УДК 512.5

ОБ ОБРАТИМОСТИ ЭЛЕМЕНТОВ В КОНЕЧНЫХ КОЛЬЦАХ

П. Г. Стеганцева, Н. В. Белая

Запорожский национальный университет

Поступила в редакцию 28.01.2014 г.

Аннотация. В статье рассматривается множество $Z_m[I]$ элементов вида $\bar{x} + \bar{y} \cdot I$, где $\bar{x}, \bar{y}$ — классы вычетов по модулю m, а $I^2 = \overline{m-1}$. Это множество является коммутативным ассоциативным кольцом с единицей относительно операций сложения и умножения классов вычетов. Исследуются необходимые и достаточные условия обратимости элементов в этом кольце. Перечисляются необратимые элементы в кольцах $Z_m[I]$ при различных значениях модуля m. Выводятся формулы для числа обратимых элементов при различных значениях модуля m. Особое внимание уделено решению этих вопросов для чисел с каноническим разложением $m = p_1^{\alpha_1} p_2^{\alpha_2}$. Частным случаем таких чисел являются числа Блюма, используемые при построении криптосистем.

Ключевые слова: кольцо, поле, класс вычетов, обратимый элемент кольца, сравнение по модулю.

ON THE INVERTIBILITY OF THE ELEMENTS IN THE FINITE RINGS

P. G. Steganceva, N. V. Belay

Abstract. This paper deals with the set $Z_m[I]$ of the elements $\bar{x} + \bar{y} \cdot I$, where $\bar{x}, \bar{y}$ - the residue class modulo m and $I^2 = \overline{m-1}$. This set is the commutative associative ring with the unit with respect to the addition and multiplication of the residue classes. The necessary and sufficient conditions of the invertibility of the elements in this ring have been investigated. The noninvertible elements of the ring $Z_m[I]$ for different values of the modulus m have been enumerated. The formulae for the number of the invertible elements for different values of the modulus m have been obtained. The special attention has been paid to the numbers with canonical factorization $m = p_1^{\alpha_1} p_2^{\alpha_2}$. The Blum numbers are the partial case of such numbers. These numbers are often used for the construction of the cryptosystems.

Keywords: ring, field, residue class, invertible element of the ring, congruence.

Среди математических структур, которыми можно наделить непустое множество, структура кольца занимает одно из важных мест. Многие утверждения алгебры и теории чисел можно сформулировать, используя понятие кольца. В теории чисел одними из основных объектов изучения являются бесконечное кольцо Z целых чисел и конечное кольцо Z_m классов вычетов по модулю m. К. Ф. Гаусс обобщил понятие целого числа на случай комплексных чисел. Множество $Z[i] = \{x + yi | x, y \in Z, i^2 = -1\}$ комплексных чисел является коммутативным ассоциативным кольцом с единицей относительно операций сложения и умножения комплексных чисел и называется кольцом целых гауссовых чисел [5]. В кольце Z обратимыми элементами являются только целые числа 1 и -1. В кольце Z_m при простом m каждый ненулевой элемент обратим, то есть такое кольцо является полем. Кольцо $Z[i]$ содержит только четыре обратимых элемента: $1, -1, i, -i$. Так же как и наряду с кольцом Z рассматривается кольцо Z_m, будет естественным наряду с кольцом $Z[i]$ рассматривать множество

$Z_m[I] = \{\bar{x} + \bar{y}I | \bar{x}, \bar{y} \in Z_m, I^2 = \overline{m-1}\}$. Целью данной статьи является построение структуры кольца на этом множестве и исследование ее свойств. В частности, решение задачи об обратимости элементов и подсчет числа обратимых элементов при различных значениях m.

ОСНОВНАЯ ЧАСТЬ

Теорема 1. *Множество $Z_m[I] = \{\bar{x} + \bar{y}I | \bar{x}, \bar{y} \in Z_m, I^2 = \overline{m-1}\}$ является коммутативным ассоциативным кольцом с единицей относительно операций сложения и умножения классов вычетов по модулю m.*

