кортеж сталих, які визначають серії розв'язків, за умови, що чисельники в останніх доданках (9) кратні знаменнику $\sqrt{c}D - \sqrt{a}E$; значення u_i належать діапазону $0 \leq u < |\sqrt{c}D - \sqrt{a}E|$.

Наприклад, для рівняння $8x^2 - 24xy + 18y^2 + 5x + 7y + 16 = 0$ маємо:

$$\sqrt{c}\,D - \sqrt{a}\,E = -3\cdot 5 - 2\cdot 7 = -29 \text{ і } \sqrt{a}gu^2 + Du + \sqrt{a}F = 4u^2 + 5u + 32.$$

Значення u знаходимо в діапазоні $[0,29)$, для яких $4u^2+5u+32$ кратне числу 29: $u_0=2$, $u_1=4$, і записуємо дві серії розв'язків:

для $u_0=2$: $\left[\begin{array}{l} x=-174t^2-17t-2, \\ y=-116t^2-21t-2; \end{array}\right.$ для $u_1=4$: $\left[\begin{array}{l} x=-174t^2-41t-4, \\ y=-116t^2-37t-4. \end{array}\right.$

Дослідження потужності множини простих чисел у формі $\boldsymbol{x^2+1}$. Коли $x=1$, маємо єдине парне просте число – двійку. Непарні прості числа, якщо такі є, отримаємо за парних $x\in\mathbf{N}$, тому перейдемо до вивчення форми $f(x)=4x^2+1$. Вісім перших членів відповідної послідовності такі:

$$f=4x^2+1=(\underline{5}_{\ 12}\ \underline{17}_{\ 20}\ \underline{37}_{\ 28}\ 65_{\ 36}\ \underline{101}_{\ 44}\ 145_{\ 52}\ \underline{197}_{\ 60}\ \underline{257}_{\ 68}\ldots), \tag{10}$$

де між елементами ч/п зазначені перші скінченні різниці – різниці між наступними і попередніми членами, а прості числа підкреслені.

Помічаємо, що $5, 17, 101, 197$ є елементами арифметичної прогресії $6n-1$ з першим членом, який дорівнює п'яти, і різницею, яка дорівнює шести. Оскільки перший член і різниця взаємно прості числа: $(5,6)=1$, то за теоремою Лежен-Диріхле прогресія містить нескінченно багато простих чисел. Наведемо перші вісім із них (вони підкреслені):

$$\begin{gathered}\beta(n)=6n-1= \\ =(\underline{5},\ \underline{11},\ \underline{17},\ 23,\ \underline{29},\ 35,\ \underline{41},\ 47, 53,\ \underline{59}, 65,\ \underline{71}, 77, 83, 89, 95, \underline{101}, \ldots).\end{gathered} \tag{11}$$

Знайдемо s-перетин прогресії $\beta(n)$ і $f(x)$, для чого розв'яжемо діофантове рівняння другого степеня (параболічного типу):

$$f \sqcap \beta:\ 4x^2+1=6n-1 \ \Rightarrow\ 3n=2x^2+1 \ \Rightarrow\ 2x^2-3n+1=0. \tag{12}$$

Згідно з (9) рівняння (12) має дві серії розв'язків (тимчасово n замінимо на y):

а) $\left[\begin{array}{l} x = 3t - 2 \\ y = 6t^2 - 8t + 3 \end{array}\right.$; б) $\left[\begin{array}{l} x = 3t - 1 \\ y = 6t^2 - 4t + 1 \end{array}\right.$, t – натуральне.

Легко переконатися, що $x = 3t$ не задовольняє рівняння $2x^2 - 3n + 1 = 0$.

Розв'язки рівняння (12) визначають послідовності однакових елементів в обох формах. Припустимо, що після деякого $n = n_0$ прості числа у формі f вичерпалися (скінчилися). Це водночас означатиме, що для $n > n_0$ не знайдеться жодного простого числа вигляду $6n - 1$, що неможливо з огляду на зліченність множини простих у формі $\beta(n)$.

Висновок. Форма f містить нескінченну множину простих чисел.

Позначимо через P_∞ властивість $<$ множина містить безліч простих чисел $>$ тоді маємо:

$$rng\ \beta \,|\, P_\infty \;\Rightarrow\; rng\ f \,|\, P_\infty, \tag{13}$$

тобто із зліченності простих у формі $\beta(n) = 6n - 1$ випливає зліченність множини простих чисел у формі $f = x^2 + 1$.

