

«ЛЕНТОЧНАЯ» ТЕОРЕМА И ЕЕ ПРИЛОЖЕНИЯ

В. В. Скобелев

Институт прикладной математики и механики НАН Украины, г. Донецк, Украина

E-mail: vv_skobelev@iamm.ac.donetsk.ua

Предлагается общий метод подсчета числа элементов конечных множеств, определенных в терминах классов вычетов, при помощи набора размеченных лент.

Ключевые слова: *классы вычетов, системы сравнений.*

1. Базовая конструкция

Объектом исследования является следующая «ленточная конструкция».

Под лентой будем понимать одностороннюю бесконечную (вправо) ленту, разбитую на идентичные клетки, занумерованные (слева направо) неотрицательными целыми числами (т. е. элементами множества $\mathbb{Z}_+$).

Зафиксируем число $n \in \mathbb{N}$ и расположим одну под другой $n+1$ лент, перенумеровав их сверху вниз числами $1, 2, \dots, n+1$. Ленты с номерами $1, 2, \dots, n$ назовем рабочими лентами, а ленту с номером $n+1$ — результирующей лентой.

Пусть $a_1, \dots, a_n$ — попарно взаимно простые натуральные числа, а $b_1, \dots, b_n$ — такие неотрицательные целые числа, что $b_i \leq a_i$ для всех $i = 1, \dots, n$.

Отметим клетки лент маркером в соответствии со следующими тремя правилами.

Правило 1. На i -й ($i = 1, \dots, n$) рабочей ленте среди первых a_i клеток отметим маркером произвольные b_i клеток.

Правило 2. На i -й ($i = 1, \dots, n$) рабочей ленте клетка с номером h ($h \geq a_i$) отмечена маркером тогда и только тогда, когда клетка с номером $h \bmod a_i$ отмечена маркером.

Правило 3. На результирующей ленте клетка с номером $j \in \mathbb{Z}_+$ отмечена маркером тогда и только тогда, когда клетка с номером j отмечена маркером на каждой рабочей ленте.

Обозначим через L_i ($i = 1, \dots, n+1$) начальный отрезок i -й ленты, состоящий из первых $\prod_{i=1}^n a_i$ клеток.

Назовем «ленточной конструкцией» упорядоченный набор лент

$$(L_1, \dots, L_{n+1}).$$

Покажем, что «ленточная конструкция» применима для подсчета числа элементов конечных множеств, определенных в терминах классов вычетов.

2. «Ленточная» теорема

Следующая теорема характеризует количество отмеченных клеток результирующей ленты в «ленточной конструкции» $(L_1, \dots, L_{n+1})$.

Теорема 1. В точности $\prod_{i=1}^n b_i$ клеток результирующей ленты L_{n+1} отмечены маркером.

Доказательство. Из определения «ленточной конструкции» $(L_1, \dots, L_{n+1})$ вытекает, что процесс разметки клеток результирующей ленты L_{n+1} можно осуществить *методом решета*, состоящим из n этапов, причем на i -м этапе ($i = 1, \dots, n$) участвует только результирующая лента L_{n+1} и i -я рабочая лента L_i . Эти этапы имеют следующий вид.

На 1-м этапе на результирующей ленте L_{n+1} маркером отмечаются те и только те клетки, для которых соответствующие клетки 1-й рабочей ленты L_1 отмечены маркером.

На i -м этапе ($i = 2, \dots, n$) изменим разметку результирующей ленты L_{n+1} следующим образом: сотрем маркеры с тех и только тех клеток результирующей ленты L_{n+1} , для которых соответствующие клетки i -й рабочей ленты L_i не отмечены маркером.

Методом индукции подсчитаем число клеток, отмеченных маркером на результирующей ленте L_{n+1} .

Рассмотрим 1-й этап. На этом этапе участвуют только 1-я рабочая лента L_1 и результирующая лента L_{n+1} , у которой ни одна из клеток не отмечена маркером.

