УДК 512.552.37+519.115

В.В. СКОБЕЛЕВ

О ДВУХ ПОСЛЕДОВАТЕЛЬНОСТЯХ МНОЖЕСТВ ОТОБРАЖЕНИЙ АБСТРАКТНЫХ МНОЖЕСТВ В ДЕДЕКИНДОВО КОЛЬЦО

Ключевые слова: *дедекиндовы кольца, отображения в полные системы вычетов, обратимые матрицы над конечными кольцами, китайская теорема об остатках.*

ВВЕДЕНИЕ

В последнее время наметилась устойчивая тенденция применения алгебраических моделей и методов при решении задач криптографии [1], например использование вычислений, осуществляемых в конечных кольцах, при построении современных стандартов шифрования. Поэтому актуальна разработка комбинаторных схем [2], предназначенных для подсчета числа объектов, построенных с помощью теории колец. Ясно, что любую такую схему можно представить в терминах отображений абстрактных множеств в соответствующее кольцо. Такое представление дает возможность установить внутренние связи между теорией колец [3–5], комбинаторным анализом [2] и прикладными задачами преобразования информации, в частности криптографии. В качестве кольца естественно выбрать кольцо наиболее общего вида, в рамки которого укладываются основные теоретико-числовые конструкции, используемые в современной криптографии. К такому типу колец относится дедекиндово кольцо [3].

Цель настоящей работы — исследование соотношений между двумя последовательностями множеств отображений абстрактного множества в дедекиндово кольцо, определенных в терминах полной системы вычетов по попарно взаимно простым модулям. В разд. 1 введены основные понятия, построены исследуемые последовательности отображений. В разд. 2 доказано равенство мощностей структур, построенных с помощью последовательностей множеств отображений. Установлена связь этих структур с теоремой Ленга об изоморфизме фактор-колец [5] и китайской теоремой об остатках для дедекиндовых колец. Показана возможность использования структур для подсчета числа обратимых матриц над конечным числовым кольцом. В разд. 3 построена ленточная модель, являющаяся интерпретацией исследуемых структур в случае, когда абстрактное множество одноэлементное, а дедекиндово кольцо — кольцо целых чисел. Показано, что в терминах этой модели можно исследовать теоретико-числовые конструкции, основанные на применении функции Эйлера и китайской теоремы об остатках для кольца целых чисел. Заключение содержит ряд выводов.

1. ОСНОВНЫЕ ПОНЯТИЯ

Под кольцом будем понимать дедекиндово кольцо [3], т.е. коммутативно-ассоциативное кольцо без делителей нуля с единицей $\mathcal{K} = (K, +, \cdot)$, в котором каждый собственный идеал J (т.е. $J \notin \{K, O\}$, где O — нуль-идеал, состоящий из одного нуля) представим в виде произведения конечного числа простых идеалов. Таким образом, если $J \notin \{K, O\}$ — идеал кольца $\mathcal{K}$, то $J = (p_1) \dots (p_n)$ $(n \in \mathbf{N})$, где $p_1, \dots, p_n$ — простые элементы кольца $\mathcal{K}$ (элемент $p \in K$, не являющийся делителем единицы, называется простым, если ab $(a, b \in K)$ делится на p тогда и только тогда, когда a или b делится на p). Элементы $a, b \in K$, отличные от нуля и не являющиеся делителями единицы, назовем взаимно простыми, если $((a), (b)) = K$ (где (J_1, J_2) — наибольший общий делитель идеалов J_1 и J_2, т.е. идеал, порожденный теоретико-множественным объединением идеалов J_1 и J_2 [4]). Из этого определения вытекает, что если $a, b \in K$ — взаимно простые элементы и ax $(x \in K)$ делится на b, то x делится на b. Обозначим $\pi(K, J)$ (J — идеал кольца $\mathcal{K}$) фактор-множество K / J, рассматриваемое как разбиение множества K. В дальнейшем нам понадобится следующая лемма.