Вважаємо, що на розглянутому шляху лежать рішення для інших теоретико-числових проблем щодо потужності множини простих чисел у многочленах. Зокрема, "чи існує для кожного натурального k нескінченно багато простих чисел вигляду $f = x^2 + k$, де x – натуральне число" (узагальнення четвертої проблеми Едмунда Ландау). Для застосування розглянутої методики таку форму слід розбити на дві:

1) x парне, k непарне: $f = 4x^2 + 2k - 1$;

2) x непарне, k парне: $f = (2x - 1)^2 + 2k = 4x(x - 1) + 2k + 1$.

Є переконання, що як форма $f = x^2 + 1$, так і форма $f = x^2 + k$ містить зліченну множину простих чисел. Технічний бік цього питання ще не розглядався.

Потужність множини простих чисел у многочлені Ейлера. Многочленом Ейлера називають тричлен $f = x^2 - x + 41$. Відомо, що за $x = 1, 2, \ldots, 40$ він дає різні прості числа [10]:

$$f = (41\,{}_2\,43\,{}_4\,47\,{}_6\,53\,{}_8\,61\,{}_{10}\,71\,{}_{12}\,83\,{}_{14}\,97\,{}_{16}\,113\,{}_{18}\,131\,{}_{20}\,\ldots{}_{78}\,1601). \qquad (14)$$

Висловлено припущення [11], що існує безліч натуральних x, для яких f є простим числом. Покажемо, що це дійсно так.

За аналогією з (12) складемо рівняння $f = \beta$:

$$x^2 - x + 41 = 6n - 1 \quad \Rightarrow \quad |\text{ замінимо } n \text{ на } y\,| \quad \Rightarrow$$

$$\Rightarrow \quad x^2 - x - 6y + 42 = 0. \qquad (15)$$

Це рівняння типу (8) із коефіцієнтами:

$$A = 1,\; B = C = 0,\; D = -1,\; E = -6,\; F = 42.$$

Обчислюємо сталі складові розв’язку:

$$g = \gcd(A, C) = \gcd(1, 0) = 1,\; a = A/g = 1,\; b = B/g = 0,\; c = C/g = 0.$$

Співвідношення (9) набувають вигляду:

$$x = 6t + u_j,\quad y = 6t^2 + (2u_j - 1)t + (u_j^2 - u_j)/6 + 7, \qquad (16)$$

де згідно з (9) u_j – скінченний кортеж сталих, які визначають серії розв'язків, за умови, що чисельник дробу у виразі для y кратний знаменнику 6; значення u_j належать діапазону $0 \le u < 6$.

Знаходимо $u_j = 0, 1, 3, 4$. Отже, рівняння (15) для має чотири серії розв'язків, у першій із яких, тобто для $u_0 = 0$, параметр t береться додатним, оскільки x має бути натуральним, а в інших $t \ge 0$:

для $u_0 = 0$: $\left[\begin{array}{l} x = 6t \\ y = 6t^2 - t + 7 \end{array}\right.$; для $u_1 = 1$: $\left[\begin{array}{l} x = 6t + 1 \\ y = 6t^2 + t + 7 \end{array}\right.$; для $u_2 = 3$: $\left[\begin{array}{l} x = 6t + 3 \\ y = 6t^2 + 5t + 8 \end{array}\right.$; для $u_3 = 4$: $\left[\begin{array}{l} x = 6t + 4 \\ y = 6t^2 + 7t + 9 \end{array}\right.$.

Наведені серії розв'язків, знайдених вручну, узгоджуються з результатами вирішувача:

x = 6�u y = 6�u^2 - �u + 7	x = 6�u + 1 y = 6�u^2 + �u + 7	x = 6�u + 3 y = 6�u^2 + 5�u + 8	x = 6�u + 4 y = 6�u^2 + 7�u + 9

Розв'язки рівняння (15) визначають послідовності однакових елементів у формі $f = x^2 - x + 41$ і арифметичній прогресії $\beta(n) = 6n - 1$. Припустимо, що після деякого $n = n_0$ прості числа у формі f вичерпалися (скінчилися). Це водночас означатиме, що для $n > n_0$ не знайдеться жодного простого числа вигляду $6n - 1$, що неможливо з огляду на зліченність множини простих у формі $\beta(n)$.

Висновок. Форма f містить нескінченну множину простих чисел.

Перші, для $t \in [0,7]$, елементи кожної з серій наведені в табл. 1.

Таблиця 1

Фрагмент послідовності спільних елементів форм $f(x)$ і $\beta(n)$

u \ t		0	1	2	3	4	5	6	7…
$u_0 = 0$	$f = \beta$		71	173	347	593	911	1301	1763…
$u_1 = 1$		41	83	197	383	641	971	1373	1847…
$u_2 = 3$		47	113	251	461	743	1097	1523	2021…
$u_3 = 4$		53	131	281	503	797	1163	1601	2111…

За стовпцями та рядками числа розташовуються в порядку зростання. Складені числа підкреслені.