Из правил 1 и 2 вытекает, что после 1-го этапа:

1) на результирующей ленте L_{n+1} отмечено маркером в точности $b_1 \cdot \prod_{j=2}^n a_j$ клеток, причем отмечены те и только те клетки, номера которых имеют вид

$$r + a_1 \cdot h \quad (h = 0, 1, \dots, \prod_{j=2}^n a_j - 1),$$

где r ($0 \leq r \leq a_1 - 1$) — номер отмеченной маркером клетки 1-й ленты;

2) среди первых a_1 клеток результирующей ленты L_{n+1} маркером отмечены в точности b_1 клеток.

Предположим, что после $(i-1)$ -го этапа ($i = 2, \dots, n$):

1) на результирующей ленте L_{n+1} отмечено маркером в точности $(\prod_{j=1}^{i-1} b_j) \cdot (\prod_{j=i}^n a_j)$ клеток, причем отмечены те и только те клетки, номера которых имеют вид

$$r_1 + (\prod_{j=1}^{i-1} a_j) \cdot h_1 \quad (h_1 = 0, 1, \dots, \prod_{j=i}^n a_j - 1),$$

где r_1 ($0 \leq r_1 \leq \prod_{j=1}^{i-1} a_j - 1$) — номер клетки, отмеченной маркером на каждой из лент $L_1, \dots, L_{i-1}$;

2) среди первых $\prod_{j=1}^{i-1} a_j$ клеток результирующей ленты L_{n+1} маркером отмечены в точности $\prod_{j=1}^{i-1} b_j$ клеток.

Рассмотрим i -й этап ($i = 2, \dots, n$). На этом этапе участвуют только i -я рабочая лента L_i и результирующая лента L_{n+1} .

Из правил 1 и 2 вытекает, что число отмеченных маркером клеток на ленте L_i равно $b_i \cdot (\prod_{j=1}^{i-1} a_j) \cdot (\prod_{j=i+1}^n a_j)$, причем на ленте L_i отмечены маркером те и только те клетки, номера которых имеют вид

$$r_2 + a_i \cdot h_2 \quad (h_2 = 0, 1, \dots, (\prod_{j=1}^{i-1} a_j) \cdot (\prod_{j=i+1}^n a_j) - 1),$$

где r_2 ($0 \leq r_2 \leq a_i - 1$) — номер отмеченной маркером клетки ленты L_i .

Рассмотрим фрагменты лент L_i и L_{n+1} , состоящие из первых

$$a_i \cdot \prod_{j=1}^{i-1} a_j = \prod_{j=1}^i a_j$$

клеток.

Зафиксируем номер r_2 ($0 \leq r_2 \leq a_i - 1$) отмеченной маркером клетки ленты L_i .

Для каждого фиксированного номера r_1 ($0 \leq r_1 \leq \prod_{j=1}^{i-1} a_j - 1$) отмеченной маркером клетки ленты L_{n+1} числа

$$r_1 + \left(\prod_{j=1}^{i-1} a_j \right) \cdot h_1 \quad (h_1 = 0, 1, \dots, a_i - 1) \quad (1)$$

образуют полную систему вычетов по модулю a_i . Следовательно, только для одного из чисел (1) истинно сравнение

$$r_1 + \left(\prod_{j=1}^{i-1} a_j \right) \cdot h_1 \equiv r_2 \pmod{a_i}.$$

Итак, в результате выполнения i -го этапа каждая пара чисел

$$(r_1, r_2) \quad (0 \leq r_1 \leq \prod_{j=1}^{i-1} a_j - 1; 0 \leq r_2 \leq a_i - 1)$$

определяет на фрагменте результирующей ленты L_{n+1} , состоящем из первых $\prod_{j=1}^i a_j$ клеток, единственную отмеченную маркером клетку.

