УДК 519.612
DOI: 10.32626/2308-5878.2022-23.5-13

В. С. Абрамчук, канд. фіз.-мат. наук,
І. В. Абрамчук, старший викладач
Вінницький національний технічний університет, м. Вінниця

АЛГОРИТМ РОЗКЛАДУ ЦІЛИХ ЧИСЕЛ І ГЛАДКОГО НАБЛИЖЕННЯ ФУНКЦІЙ

Узагальнено задачу про розклад степенів на розклад цілих додатних чисел за послідовністю степенів різних порядків, виведені умови розкладу, побудовано алгоритм розкладу. Алгоритм заснований на двох процедурах: 1) досягнення мінімуму нев'язки на кожному кроці алгоритму, 2) прискорення швидкості розкладу шляхом розширення локального базису за рахунок пониження показника степенів розкладу, що забезпечує скінченність алгоритму. Алгоритм володіє такими факторами ефективності, як висока швидкість розкладу, простота реалізації, можливість різних варіантів розкладу чисел у розширеному, звуженому, розрідженому базисах, що захищає закодовану інформацію від зовнішніх впливів. Алгоритм можна застосувати для кодування цифрової інформації великих об'ємів за базисними системами малих розмірностей.

Розклад додатних чисел за послідовністю степенів є оптимальним і коректним. Оптимальність розкладу випливає з умови, що на кожному кроці алгоритму досягається мінімальне значення нев'язки у просторі змішаних параметрів $x \in N$, $y \in R$. Коректність алгоритму є наслідком того, що при зменшенні нев'язки алгоритм розширює базис розкладу за рахунок зменшення показників степеня на одиницю. Перейшовши від дискретної моделі до неперервної шляхом заміни степенів на степеневі функції, дістанемо гладке наближення погано зумовленої функції в околі розкладу. Побудова позіномиальних многочленів на базі гладких многочленів є одним з перспективних напрямів інтегрування погано зумовлених недиференційовних функцій, гладкої заміни змінних в теорії катастроф.

Позіноми (функції із змінним показником степеня) прогнозують крок розбиття проміжка інтегрування на частини, оскільки визначають логарифмічну швидкість зміни довільної монотонної функції. Метод розкладу цілих чисел забезпечує оптимальний розклад на суму степенів, і, тому перехід від дискретної моделі до неперервної в околі розкладу шляхом заміни степенів на степеневі функції, дозволяє отримати високу точність наближення.

Ключові слова: *розкладання степенів цілих чисел, алгоритм кодування, гладке наближення погано зумовлених функцій.*

Вступ. В адитивній теорії чисел досліджуються задачі про розбиття чисел на доданки того чи іншого виду. До таких задач належать, наприклад, проблеми Варінга, Гольдбаха-Ейлера, Ферма. Методи Шнірельмана і Виноградова відкрили нові можливості для розв'язання багатьох проблемних задач адитивної теорії чисел [1], ряд з яких залишились не розв'язаними до сьогодення. Однією з важливих практичних задач є розроблення алгоритмів кодування великих об'ємів цифрової інформації. До таких алгоритмів ставляться вимоги надійності методу, швидкодії обробки інформації, захисту інформації від зовнішніх впливів. Наприклад, твердження, що ступінь захисту криптографічної схеми зумовлений складністю розкладу великих цілих чисел на множники, не доведене [9].

Методи адитивної теорії чисел за своєю структурою тісно пов'язані з методами наближення погано зумовлених функцій, оскільки в обох задачах достатньо знаходити оптимальні складові.

Постановка проблеми. Розробити методи:

1) кодування цифрової інформації великих об'ємів на основі базисних систем малих розмірностей;
2) гладкого наближення погано зумовлених недиференційовних функцій.

Мета статті:

1) узагальнити задачу розкладу степенів цілих додатних чисел, вивести умови розкладу, побудувати алгоритм розкладу (алгоритм кодування);
2) розробити алгоритм гладкого наближення погано зумовлених недиференційовних функцій.

Основна частина.

1. Алгоритм розкладу цілих додатних чисел $w \in D(w,n)$ за степенями $x_{i,k}^{n-k}$, $x_{i,k} \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 3$, $k \in \{0,1,...,n-2\}$, методом мінімізації нев'язки (модуля нев'язки). Для заданого показника $n \in \mathbb{N}$, $n \geq 3$, ціле додатне число w задовольняє умову розкладу $D(w,n)$, якщо виконується нерівність $M^n > \frac{w}{2}$, де $M = \max\left\{x \in \mathbb{N} : x^n < w\right\}$. Позначимо $\bar{x} = \sqrt[n]{w}$.

