# Тема 3. ИСЧЕРПЫВАЮЩИЙ ПОИСК

## *3.4. Методы решета*

Для многих теоретико-числовых вычислений широко используется другой метод исчерпывающего поиска – *метод решета*. В отличие от поиска с возвратом, в котором осуществляется поиск решений, метод решета рассматривает конечное множество элементов и исключает из него все элементы, не являющиеся решениями. В результате такого просеивания в множестве остаются только те элементы, которые являются решениями.

Работу метода решета можно показать на примере решета Эратосфена для отыскания простых чисел между $N$ и $N^2$. Просеивание начинается с формирования исходного множества всех целых чисел от $N$ до $N^2$. Затем поэтапно удаляются составные числа: сначала все числа, кратные двум, затем – все, кратные трем, и т. д. Процесс прекращается после просеивания для наибольшего простого числа, меньшего или равного $N$. Процесс просеивания для $N = 5$ выглядит следующим образом:

Шаг 0 (исходный)
5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Шаг 1 (исключаются кратные 2)
5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25

Шаг 2 (исключаются кратные 3)
5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25

Шаг 3 (исключаются кратные 5, кроме простого числа 5)
5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ ~~25~~

Результат – простые числа: 5, 7, 11, 13, 17, 19, 23.

Основное достоинство методов решета очевидно. Если все элементы в множестве возможных решений можно пронумеровать натуральными числами, то хранить нужно только характеристический вектор. В этом векторе *i*-й разряд равен нулю, если *i*-й элемент не является решением, и равен единице в противном случае. Поэтому в множествах, состоящих из очень большого числа элементов, возможен поиск без явного порождения и исследования каждого элемента. Кроме того, в вычислительных устройствах логические операции можно выполнять параллельно над многими разрядами, что позволяет существенно увеличить эффективность вычислений.

Решето Эратосфена является специальным случаем *обобщенного модульного решета*. Пусть $m_1, m_2, ..., m_t$ – множество из $t$ целых чисел, называемых *модулями*. Для каждого $m_i$ рассматривается $n_i$ арифметических прогрессий

$$m_i\, k + a_{ij},\ k = 1, 2, ...,\ j = 1, 2, ..., n_i.$$

Задача состоит в отыскании всех целых чисел, заключенных в пределах некоторых целых $A$ и $B$, которые для каждого $m_i$ одновременно принадлежат одной из $n_i$ прогрессий. В решете Эратосфена $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, ..., $m_i = p$ ($p$ – наибольшее простое число, меньшее или равное $N$), $n_i = m_i - 1$ и $a_{ij} = j$.

Таким образом, решето Эратосфена можно интерпретировать как поиск всех чисел между $N$ и $N^2$, которые одновременно являются членами одной из арифметических прогрессий в каждом из следующих множеств:

$$\{2k+1\},$$
$$\{3k+1,\ 3k+2\},$$
$$\{5k+1,\ 5k+2,\ 5k+3,\ 5k+4\},$$
$$\vdots$$
$$\{pk+1,\ \ldots,\ pk+p-1\}.$$

То, что число принадлежит прогрессии $2k + 1$, означает, что оно нечетно; то, что оно принадлежит одной из прогрессий $3k + 1$ или $3k + 2$, означает, что оно не является кратным трем, и т. д.

Существует много решет, в которых модули $m_1$, $m_2$, ... заранее не известны, т. е. значение $m_i$ будет зависеть от чисел, еще не удаленных после просеивания по модулю $m_{i-1}$. Поэтому многие решета строятся рекурсивным образом (*рекурсивные решета*). Обычно решето Эратосфена так и строится. После выписывания всех чисел от 2 до $N$ вычеркиваются все числа, кратные двум, кроме самой двойки. Затем, поскольку наименьшее оставшееся число, кратные которому остались неудаленными, равно трем, удаляются все числа, кратные трем, кроме самой тройки, и т. д. Следует отметить, что на каждом шаге первое удаленное число является квадратом числа, с которого начинается просеивание. Процесс заканчивается, когда число, относительно которого производится просеивание, становится больше $\sqrt{N}$, так как никакие числа уже не могут быть удалены. Обычно размер ячеек решета Эратосфена удваивается, осуществляя предпросеивание четных чисел, т. е. просеивание начинается для исходного множества, состоящего только из нечетных чисел. Пусть $X$ – двоичный набор; тогда рекурсивный вариант решета Эратосфена с предпросеиванием для числа 2 для нечетных простых чисел до $2n + 1$ представлен алгоритмом 3.7.

$X \leftarrow (1, 1, ..., 1)$
**for** $k \leftarrow 3$ **to** $\sqrt{2n+1}$ **by** $2$ **do**
$\begin{cases} // \; X_{(k-1)/2} \text{ представляет нечетное число } k \\ \textbf{if } X_{(k-1)/2} = 1 \\ \quad \textbf{then for } i \leftarrow k^2 \textbf{ to } 2n+1 \textbf{ by } 2k \textbf{ do } X_{(i-1)/2} \leftarrow 0 \end{cases}$
**for** $k \leftarrow 1$ **to** $n$ **do if** $X_k = 1$ **then** вывести $2k+1$

Алгоритм 3.7. Рекурсивное решето Эратосфена

Примером более сложного решета является решето для вычисления следующей числовой последовательности $U$ [21]. Вначале $U = (1, 2)$. Если вопрос о вхождении в $U$ решен для всех целых чисел, меньших $m$, то $m \in U$ тогда и только тогда, когда $m$ является суммой единственной пары различных элементов из $U$. Таким образом, $U = (1, 2, 3, 4, 6, 8, 11, 13, 16, 18, 26, \ldots)$. Эту последовательность можно вычислить с помощью двух параллельных просеиваний: целое должно быть просеяно, если является суммой, получаемой не менее чем одним способом, и не должно быть отсеяно, если является суммой, получаемой не более чем одним способом. Используются два двоичных вектора. Для $i > 2$

$X_i = 1$, если и только если $i$ представимо в виде суммы не менее чем одним способом;

$Y_i = 1$, если и только если $i$ представимо в виде суммы не более чем одним способом.

Двойное рекурсивное решето для вычисления элементов $U$ до некоторого числа $N$ представлено алгоритмом 3.8. Значение счетчика $k$ увеличивается до тех пор, пока оно не достигнет первого целого числа, большего предыдущего элемента из $U$, представимого точно одним способом. Это целое принадлежит $U$, и поэтому разряды, соответствующие всем целым $k + i$ для $i < k$, должны быть обновлены.

$X \leftarrow (1, 1, 0, 0, \ldots, 0)$
$Y \leftarrow (1, 1, 1, 1, \ldots, 1)$
$k \leftarrow 1$

$$\textbf{while } k < N \textbf{ do } \begin{cases} k \leftarrow k+1 \\ \textbf{while } X_k \wedge Y_k = 0 \textbf{ and } k < N \textbf{ do } k \leftarrow k+1 \\ \textbf{for } i \leftarrow 1 \textbf{ to } \min(k-1, N-k) \textbf{ do} \\ \quad \begin{cases} Y_{k+i} \leftarrow Y_{k+i} \wedge (X_{k+i} \wedge X_i \wedge Y_i) \\ X_{k+i} \leftarrow X_{k+i} \vee (X_i \wedge Y_i) \end{cases} \end{cases}$$

$$\textbf{for } i \leftarrow 1 \textbf{ to } N \textbf{ do if } X_i \wedge Y_i = 1 \textbf{ then} \text{ вывести } i$$

Алгоритм 3.8. Двойное рекурсивное решето