Лемма. Если a и b — взаимно простые элементы дедекиндового кольца $\mathcal{K}$, то истинно равенство

$$\pi(K,(ab)) = \pi(K,(a)) \cdot \pi(K,(b)). \tag{1}$$

Доказательство. Пусть $a, b \in K$ — взаимно простые элементы кольца $\mathcal{K}$.

Покажем, что истинно неравенство

$$\pi(K,(ab)) \le \pi(K,(a)) \cdot \pi(K,(b)). \tag{2}$$

Пусть $x \equiv y(\pi(K,(ab)))$. Тогда $x - y \in (ab)$. Следовательно, существует такой элемент $z \in K$, что $x - y = abz$.

Отсюда вытекает, что $x \equiv y(\pi(K,(a)))$ и $x \equiv y(\pi(K,(b)))$, т.е. $x \equiv y(\pi(K,(a)) \times \times \pi(K,(b)))$, что и требовалось показать.

Установим, что истинно неравенство

$$\pi(K,(ab)) \ge \pi(K,(a)) \cdot \pi(K,(b)). \tag{3}$$

Пусть $x \equiv y(\pi(K,(a)))$ и $x \equiv y(\pi(K,(b)))$. Тогда существуют такие элементы $u, v \in K$, что $x - y = au$ и $x - y = bv$. Так как au делится на b, а a и b — взаимно простые элементы кольца $\mathcal{K}$, то u делится на b. Следовательно, $u = bw$, т.е. $x - y = abw$, откуда вытекает, что $x \equiv y(\pi(K,(ab)))$.

Из (2) и (3) вытекает (1).

Лемма доказана.

Воспользовавшись леммой, индукцией по числу $m \in \mathbf{N}$ несложно доказать истинность следствия.

Следствие. Если $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ — попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$, то истинно равенство

$$\pi\left(K, \left(\prod_{i=1}^{m} a_i\right)\right) = \prod_{i=1}^{m} \pi(K,(a_i)). \tag{4}$$

Зафиксировав в каждом блоке разбиения $\pi(K,(a))$ $(a \in K)$ по одному элементу, получим полную систему вычетов $\mathrm{MOD}(a)$ по модулю a. Обозначим $b < \mathrm{mod}\, a > (a, b \in K)$ такой единственный элемент $c \in \mathrm{MOD}(a)$, что элементы b и c принадлежат одному и тому же блоку разбиения $\pi(K,(a))$.

Для произвольного абстрактного множества S и произвольных попарно взаимно простых элементов $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ кольца $\mathcal{K}$ определим следующие множества отображений:

$$F_{a_i}(S) = \{f \mid f : S \to \mathrm{MOD}\,(a_i)\}\ (i = 1, \ldots, m),$$

$$F(S) = \left\{ f \mid f : S \to \mathrm{MOD}\left(\prod_{i=1}^{m} a_i\right)\right\}.$$

Зафиксировав подмножества отображений $\hat{F}_{a_i}(S) \subseteq F_{a_i}(S)$ $(i = 1, \ldots, m)$, положим

$$\tilde{F}_{a_i}(S) = \{f \in F(S) \mid f_{\mathrm{mod}\, a_i} \in \hat{F}_{a_i}(S)\} \quad (i = 1, \ldots, m),$$

где отображение $f_{\mathrm{mod}\, a_i}$ $(i = 1, \ldots, m)$ определяется равенством

$$f_{\mathrm{mod}\, a_i}(s) = f(s) < \mathrm{mod}\, a > \quad (s \in S).$$

2. СООТНОШЕНИЕ МЕЖДУ $\hat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ И $\tilde{F}_{a_i}(S)$ $(i = 1, \ldots, m)$

Основное соотношение между последовательностями множеств отображений $\hat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ и $\tilde{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ характеризуется следующей теоремой.

Теорема 1. Для любого множества S и произвольных попарно взаимно простых элементов $a_1, \dots, a_m$ $(m \in \mathbf{N})$ дедекиндового кольца $\mathcal{K}$ истинно равенство

$$\left| \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S) \right| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right|. \tag{5}$$

Доказательство. Для доказательства равенства (5) достаточно построить инъекции $\varphi : \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S) \to \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S)$ и $\psi : \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \to \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S)$.

