УДК 519.612
DOI: 10.32626/2308-5878.2024-25.6-19
В. С. Абрамчук, канд. фіз.-мат. наук,
І. В. Абрамчук
Вінницький національний технічний університет, м. Вінниця

ДВОЇСТИЙ АЛГОРИТМ ПОШУКУ ПРОСТИХ ЧИСЕЛ НА ВІДРІЗКАХ ВЕЛИКИХ РОЗМІРНОСТЕЙ

Запропоновано матричну модель підпослідовності натуральних чисел з мультиплікативним базисом з перших простих чисел. Матрична модель – квадратна матриця, вектор-стовпці якої є арифметичними прогресіями з різницею і кількістю прогресій, що дорівнює добутку елементів базису. Викресливши арифметичні прогресії з першими членами, кратними елементам базису, дістанемо симетричну розріджену матрицю, яка містить усі прості числа підпослідовності натуральних чисел, крім базисних, що підвищує щільність простих чисел у розріджених матрицях. Розріджені матриці явно не формуються. Формується лише вектор перших членів арифметичних прогресій. Доведені властивості розріджених матриць, виведені формули, що прискорюють обчислення складених чисел в арифметичних прогресіях, визначена структура елементів вектора перших членів арифметичних прогресій, досліджена зв'язність симетричних частин розріджених матриць. З розширенням базису зростає у векторі перших членів кількість пар елементів з різницею, що дорівнює степеню двійки («близнята», «четвірки» тощо). Це є необхідною умовою існування констант, для яких лінійні рівняння двох змінних можуть мати нескінченну множину розв'язків у простих числах. Іррегулярність розподілу простих чисел у підпослідовностях натуральних чисел пов'язана з структурою елементів вектора перших членів. Побудовано алгоритм пошуку простих чисел на відрізках великих розмірностей з паралельним процесом обчислень. Запропонований алгоритм є двоїстим до алгоритмів просіювання підпослідовностей натуральних чисел за простими дільниками. У цих алгоритмах не можна розпаралелити процес обчислень, оскільки процедура просіювання вимагає зберігання числової інформації попередніх кроків (векторна модель обробки масивів). Двоїстий алгоритм паралельно обчислює складені числа в кожній парі арифметичних прогресій з симетричними першими членами, використовуючи лише вектор перших членів арифметичних прогресій, що дозволяє обробляти масиви великих розмірностей.

Ключові слова: *матрична модель, мультиплікативний базис, розріджена матриця, зв'язність, найменші складені числа.*

Вступ. Значна іррегулярність у розподілі простих чисел «протиречить будь-якій закономірності» і є наслідком поведінки різниці $d_i = \rho_{i+1} - \rho_i$ сусідніх простих чисел, яка змінюється від двох до як завгодно великих значень [1, с. 12, 74, 104]. Використаємо, «що прості числа є елементами мутильплікативної побудови натуральних чисел» [1, с. 10]. Позначимо: $D^{(k)} = p_1 \times \ldots \times p_k$ (добуток перших простих чисел), $k \in N, k \geq 2$, і будемо послідовно виділяти з множини натуральних чисел N підмножини N_k – відрізки (підпослідовності) $\left[1; \left(D^{(k)}\right)^2\right]$. Прості числа p_k – множники $D^{(k)}$, називатимемо базисними елементами підмножини $N_k, k \in N, k \geq 2$. Базис позначатимемо $E_k = \{p_1, \ldots, p_k\}, k \in N, k \geq 2$.

Підпослідовність $\left[1; \left(D^{(k)}\right)^2\right]$ запишемо як $D^{(k)}$ арифметичних прогресій з першими членами $\left\{1, 2, \ldots, D^{(k)}\right\}$ і різницею $D^{(k)}, k \in N, k \geq 2$. Таке розміщення натуральних чисел підмножини N_k, запропоновано у роботі [3], назвемо матричною моделлю і позначатимемо $A^{(k)} = A^{(k)}\left[D^{(k)} \times D^{(k)}\right] = \left(j + D^{(k)}(i-1)\right), i, j \in \left[1; D^{(k)}\right]$. Просіємо елементи $A^{(k)}$ за простими дільниками-множниками $D^{(k)}$.

