УДК 512.552.37+519.115

В. В. Скобелев

Анализ некоторых отображений множеств в дедекиндовы кольца

(Представлено академиком НАН Украины А. А. Летичевским)

Досліджено співвідношення між множинами відображень абстрактної множини S у повні системи залишків за скінченним набором попарно взаємно простих елементів дедекіндового кільця та множинами відображень множини S у повну систему залишків за добутком цих елементів. Встановлено, що отримані результати можуть бути застосовані для комбінаторного аналізу об'єктів, побудованих у термінах скінченних числових кілець і використовуваних у прикладних задачах перетворення інформації.

1. Исследование различных классов отображений абстрактных множеств в те или иные кольца дает возможность установить внутренние связи между теорией колец [1–3], комбинаторикой [4], а также приложениями теории колец к решению задач преобразования информации [5]. Актуальность таких исследований обоснована, в частности, тем, что практически каждый кандидат на современный стандарт шифрования (например, в европейском и японском проектах, соответственно, NESSIE и CRYPTREC) основан на фрагментарном использовании вычислений в конечных кольцах.

2. Пусть $\mathcal{K} = (K, +, \cdot)$ — дедекиндово кольцо, а (a) $(a \in K)$ — идеал, порожденный элементом a. Зафиксировав в каждом классе фактор-кольца $\mathcal{K}/(a)$ $(a \in K)$ по одному элементу, получим полную систему вычетов $\mathtt{MOD}(a)$ по модулю a. Обозначим через $b\langle \mathtt{mod} a\rangle$ $(a, b \in K)$ такой единственный элемент $c \in \mathtt{MOD}(a)$, что элементы b и c принадлежат одному и тому же классу фактор-кольца $\mathcal{K}/(a)$. Отличные от нуля и не являющиеся делителями единицы элементы a, $b \in K$ назовем взаимно простыми, если $((a), (b)) = \mathcal{K}$.

Пусть S — произвольное (абстрактное) множество, а $a_1, \ldots, a_m \in K$ $(m \in \mathbb{N})$ — попарно взаимно простые элементы кольца $\mathcal{K}$. Положим

$$\mathcal{F}_{a_i}(S) = \{f \mid f\colon S \to \mathtt{MOD}(a_i)\} \qquad (i = 1, \ldots, m),$$

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

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

$$\widetilde{\mathcal{F}}_{a_i}(S) = \{f \in \mathcal{F}(S) \mid f_{\mathtt{mod}\ a_i} \in \widehat{\mathcal{F}}_{a_i}(S)\} \qquad (i = 1, \ldots, m),$$

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

$$f_{\mathtt{mod}a_i}(s) = f(s)\langle \mathtt{mod}\ a_i\rangle \qquad (s \in S).$$

Построением инъективных отображений $\varphi\colon \widehat{\mathcal{F}}_{a_1}(S) \times \cdots \times \widehat{\mathcal{F}}_{a_m}(S) \to \bigcap\limits_{i=1}^{m} \widetilde{\mathcal{F}}_{a_i}(S)$ и $\psi\colon \bigcap\limits_{i=1}^{m} \widetilde{\mathcal{F}}_{a_i}(S) \to \varphi\colon \widehat{\mathcal{F}}_{a_1}(S) \times \cdots \times \widehat{\mathcal{F}}_{a_m}(S)$ доказывается, что истинна

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

$$|\widehat{\mathcal{F}}_{a_1}(S) \times \cdots \times \widehat{\mathcal{F}}_{a_m}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{\mathcal{F}}_{a_i}(S) \right|. \tag{1}$$

В случае, когда $\widehat{\mathcal{F}}_{a_i}(S)$ $(i = 1, \ldots, m)$ — конечные множества, равенство (1) естественно переписать в виде

$$\prod_{i=1}^{m} |\widehat{\mathcal{F}}_{a_i}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{\mathcal{F}}_{a_i}(S) \right|. \tag{2}$$

3. Рассмотрим некоторые применения равенств (1) и (2).

Пример 1. Пусть $a_1, \ldots, a_m \in K$ $(m \in \mathbb{N})$ — попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$. В [6, с. 83] доказано существование изоморфизма между фактор-кольцами, специальным случаем которого является изоморфизм

$$\mathcal{K} \Big/ \prod_{i=1}^{m} (a_i) \longleftrightarrow \prod_{i=1}^{m} \mathcal{K}/(a_i).$$

Пусть $|S| = 1$. Тогда множество $\mathcal{F}_{a_i}(S)$ можно отождествить с множеством $\mathtt{MOD}(a_i)$. Положив $\widehat{\mathcal{F}}_{a_i}(S) = \mathcal{F}_{a_i}(S)$ $(i = 1, \ldots, m)$, заключаем, что равенство (1) устанавливает равномощность фактор-колец $\mathcal{K}/\prod\limits_{i=1}^{m}(a_i)$ и $\prod\limits_{i=1}^{m} \mathcal{K}/(a_i)$, а используемые при доказательстве теоремы 1 отображения φ и $\psi = \varphi^{-1}$ — изоморфизм этих фактор-колец.