Определим отображение $\varphi : \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S) \to F(S)$ следующим образом: значением $\varphi(f_1, \dots, f_m)$ $((f_1, \dots, f_m) \in \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S))$ является такое отображение $f \in F(S)$, что $f(s)$ $(s \in S)$ — элемент $\alpha_s \in \mathrm{MOD}\left(\prod_{i=1}^{m} a_i \right)$, содержащийся в блоке B разбиения $\pi\left(K, \left(\prod_{i=1}^{m} a_i \right) \right)$, являющемся пересечением таких блоков $B_1, \dots, B_m$, соответственно разбиений $\pi(K, (a_1)), \dots, \pi(K, (a_m))$, что элемент $f_i(s) \in \mathrm{MOD}(a_i)$ $(i = 1, \dots, m)$ принадлежит блоку B_i. В силу следствия 1 такое определение корректно.

Поскольку $f_{\mathrm{mod}\, a_i} = f_i$ $(i = 1, \dots, m)$, то $f \in \widetilde{F}_{a_i}(s)$ $(i = 1, \dots, m)$. Значит, $f \in \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S)$. Таким образом, $\varphi : \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S) \to \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S)$. А так как

$$(f_1^{(1)}, \dots, f_m^{(1)}) \neq (f_1^{(2)}, \dots, f_m^{(2)}) \Rightarrow \varphi(f_1^{(1)}, \dots, f_m^{(1)}) \neq \varphi(f_1^{(2)}, \dots, f_m^{(2)})$$

для любых $(f_1^{(1)}, \dots, f_m^{(1)}), (f_1^{(2)}, \dots, f_m^{(2)}) \in \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S)$, то φ — инъекция.

Определим отображение $\psi : \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \to \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S)$ равенством

$$\psi(f) = (f_{\mathrm{mod}\, a_1}, \dots, f_{\mathrm{mod}\, a_m}) \left(f \in \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right).$$

Такое определение корректно, поскольку

$$f \in \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \Leftrightarrow (\forall\, i = 1, \dots, m)(f \in \widetilde{F}_{a_i}(S)) \Leftrightarrow (\forall\, i = 1, \dots, m)(f_{\mathrm{mod}\, a_i} \in \hat{F}_{a_i}(S)) \Leftrightarrow$$

$$\Leftrightarrow (f_{\mathrm{mod}\, a_1}, \dots, f_{\mathrm{mod}\, a_m}) \in \underset{i=1}{\overset{m}{\times}} \hat{F}_{a_i}(S).$$

Пусть $f \neq g$ $\left(f, g \in \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S)\right)$. Тогда существует такой элемент $s \in S$, что $f(s) \neq g(s)$. Это означает, что элементы $f(s)$ и $g(s)$ принадлежат разным блокам B' и B'' разбиения $\pi\left(K, \left(\prod_{i=1}^{m} a_i \right) \right)$.

В силу следствия блоки разбиения $\pi\left(K, \left(\prod_{i=1}^{m} a_i \right) \right)$ являются пересечениями блоков разбиений $\pi(K, (a_1)), \dots, \pi(K, (a_m))$. Поэтому $B' = \bigcap_{i=1}^{m} B_i'$ и $B'' = \bigcap_{i=1}^{m} B_i''$, где B_i', B_i'' $(i = 1, \dots, m)$ — блоки разбиения $\pi(K, (a_i))$.

Поскольку $B' \neq B''$, то существует такое $j \in \{1, \ldots, m\}$, что $B'_j \neq B''_j$. Отсюда вытекает, что $f_{\bmod a_j}(s)$ и $g_{\bmod a_j}(s)$ — различные элементы множества MOD(a_j), т.е. $f_{\bmod a_j} \neq g_{\bmod a_j}$.

Следовательно, $\psi(f) \neq \psi(g)$, т.е. ψ — инъекция.

Теорема доказана.

Если $\hat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ — конечные множества, то равенство (5) естественно переписать в виде

$$\prod_{i=1}^{m} |\hat{F}_{a_i}(S)| = \left| \bigcap_{i=1}^{m} \tilde{F}_{a_i}(S) \right|. \tag{6}$$

Рассмотрим некоторые применения равенств (5) и (6).