Лема. Якщо ціле додатне число w задовольняє умову розкладу $D(w,n)$ для заданого $n \in \mathbb{N}, n \geq 3$, то w задовольняє умови розкладу $D(w,n-k)$ для всіх $k = 0,1,...,n-2$.

Доведення леми випливає із ланцюжка нерівностей для додатних чисел: $M^n > \frac{w}{2} \Rightarrow M > \frac{\overline{x}}{\sqrt[n]{2}} \Rightarrow M^{n-k} > \frac{\overline{x}^{n-k}}{2^{\frac{n-k}{n}}} > \frac{\overline{x}^{n-k}}{2}$. Остання нерівність є наслідком нерівності $2^{\frac{n-k}{n}} = 2^{1-\frac{k}{n}} < 2$, оскільки $0 < \frac{k}{n} < 1$, $k = 0,1,...,n-2$.

Теорема 1. Ціле додатне число w, що задовольняє умову розкладу $D(w,n)$ для заданого показника $n \in \mathbb{N}, n \geq 3$, розкладається на суму степенів $x_{i,k}^{n-k}$, $x_{i,k} \in \mathbb{N}$, $k \in \{0,1,...,n-2\}$,

$$w = \sum_{k=0}^{n-2} \sum_{i \in J_k} \gamma_{i,k} x_{i,k}^{n-k}, \qquad (1)$$

де $\gamma_{ik} = \pm 1$, множина індексів J_k формується для кожного $k \in \{0,1,...,n-2\}$, поки не обнулиться нев'язка $\delta_{i,k} = \Delta_k - x_{i,k}^{n-k} - y_{i,k}^{n-k}$ або $|\delta_{i,k}| \leq 2^2$.

Доведення теореми (алгоритм розкладу). Якщо ціле додатне число w задовольняє умову $D(w,n)$ для заданого показника $n \in \mathbb{N}$, $n \geq 3$, то на відрізку $[0;\overline{x}]$ існують дві неперервні монотонні функції: спадна $u = w - x^n$ і зростаюча $v = y^n$, які перетинаються в єдиній точці $d < M = \max\{x \in \mathbb{N} : x^n < w\}$, $d \in \mathbb{R}$ (прийнято, що вісі x, y збігаються). Тому для всіх цілих додатних чисел $x \in [m;M]$, $m = \text{ceil}(d)$, існують числа $\overline{y} \in \mathbb{R}$ такі, що $w = x^n + \overline{y}^n$. Якщо $\overline{y} \in \mathbb{N}$, то розклад завершений, у протилежному випадку $\beta < \overline{y} < \beta + 1$, $\beta \in \mathbb{N}$, $\beta = \text{trunc}(\overline{y})$ і за y виберемо $y = \beta$, якщо мінімізується нев'язка $\Delta(x,y) = w - x^n - y^n \geq 0$; якщо мінімізується модуль нев'язки, то $y = \beta$, якщо $\overline{y} - \beta \leq 0.5 i y = \beta + 1$ у протилежному випадку. В обох випадках $|\Delta(x,y)| = |w - x^n - y^n|$ – мінімізується модуль нев'язки для цілих додатних чисел x, y. Замінивши w на $|\Delta|$ алгоритм продовжити, поки виконуватиметься умова розкладу, або не обнулиться нев'язка, або $|\Delta(x,y)| \leq 2^2$. Якщо умова розкладу не ви-

конуватиметься, то послідовно замінюватимемо показник степеня на $n-k$, $k=0,1,...,n-2$ (розширюватимемо локальний базис, який звузився при мінімізації нев'язки). У протилежному випадку для $n-k=2$ модуль нев'язки $|\Delta(x,y)| \le 2^2 < 3^2+1=10$ і всі числа із проміжку $[1;10]$ можна подати як степені, замінивши 2 на 3^2-2^3+1. Алгоритм завершений. Швидкий розклад(швидке кодування цифрової інформації великих об'ємів) пояснюється тим, що нев'язка у просторі $x \in \mathbb{N}, \bar{y} \in \mathbb{R}$, мінімізується точно і похибка виникає лише за рахунок заміни $\bar{y} \in \mathbb{R}$ на $y \in \mathbb{N}$.

Теорему доведено.

