DOI: 10.17117/na.2016.06.02.267

<http://ucom.ru/doc/na.2016.06.02.267.pdf>

Поступила (Received): 21.06.2016

Муратшин Т.И. Эффективное вычисление первых значений функции Пиллаи

Muratshin T.I.
Efficient calculating first values of Pillai's function

В данной статье представлены исследования основных свойств функции Пиллаи. Также был разработан и обоснован алгоритм, который находит первые n значений функции Пиллаи за время, линейно зависящее от n , основанный на свойствах, рассмотренных ранее

Ключевые слова: функция Пиллаи, суммирование наибольших общих делителей

This article presents the study of the basic properties of Pillai's function. Also article was developed and proved algorithm based on studied properties that finds first n values of function and has complexity $O(n)$

Key words: Pillai's function, summation of great common divisors

Муратшин Тимур Ильшатович

Бакалавр

Национальный исследовательский университет
«Московский институт электронной техники»

г. Москва, Зеленоград, пл. Шокина, 1

Muratshin Timur Ilshatovich

Bachelor

National research university of electronic technology
Moscow, Zelenograd, Shokina sq., 1

Функция Пиллаи [1] – теоретико-числовая функция, которая определяется следующим образом: $S(n) = \sum_{i=1}^n \gcd(i, n)$

Здесь $\gcd(a, b)$ – наибольший общий делитель чисел a и b [2].

Для фиксированного значения n значение функции по определению можно посчитать за $O(n \log n)$. В данной статье рассматриваются основные свойства данной функции, на основе которых строится метод, с помощью которого можно вычислять все значения функции Пиллаи от 1 до n за $O(n)$ (пользуясь лишь прямым определением, эту же задачу можно выполнить за $O(n^2 \log n)$).

Заметим, что $\gcd(i, n)$ для любых $1 \leq i \leq n$ является делителем числа n . Поэтому можно переписать формулу для функции Пиллаи следующим образом:

$$S(n) = \sum_{d|n} d * cnt(n, d)$$

Здесь суммирование проводится по всем делителям d числа n . $cnt(n, d)$ – количество таких чисел i от 1 до n , что $\gcd(i, n) = d$.

Лемма. Если d – делитель числа n , то $cnt(n, d) = \varphi(\frac{n}{d})$, где $\varphi(n)$ – функция Эйлера [3].

Док-во. $\gcd(i, n) = d \Rightarrow \gcd\left(\frac{i}{d}, \frac{n}{d}\right) = 1$. Это означает, что для всех чисел, для которых $\gcd(i, n) = d$, можно однозначным образом найти число, взаимно простое с $\frac{n}{d}$. Отсюда $\text{cnt}(n, d) \leq \varphi\left(\frac{n}{d}\right)$.

$\gcd\left(i, \frac{n}{d}\right) = 1 \Rightarrow \gcd(i * d, n) = d$. Таким образом, для любого числа, взаимно простого с $\frac{n}{d}$, можно найти число, для которого $\gcd(i * d, n) = d$. Тогда $\text{cnt}(n, d) \geq \varphi\left(\frac{n}{d}\right)$.

Итого имеем $\varphi\left(\frac{n}{d}\right) \leq \text{cnt}(n, d) \leq \varphi\left(\frac{n}{d}\right)$. Что влечет за собой равенство $\text{cnt}(n, d) = \varphi\left(\frac{n}{d}\right)$.

С учетом леммы, формулу для функции Пиллаи можно переписать следующим образом:

$$S(n) = \sum_{d|n} d * \varphi\left(\frac{n}{d}\right)$$

Теперь можно перейти к ключевому моменту статьи – мультипликативность функции Пиллаи.

Теорема. $\gcd(m, n) = 1 \Rightarrow S(n * m) = S(n) * S(m)$.

Док-во. $S(n * m) = \sum_{d|(n*m)} d * \varphi\left(\frac{n*m}{d}\right) = \sum_{d_1|n, d_2|m} d_1 * d_2 * \varphi\left(\frac{n*m}{d_1*d_2}\right) = \left(\sum_{d_1|n} d_1 * \varphi\left(\frac{n}{d_1}\right)\right) * \left(\sum_{d_2|m} d_2 * \varphi\left(\frac{m}{d_2}\right)\right) = S(n) * S(m)$. Здесь было использовано свойство мультипликативности функции Эйлера.

Теперь можно переходить к методу. Найдем формулу для значения $S(p^a)$, где p – простое, a – неотрицательное целое.

$$\begin{aligned} S(p^a) &= \sum_{d|p^a} d \varphi\left(\frac{p^a}{d}\right) = \sum_{i=0}^a p^i \varphi(p^{a-i}) = p^a \varphi(1) + \sum_{i=0}^{a-1} p^i (p^{a-i} - p^{a-i-1}) \\ &= p^a + \sum_{i=0}^{a-1} p^a - p^{a-1} = p^a + ap^a - ap^{a-1} = (a+1)p^a - ap^{a-1} \end{aligned}$$

Следующим этапом будет нахождение формулы для $S(p^a)$, опираясь на формулу $S(p^{a-1})$. Для этого сделаем следующие преобразования:

$$S(p^a) = (a+1)p^a - ap^{a-1} = p((a+1)p^{a-1} - ap^{a-2}) = p(ap^{a-1} + p^{a-1} - (a-1)p^{a-2} - p^{a-2}) = p(S(p^{a-1}) + p^{a-1} - p^{a-2}) = pS(p^{a-1}) + p^a - p^{a-1}.$$

Стоит заметить, что данные преобразования являются корректными только для $a \geq 2$, но легко проверить, что получившаяся формула выполняется и для $a = 1$.