Пример 1. Пусть $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ — попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$. В [5, с. 83] установлен изоморфизм фактор-колец, специальным случаем которого является изоморфизм $\mathcal{K} / \prod_{i=1}^{m} (a_i) \leftrightarrow \prod_{i=1}^{m} \mathcal{K} / (a_i)$.

Пусть $|S| = 1$. Тогда множество $F_{a_i}(S)$ $(i = 1, \ldots, m)$ можно рассматривать как множество MOD(a_i). Положив $\hat{F}_{a_i}(S) = F_{a_i}(S)$ $(i = 1, \ldots, m)$, заключаем, что в рассматриваемом случае равенство (5) устанавливает равномощность фактор-колец $\mathcal{K} / \prod_{i=1}^{m} (a_i)$ и $\prod_{i=1}^{m} \mathcal{K} / (a_i)$, а отображения φ и $\psi = \varphi^{-1}$, построенные в доказательстве теоремы 1, — изоморфизм соответствующих фактор-колец.

Пример 2. Пусть $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ — попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$, а $|S| = 1$. Зафиксировав произвольные элементы $b_1, \ldots, b_m$ кольца $\mathcal{K}$, положим $\hat{F}_{a_i}(S) = \{f_i\}$ $(i = 1, \ldots, m)$, где $f_i(s) = b_i < \bmod a_i >$. Тогда равенство (6) примет вид

$$\left| \bigcap_{i=1}^{m} \tilde{F}_{a_i}(S) \right| = 1,$$

где $f \in \bigcap_{i=1}^{m} \tilde{F}_{a_i}(S)$ — такое отображение, что $f(s)$ — единственный элемент $c \in \mathrm{MOD}\left(\prod_{i=1}^{m} a_i \right)$, удовлетворяющий условию $c = b_i < \bmod a_i >$ для всех $i = 1, \ldots, m$.

Таким образом, показано, что система сравнений $x \equiv b_i \,(\mathrm{mod}\,(a_i))$ $(i = 1, \ldots, m)$ имеет единственное решение, принадлежащее множеству $\mathrm{MOD}\left(\prod_{i=1}^{m} a_i \right)$, т.е. доказан вариант китайской теоремы об остатках для дедекиндовых колец.

Пример 3. В [6, 7] установлено, что основные нетривиальные подмножества линейных автоматов над кольцом $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$ $(n \in \mathbf{N})$ (где $a \oplus b = a + b (\mathrm{mod}\, n)$, $a \circ b = ab (\mathrm{mod}\, n)$) характеризуются в терминах обратимых матриц над кольцом $\mathcal{Z}_n$. По этой причине оценки мощностей этих подмножеств автоматов включают в себя в явном виде число обратимых матриц над кольцом $\mathcal{Z}_n$.

В [8] показано, что схему подсчета числа обратимых матриц над кольцом $\mathcal{Z}_n$ можно представить в следующем виде.

Пусть $\mathbf{M}_l^{\mathrm{inv}}(p, k)$ (где p — простое число, а $k \in \mathbf{N}$) — множество всех обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_{p^k}$. Непосредственный анализ линейной независимости столбцов матрицы $A \in \mathbf{M}_l^{\mathrm{inv}}(p, 1)$ показывает, что $|\mathbf{M}_l^{\mathrm{inv}}(p, 1)| = p^{l^2} \prod_{i=1}^{l} (1 - p^{-i})$.

Далее, любая матрица $A \in \mathbf{M}_l^{\mathrm{inv}}(p, k)$ единственным образом может быть пред-

ставлена в виде $A = B \oplus C$, где $B \in \mathbf{M}_l^{\text{inv}}(p,1)$, а C — $l \times l$-матрица, каждый элемент которой является необратимым элементом кольца $\mathcal{Z}_{p^k}$. Следовательно, $|\mathbf{M}_l^{\text{inv}}(p,k)| = |\mathbf{M}_l(p,k)| \prod_{i=1}^{l}(1-p^{-i})$, где $\mathbf{M}_l(p,k)$ — множество всех $l \times l$-матриц над кольцом $\mathcal{Z}_{p^k}$.