Пример 2. Пусть $a_1, \ldots, a_m \in K$ $(m \in \mathbb{N})$ — попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$, $|S| = 1$ и $b_i \in K$ $(i = 1, \ldots, m)$. Положив $\widehat{\mathcal{F}}_{a_i}(S) = \{f_i\}$ $(i = 1, \ldots, m)$, где $f_i(s) = b_i \langle \mathtt{mod} a_i \rangle$, получим, что равенство (2) имеет вид

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

где $f \in \bigcap\limits_{i=1}^{m} \widetilde{\mathcal{F}}_{a_i}(S)$ — отображение, для которого $c = f(s)$ — единственный такой элемент множества $\mathtt{MOD}\left(\prod\limits_{i=1}^{m} a_i\right)$, что $c = b_i \langle \mathtt{mod}\ a_i \rangle$ для всех $i = 1, \ldots, m$. Это означает, что система сравнений $x \equiv b_i (\mathtt{mod}\ a_i)$ $(i = 1, \ldots, m)$ имеет единственное решение, принадлежащее множеству $\mathtt{MOD}\left(\prod\limits_{i=1}^{m} a_i\right)$, т. е. равенство (2) дает возможность доказать вариант китайской теоремы об остатках для дедекиндовых колец.

Пример 3. В [7, 8] доказано, что структура основных нетривиальных подмножеств линейных автоматов над кольцом $\mathcal{Z}_n = (\mathbb{Z}_n, \oplus, \circ)$ (где $a \oplus b = a + b (\mathtt{mod}\ n)$ и $a \circ b = ab (\mathtt{mod}\ n)$) может быть охарактеризована в терминах обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$. В силу этого обстоятельства в оценках мощностей указанных множеств автоматов присутствует число обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$. В [9] показано, что подсчет числа обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$ можно осуществить в соответствии со следующей схемой.

Пусть $\mathtt{M}_l^{\mathrm{inv}}(p, k)$ (p — простое число, $k \in \mathbb{N}$) — множество всех обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_{p^k}$. Анализируя линейную независимость столбцов матрицы $A \in \mathtt{M}_l^{\mathrm{inv}}(p, 1)$, заключаем, что

$$|\mathtt{M}_l^{\mathrm{inv}}(p, 1)| = p^{l^2} \prod_{i=1}^{l} (1 - p^{-i}).$$

А так как для любой матрицы $A \in \mathtt{M}_l^{\mathrm{inv}}(p,k)$ существует единственное представление в виде $A = B \oplus C$, где $B \in \mathtt{M}_l^{\mathrm{inv}}(p,1)$, а C — $l \times l$-матрица, каждый элемент которой — необратимый элемент кольца $\mathcal{Z}_{p^k}$, то

$$|\mathtt{M}_l^{\mathrm{inv}}(p,k)| = |\mathtt{M}_l(p,k)| \prod_{i=1}^{l}(1-p^{-i}),$$

где $\mathtt{M}_l(p,k)$ — множество всех $l \times l$-матриц над кольцом $\mathcal{Z}_{p^k}$.

Вычислим теперь мощность множества $\mathtt{M}_n^{\mathrm{inv}}(l)$ всех обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$, где $n = p_1^{k_1} \cdots p_m^{k_m}$ — каноническое разложение числа n.

Положим $\mathcal{K} = (\mathbb{Z}, +, \cdot)$ и зафиксируем l^2-элементное множество S. Отождествив множество $\mathcal{F}_{p_i^{k_i}}(S)$ $(i = 1, \ldots, m)$ с множеством $\mathtt{M}_l(p,k)$, а множество $\widehat{\mathcal{F}}_{p_i^{k_i}}(S)$ $(i = 1, \ldots, m)$ — с множеством $\mathtt{M}_l^{\mathrm{inv}}(p,k)$, заключаем, что $\widetilde{\mathcal{F}}_{p_i^{k_i}}(S)$ — это множество всех $l \times l$-матриц над кольцом $\mathcal{Z}_n$, определитель которых не сравним с нулем по модулю p_i. Следовательно,

$$\mathtt{M}_n^{\mathrm{inv}}(l) = \bigcap_{i=1}^{m} \widetilde{\mathcal{F}}_{p_i^{k_i}}(S).$$