Лема 1 [3]. *Для кожного простого числа $p \leq p_k$, що є множником $D^{(k)}$, складені числа матриці $A^{(k)}$ з дільником p належать стовпцям $A_{\cdot j}^{(k)}$ з індексами $j \in \left[1; D^{(k)}\right]$ кратними p (належать арифметичним прогресіям з першими членами j кратними p), $k \in N, k \geq 2$.*

Дійсно, всі члени арифметичних прогресій, що належать стовпцям j кратним

$$p : A_{\cdot j}^{(k)} = A_{\cdot mp}^{(k)} = \left(mp + D^{(k)}(i-1)\right), i \in \left[1; D^{(k)}\right], mp \leq D^{(k)}$$

є складеними числами з дільником p, оскільки $D^{(k)} \vdots p$. У стовпцях j некратних p, складених чисел з дільником p не існує. Після викреслення з матриці $A^{(k)}$ вектор-стовпців $A_{\cdot j}^{(k)}$ з індексами j кратними множникам $D^{(k)}$, дістанемо розріджену матрицю $B^{(k)}$ розмірності

$D^{(k)} \times \varphi(D^{(k)})$, де $\varphi\left(D^{(k)}\right)$ – функція Ейлера [3]. Оскільки арифметичні прогресії однозначно визначаються першими членами, різницею і числом членів, то для задання матриці $B^{(k)}$ достатньо мати вектор перших членів, позначимо його $\vec{u}^{(k)}$, різницю $D^{(k)}$, число членів $n = D^{(k)}, k \in N, k \geq 2$. Розмірність вектора $\vec{u}^{(k)}$ дорівнює $\varphi(D^{(k)})$. Всі елементи $u_j^{(k)}$ вектора $\vec{u}^{(k)}$ є спряженими відносно $D^{(k)}$ і симетричними відносно $D^{(k)}/2$ (два числа $u, v \in \vec{u}^{(k)}$ є спряженими, якщо $v = D^{(k)} - u$, позначатимемо $v = u^*$. Елемент $\frac{D^{(k)}}{2} \notin \vec{u}^{(k)}$ [3].

Постановка проблеми. Обґрунтувати, що іррегулярність розподілу простих чисел у підпослідовностях натуральних чисел з мультиплікативним базисом пов'язана з структурою елементів вектора перших членів арифметичних прогресій розріджених матриць.

Мета статті:

1) дослідити структуру елементів вектора перших членів арифметичних прогресій;
2) побудувати алгоритм пошуку простих чисел на відрізках великих розмірностей.

Основна частина.

1. Властивості розріджених матриць. Основні властивості матриць $B^{(k)}$ досліджені в роботі [3]. Розширимо і узагальнимо результати цих досліджень. Оскільки всі прості числа послідовності $\left[1; D^{(k)}\right]$ належать арифметичним прогресіям матриці $B^{(k)}$, то визначимо їх щільність γ_k у матриці $A^{(k)}: \gamma_k = \frac{\varphi(D^{(k)})}{D^{(k)}}$. Середня щільність простих чисел в арифметичних прогресіях матриць $B^{(k)}$ для великих k визначається за формулою [3]:

$$\rho_k\left(B^{(k)}\right) = \frac{\left(\pi(D^{(k)})^2 - \rho_{k+1} - 1\right)}{D^{(k)}\varphi(D^{(k)})} = \frac{1}{2}\gamma_k \ln D^{(k)}.$$

Щоб визначити алгоритмічно ступінь розрідженості в арифметичних прогресіях, після видалення з них складених чисел, необхідно мати правила і формули задання складених чисел [3]. Складені числа матриць $B^{(k)}$ розділимо на дві групи: до першої групи віднесемо

найменші складені числа, що є добутками елементів вектора $\vec{u}^{(k)}$; до другої групи – складені числа, які отримаємо при паралельному зміщенні складених чисел першої групи.

Теорема 1. *Добутки* $vu_j^{(k)}$, *довільного числа* $v \in \vec{u}^{(k)}, v > 1$, *на різні елементи* $u_j^{(k)} \in \vec{u}^{(k)}$, *належать різним вектор-стовпцям (різним арифметичним прогресіям) матриці* $B^{(k)}, k \in N, k \geq 2$.

Доведення. Нехай $v \in \vec{u}^{(k)}, v > 1, q_1, q_2$ – довільна пара чисел, що належать $\vec{u}^{(k)}, 1 \leq q_1 < q_2 < D^{(k)}$. В залежності від значень добутків vq_1, vq_2 розглянемо три випадки.