Теперь мощность множества $\mathbf{M}_l^{\text{inv}}(n)$ всех обратимых $l \times l$-матриц над кольцом $\mathbf{Z}_n$, где $n = p_1^{k_1} \dots p_m^{k_m}$ $(m \in \mathbf{N})$, а $p_1, \dots p_m$ — попарно различные простые числа, может быть вычислена следующим образом.

Пусть дедекиндово кольцо $\mathcal{K}$ совпадает с кольцом целых чисел, а множество S содержит l^2 элементов. Тогда множество отображений $F_{p_i^{k_i}}(S)$ $(i = 1, \dots, m)$ может быть отождествлено с множеством матриц $\mathbf{M}_l(p_i, k_i)$. Выбрав в качестве множества отображений $\hat{F}_{p_i^{k_i}}(S)$ $(i = 1, \dots, m)$ множество матриц $\mathbf{M}_l^{\text{inv}}(p_i, k_i)$, заключаем, что множество отображений $\widetilde{F}_{p_i^{k_i}}(S)$ $(i = 1, \dots, m)$ состоит из всех $l \times l$-матриц над кольцом $\mathcal{Z}_n$, определитель которых не сравним с нулем по mod p_i. Следовательно, $\mathbf{M}_l^{\text{inv}}(n) = \bigcap_{i=1}^{m} \widetilde{F}_{p_i^{k_i}}(S)$. Применив равенство (6), получим

$$\left|\mathbf{M}_l^{\text{inv}}(n)\right| = \left(\prod_{i=1}^{m} |\mathbf{M}_l(p_i, k_i)|\right) \prod_{j=1}^{m}\prod_{i=1}^{l}(1-p_j^{-i}).$$

3. ЛЕНТОЧНАЯ МОДЕЛЬ

Рассмотрим случай, когда дедекиндово кольцо $\mathcal{K}$ совпадает с кольцом целых чисел, S — одноэлементное множество, а $a_1, \dots, a_m \in \mathbf{N} \setminus \{1\}$ $(m \in \mathbf{N})$ — попарно взаимно простые числа. В этом случае, как обычно, считаем, что $\text{MOD}(a_i) = \{0,1, \dots, a_i - 1\}$.

Выбрав произвольные неотрицательные целые числа $b_1, \dots, b_m$ такие, что $b_i \le a_i$ $(i = 1, \dots, m)$ и положив $|\hat{F}_{a_i}(S)| = b_i$ $(i = 1, \dots, m)$, получим, что равенство (6) имеет следующий вид:

$$\left|\bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S)\right| = \prod_{i=1}^{m} b_i. \tag{7}$$

Равенство (7) имеет содержательную интерпретацию в терминах следующей геометрической модели, исследованной в [9], которую назовем ленточной моделью.

Под лентой будем понимать одностороннюю бесконечную вправо ленту, разбитую на клетки, занумерованные неотрицательными целыми числами. Расположив $m+1$ лент одну над другой, занумеруем их сверху вниз целыми неотрицательными числами. Ленты с номерами $1, \dots, m$, назовем рабочими лентами, а ленту с номером 0 — результирующей лентой. Разметим ленты маркером в соответствии со следующими правилами.

Правило 1. Среди первых a_i $(i = 1, \dots, m)$ клеток рабочей ленты с номером i отметим маркером те и только те b_i клеток, номера которых являются значениями отображений, принадлежащих множеству $\hat{F}_{a_i}(S)$.

Правило 2. На рабочей ленте с номером i $(i = 1, \dots, m)$ клетка с номером h $(h \ge a_i)$ отмечена маркером тогда и только тогда, когда маркером отмечена клетка этой ленты, номер которой равен $h <$ mod $a_i >$.

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

Замечание 1. Из правил 1–3 вытекает, что все многообразие разметок лент определяется именно правилом 1, т.е. выбором множеств $\hat{F}_{a_i}(S)$ $(i = 1, \dots, m)$.