Применив равенство (2), получим

$$|\mathtt{M}_n^{\mathrm{inv}}(l)| = \left(\prod_{i=1}^{m} \mathtt{M}_l(p,k) \right) \prod_{j=1}^{m} \prod_{i=1}^{l} (1 - p_j^{-i}).$$

4. Пусть $\mathcal{K}$ — кольцо целых чисел, $\mathtt{MOD}(a) = \{0, 1, \ldots, a-1\}$, S — одноэлементное множество, а $a_1, \ldots, a_m \in \mathbb{N} \setminus \{1\}$ $(m \in \mathbb{N})$ — попарно взаимно простые числа. Тогда $|\widehat{\mathcal{F}}_{a_i}(S)| = b_i \leqslant a_i$ $(i = 1, \ldots, m)$ и равенство (2) принимает следующий вид:

$$\left| \bigcap_{i=1}^{m} \widetilde{\mathcal{F}}_{a_i}(S) \right| = \prod_{i=1}^{m} b_i. \tag{3}$$

Равенство (3) допускает интерпретацию в терминах следующей ленточной модели, построенной в [10].

Разобьем одностороннюю бесконечную вправо ленту на идентичные клетки, которые занумеруем неотрицательными целыми числами. Расположим $m+1$ лент одну над другой и занумеруем их сверху вниз неотрицательными целыми числами. Ленты с номерами $1, \ldots, m$ — рабочие ленты, а лента с номером 0 — результирующая лента. Разметим ленты маркером в соответствии с правилами:

1) среди первых a_i $(i = 1, \ldots, m)$ клеток i-й рабочей ленты маркером отмечены b_i клеток, номера которых — значения отображений, принадлежащих множеству $\widehat{\mathcal{F}}_{a_i}(S)$;

2) на i-й рабочей ленте $(i = 1, \ldots, m)$ клетка с номером h $(h \geqslant a_i)$ отмечена маркером тогда и только тогда, когда отмечена маркером клетка этой же ленты, имеющая номер $h\langle \mathtt{mod}\ a \rangle$;

3) клетка результирующей ленты, имеющая номер $j \in \mathbb{Z}_+$, отмечена маркером тогда и только тогда, когда клетка с этим номером отмечена маркером на каждой из рабочих лент.

Пусть $\mathtt{L}_i$ $(i = 1, \ldots, m)$ — начальный отрезок i-й ленты, состоящий из первых $\prod\limits_{i=1}^{m} a_i$ клеток. Назовем ленточной моделью упорядоченный набор лент

$$(\mathtt{L}_0; \mathtt{L}_1, \ldots, \mathtt{L}_m). \tag{4}$$

В терминах модели (4) равенство (3) может быть представлено следующим образом.

Теорема 2. *Пусть $a_1, \ldots, a_m \in \mathbb{N} \setminus \{1\}$ $(m \in \mathbb{N})$ — попарно взаимно простые числа. Для любых таких чисел $b_1, \ldots, b_m \in \mathbb{Z}_+$, что $b_i \leqslant a_i$ $(i = 1, \ldots, m)$ в точности $\prod\limits_{i=1}^{m} b_i$ клеток результирующей ленты $\mathtt{L}_0$ отмечено маркером.*

Покажем, что теорема 2 может быть применена для решения задач теории чисел. С это целью в следующих примерах построим соответствующую ленточную модель.

Пример 4. Ленточная модель (4), предназначенная для доказательства свойства мультипликативности функции Эйлера $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$, где $a_1.a_2 \in \mathbb{N} \setminus \{1\}$ — взаимно простые числа, имеет вид $(\mathtt{L}_0; \mathtt{L}_1, \mathtt{L}_2)$, где $\widehat{\mathcal{F}}_{a_i}(S)$ $(i = 1, 2)$ состоит из всех $f \in \mathcal{F}_{a_i}(S)$, значение которых — число, взаимно простое с числом a_i.

Отсюда вытекает, что для доказательства формулы Эйлера $\varphi(n) = n \prod\limits_{i=1}^{m}(1 - p_i^{-1})$, где $n = p_1^{k_1} \cdots p_m^{k_m}$ — каноническое разложение числа n, можно применить ленточную модель (4), для которой $a_i = p_i^{k_i}$ $(i = 1, \ldots, m)$, а $\widehat{\mathcal{F}}_{a_i}(S)$ $(i = 1, \ldots, m)$ состоит из всех $f \in \mathcal{F}_{a_i}(S)$, значение которых — число, взаимно простое с числом a_i.

