УДК 518.6+681.3

©2009. **В.В. Скобелев**

ТОЧНАЯ ФОРМУЛА ДЛЯ ЧИСЛА ОБРАТИМЫХ МАТРИЦ НАД КОНЕЧНЫМ КОЛЬЦОМ

Развит математический аппарат, на основе которого найдена формула для точного подсчета числа обратимых матриц над кольцом $\mathbf{Z}_l$ ($l \in \mathbf{N}$).

Введение. Для широкого класса задач дискретной математики типичными являются объекты, определяемые таким набором $n \times n$-матриц $(A_1, \ldots, A_l)$ над кольцом $Z_m = (\mathbf{Z}_m, \oplus, \circ)$ (где $a \oplus b = (a+b)\ (mod\ m)$, $a \circ b = a \cdot b\ (mod\ m)$), что l_1 матриц являются обратимыми, l_2 матриц – необратимыми, а l_3 матриц – произвольными, где $l_1, l_2, l_3 \in \mathbf{Z}_+$ – такие фиксированные числа, что $l_1 + l_2 + l_3 = l$.

Именно в таких терминах в [1] охарактеризованы системы линейных уравнений, а также нетривиальные множества обратимых автоматов над кольцом Z_{p^k} (где p – простое число, $k \in \mathbf{Z}$). При этом для подсчета мощностей подмножеств автоматов использовалась следующая установленная в [2] оценка числа обратимых $n \times n$-матриц над кольцом Z_{p^k}

$$n! \cdot (p-1)^n \cdot p^{-n^2} \cdot |\mathtt{M}_n(p,k)| \le |\mathtt{M}_n^{inv}(p,k)| \le (1-p^{-n})^n \cdot |\mathtt{M}_n(p,k)|, \qquad (1)$$

где $\mathtt{M}_n(p,k)$ и $\mathtt{M}_n^{inv}(p,k)$ – множество, соответственно, всех и всех обратимых $n \times n$-матриц над кольцом Z_{p^k}.

Недостаток оценки (1) состоит в том, что отношение верхней оценки к нижней оценке неограниченно возрастает с ростом числа n. Поэтому естественно возникает задача поиска обозримой точной формулы для числа обратимых матриц над произвольным кольцом Z_m. Решение этой задачи и является основной целью настоящей работы.

Структура работы следующая. В п.1 получена точная формула для числа обратимых $n \times n$-матриц над кольцом Z_{p^k}. В п.2 решена задача подсчета мощности множества общих элементов для периодических структур. На основе этих результатов в п.3 получена точная формула для числа обратимых $n \times n$-матриц над кольцом Z_m.

1. Число обратимых матриц над кольцом Z_{p^k}. Нам понадобится следующая

Лемма 1. *Для любого простого числа p истинно равенство*

$$|\mathtt{M}_n^{inv}(p,1)| = p^{n^2} \cdot \prod_{i=1}^{n}(1-p^{-i}). \qquad (2)$$

Доказательство. Так как $Z_p = GF(p)$, то $A = [\mathbf{a}_1, \ldots, \mathbf{a}_n] \in \mathtt{M}_n^{inv}(p,1)$ – обратимая матрица тогда и только тогда, когда $\mathbf{a}_1 \in \mathbf{Z}_p^n$ – ненулевой вектор-столбец и

для всех $i = 2, \ldots, n$ вектор-столбец $\mathbf{a}_i \in \mathbf{Z}_p^n$ не является линейной комбинацией вектор-столбцов $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1} \in \mathbf{Z}_p^n$. А так как число линейных комбинаций векторов $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1} \in \mathbf{Z}_p^n$ $(i = 1, \ldots, n-1)$ равно p^i, то

$$|\mathtt{M}_n^{inv}(p,1)| = (p^n - 1) \cdot (p^n - p) \cdot \cdots \cdot (p^n - p^{n-1}),$$

откуда и вытекает равенство (2). □

Теорема 1. *Для любого натурального числа k и для любого простого числа p истинно равенство*

$$|\mathtt{M}_n^{inv}(p,k)| = |\mathtt{M}_n(p,k)| \cdot \prod_{i=1}^{n}(1 - p^{-i}). \tag{3}$$

Доказательство. Каждая матрица $A \in \mathtt{M}_n(p,k)$ может быть единственным образом представлена в виде $A = B + C$, где $B \in \mathtt{M}_n(p,1)$, а $C \in \mathtt{M}_n(p,k)$ – матрица, каждый элемент которой является необратимым элементом кольца Z_{p^k}. При этом $det(A)\ (mod\ p) = det(B)\ (mod\ p)$ и $B_1 + C_1 \neq B_1 + C_1$ для любых различных матриц $B_1, B_2 \in \mathtt{M}_n(p,1)$ при любых матрицах $C_1, C_2 \in \mathtt{M}_n(p,k)$, каждый элемент которых – необратимый элемент кольца Z_{p^k}. Следовательно, $|\mathtt{M}_n^{inv}(p,k)|$ равно числу матриц $B+C$, где $B \in \mathtt{M}_n^{inv}(p,1)$, а $C \in \mathtt{M}_n(p,k)$ – матрица, каждый элемент которой является необратимым элементом кольца Z_{p^k}.

Ясно, что число матриц $C \in \mathtt{M}_n(p,k)$, у которых каждый элемент является необратимым элементом кольца Z_{p^k}, равно $p^{(k-1)\cdot n^2}$.