Пусть L_i $(i = 0, 1, \ldots, m)$ — начальный отрезок ленты с номером i, состоящий из первых $\prod_{r=1}^{m} a_r$ клеток. Назовем ленточной моделью упорядоченный набор лент

$$(L_0; L_1, \ldots, L_m). \tag{8}$$

В терминах ленточной модели формулировка равенства (7) имеет следующий вид.

Теорема 2 (ленточная теорема). Для любых попарно взаимно простых чисел $a_1, \ldots, a_m \in \mathbf{N} \setminus \{1\}$ $(m \in \mathbf{N})$ при любых таких неотрицательных целых числах $b_1, \ldots, b_m$, что $b_i \le a_i$ $(i = 1, \ldots, m)$, маркером отмечено в точности $\prod_{r=1}^{m} b_r$ клеток результирующей ленты L_0.

Замечание 2. Ленточная модель исследована в [9] непосредственно, без использования математического аппарата, введенного в настоящей работе для формулировки и доказательства теоремы 1. Приведенное в [9] доказательство теоремы 2 в «лоб» достаточно длинное, громоздкое и основано на комбинации метода решета и индукции по числу рабочих лент.

Рассмотрим некоторые приложения ленточной модели.

Пример 4. Пусть φ — функция Эйлера, т.е. $\varphi(n)$ $(n \in \mathbf{N})$ — количество чисел, взаимно-простых с числом n и меньших, чем число n. Докажем мультипликативность функции Эйлера: для любых взаимно простых чисел $k_1, k_2 \in \mathbf{N} \setminus \{1\}$ истинно равенство

$$\varphi(k_1 k_2) = \varphi(k_1)\varphi(k_2).$$

Положив $m = 2$ в (8), построим ленточную модель $(L_0; L_1, L_2)$, для которой $a_i = k_i$ $(i = 1, 2)$, а множество $\hat{F}_{a_i}(S)$ состоит из всех отображений $f \in F_{a_i}(S)$, значением которых является число, взаимно простое с числом a_i.

Для этой модели $b_i = \varphi(a_i)$ $(i = 1, 2)$, а среди первых a_i $(i = 1, 2)$ клеток рабочей ленты L_i маркером отмечены те и только те b_i клеток, номера которых — числа, взаимно простые с числом a_i.

Числа a_1 и a_2 взаимно простые. Поэтому число a взаимно просто с числом $a_1 a_2$ тогда и только тогда, когда a взаимно простое с каждым из чисел a_1 и a_2. Отсюда вытекает, что клетка результирующей ленты L_0 отмечена маркером тогда и только тогда, когда ее номер — число, взаимно простое с числом $a_1 a_2$. Следовательно, число клеток результирующей ленты L_0, отмеченных маркером, равно $\varphi(a_1 a_2)$.

Применив ленточную теорему, получим $\varphi(k_1 k_2) = \varphi(a_1 a_2) = b_1 b_2 = \varphi(k_1)\varphi(k_2)$, что и требовалось доказать.

Пример 5. Пусть φ — функция Эйлера. Докажем формулу Эйлера: если $n = p_1^{k_1} \ldots p_m^{k_m}$ $(n \in \mathbf{N} \setminus \{1\})$ — каноническое разложение числа n, то

$$\varphi(n) = n \prod_{i=1}^{m} (1 - p_i^{-1}). \tag{9}$$

Числа $p_1^{k_1}, \ldots, p_m^{k_m}$ попарно взаимно простые. Построим ленточную модель (8), для которой $a_i = p_i^{k_i}$ $(i = 1, \ldots, m)$, а множество $\hat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ состоит из всех отображений $f \in F_{a_i}(S)$, значением которых является число, взаимно простое с числом a_i.

Для этой модели $b_i = \varphi(a_i)$ $(i = 1, \ldots, m)$, а среди первых a_i $(i = 1, \ldots, m)$ клеток рабочей ленты L_i маркером отмечены те и только те b_i клеток, номера которых — числа, взаимно простые с числом a_i.