1. $vq_1 \in \vec{u}^{(k)}, vq_2 \in \vec{u}^{(k)}$. Оскільки $q_1 < q_2$, то $vq_1 = T_1 < vq_2 = T_2$, де T_1, T_2 – різні стовпці матриці $B^{(k)}$.
2. Нехай $vq_1 \in \vec{u}^{(k)}, vq_2 \notin \vec{u}^{(k)}$. Допустимо, що $vq_1 = T_1, vq_2 = T_1 + D^{(k)}(i-1)$, $i > 1$, належать одному стовпцю T_1. Тоді
$$0 < vq_2 - vq_1 = v(q_2 - q_1) = D^{(k)}(i-1)(q_2 - q_1) \vdots D^{(k)},$$
оскільки $\left(v, D^{(k)}\right) = 1$. Це протирічить умові, що $(q_2 - q_1) < D^{(k)}$. Тому $vq_2 = T_2 + D^{(k)}(i-1), T_2 \neq T_1$.
3. Нехай $vq_1 \notin \vec{u}^{(k)}$, $vq_2 \notin \vec{u}^{(k)}$. Допустимо, що $vq_2 = T + D^{(k)}(i_2 - 1)$, $vq_1 = T + D^{(k)}(i_1 - 1), i_2 > i_1$, належать одному стовпцю T. Тоді $0 < vq_2 - vq_1 = v(q_2 - q_1) = D^{(k)}(i_2 - i_1)(q_2 - q_1) \vdots D^{(k)}$, оскільки $\left(v, D^{(k)}\right) = 1$. Це протирічить умові, що $q_2 - q_1 < D^{(k)}$. Отже $vq_1 = T_1 + D^{(k)}(i_1 - 1), vq_2 = T_2 + D^{(k)}(i_2 - 1), T_1 \neq T_2$, якщо $q_1 \neq q_2$.

Теорему доведено.

Лема 2. *Найменші складені числа* $u_1 v_1 \neq u_2 v_2$, *що є добутком різних пар елементів вектора* $\vec{u}^{(k)}$ *і є компонентами одного стовпця, належать різним вектор-рядкам матриці* $B^{(k)}, k \in N, k \geq 2$.

Доведення. В силу єдиності розкладу натуральних чисел, елементи відрізка $\left[1; (D^{(k)})^2\right]$ є різними, $k \in N, k \geq 2$. Тому після прості-

ювання за базисними елементами $p_1,\ldots,p_k$, елементи вектора $\vec{u}^{(k)}$ будуть різними. Добутки різних пар елементів вектора $\vec{u}^{(k)}$ прийматимуть різні значення. Якщо найменші складені числа u_1v_1, u_2v_2 з різними елементами належать одному стовпцю: $u_1v_1 = T + D^{(k)}(i_1 - 1)$, $u_2v_2 = T + D^{(k)}(i_2 - 1)$, де $u_1v_1 \neq u_2v_2$, тоді $i_2 \neq i_1$. У протилежному випадку $i_2 = i_1$, тому $0 \neq u_2v_2 - u_1v_1 = D^{(k)}(i_2 - i_1) = 0$. Отримане протиріччя доводить лему.

Лему доведено.

Лема 3. *Кожне найменше складене число* $a_{i,T} = uv$, $1 < u \le v < D^{(k)}$, $u, v \in \vec{u}^{(k)}$, *з меншим дільником* u, *належить вектор-рядку* $i \le u, k \in N, k \ge 2$.

Доведення. Допустимо протилежне, $i > u, i = u + d, d > 1$. Тоді $a_{i,T} = T + (u + d - 1)D^{(k)} = uvu\left(D^{(k)} - v\right) = -D^{(k)}(d - 1) - T$. Дістали протиріччя, оскільки ліва частина рівності додатна, а права – від'ємна. Таким чином, якщо $a_{i,T} = uv$, $u, v \in \vec{u}^{(k)}, 1 < u \le v$, то $i \le u$.

Лему доведено.

Лема 4. *Якщо* $a_{i,T} = uv$ *– найменше складене число,* $u, v \in \vec{u}^{(k)}$, $u > 1$, *то складені числа паралельного зміщення у стовпці* T *з дільником* u *обчислюються за формулою* $a_{i_0 + mu,\, T} = u\left(v + mD^{(k)}\right)$, *де* $m \in [1; M], M = \left[\dfrac{\left(D^{(k)} - i_0\right)}{u}\right], k \in N, k \ge 2$.

Доведення. Дійсно,

$$a_{i_0 + mu, T} = T + (i_0 + mu - 1)D^{(k)} =$$

$$= T + (i_0 - 1)D^{(k)} + muD^{(k)} = uv + muD^{(k)} = u\left(v + mD^{(k)}\right)$$

– складене число з дільником u. Якщо також $v > 1$, то складені числа паралельного зміщення з дільником v обчислюються за формулою

$$a_{i_0 + \delta v, T} = v\left(u + \delta D^{(k)}\right), \delta \in [1; M_1], M_1 = \left[\frac{D^{(k)} - i_0}{v}\right].$$

Зазначимо:

1) якщо $v=1$, то $i_0=1$;
2) найменшими дільниками складених чисел матриці $B^{(k)}$ є елементи вектора $\vec{u}^{(k)}$ [3].

Лему доведено.

Алгоритми обчислення параметрів i_0, T найменших складених чисел в арифметичних прогресіях матриць $B^{(k)}, k \in N, k \geq 2$.

Алгоритм 1.

Покласти $u = \rho_{k+1}$ – найменший елемент $\vec{u}^{(k)}$ більший за одиницю (ρ_{k+1} – просте число).