Гадаємо, що численні нові результати щодо потужності множини простих чисел у многочленах отримаємо, якщо залучити до розгляду степеневі лишки [12].

Насамкінець зазначимо, що алгебро-логічний підхід до аналітичного опису множини точок цілочислового евклідового простору, є основою методу накладання цілочислових сіток (НЦС) в задачах цілочислового математичного програмування [13; 14]. Суть методу полягає в такому: здійснюємо логічний перетин нумерації цілочислового простору з областю допустимих розв'язків, які визначаються сукупністю обмежень, що накладаються на змінні; потім серед елементів отриманого числового масиву визначаємо оптимальне значення цільової функції і знаходимо відповідний оптимальний план (або плани), тобто за відомим оптимумом установлюємо координати точок екстремуму.

Як точний метод "грубої сили" він застосовний до задач: із довільною обмеженою областю (опуклою, неопуклою; однозв'язною, многозв'язною); з будь-якою цільовою функцією (лінійною, нелінійною; неперервною, розривною; диференційовною, недиференційованою).

Завдяки вказаним достоїнствам метод НЦС має досить широку сферу можливих практичних застосувань. Це, перш за все, моделювання нелінійних процесів в економіці [15], а саме: укрупнення планування виробництва, планування асортименту виробів, маршрутизація виробництва виробу, управління технологічним процесом і т. ін.

Звичайно, метод НЦС застосовний до розв'язання інших задач математичного програмування, і узагалі до задач дискретної математики, які потребують аналітичного опису дискретних множин: в теорії кодування, в задачах оптимального розкрою матеріалів.

Впровадження методу НЦС в кристалографію дає можливість здійснити нумерацію вершин кристалічної решітки і описувати її підпослідовності, які мають ті чи інші властивості. Якщо торкатися криптографії (до речі, саме в криптографії метод повного перебору називають методом "грубої сили" (від англ. *brute force*)), то, спираючись на структуру послідовності простих чисел, стає можливим розв'язання криптографічної задачі шляхом перебору всіх можливих варіантів ключа.

Справа обчислювачів з'ясувати, до якого класу складності слід віднести задачі, що розв'язуються методом НЦС. Сподіваємось, зважаючи на бурхливий розвиток електронної, і, разом із тим, обчислювальної техніки, що в методу НЦС як точного методу "грубої сили" є майбутнє.

Література:

1. Рвачев В. Л. Теория R-функций и некоторые ее приложения / В. Л. Рвачев. – Київ : Наукова думка, 1982. – 552 с.

2. Сенчуков В. Ф. Послідовнісна модель булевої алгебри / В. Ф. Сенчуков // Доп. АН УРСР. Сер. А. – 1988. – №2. – С. 19 – 20.

3. Сенчуков В. Ф. Логические операции над последовательностями и закон простых чисел / В. Ф. Сенчуков // Докл. АН УССР. Сер. А. – 1988. – №6. – С. 20 – 23.

4. Серпинский В. Сто простых, но одновременно трудных вопросов арифметики / В. Серпинский ; перевод с польского В. А. Голубева. – Москва : Учпедгиз, 1961. – 76 с.

5. Серпинский В. Что мы знаем и чего не знаем о простых числах / В. Серпинский; перевод с польского И. Г. Мельникова. – Москва-Ленинград : ГИФМЛ, 1963. – 92 с.

6. Гельфонд А. О. Элементарные методы в аналитической теории чисел / А. О. Гельфонд, Ю. В. Линник. – Москва : Физматгиз, 1962. – 272 с.

7. Трост Э. Простые числа / Э. Трост ; перевод с нем. Н. И. Фельдмана под ред. А. О. Гельфонда. – Москва : ГИФМЛ, 1959. – 136 с.

8. Маркушевич А. И. Возвратные последовательности / А. И. Маркушевич. – 2-е издание. – Москва : Наука, 1975. – 48 с.

9. Alpern, Dario. Quadratic Diophantine Equation Solver [Electronic resource] / Dario, Alpern. – Access mode : www.alpertron.com.ar/quad.htm.

10. F. Le Lionnais. Les Nombres Remarquables. – Paris : Hermann, 1983. – P. 88–144.

11. Голубев В. А. Число групп простых чисел и простых чисел степенных форм / В. А. Голубев // Изв. вузов. – 1962. – № 6 (31). – С. 28–33.

12. Виноградов И. М. Основы теории чисел / И. М. Виноградов. – Москва : Наука, 1981. – 176 с.

13. Сенчуков В. Ф. Цілочислові сітки на площині в задачах дискретної оптимізації / В. Ф. Сенчуков // Економіка розвитку. – 2014. – № 3 (71). С. 107–112.

14. Сенчуков В. Ф. Просторові цілочислові сітки в задачах дискретної оптимізації / В. Ф. Сенчуков // Управління розвитком. – 2015. – № 2 (180). С. 116–123.