Наведемо приклади розкладів:

$$63^3 = 250\,047 = 58^3 + 38^3 + 4^3 - 1; 90^5 = 5\,904\,900\,000 =$$

$$= 87^5 + 62^5 + 21^5 + 13^5 + 10^5 + 4^5 + 6^4 + 3^4 + 5^3 + 3^3 + 3^2 + 2^2 + 1;$$

для $w \in D(w,6)$

$$w = 100000002 = 20^6 + 18^6 + 11^6 + 7^6 + 9^5 + 8^5 + 9^4 + 3^4 + 4^3 + 3^3 + 4^2 + 2,$$

$$2 = 3^2 - 2^3 + 1;$$

виконати розклад $w_1 \in D(w_1,5)$ за базисом простих чисел:

$$w_1 = 6500000 = 23^5 + 7^5 + 13^4 + 11^4 + 7^4 + 5^4 + 7^3 + 5^3 + 11^2 + 5^2 + 2^3.$$

2. Ефективність алгоритму розкладу цілих додатних чисел за степенями $x_{i,k}^{n-k}, k=0,1,\ldots,n-2, n \in \mathbb{N}, n \ge 3$. Аналіз варіантів розкладу. Базисом розкладу цілих додатних великих чисел w за степенями є підмножина цілих додатних чисел з множини $\mathbb{N}$, за допомогою якої для заданого $n \in \mathbb{N}, n \ge 3$ (заданої послідовності показників $(n, n-1, \ldots, 2)$) формується розклад (1). Якщо розклад числа w у добуток простих множників вимагає наявності усіх простих множників числа w, то розклад w на суму степенів може здійснюватися для різних базисів, обов'язковою є лише наявність найменших елементів $\{1,2,3,\ldots\}$ базису.

Ефективність алгоритму розкладу залежить від швидкості розкладу, надійності розкладу, однозначності розкладу, простоти алгоритму, захисту закодованої цифрової інформації, можливостей обробляти великі об'єми цифрової інформації при невеликих розмірностях базисів. Наприклад, в криптографічних системах, що засновані на великих простих числах порядків $10^{20} - 10^{40}$, необхідно використову-

вати рандомізовані або евристичні алгоритми [9], що зменшує їх надійність. При розкладі за степенями чисел обмежених, наприклад, числом 10^{50} , матимемо $10^{50} = 100^{25}$ і достатньо використати базис невеликої розмірності, що є підмножиною множини $\{1,2,3,\ldots,100\}$ з послідовністю показників $\{25,24,\ldots,2\}$.

Аналізуючи розклади великих чисел, виділимо ті особливості, які можуть бути присутніми у варіантах алгоритму: A_1) розклад у розширеному базисі; A_2) розклад у звуженому базисі; A_3) розклад у розрідженому базисі (наприклад, за базисом з простих чисел); A_4) розклад на основі мінімізації нев'язки і мінімізації модуля нев'язки. Аналіз цих варіантів має важливе значення при розкладі (кодуванні) великих чисел, оскільки основою алгоритму є дві процедури: 1) досягнення мінімуму нев'язки $\Delta(x,y) = w - x^n - y^n$ у просторі параметрів $x \in \mathbb{N}$, $y \in \mathbb{R}$, w – задане число; 2) прискорення швидкості розкладу шляхом розширення локального базису за рахунок пониження показника степенів x^n, y^n.

Для довільно заданого додатного числа w, що задовольняє умову розкладу $D(w,n)$, розширення або звуження локального базису розкладу пов'язане відповідно із зменшенням або збільшенням показників $n-k, k = 0,1,...,n-2$. Розрідження базису шляхом вилучення деяких цілих чисел з повного базису розкладу пов'язане із заміною одного базису іншим, при цьому елементи базису можуть повторюватись у розкладі з різними показниками.

А1) розширення початкового базису при фіксованих показниках степенів не відіграє суттєвої ролі у розкладі, оскільки при мінімізації нев'язки, алгоритм швидко приводить нев'язку в підобласть малих базисних елементів. Головну роль відіграє розширення локального базису (який звузився після ряду кроків мінімізації нев'язки), що запобігає процесу гальмування швидкості розкладу і приводить до завершення розкладу послідовним зменшенням показника $n-k \geq 2$.

А2) звуження базису із збільшеням показника n степеня розкладу необхідне лише для кодування великих чисел з базисом невеликої розмірності. Основна роль належить наближенню w дійсним числом $\bar{x}^n = w \Rightarrow \bar{x} = \sqrt[n]{w} \in R \Rightarrow M = \text{trunc}(\bar{x})$, M – верхня межа елементів базису, $M = \max\{x \in N : x^n < w\}$. Якщо виконувати не по-

вний розклад, тобто переривати розклад, якщо нев'язка $\Delta_k \le w_1$ (менше заданої межі) $\Rightarrow \Delta_{k-1} > w_1 \ge \Delta_k$, то обидві межі M і w_1 можуть бути прихованими даними кодування великих об'ємів цифрової інформації.