Для всіх $u \in \vec{u}^{(k)}$, для всіх $v \in \vec{u}^{(k)}, v \geq u$ обчислити найменше число $a_{i_0,T} = uv$, де $i_0 - 1 = \left[\frac{uv}{D^{(k)}}\right], T = uv\left(i_0 - 1\right)D^{(k)}$.

Кінець циклу для v, кінець циклу для u.

Практична рекомендація, що спрощує процес обчислень найменших складених чисел $a_{i_0,T} = T + D^{(k)}\left(i_0 - 1\right) = uv,\ u, v \in \vec{u}^{(k)}$. Оскільки елементи $\vec{u}^{(k)}$ взаємно прості з $D^{(k)}$, то розділимо їх на чотири групи з закінченнями цифрами 1, 3, 7, 9. Якщо, наприклад, T закінчується цифрою 1, а u – цифрою 3, то за v необхідно вибрати елементи з групи, що закінчується цифрою 7. Процес обчислень максимально розпаралелиться на обчислення в спряжених парах вектор-стовпців з використанням формул складених чисел φ_1 - φ_4 (теорема 2).

Теорема 2. *Якщо найменше складене число матриці* $B^{(k)}$ *задане формулою*

$$\left(\varphi_1\right)\ a_{i_0,T} = uv, 1 < u \leq v, ,\ u, v \in \vec{u}^{(k)},$$

то справедливі формули:

$$\left(\varphi_2\right) a_{u+1-i_0,T^*} = uv^*,\ \left(\varphi_3\right) a_{v+1-i_0,T^*} = u^* v,\ \left(\varphi_4\right) a_{D^{(k)}+i_0-u-v,T} = u^* v^*,$$

де $u^* = D^{(k)} - u$, $v^* = D^{(k)} - v, T^* = D^{(k)} - T, k \in N, k \geq 2$.

Доведення.

1. На основі леми 3 із формули $\left(\varphi_1\right)$ випливає нерівність $u + 1 - i_0 > 1$. Тому у вектор-стовпці T^* існує елемент a_{u+1-i_0,T^*} і мають місце перетворення

$$a_{u+1-i_0,T^*} = T^* + D^{(k)}\left(u+1-i_0-1\right) = D^{(k)} - T + D^{(k)}\left(u-i_0\right) =$$

$$= D^{(k)} + D^{(k)}u - \left(T + D^{(k)}\left(i_0-1\right)\right) - D^{(k)} = D^{(k)}u - uv = u\left(D^{(k)} - v\right) = uv^*.$$

Формулу (φ_2) доведено.

2. Оскільки $v \geq u$, то $v+1-i_0 > 1$ і у вектор-стовпці T^* існує елемент

$$a_{v+1-i_0,T^*} = T^* + D^{(k)}\left(v+1-i_0-1\right) = D^{(k)} - T + D^{(k)}\left(v-i_0\right) =$$

$$= D^{(k)} + D^{(k)}v - \left(T + D^{(k)}\left(i_0-1\right)\right) - D^{(k)} = D^{(k)}v - uv = v\left(D^{(k)} - u\right) = vu^*$$

Формулу (φ_3) доведено.

3. Оскільки $u, v \in \bar{u}^{(k)}$, то $u^*, v^* \in \bar{u}^{(k)}$ і u^*v^* – найменше складне число матриці $B^{(k)}$. Виконаємо еквівалентні перетворення:

$$u^*v^* = \left(D^{(k)} - u\right)\left(D^{(k)} - v\right) = \left(D^{(k)}\right)^2 - D^{(k)}u - D^{(k)}v + uv =$$

$$= \left(D^{(k)}\right)^2 - D^{(k)}u - D^{(k)}v + \left(T + D^{(k)}\left(i_0-1\right)\right) =$$

$$= T + D^{(k)}\left(D^{(k)} + i_0 - u - v - 1\right) = a_{D^{(k)}+i_0-u-v,T}$$

– елемент матриці $B^{(k)}$.

Формулу (φ_4) доведено.

Теорему доведено.

Із теореми 2 випливають властивості найменших складених чисел матриці $B^{(k)}$. Якщо обчислене найменше складене число $a_{i_0,T} = uv, u, v \in \bar{u}^{(k)}$ і $u \neq v$, то у спряжених стовпцях T, T^* визначена четвірка найменших складених чисел uv, uv^*, u^*v, u^*v^*; якщо $u = v$, то у спряжених стовпцях T, T^* визначена трійка найменших складених чисел uu, uu^*, u^*v^*. Це дає змогу скоротити обчислювальний процес визначення найменших складених чисел для всіх спряжених вектор-стовпців матриці $B^{(k)}, k \in N, k \geq 2$. Для спряженої пари $\{1, D-1\}$ матимемо одне найменше складене число $a_{D-1,1} = (D-1)^2$ і одне число паралельного зміщення $a_{D,D-1} = (D-1)(D+1)$.