15. Экономическая энциклопедия / под ред. А. И. Абалкина. – Москва : Экономика, 1999. – 1056 с.

References:

1. Rvachev V. L. *Teoriya R-funкtsy i neкotorye eye prilozheniya* [Rvachev V. L. Theory of R-functions and some of its applications] / V. L. Rvachev. – Кiev : Nauкova duмкa, 1982. – 552 p.

2. Senchukov V. F. *Poslidovnisna мodel bulevoi alhebry* [A sequential model of the Boolean algebra] / V. F. Senchukov // Dop. AN USSR. Ser. A. – 1988. – №2. – P. 19 – 20.

3. Senchukov V. F. *Logicheskie operatsii nad posledovatelnostyami i zakon prostykh chisel* [Logical operations on sequences and prime number theorem] / V. F. Senchukov // Dokl. AN USSR. Ser. A. – 1988. – №6. – P. 20 – 23.

4. Serpinskiy V. Sto prostykh i odnovremenno trudnykh voprosov arifmetiki [Hundred simple but at the Same Time Difficult Questions of Arithmetic] / V. Serpinskiy. – Moskva : Uchpedgiz, 1961 – 76 p.

5. Serpinskiy V. *Chto my znayem i chego ne znayem o prostykh chislakh* [What we know and do not know about prime numbers] / V. Serpinskiy, perevod s polsкogo I. G. Melniкova. – Moskva-Leningrad: Fizmatgiz, 1963 – 92 p.

6. Gelfond A. O. *Eleмenmarnye мetody v analiticheskoy teorii chisel* [Elementary methods in analytic number theory] / A. O. Gelfond, Yu. V. Linniк. – Mosкva : Fizmatgiz, 1962. – 272 p.

7. Trost E. *Prostye chisla* [Prime numbers] / E. Trost; perevod s neм. N. I. Feldмana pod red. A. O. Gelfonda. – Mosкva : GIFML, 1959. – 136 p.

8. Marкushevich A. I. *Vozvratnye posledovatelnosti* [Return sequences] / A. I. Marкushevich. – 2-e izdanie. – Mosкva : Nauкa, 1975. – 48 p.

9. Alpern, Dario. Quadratic Diophantine Equation Solver [Electronic resource] / Dario, Alpern. – Access mode : www.alpertron.com.ar/quad.htm.

10. F. Le Lionnais. Les Nombres Remarquables. – Paris : Hermann, 1983. – P. 88–144.

11. Golubev V. A. *Chislo grupp prostykh chisel i prostykh chisel stepennykh forм* [Number of groups of prime numbers and primes of power forms] / V. A. Golubev // Izv. vuzov. – 1962. – № 6 (31). – P. 28–33.

12. Vinogradov I. M. *Osnovy teorii chisel* [Fundamentals of number theory] / I. M. Vinogradov. – Mosкva : Nauкa, 1981. – 176 p.

13. Senchukov V. F. *Tsilochislovi sitky na ploshchini v zadachakh dyskretnoi optymizatsii* [Integer nets on the plane in the tasks of discrete optimization] / V. F. Senchukov // Ekonomika rozvytku – 2014. – № 3 (71). – P. 107–112.

14. Senchukov V. F. *Prostorovi tsilochislovi sitky v zadachakh dyskretnoi optyminizatsii* [Spatial integer meshes in discrete optimization problems] / V. F. Senchukov // *Upravlinnia rozvytkom.* – 2015. – № 2 (180). P. 116–123.

15. *Екопомісheскуа entsyкlopediya* [Economic Encyclopedia] / pod red. A. I. Abalкina. – Mosкva : Екопомікa, 1999. – 1056 p.

Інформація про автора

Сенчуков Віктор Федорович – канд. фіз.-мат. наук, доцент кафедри вищої математики й економіко-математичних методів Харківського національного економічного університету імені Семена Кузнеця (61166, Україна, м. Харків, пр. Науки, 9а, e-mail: Viktor. Senchukov@m.hneu.edu.ua).

Информация об авторе

Сенчуков Виктор Федорович – канд. физ.-мат. наук, доцент кафедры высшей математики и экономико-математических методов Харьковского национального экономического университета имени Семена Кузнеца (61166, Украина, г. Харьков, пр. Науки, 9а, e-mail: Viktor. Senchukov@m.hneu.edu.ua).

Information about the author

Victor Senchukov – PhD in Physics and Mathematics, docent of the Department of Higher Mathematics and Economics and Mathematical Methods of Simon Kuznets Kharkiv National University of Economics (9a Science Prospekt, Kharkiv, Ukraine, 61116, e-mail: Viktor. Senchukov@m.hneu.edu.ua).