Заведем массив $\text{minPrime}[1..N]$, где будем для каждого числа хранить минимальный простой делитель. Следующая цель – заполнить этот массив таким образом, чтобы каждый элемент заполнялся лишь один раз. Тогда мы сможем заполнить данный массив за $O(N)$. Заметим, что число i можно однозначным способом представить в виде $i = \text{minPrime}[i] * x$, где x – число, у которого нету делителей, меньших, чем $\text{minPrime}[i]$. Тогда можно сделать следующее. Переберем x от 2 до N . Тогда возможны два случая:

1) Мы уже нашли $\text{minPrime}[x]$;

2) Мы еще не нашли $\minPrime[x]$, тогда x является простым и $\minPrime[x] = x$.

После этого мы домножаем x на все простые $p \leq \minPrime[x]$. И тогда получим, что $\minPrime[x * p] = p$. Так как такое разложение существует и единственно, то каждое число будет пройдено лишь по разу.

Приведем псевдокод алгоритма:

```

 $\minPrime[1..N] \leftarrow \{0, 0, \dots, 0\}$ 
 $primes \leftarrow \emptyset$ 
for  $x \in 2..N$ 
  if  $\minPrime[x] = 0$ 
     $\minPrime[x] \leftarrow x$ 
     $primes \leftarrow primes \cup x$ 
  for  $p \in primes$ 
    if  $p > \minPrime[x]$  or  $x * p > N$ 
      break
     $\minPrime[x * p] \leftarrow p$ 

```

Теперь можно модифицировать данный алгоритм таким образом, чтобы также считались и значения $S(N)$. Для этого заметим, что если x является простым, то $S(x) = x * S(1) + x - 1 = 2x - 1$. Теперь осталось выяснить, как надо изменять значения $S(x * p)$ во внутреннем цикле. Заведем еще один массив $R[N]$, элементы которого удовлетворяют условиям:

- 1) $R[N]$ не делится на $\minPrime[N]$;
- 2) $N = \minPrime[N]^a * R[N]$.

Например, $R[30] = R[2 * 3 * 5] = 3 * 5 = 15$, $R[24] = R[2^3 * 3] = 3$. Тогда $R[p^a] = 1$, где p – простое.

Заметим, что при обновлении во внутреннем цикле p является простым, а x не имеет простых делителей, меньших p . Отсюда вытекают 2 случая:

- 1) $\minPrime[x] = p$

Здесь также возможны два случая:

- а) $[x] = 1$. Это означает, что $x = p^a$, $x * p = p^{a+1}$. Тогда:

$$R[x * p] = 1;$$

$$S[x * p] = p * S[x] + p * x - x$$

- б) $R[x] > 1$. Это означает, что $x = p^a * R[x]$. Тогда:

$$R[x * p] = R[x];$$

$$S[x * p] = S[R[x]] * S\left[\frac{x * p}{R[x]}\right] \text{ (Ввиду того, что } R[x] \text{ и } \frac{x * p}{R[x]} \text{ являются взаимно простыми числами)}$$

$$\minPrime[x] > p$$

В этом случае p и x являются взаимно простыми числами, и тогда:

$$R[x * p] = x;$$

$$S[x * p] = S[x] * S[p]$$

Теперь можно написать конечный алгоритм:

```

 $\minPrime[1..N] \leftarrow \{0, 0, \dots, 0\}$ 
 $S[1..N] \leftarrow \{0, 0, \dots, 0\}$ 
 $R[1..N] \leftarrow \{0, 0, \dots, 0\}$ 

```

```

primes  $\leftarrow \emptyset$ 
S[1]  $\leftarrow 1$ 
for  $x \in [2..N]$ 
  if minPrime[x] = 0
    minPrime[x]  $\leftarrow x$ 
    S[x]  $\leftarrow 2 * x - 1$ 
    R[x]  $\leftarrow 1$ 
  primes  $\leftarrow$  primes  $\cup x$ 
  for  $p \in$  primes
    if  $p > \text{minPrime}[x]$  or  $x * p > N$ 
      break
    num  $\leftarrow x * p$ 
    minPrime[num]  $\leftarrow p$ 
    if minPrime[x] = p
      if R[x] = 1
        R[num]  $\leftarrow 1$ 
      S[num]  $\leftarrow S[x] * p + \text{num} - x$ 
    else
      R[num]  $\leftarrow R[x]$ 
      S[num]  $\leftarrow S[\frac{\text{num}}{R[\text{num}]}] * S[R[\text{num}]]$ 
    else
      R[num]  $\leftarrow x$ 
      S[num]  $\leftarrow S[x] * S[p]$ 

```

После выполнения данного алгоритма в массиве $S[N]$ будут корректные значения функции Пиллаи.

В данной статье были рассмотрены основные свойства функции Пиллаи, а также приведен метод, с помощью которого возможно за $O(n)$ найти первые n значений функции Пиллаи.

Список используемых источников:

1. Pillai S.S. On an arithmetic function. Annamalai University Journal II. P. 242–248.
2. Виноградов И.М. Основы теории чисел. Гос. изд. технико-теоретической литературы, 1952. 180 с.
3. Hardy G.H., Wright E.M. An Introduction to the Theory of Numbers. Fourth edition. Oxford: Oxford University Press, 1975. 421 p.