2. Зв'язність симетричних частин матриць $B^{(k)}, k \in N, k \geq 2$. Зв'язність симетричних частин матриць $B^{(k)}$ означає наявність прос-

тих чисел в арифметичних прогресіях з симетричними першими членами, що є наслідком існування простих чисел в арифметичних прогресіях з першими членами взаємно простими з різницею $D^{(k)}$ для всіх $k \in N, k \geq 2$.

2.1 Правило рекурентного формування вектора перших членів арифметичних прогресій матриць $B^{(k)}, k \in N, k \geq 2$**.** Зростання розмірності мультиплікативного базису E_k підпослідовності N_k шляхом введення в базис простого числа p_{k+1}, приводить до «руйнування» зав'язків у матриці $B^{(k)}$ (видалення складених чисел з дільником p_{k+1}), розширення вектора перших членів матриці $B^{(k+1)}$, встановлення нових зав'язків у матриці $B^{(k+1)}$ з циклічними повтореннями формувань і перетворень при введені в базис наступних простих чисел.

Правило (алгоритм 2).

Вхідні дані:

$$E_2 = \{p_1, p_2\} = \{2,3\}, D^{(2)} = p_1 \cdot p_2 = 2 \cdot 3 = 6, \varphi\left(D^{(2)}\right) = 2, \vec{u}^{(2)} = \{1,5\}.$$

1. Присвоїти $k \cdot k + 1$. Розширити базис: $E_{k+1} = E_k \cup \{p_{k+1}\}$, де p_{k+1} – перший елемент вектора $\vec{u}^{(k)}\left[\varphi\left(D^{(k)}\right)\right]$ більший за одиницю (просте число). Обчислити

$$D^{(k+1)} = D^{(k)} p_{k+1}, \varphi\left(D^{(k+1)}\right) = \varphi\left(D^{(k)}\right)\left(p_{k+1} - 1\right).$$

2. Сформувати підматрицю

$$\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right] = \left(u_j^{(k)} + D^{(k)}(i-1)\right), i \in \left[1; p_{k+1}\right],$$

числа $u_j^{(k)}$ послідовно набувають значення елементів вектора $u^{(k)}\left[\varphi\left(D^{(k)}\right)\right]$.

3. Просіяти підматрицю $\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right]$ за дільником p_{k+1} (у кожному стовпці підматриці обчислити складне число з дільником p_{k+1} – існує єдине складне число). Складне число замінити нулем.

4. Записати просіяну підматрицю $\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right]$ як вектор $\vec{u}^{(k+1)}$ (запис проводити з рядків підматриці, пропускаючи нульові елементи). Розмірність вектора $\vec{u}^{(k+1)}$ дорівнює $\varphi\left(D^{(k+1)}\right)$.

2.2 Структура елементів вектора $\vec{u}^{(k)}, k \in N, k \geq 3$**.** Якщо для характеристики розрідженості S_k в N_k достатньо мати числові параметри γ_k, ρ_k то для характеристики зв'язаності матриць $B^{(k)}$, крім числових параметрів необхідно досліджувати структуру елементів вектора перших членів арифметичних прогресій.

Оскільки елементи вектора $\vec{u}^{(k)}$ є симетричними відносно $\frac{D^{(k)}}{2}\left(\frac{D^{(k)}}{2} \notin \vec{u}^{(k)}\right)$ і взаємно простими з $D^{(k)}$, то їх можна записати у формі: $u_j^{(k)} = \frac{D^{(k)}}{2} \mp 2^{S_j} v_j^{(k)}$, де $v_j^{(k)} \in \vec{u}^{(k)}$, $v_j^{(k)} < \frac{D^{(k)}}{2}$,

$$S_j \leq S_k = \max\left\{S_j \in N : \frac{D^{(k)}}{2} - p_{k+1} \geq 2^{S_j}\right\}.$$

Найменшим значенням виразу $2^{S_j} v^{(k)}$ є $2p_{k+1}$, тому для всіх $k \in N, k \geq 3$, вектор $\vec{u}^{(k)}$ запишеться у формі

$$\left(1, p_{k+1}, \ldots, \frac{D^{(k)}}{2} - 2p_{k+1}, \frac{D^{(k)}}{2} - 2^{tk}, \ldots, \frac{D^{(k)}}{2} - 2^2, \frac{D^{(k)}}{2} - 2, \frac{D^{(k)}}{2} + 2,\right.$$
$$\left.\frac{D^{(k)}}{2} + 2^2, \ldots, \frac{D^{(k)}}{2} + 2^{tk}, \frac{D^{(k)}}{2} + 2p_{k+1}, \ldots, D^{(k)} - p_{k+1}, D^{(k)} - 1\right),$$

де $tk = \max\left\{S_j \in N : 2p_{k+1} > 2^{S_j}\right\}$.