А3) розріджений базис – вилучення довільних цілих чисел з повного базису $\{1,2,3,...,M\}$ робить надійним алгоритм до зовнішніх впливів для захисту закодованої інформації, оскільки не можна виявити закономірностей, які елементи вилучені з повного базису.

А4) алгоритм розкладу числа за степенями на основі мінімізації модуля нев'язки може мати незначне прискорення швидкості розкладу лише на початкових кроках. Метод мінімізації нев'язки має простішу реалізацію алгоритму, розкладає число w на суму степенів, у той час як при мінімізації модуля нев'язки у розкладі наявні як суми, так і різниці степенів.

3. Гладке наближення погано зумовлених недиференційовних функцій. У теорії катастроф однією з основних задач є гладка заміна змінних, яка дозволяє аналізувати математичну модель на стійкість. Проблемною задачею є задача інтегрування погано зумовлених недиференційовних функцій. Нехай на відрізку $[a;b]$ задана неперервна монотонна погано зумовлена додатна функція. Обчислимо значення функції у центральному вузлі. Розкладемо це значення за послідовністю степенів, вибравши за n показник, узгоджений з числом зумовленості функції.

Приклад. Побудувати апроксимаційний многочлен з оптимальними показниками степенів для погано зумовленої функції

$$f(x) = 300e^{5.7+x} + |x|, x \in [-1;1].$$

Обчислимо

$$f(-1) = 32985.15174,\ f(1) = 243722.7476,$$

$$f(0) = 89661.22029.$$

Розкладемо за послідовністю степенів значення $f(0)$, обравши $n = 5$ на основі числа зумовленності функції:

$$89661 = 9^5 + 7^5 + 6^5 + 5^5 + 7^4 + 4^4 + 6^3 + 3^3 + 2^2.$$

На основі дискретної моделі розкладу $f(0)$ для заданого $n = 5$ побудуємо неперервну модель в околі центрального вузла $c = 0$ з оптимальними показниками степенів, наприклад, у формі многочлена

$$P(x)=(9+p_1x)^5+(7+p_2x)^5+(6+p_3x)^5+(5+p_4x)^5+$$
$$+(7+p_5x)^4+(4+p_6x)^4+(6+p_7x)^3+(3+p_8x)^3+(2+p_9x)^2,$$

де параметри $p_i, i=1,\ldots,9$ знайдемо, мінімізуючи середньо квадратичне відхилення $P(x)$ від $f(x)$ на сітці відрізка $[-1;1]$. Апріорно приймемо $p_i=1,7$. Відносна похибка наближення на відрізку $[-1;1]$ складає $0,17$, що свідчить про високу точність наближення погано зумовленої недиференційовної функції $f(x)$ на відрізку $[-1;1]$ гладким многочленом $P(x)$.

За другу гладку функцію виберемо позіном, наприклад, $Q(x)=f(-1)\left(1+\frac{x+1}{2}\right)^{\infty}$, який визначає логарифмічну швидкість зміни функції $f(x)$ при переході від точки $x=-1$ до точки $x=1$ і задовольняє граничні умови на кінцях проміжка $[-1;1]$ для значення $\infty=\ln\left(f(1)/f(-1)\right)/\ln 2=2.88534741$. Комбінуючи дві гладкі функції $P(x)$, $Q(x)$, дістали гладке наближення $Q(x)+(x-1)(x+1)P(x)$ погано зумовленої функції $f(x)$.

Висновок. Важливими проблемними задачами є задача кодування цифрової інформації великих об'ємів та задача гладкого наближення погано зумовлених недиференційовних функцій.