Числа $a_1, \ldots, a_m$ попарно взаимно простые. Поэтому число a взаимно простое с числом $\prod_{i=1}^{m} a_i$ тогда и только тогда, когда оно взаимно простое с каждым из чисел $a_1, \ldots, a_m$. Отсюда вытекает, что клетка результирующей ленты L_0 отмечена мар-

кером тогда и только тогда, когда ее номер взаимно прост с числом $\prod_{i=1}^{m} a_i$. Следовательно, число клеток результирующей ленты L_0, отмеченных маркером, равно $\varphi\left(\prod_{i=1}^{m} a_i\right)$.

Применив ленточную теорему, получим

$$\varphi(n) = \varphi\left(\prod_{i=1}^{m} a_i\right) = \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} \varphi(p_i^{k_i}). \tag{10}$$

Воспользовавшись в (10) равенствами $\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1}$ $(i = 1, \dots, m)$, получим (9).

Пример 6. Докажем следующий вариант китайской теоремы об остатках: если $k_1, \dots, k_m \in \mathbf{N} \setminus \{1\}$ — попарно взаимно простые числа, то для любых чисел $c_1, \dots, c_m \in \mathbf{Z}$ система сравнений

$$x \equiv c_i \pmod{k_i} \quad (i = 1, \dots, m) \tag{11}$$

имеет единственное решение по модулю $\prod_{i=1}^{m} k_i$.

Обозначим r_i $(i = 1, \dots, m)$ остаток от деления числа c_i на число k_i. Заменим систему сравнений (11) эквивалентной системой сравнений

$$x \equiv r_i \pmod{k_i} \quad (i = 1, \dots, m). \tag{12}$$

Построим ленточную модель (8), для которой $a_i = k_i$ $(i = 1, \dots, m)$, а множество $\hat{F}_{a_i}(S)$ $(i = 1, \dots, m)$ состоит из единственного отображения $f \in F_{a_i}(S)$, значением которых является число r_i.

Для этой модели $b_i = 1$ $(i = 1, \dots, m)$, а среди первых a_i $(i = 1, \dots, m)$ клеток рабочей ленты L_i маркером отмечена единственная клетка, номер которой равен r_i.

Отсюда вытекает, что клетка результирующей ленты L_0, имеющая номер j $(j = 0, 1, \dots, \prod_{i=1}^{m} a_i - 1)$, отмечена маркером тогда и только тогда, когда число j сравнимо с каждым из чисел r_i $(i = 1, \dots, m)$ по модулю a_i. Последнее означает, что число j — решение системы сравнений (12), т.е. число j — решение системы сравнений (11).

Применив ленточную теорему, получим, что число решений системы сравнений (11) по модулю $\prod_{i=1}^{m} k_i$ равно $\prod_{i=1}^{m} b_i = \prod_{i=1}^{m} 1 = 1$.

Пример 7. В теореме 1 используется конечный набор попарно взаимно простых элементов $a_1, \dots, a_m$ $(m \in \mathbf{N})$ дедекиндового кольца $\mathcal{K}$. Покажем, что теорему 1 нельзя обобщить на бесконечный набор попарно взаимно простых элементов a_i $(i \in \mathbf{N})$, т.е., что ложно утверждение о том, что для любого множества S и произвольного бесконечного набора a_i $(i \in \mathbf{N})$ попарно взаимно простых элементов дедекиндового кольца $\mathcal{K}$ истинно равенство

$$\left|\prod_{i=1}^{\infty} \hat{F}_{a_i}(S)\right| = \left|\bigcap_{i=1}^{\infty} \tilde{F}_{a_i}(S)\right|.$$

Для этого достаточно показать, что для обобщения ленточной модели на бесконечное число лент, т.е. для модели

$$(L_0; L_1, \dots, L_m, \dots) \tag{13}$$

не имеет места следующее обобщение ленточной теоремы: для любых попарно взаимно простых чисел a_i $(i \in \mathbf{N})$ при любых таких неотрицательных целых числах b_i $(i \in \mathbf{N})$, что $b_i \le a_i$ $(i \in \mathbf{N})$, маркером отмечено в точности $\prod_{r=1}^{\infty} b_r$ клеток результирующей ленты L_0.