Наприклад, для $k = 3, p_{k+1} = p_4 = 7, tk = 3$; для $k = 31$, $p_{k+1} = p_{32} = 131, tk = 8$. Оскільки tk з ростом k неспадає, то для фіксованого $k_0 \in N, k_0 \geq 3$ і для всіх $k \in N$, $k \geq k_0$ матимемо константи $c \in G = \left\{2, 2^2, \ldots, 2^{tk-1}\right\}$, для яких виконується необхідна умова, що невизначені рівняння $x - y = c, c \in G$, можуть мати нескінченну множину розв'язків у простих числах.

2.3. «Близнята» вектора $\vec{u}^{(k)}, k \in N, k \geq 3$**.** Під терміном «близнята» вектора $\vec{u}^{(k)}$ будемо розуміти пари натуральних чисел з різницею два. Відповідні арифметичні прогресії повністю складені з «близнят». З ростом розмірності мультиплікативного базису E_k зростає у векторі $\vec{u}^{(k)}$ число пар «близнят».

Теорема 3. *При переході від базису* E_k *підпослідовності натуральних чисел* $N_k = \left[1; \left(D^{(k)}\right)^2\right]$ *до базису* E_{k+1} *підпослідовності* $N_{k+1} = \left[1; \left(D^{(k+1)}\right)^2\right]$, $D^{(k)} = p_1 \times \ldots \times p_k$, $D^{(k+1)} = D^{(k)} \times p_{k+1}$ *зростає число «близнят» з* m_k *у векторі* $\vec{u}^{(k)}$ *до* $m_{k+1} = (m_k + 1)(p_{k+1} - 2) - 1$ *у векторі* $\vec{u}^{(k+1)}$ *для всіх* $k \in N, k \geq 2, m_2 = 0$.

Доведення. Застосуємо правило рекурентного формування вектора $\vec{u}^{(k+1)}$. Після k-го кроку вектор $\vec{u}^{(k+1)}$ еквівалентний підматриці $\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right]$, яку необхідно просіяти за простим числом p_{k+1}. Підматриця $\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right]$ за умовою містить m_k пар вектор-стовпців «близнят» і пару спряжених вектор-стовпців $\left(B^{(k)}_{.1}, B^{(k)}_{.D^{(k)}-1}\right)$ з близнятами $\left(b^{(k)}_{i+1,1}, b^{(k)}_{i,D^{(k)}-1}\right)$ $i \in \left[1; p_{k+1}\right]$. Після просіювання підматриці з кожного стовпця видалиться по одному складеному числу з дільником p_{k+1}. Таким чином з кожної пари вектор-стовпців «близнят» видалиться по дві пари елементів (вилучення одного елемента з пари «руйнує» пару). У підматриці $\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right]$ залишиться $(m_k + 1)(p_{k+1} - 2) - 1$ пар елементів «близнят» (враховано, що вектор-стовпець $B^{(k)}_{.1}$ містить одиницю). Записавши просіяну підматрицю $\tilde{B}^{(k)}\left[p_{k+1} \times \varphi\left(D^{(k)}\right)\right]$ як вектор, матимемо рекурентну формулу утворення пар елементів «близнят»: $m_{k+1} = (m_k + 1)(p_{k+1} - 2) - 1$ у векторі $\vec{u}^{(k+1)}$ для всіх $k \in N, k \geq 2$.

Теорему доведено.

Прості числа «близнята» мають важливе значення для зв'язаності розріджених матриць $B^{(k)}$, а саме, прості числа вектор-стовпців $B^{(k)}_1, B^{(k)}_{D^{(k)}-1}$ забезпечують зв'язність крайніх арифметичних прогресій, а прості числа двох пар вектор-стовпців $\left(B^{(k)}_{\left(\frac{D^{(k)}}{2}-2^2\right)}, B^{(k)}_{\left(\frac{D^{(k)}}{2}-2\right)}\right)$, $\left(B^{(k)}_{\left(\frac{D^{(k)}}{2}+2\right)}, B^{(k)}_{\left(\frac{D^{(k)}}{2}+2^2\right)}\right)$ забезпечують зв'язність в середині матриці $B^{(k)}$.

Якщо позначити у векторі $\vec{u}^{(k)}$ через $z_{j,k}$ кількість пар елементів з різницею 2^{S_j}, $1 < S_j < tk-1$, то у векторі $\vec{u}^{(k+1)}$ ця кількість елементів зросте до $z_{j,k+1} = z_{j,k}\left(p_{k+1}-2\right)$.

3. Двоїстий алгоритм пошуку простих чисел. Алгоритм, що пропонується, є двоїстим до алгоритму [3]. Алгоритм [3] просіює матрицю $B^{(k)}$ за простими дільниками, а двоїстий алгоритм обчислює складені числа в матриці $B^{(k)}$.