Доказательство. Напомним определение операций над классами вычетов: $\bar{a}+\bar{b} = \overline{a+b}; \bar{a}\bar{b} = \overline{ab}$. Проверка аксиом кольца выполняется стандартным образом. Например, выполнимость аксиомы коммутативности умножения подтверждается следующим рассуждением: $\forall \bar{z_1} = \bar{x_1} + \bar{y_1}I, \bar{z_2} = \bar{x_2} + \bar{y_2}I \in Z_m[I]$ имеем

$$\bar{z_1} \cdot \bar{z_2} = (\bar{x_1} + \bar{y_1}I)(\bar{x_2} + \bar{y_2}I) = \overline{x_1x_2} - \overline{y_1y_2} + \overline{x_1y_2}I + \overline{y_1x_2}I$$
$$= \overline{x_2x_1} - \overline{y_2y_1} + \overline{y_2x_1}I + \overline{x_2y_1}I = (\bar{x_2} + \bar{y_2}I)\bar{x_1} + (\bar{x_2} + \bar{y_2}I)\bar{y_1}I =$$
$$= (\bar{x_2} + \bar{y_2}I)(\bar{x_1} + \bar{y_1}I) = \bar{z_2} \cdot \bar{z_1}$$

Роль нуля в этом кольце играет элемент $\bar{0} + \bar{0}I$, а единицей является $\bar{1} + \bar{0}I$. Для каждого элемента $\bar{z} = \bar{x} + \bar{y}I$ существует противоположный элемент $-\bar{z} = \overline{m-x} + \overline{m-y}I$. □

ОБРАТИМОСТЬ ЭЛЕМЕНТОВ В КОЛЬЦЕ $Z_m[I]$

Как и в любом кольце, ненулевой элемент $\bar{z}_1 = \bar{a} + \bar{b}I$ кольца $Z[I]$ называется обратимым, если существует такой ненулевой элемент $\bar{z}_2 = \bar{x} + \bar{y}I$ этого кольца, что $\bar{z_1} \cdot \bar{z_2} = \bar{1} + \bar{0}I$. После умножения в левой части придем к системе уравнений

$$\begin{cases} \overline{a} \cdot \overline{x} - \overline{b} \cdot \overline{y} = \overline{1}, \\ \overline{b} \cdot \overline{x} - \overline{a} \cdot \overline{y} = \overline{0} \end{cases} \tag{1}$$

относительно $\bar{x}$ и $\bar{y}$. Совместность этой системы является необходимым и достаточным условием обратимости элемента $\bar{z}_1 = \bar{a} + \bar{b}I$. Следствием системы уравнений (1) является система сравнений

$$\begin{cases} x(a^2 + b^2) \equiv a(mod\ m), \\ y(-a^2 - b^2) \equiv b(mod\ m). \end{cases} \tag{2}$$

Заметим, что в случае простого m переход от системы (1) к системе (2) будет равносильным.

Теорема 2 (критерий необратимости при простом модуле)**.** *Для необратимости элемента $\bar{a} + \bar{b}I$ в кольце $Z_m[I]$ при простом модуле m необходимо и достаточно выполнение условия $\bar{a}^2 + \bar{b}^2 = \bar{0}$, или, в форме сравнения $a^2 + b^2 \equiv 0(mod\ m)$.*

Доказательство. Прямую теорему будем доказывать методом от противного. Предположим, что $\overline{a^2} + \overline{b^2} \neq \bar{0}$. Тогда $\overline{a^2} + \overline{b^2}$ является элементом множества $\{\bar{1}, \bar{2}, \ldots, \overline{m-1}\}$. Так как m простое, то $(a^2 + b^2, m) = 1$ (символ (a, b) означает НОД чисел a и b). Следовательно, система (2), а значит и система (1), имеет решение, то есть элемент $\bar{a} + \bar{b}I$ обратим. Это противоречие доказывает прямую теорему. Обратно, пусть $\bar{a}^2 + \bar{b}^2 = \bar{0}$, или $a^2 + b^2 \equiv 0(modm)$. Отсюда получим две возможности: $(a^2+b^2, m) = m$ или $a^2+b^2 = 0$. В первом случае, так как $(a, m) = 1$ и $(b, m) = 1$, система (2) , а значит и система (1) , не имеет решений, то есть элемент $\bar{a} + \bar{b}I$ необратим. Во втором случае имеем $a = b = 0$, но элемент $\bar{0} + \bar{0}I$ тоже необратим. □

Лемма 1. *Если $\bar{a}+\bar{b}I$ обратим и в $Z_m[I]$ и в $Z_n[I]$ при различных простых m и n, то он обратим в $Z_{mn}[I]$.*