Построим следующую обобщенную ленточную модель (13).

Зафиксируем возрастающую последовательность попарно взаимно простых чисел a_i ($i \in \mathbf{N}$), а множества отображений $\hat{F}_{a_i}(S)$ ($i \in \mathbf{N}$) выберем так, что:

1) $\hat{F}_{a_1}(S)$ состоит из любого одного отображения $f \in F_{a_1}(S)$;

2) $\hat{F}_{a_i}(S)$ ($i \geq 2$) состоит из любого одного такого отображения $f \in F_{a_i}(S)$, что $a_{i-1} \leq f(s) < a_i$.

Тогда $b_i = 1$ для всех $i \in \mathbf{N}$ и, следовательно, $\prod_{r=1}^{\infty} b_r = 1$.

Покажем, что ни одна клетка результирующей ленты L_0 не отмечена маркером.

Предположим противное, т.е., что существует клетка результирующей ленты L_0, отмеченная маркером. Пусть j ($j \in \mathbf{Z}_+$) — номер этой клетки.

Так как a_i ($i \in \mathbf{N}$) — возрастающая последовательность натуральных чисел, то существует такое число i_0, что $a_{i_0} > j$. Клетка с номером j рабочей ленты L_{i_0+1} не отмечена маркером. Поэтому клетка с номером j результирующей ленты L_0 также не отмечена маркером. Получено противоречие.

Следовательно, ложно предположение о том, что существует клетка результирующей ленты L_0, отмеченная маркером, т.е. ни одна клетка результирующей ленты L_0 не отмечена маркером.

ЗАКЛЮЧЕНИЕ

В настоящей работе показано, что равенства (5) и (6) дают возможность с единых позиций исследовать задачи, сформулированные в терминах последовательностей множеств отображений $\hat{F}_{a_i}(S)$, $\tilde{F}_{a_i}(S)$ ($i = 1, \ldots, m$). Возможность подсчета числа соответствующих комбинаторных объектов проиллюстрирована в примерах 2, 3 и 6. Построение и анализ последовательностей множеств отображений $\hat{F}_{a_i}(S)$, $\tilde{F}_{a_i}(S)$ ($i = 1, \ldots, m$), представляющих применяемые в криптографии комбинаторные объекты, определенные в терминах конечных колец, представляет одно из возможных направлений исследований.

Ленточная модель (9) дает возможность подсчитать число решений системы сравнений (пример 6). Однако она не дает возможности вычислить эти решения. Такая ситуация обусловлена правилом разметки результирующей ленты L_0, которое, в свою очередь, однозначно определяется правилом построения последовательности $\hat{F}_{a_i}(S)$ ($i = 1, \ldots, m$). Исследование влияния правил разметки результирующей ленты L_0 на правила построения исходных последовательностей множеств отображений абстрактного множества в дедекиндовы кольца и анализ соотношений между этими последовательностями отображений — другое направление исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Харин Ю.С., Берник В.И., Матвеев Г.В. и др. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 382 с.
2. Сачков В.Н. Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982. — 384 с.
3. Курош А.Г. Лекции по общей алгебре. — М.: Наука, 1973. — 400 с.
4. Ван дер Варден Б.Л. Алгебра. — М.: Наука, 1979. — 624 с.
5. Ленг С. Алгебра. — М.: Мир, 1968. — 564 с.
6. Скобелев В.В. Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Доп. НАНУ. — 2007. — № 10. — С. 44–49.
7. Скобелев В.В. Анализ структуры класса линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Кибернетика и системный анализ. — 2008. — № 3. — С. 60–74.
8. Скобелев В.В. Точная формула для числа обратимых матриц над конечным кольцом // Труды ИПММ НАН Украины. — 2009. — 18. — С. 155–158.
9. Скобелев В.В. «Ленточная» теорема и ее приложения // Прикладная дискретная математика. — 2009. — № 4 (6). — С. 84–89.

Поступила 07.06.2010