А так как в представлении $B + C$ выбор матриц B и C осуществляется независимо, то с учетом леммы 1 получим

$$|\mathtt{M}_n^{inv}(p,k)| = p^{n^2} \cdot \prod_{i=1}^{n}(1 - p^{-i}) \cdot p^{(k-1)\cdot n^2},$$

откуда и вытекает равенство (3). □

2. Мощность множества общих элементов для периодических структур. Пусть S – непустое конечное множество, а $a_1, \ldots, a_m \in \mathbf{N}$ – взаимно простые числа. Положим

$$F_{a_i}(S) = \{f | f : S \to \mathbf{Z}_{a_i}\}\ \ (i = 1, \ldots, m)$$

и

$$F(S) = \{f | f : S \to \mathbf{Z}_{\prod\limits_{i=1}^{n} a_i}\}.$$

Определим отображение $f_{mod\ a_i}$ $(f \in F(S); i = 1, \ldots, m)$ равенством

$$f_{mod\ a_i}(s) = f(s)\ (mod\ a_i)\ \ (s \in S).$$

Зафиксируем подмножества $\widehat{F_{a_i}}(S) \subseteq F_{a_i}(S)$ $(i = 1, \ldots, m)$ и положим

$$\widetilde{F_{a_i}}(S) = \{f \in F(S) | f_{mod\ a_i} \in \widehat{F_{a_i}}(S)\ (i = 1. \ldots, m)\}.$$

Теорема 2. *Для любого непустого множества S и для любых взаимно простых чисел $a_1, \dots, a_m \in \boldsymbol{N}$ $(a_1 < \dots < a_m)$ истинно равенство*

$$|\bigcap_{i=1}^{m} \widetilde{F_{a_i}}(S)| = \prod_{i=1}^{m} |\widehat{F_{a_i}}(S)|. \tag{4}$$

Доказательство. Представим множество $\widetilde{F_{a_i}}(S)$ $(i = 1, \dots, m)$ в виде объединения попарно непересекающихся множеств

$$F(S, f_i) = \{f \in F(S) | f_{mod\ a_i} = f_i\} \ \ (f_i \in \widehat{F_{a_i}}(S)).$$

Очевидно, что для любых $i = 1, \dots, m-1$ и $j = i+1, \dots, m$ любой элемент $\widetilde{f_i} \in F(S, f_i)$ единственным образом представим в виде

$$\widetilde{f_i}(s) = f_i(s) + a_i \cdot g_j(s),$$

где $g_j \in F_{a_j}(S)$. Отсюда вытекает, что для каждого $i = 1, \dots, m-1$ существует такое единственное отображение $g_j \in F_{a_j}(S)$ $(j > i)$, что при всех $s \in S$ имеет место равенство

$$(f_i(s) + a_i \cdot g_i(s))\ (mod\ a_j) = f_j(s).$$

Следовательно,

$$|\bigcap_{i=1}^{m} F(S, f_i)| = 1$$

для любых множеств $F(S, f_1), \dots F(S, f_m)$. А это и означает, что

$$|\bigcap_{i=1}^{m} \widetilde{F_a}(S)| = |\widehat{F_{a_1}}(S) \times \dots \times \widehat{F_{a_m}}(S)| = |\prod_{i=1}^{m} \widehat{F_{a_i}}(S)|,$$

что и требовалось показать. □

3. Число обратимых матриц над кольцом Z_l. Пусть $l = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m}$, где $p_1, \dots, p_m$ – простые числа. Обозначим через $\mathtt{M}_n(l)$ и $\mathtt{M}_n^{inv}(l)$ – множество всех и всех обратимых $n \times n$-матриц над кольцом Z_l.

Теорема 3. *Для любого числа $l = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m} \in \boldsymbol{N}$ при всех $n \in \boldsymbol{N}$ истинно равенство*

$$|\mathtt{M}_n^{inv}(l)| = (\prod_{i=1}^{m} |\mathtt{M}_n(p_i, \alpha_i)|) \cdot \prod_{j=1}^{m} \prod_{i=1}^{n} (1 - p_j^{-i}). \tag{5}$$

Доказательство. Пусть множество S содержит n^2 элементов. Ясно, что множество $F_{p_i^{\alpha_i}}(S)$ $(i = 1, \dots, m)$ может быть отождествлено с множеством $\mathtt{M}_n(p_i, \alpha_i)$. Выберем в качестве множества $\widehat{F_{p_i^{\alpha_i}}}(S)$ $(i = 1, \dots, m)$ множество $\mathtt{M}_n^{inv}(p_i, \alpha_i)$. Тогда

множество $\widetilde{F_{p_i^{\alpha_i}}}(S)$ представляет собой множество всех таких матриц $A \in \mathtt{M}_n(l)$, определитель которых не сравним с нулем по $mod\ p_i$. Следовательно, истинно равенство

$$\mathtt{M}_n^{inv}(l) = \bigcap_{i=1}^{m} \widetilde{F_{p_i^{\alpha_i}}}(S). \tag{6}$$

Из (3), (4) и (6) вытекает (5), что и требовалось доказать. □

Заключение. Формула (3) дает возможность найти точные оценки мощностей нетривиальных классов автоматов над кольцом Z_{p^k}, что существенно улучшает некоторые оценки, установленные в [1, 2]. Формула (5) дает возможность существенно обобщить ряд результатов, представленных в [1, 2]. Значение теоремы 2 не исчерпывается ее применением к выводу формулы числа обратимых матриц над конечным кольцом. О широких ее возможностях можно судить хотя бы по тому, что китайская теорема об остатках и формула Эйлера для количества чисел, взаимно-простых с данным числом являются следствиями из этой теоремы. Можно показать, что теорема 2 может быть обобщена на случай отображений в кольцо многочленов над произвольным полем [3].

1. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479с.
2. *Скобелев В.В.* Об обратимых матрицах над кольцом Z_{p^k} // Труды ИПММ НАНУ. – 2006. – Т.13. – С.185-192.
3. *Харин Ю.С. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. –382с.

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 19.03.09