Отсюда вытекает, что после выполнения i -го этапа на фрагменте результирующей ленты L_{n+1} , состоящем из первых $\prod_{j=1}^i a_j$ клеток, число отмеченных маркером клеток равно

$$\left(\prod_{j=1}^{i-1} b_j \right) \cdot b_i = \prod_{j=1}^i b_j.$$

На оставшейся части результирующей ленты L_{n+1} эта разметка периодически повторяется. Следовательно, после выполнения i -го этапа общее число отмеченных маркером клеток результирующей ленты L_{n+1} равно

$$\left(\prod_{j=1}^i b_j \right) \cdot \left(\prod_{j=i+1}^n a_j \right). \quad (2)$$

Положив $i = n$ в (2), получим утверждение теоремы. ■

3. Приложения

Покажем, каким образом теорема 1 может быть применена при решении задач теории чисел, связанных с подсчетом количеств натуральных чисел, обладающих заданным свойством [1, 2].

Пример 1. Докажем свойство *мультипликативности* функции Эйлера $\varphi(k)$ ($k \in \mathbb{N}$), определяющей количество чисел, взаимно простых с числом k и не превосходящих k , а именно: для любых взаимно простых чисел $l_1, l_2 \in \mathbb{N}$ истинно равенство

$$\varphi(l_1 \cdot l_2) = \varphi(l_1) \cdot \varphi(l_2).$$

Положим $n = 2$ и рассмотрим «ленточную конструкцию»

$$(L_1, L_2, L_3),$$

где $a_i = l_i$ и $b_i = \varphi(l_i)$ для $i = 1, 2$.

Сформулируем правило 1 в следующем виде: на i -й ($i = 1, 2$) рабочей ленте среди первых a_i клеток маркером отмечены те и только те b_i клеток, номера которых — числа, взаимно простые с числом l_i .

Известно, что число a взаимно просто с числом $l_1 \cdot l_2$ тогда и только тогда, когда число a взаимно просто как с числом l_1 , так и с числом l_2 .

Отсюда вытекает, что в силу правила 3 клетка с номером r результирующей ленты L_3 отмечена маркером тогда и только тогда, когда число r взаимно просто с числом $l_1 \cdot l_2$.

Следовательно, число отмеченных маркером клеток результирующей ленты L_3 равно $\varphi(l_1 \cdot l_2)$.

Из теоремы 1 вытекает, что

$$\varphi(l_1 \cdot l_2) = b_1 \cdot b_2 = \varphi(l_1) \cdot \varphi(l_2),$$

что и требовалось доказать.

Пример 2. Докажем формулу Эйлера, а именно: если $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, где $p_1, \dots, p_n$ — попарно различные простые числа, то

$$\varphi(m) = m \cdot \prod_{i=1}^n (1 - p_i^{-1}).$$

Рассмотрим «ленточную конструкцию»

$$(L_1, \dots, L_{n+1}),$$

где $a_i = p_i^{\alpha_i}$ и $b_i = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1}$ для всех $i = 1, \dots, n$.

Сформулируем правило 1 в следующем виде: на i -й ($i = 1, \dots, n$) рабочей ленте среди первых a_i клеток маркером отмечены те и только те b_i клеток, номера которых — числа, взаимно простые с числом p_i .

Отсюда вытекает, что в силу правила 3 клетка с номером r результирующей ленты L_{n+1} отмечена маркером тогда и только тогда, когда число r взаимно просто с каждым из чисел $p_1, \dots, p_n$.

Следовательно, число отмеченных маркером клеток результирующей ленты L_{n+1} равно $\varphi(m)$.

Из теоремы 1 вытекает, что

$$\varphi(m) = \prod_{i=1}^n b_i = \prod_{i=1}^n (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = m \cdot \prod_{i=1}^n (1 - p_i^{-1}),$$

что и требовалось доказать.

Принимая во внимание, что в последнее время наблюдается тенденция к систематическому применению теории конечных колец и модулей линейных форм над конечными кольцами в процессе решения задач криптографии (по крайней мере, при решении задач анализа и синтеза поточных шифров), можно заключить, что теоретическое исследование этой общей комбинаторной схемы является актуальным как для комбинаторного анализа, так и с прикладной точки зрения. Анализ такой общей комбинаторной схемы является предметом дальнейших исследований.

В заключение автор выражает благодарность рецензенту, замечания которого позволили уточнить некоторые результаты.

ЛИТЕРАТУРА

1. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003. 382 с.
2. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. М.: Мир, 1988. 430 с.