Пример 5. Для доказательства варианта китайской теоремы об остатках, утверждающего, что для любых попарно взаимно простых чисел $a_1, \ldots, a_m \in \mathbb{N} \setminus \{1\}$ система сравнений

$$x \equiv c_i (\mathtt{mod}\ a_i) \qquad (i = 1, \ldots, m)$$

имеет единственное решение по модулю $\prod\limits_{i=1}^{m} a_i$, можно применить ленточную модель (4), для которой $\widehat{\mathcal{F}}_{a_i}(S) = \{f_i\}$ $(i = 1, \ldots, m)$, где $f_i \in \mathcal{F}_{a_i}(S)$ — отображение, значение которого — число $c_i \langle \mathtt{mod}\ a_i \rangle$.

5. Ленточная модель (4) и теорема 2 характеризуют потенциальную возможность или невозможность усиления формулировки теоремы 1, так как они представляют собой интерпретацию равенств (1) и (2).

В частности, теорема 1 не может быть усилена за счет перехода к бесконечной последовательности попарно простых элементов a_i $(i \in \mathbb{N})$ дедекиндового кольца $\mathcal{K}$. Возможность такого усиления теоремы 1 автоматически приводит к обобщенной ленточной модели $(\mathtt{L}_0; \mathtt{L}_1, \ldots, \mathtt{L}_m, \ldots)$ и к истинности утверждения о том, что для любых попарно взаимно простых чисел $a_i \in \mathbb{N} \setminus \{1\}$ $(i \in \mathbb{N})$ при любых таких числах $b_i \in \mathbb{Z}_+$ $(i \in \mathbb{N})$, что $b_i \leqslant a_i$ $(i \in \mathbb{N})$ в точности $\prod\limits_{i=1}^{\infty} b_i$ клеток результирующей ленты $\mathtt{L}_0$ отмечено маркером.

Контрпример этого утверждения — последовательность $\widehat{\mathcal{F}}_{a_i}(S) = \{f_i\}$ $(i \in \mathbb{N})$, где $f_1 \in \mathcal{F}_{a_1}(S)$ — произвольное отображение, а $f_i \in \mathcal{F}_{a_i}(S)$ $(i \geqslant 2)$ — произвольное такое отображение, что $a_{i-1} \leqslant f_i(s) < a_i$.

В заключение отметим: полученные результаты показывают, что рассмотренный класс отображений абстрактных множеств в дедекиндовы кольца дает возможность исследовать с единых позиций прикладные задачи, в которых применяются объекты, построенные в терминах конечных числовых колец. Класс таких прикладных задач определяет выбор дедекиндового кольца $\mathcal{K}$, абстрактного множества S и множеств отображений $\widehat{\mathcal{F}}_{a_i}(S)$ $(i = 1, \ldots, m)$. Таким образом, в работе созданы основы построения комбинаторной схемы,

предназначенной для анализа характеристик объектов, построенных в терминах конечных числовых колец. Детальное исследование этой схемы — возможное направление дальнейших исследований.

1. *Ван дер Варден Б. Л.* Алгебра. – Москва: Наука, 1979. – 624 с.
2. *Курош А. Г.* Лекции по общей алгебре. – Москва: Наука, 1973. – 400 с.
3. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 1. – Москва: Изд-во иностр. лит., 1963. – 374 с.
4. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. – Москва: Наука, 1982. – 384 с.
5. *Харин Ю. С., Берник В. И., Матвеев Г. В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
6. *Ленг С.* Алгебра. – Москва: Мир, 1968. – 564 с.
7. *Скобелев В. В.* Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathcal{Z}_{p^k}$ // Доп. НАН України. – 2007. – No 10. – С. 44–49.
8. Скобелев *В. В.* Анализ структуры класса линейных автоматов над кольцом $\mathcal{Z}_{p^k}$ // Кибернетика и системн. анализ. – 2008. – No 3. – С. 60–74.
9. Скобелев *В. В.* Точная формула для числа обратимых матриц над конечным кольцом // Тр. ИПММ НАН Украины. – 2009. – **18**. – С. 155–158.
10. *Скобелев В. В.* "Ленточная" теорема и ее приложения // Прикл. дискрет. математика. – 2009. – No 4(6). – С. 84–89.

Институт прикладной математики и механики НАН Украины, Донецк

Поступило в редакцию 10.06.2010

V. V. Skobelev

Analysis of some mappings of sets to Dedekind rings

Some interrelation between sets of mappings of an abstract set S to complete residue systems by a finite collection of pairwise relatively prime elements of any Dedekind ring and sets of mappings of the set S to the complete residue system by the product of above-pointed elements is studied. It is illustrated that the established results can be applied to combinatorial analysis of objects determined into terms of finite number rings used in applied problems of information transformation.