Результати досліджень. 1. Узагальнено задачу про розклад степенів на розклад цілих додатних чисел за степенями різних порядків, виведені умови розкладу, побудований алгоритм розкладу (алгоритм кодування цифрової інформації). 2. На основі дискретної моделі розкладу цілих додатних чисел за степенями запропонована побудова гладких многочленів шляхом заміни степенів на степеневі функції. Оскільки дискретна модель розкладу оптимальна (на кожному кроці нев'язка у просторі змішаних параметрів $x\in N$, $y\in R$ досягає мінімуму), то гладка модель в околі розкладу забезпечує наближення з високою точністю. Модель наближення коректна (при зменшенні нев'язки розкладу алгоритм розширює базис розкладу за рахунок пониження показника степеня). Модель гладкого наближення не використовує інтерполяційних многочленів, у яких при збільшенні числа зумовленості функції зростає порядок інтерполяційного многочлена, а зближення вузлів сітки інтерполяції приводить до осциляції (некоректність на-

ближення інтерполяційними многочленами погано зумовлених недиференційовних функцій). Позіноміальні доданки прогнозують крок розбиття проміжка задання погано зумовленої функції. Перспективність подальших досліджень: 1) застосувати алгоритм розкладу цілих чисел в криптографічних схемах, 2) узагальнити гладке наближення функції однієї змінної на функції багатьох змінних.

Список використаних джерел:

1. Боревич З. И., Шафаревич И. Р. Теория чисел. Москва: Наука. Гл. ред. физ.-мат. лит., 1972. 486 с.
2. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение / пер. с англ. Москва: Мир, 2001, 575 с.
3. Воеводин В. В., Кузнецов Ю. А. Матрицы и вычисления. Москва: Наука. Гл. ред. физ.-мат. лит., 1984. 390 с.
4. Лоусон Ч., Хенсон Р. Численное решение задач метода наименьших квадратов. Пер. с англ. Москва: Наука. Гл. ред. физ.-мат. лит., 1986. 232 с.
5. Прасолов В. В., Соловьев Ю. П. Эллиптические функции и алгебраические уравнения. Москва: Факториал, 1997. 288 с.
6. Корнейчук Н. П., Никольский С. М. О новых результатах по экстремальным задачам теории квадратур. *Квадратурные формулы.* 1974. С. 138-221.
7. Тихонов А. П., Арсенин В. Я. Методы решения некорректных задач. 2-е изд. Москва: Наука. Гл. ред. физ.-мат. лит., 1979. 284 с.
8. Хорн Р., Джонсон Ч. Матричный анализ. Пер. с англ. Москва: Мир, 1989. 655 с.
9. Кормен Т., Лейзерсон Ч., Риверст Р., Штайн К. Алгоритмы: построение и анализ. 2-е изд / Пер.с англ. Москва: Вильямс, 2005. 1296 с.
10. Абрамчук В. С. та ін. Позіомінальні інтерполяційні многочлени і квадратурні формули. *Фізико-математична освіта*. 2018. Випуск 1(15). С. 11-15.
11. Абрамчук В. С. О быстром алгоритме поиска простых чисел, не превосходящих числа x. *Доповіді НАН України*. 1996. № 10. С. 7-10.

ALGORITHM FOR DECOMPOSITION OF INTEGERS AND SMOOTH APPROXIMATION OF FUNCTIONS

The problem of expansion in powers is generalized into decomposition of positive integers in the sequence of degrees of different orders, the conditions of decomposition are determined, and the algorithm for decomposition is constructed. The algorithm is based on two procedures: 1) achievement a minimum of residual at each algorithm step; 2) speeding of decomposition through expanding the local base by reducing decomposition index, which ensures finiteness of algorithm. The algorithm has such efficiency factors as high rate of decomposition, ease of implementation, availability of different options for the decomposition of numbers as in extended, narrowed, sparse bases, which protects the encoded information from external influences. The algorithm can be used to encode large amounts of digital information under basic systems of small dimensions.

Decomposition of positive integers into a sequence of powers is optimal and correct. Optimality of decomposition follows from the condition that at each step of algorithm the minimum value of disjunction in the space of mixed parameters $x \in N$, $y \in R$ is achieved. Correctness of algorithm is due to the fact that when the disjunction is reduced, the algorithm expands the basis of decomposition by reducing the degree indicators by one. By switching from a discrete model to a continuous model by replacing the degrees with power functions, we obtain a smooth approximation of the ill-conditioned function in the neighborhood of decomposition. The construction of posinomial polynomials on the basis of smooth polynomials is one of the promising directions of integration of ill-conditioned nondifferentiable functions and smooth replacement of variables in the catastrophe theory.

Posinomials (functions with a variable exponent) predict the step of splitting the integration interval into parts, since they determine the logarithmic rate of change of an arbitrary monotonic function. The method of decomposition of positive integers provides an optimal decomposition into the sum of powers, and therefore the transition from a discrete model to a continuous model in the neighborhood of decomposition by replacing powers with power functions as well as allows to achieve the high accuracy of approximation.

Key words: *decomposition of powers of integers, coding algorithm, smooth approximation of ill-conditioned functions.*

Отримано: 18.10.2022