Ефективність двоїстого алгоритму полягає в наступному:

1) за k кроків, $k \in N, 3 \le k \le k_0$, що визначає розмірність $E_k = \{p_1, \ldots, p_k\}$ підпослідовності натуральних чисел N_k, алгоритм обробляє масив $N_k = \left[1; \left(D^{(k)}\right)^2\right], D^{(k)} = p_1 \times \ldots \times p_k$ великих розмірностей. Підпослідовність N_k задається матрицею $A^{(k)}\left[D^{(k)} \times D^{(k)}\right]$;
2) оскільки усі прості числа підпослідовності N_k, крім базисних, належать розрідженій матриці $B^{(k)}$, то щільність простих чисел в $B^{(k)}$ зростає в $\dfrac{1}{\gamma_k}$ разів $\gamma_k = \dfrac{\varphi\left(D^{(k)}\right)}{D^{(k)}}$;
3) матриця $B^{(k)}$ явно не зберігається, задається вектор $\vec{u}^{(k)}$ перших членів і різниця $D^{(k)}$;
4) обчислення складених чисел матриць $B^{(k)}$ здійснюється з застосуванням формул $\varphi_1 - \varphi_4$ з паралельними обчисленнями для кожної спряженої пари вектор-стовпців;
5) для зчитування простих чисел формується матриця з елементами 0, 1. Зчитування проводиться за правилом формування арифметичних прогресій і кодом 1. Для зберігання інформації масиву N_{k_0}, формується вектор $\vec{u}^{(k_0)}$ і різниця $D^{(k_0)}$, k_0 – задане число.

Алгоритм 3.

Вхідні дані:

$$k = 2, E_2 = \{2,3\},\ D^{(2)} = 6, \varphi(D^{(2)}) = 2, \vec{u}^{(2)} = \{1,5\}, k_0 \ge 3$$

– задане число.

Алгоритм складається з двох процедур A, B.

A. Сформувати алгоритмом 2 вектор перших членів $\vec{u}^{(k_0)}$ матриці $B^{(k_0)}$, різницю $D^{(k_0)}, \varphi(D^{(k_0)})$.

B. Кодування матриці $C^{(k_0)}$ і зчитування простих чисел.

*B.*1. Сформувати матрицю $C^{(k_0)}\left[D^{(k_0)}\varphi(D^{(k_0)})\right]$ з елементів $C_{i,j}=1$.

*B.*2. Паралельно за формулами $\varphi_1-\varphi_4$ обчислити найменші складені числа. Найменші складені числа та складені числа паралельного зміщення позначити цифрою 0.

*B.*3. Зчитування простих чисел з закодованої матриці $C^{(k_0)}$ здійснити за правилом формування арифметичних прогресій і кодом 1.

Алгоритм завершений.

Для зберігання інформації про N_{k_0} достатньо зберігати половину симетричного вектора $\vec{u}^{(k_0)}$, параметри $D^{(k_0)}, \varphi(D^{(k_0)})$. Ефективність матричної моделі дослідження підпослідовностей натуральних чисел проілюструємо на прикладі двох підпослідовностей з мультиплікативними базисами E_5 і E_{31}:

$$E_5=\{p_1,\ldots,p_5\}, E_{31}=\{p_1,\ldots,p_{31}\}, p_1=2, p_5=11, p_{31}=127;$$

відрізки натуральних чисел $N_5=[1;5336100]$, $N_{31}=\left[1;\approx 1.612.10^{97}\right]$; щільність простих чисел у розріджених матрицях $\rho\left(B^{(5)}\right)\approx 0.3107$, $\rho\left(B^{(31)}\right)\approx 0.0393$; кількість пар «близнят» у векторі перших членів розріджених матриць $m_5=134, m_{31}\approx 7.085.10^{46}$; γ_k – розрідженість матриць (обернена величина $\frac{1}{\gamma_k}$ наближено вказує у скільки разів зросла щільність простих чисел в арифметичних прогресіях розріджених матриць)

$$\gamma_5\approx 0.20779, \frac{1}{\gamma_5}\approx 4.813, \gamma_{31}=0.1135, \frac{1}{\gamma_{31}}\approx 8.81;$$

tk – кількість елементів вектора перших членів, що задаються у формі $\left(\frac{D^{(k)}}{2}\mp 2^{S_j}\right), 1\le S_j<tk$. Серед цих елементів є пари «близнят», «четвірок» тощо, $t_5=4, t_{31}=8$.

Висновки. Побудова ефективного алгоритму пошуку простих чисел на відрізках великих розмірностей вимагає розв'язання ряду теоретичних і практичних задач: аналітичне виділення з послідовності натуральних чисел N підпослідовностей $N_k, k \in N$, що покривають N, складених з арифметичних прогресій з спільною різницею (матрична модель); видалення арифметичних прогресій, що містять складені числа з дільниками базису (утворення розріджених матриць для підвищення в них щільності простих чисел); швидке обчислення складених чисел в арифметичних прогресіях з використанням аналітичних формул і розпаралелюванням процесу обчислень; задання вектора перших членів арифметичних прогресій і спільної різниці позбавляє необхідності формування масивів великих розмірностей для зберігання і обробки підпослідовностей. На основі доведених властивостей розріджених матриць побудований алгоритм пошуку простих чисел у підпослідовностях натуральних чисел, що дозволяє прослідкувати еволюцію формувань і перетворень підпослідовностей з розширенням мультиплікативного базису.

Список використаних джерел:

1. Трост Э. Простые числа. Москва: Госиздат, 1959. 135 с.
2. Бородін О. І. Теорія чисел: підручник. Київ: Вища школа, 1970. 270 с.
3. Абрамчук В. С. О быстром алгоритме поиска простых чисел, не превосходящих числа. *Доп. НАН України*. 1996. № 10. С. 7-10.

BINARY ALGORITHM FOR FINDING PRIME NUMBERS ON SEGMENTS OF LARGE DIMENSIONS

A matrix model of subsequence of natural numbers with a multiplicative basis from the first prime numbers is proposed. The matrix model is a square matrix, where vector columns are arithmetic progressions with difference and number of progressions equal to product of base elements. By crossing out arithmetic progressions with first terms which are multiples of base elements, we obtain a symmetric sparse matrix that contains all the prime numbers of subsequence of natural numbers, except for the base ones, which increases the density of prime numbers in sparse matrices. Sparse matrices are not formed clearly, only the vector of first terms of arithmetic progressions is formed. Properties of sparse matrices have been proven. Formulas that speed up the calculation of compound numbers in arithmetic progressions have been derived, the structures of vector elements of first terms of arithmetic progressions have been determined, the connectivity of symmetric parts of sparse matrices has been investigated. With the expansion of the base the number of pairs of elements with the difference equal to the power of two («twins», «fours», etc.) increases in the vector of first terms. This is a necessary condition for the existence of constants for which linear equations of two variables can have an infinite set of solutions in prime numbers. The irregularity of distribution of prime numbers in subsequences of natu-

ral numbers is related to the structure of elements of the vector of first terms. An algorithm for finding prime numbers on segments of large dimensions with a parallel calculation process has been built. The proposed algorithm is binary to algorithms for sifting subsequences of natural numbers by prime divisors. In these algorithms, it is not possible to parallelize the calculation process, since screening procedure requires storing the numerical information from the preceding steps (vector model of array processing).

The binary algorithm calculates compound numbers in each pair of arithmetic progressions with symmetric first terms simultaneously, using only vector of the first terms of arithmetic progressions, which makes possible processing of large-dimensional arrays.

Key words: *matrix model, multiplicative basis, sparse matrix, connectivity, smallest compound numbers.*

Отримано: 26.06.2024

УДК 517.95:519.63
DOI: 10.32626/2308-5878.2024-25.19-26

К. В. Василишин

Харківський національний університет радіоелектроніки, м. Харків

ЗАСТОСУВАННЯ МЕТОДУ ДВОБІЧНИХ НАБЛИЖЕНЬ ДО РОЗВ'ЯЗАННЯ ПЕРШОЇ КРАЙОВОЇ ЗАДАЧІ ДЛЯ ОДНОВИМІРНОГО РІВНЯННЯ ТЕПЛОПРОВІДНОСТІ З ЕКСПОНЕНЦІАЛЬНО НЕЛІНІЙНИМ КОЕФІЦІЄНТОМ ТЕПЛОПРОВІДНОСТІ

Задача про теплопровідність об'єктів у нелінійних середовищах зводиться до розв'язання крайових задач для нелінійного рівняння теплопровідності, де коефіцієнти рівняння або функція потужності теплових джерел залежать від температури за деяким законом. Серед чисельних методів розв'язання задач для нелінійних рівнянь математичної фізики можна виділити методи скінченних різниць, скінченних елементів, варіаційні та проекційні, а також ітераційні методи. Серед останньої групи методів найбільш привабливим є метод двобічних наближень завдяки можливості отримати зручну оцінку для похибки наближеного розв'язку і довести існування розв'язку вихідної задачі.

Теорія лінійних напівупорядкованих просторів була побудована Л. В. Канторовичем у другій половині 30-х років XX ст. Подальший розвиток цієї теорії пов'язаний з роботами М. А. Красносельського, H. Amann'a, В. І. Опойцева, Н. С. Курпеля, Б. А. Шувара, А.І. Колосова та інших.

Метою статті є розробка методу двобічних наближень на основі використання функцій Гріна для розв'язання першої кра-