Доказательство. По условию леммы системы $\begin{matrix} ax-by\equiv 1(mod\ m), \\ bx+ay\equiv 0(mod\ m) \end{matrix}$ и $\begin{matrix} ax-by\equiv 1(mod\ n), \\ bx+ay\equiv 0(mod\ n) \end{matrix}$ совместны, а значит, и система $\begin{matrix} ax-by\equiv 1(mod\ mn), \\ bx+ay\equiv 0(mod\ mn) \end{matrix}$ тоже совместна. Таким образом, $\bar{a}+\bar{b}I$ обратим в $Z_{mn}[I]$, что и требовалось доказать. □

Лемма 2. *Если элемент $\bar{a}+\bar{b}I$ обратим (необратим) в кольце $Z_m[I]$, то элемент $\bar{b}+\bar{a}I$ такжде обратим (необратим) в этом же кольце.*

Теорема 3 (критерий необратимости при непростом модуле)**.** *Пусть $m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ - каноническое разложение числа m. Для необратимости элемента $\bar{a}+\bar{b}I$ в кольце $Z_m[I]$ необходимо и достаточно выполнение условия $a^2+b^2\equiv 0(modp_i)$ для некоторого $i=\overline{1,k}$.*

Доказательство. Для прямой теоремы применим метод от противного. Пусть для любого $i=\overline{1,k}$ выполняется $a^2+b^2\not\equiv 0(modp_i)$. Тогда по теореме 2 элемент $\bar{a}+\bar{b}I$ обратим в $Z_{p_i}[I]$ для любого $i=\overline{1,k}$, а по лемме 1 он обратим и в $Z_m[I]$. Обратно, пусть существует $i=\overline{1,k}$ такое, что $a^2+b^2\equiv 0(modp_i)$. Тогда, $(a^2+b^2,p_i)=p_i$ или $a^2+b^2=0$. Рассмотрим первый случай. Если либо $a\not\equiv 0(modp_i)$, либо $b\not\equiv 0(modp_i)$, то система (2) , а значит и система (1) , несовместна. Если одновременно $a\equiv 0(modp_i)$ и $b\equiv 0(modp_i)$, то система (1) в форме сравнения имеет вид $\begin{matrix} kp_ix-lp_iy\equiv 1(mod\ m), \\ lp_ix+kp_iy\equiv 0(mod\ m). \end{matrix}$ Очевидно, что эта система не имеет решений. □

ПЕРЕЧИСЛЕНИЕ И ПОДСЧЕТ ОБРАТИМЫХ ЭЛЕМЕНТОВ В КОЛЬЦЕ $Z_m[I]$

Полученные критерии позволяют исследовать вопросы о виде обратимых и необратимых элементов, а также подсчитать их число для различных значений модуля m. В случае $m=2$ прямым вычислением легко получить, что единственным ненулевым необратимым будет элемент $\bar{1}+\bar{1}I$. Заметим, что для него условие теоремы 2 выполняется.

Теорема 4. *В кольце $Z_m[I]$, где $m=p^\alpha, p=4n+1, \alpha\geqslant 1, n\in N$ для каждого $\bar{a}=\bar{0}$ и такого, что $(a,p^\alpha)=1$ существует ровно два значения $\bar{b}=\bar{0}$ таких, что $a^2+b^2\equiv 0(mod\ p)$.*

Доказательство. Для любого a, удовлетворяющего условию $(a,p^\alpha)=1$ будет выполняться и условие $(a,p)=1$. Из теории сравнений известно, что сравнение вида $x^2\equiv a(mod\ p)$, где p простое нечетное число, имеет ровно 2 решения в том случае, когда a является квадратичным вычетом по модулю p [4, с 131]. Докажем, что для квадратичного относительно b сравнения $a^2+b^2\equiv 0(mod\ p)$ число $-a^2$ является квадратичным вычетом. Действительно, $(-a^2)^{\frac{m-1}{2}}=(-a^2)^{\frac{4n+1-1}{2}}=(-a^2)^{2n}=(-1)^{2n}\cdot a^{4n}=a^{4n+1-1}=a^{m-1}\equiv 1(mod\ m)$. Последнее сравнение записано в соответствии с малой теоремой Ферма. Таким образом, для любого a, удовлетворяющего условию $(a,p^\alpha)=1$, сравнение $a^2+b^2\equiv 0(mod\ p)$ имеет ровно два решения. □

Теорема 5. *В кольце $Z_m[I]$, где $m=p^\alpha, p=4n+1, \alpha\geqslant 1, n\in N$ для каждого $a\equiv 0(mod\ p)$существует $p^{\alpha-1}$ значений $b\equiv 0(mod\ p)$ таких, что $a^2+b^2\equiv 0(mod\ p)$.*

Доказательство. Существование решений (a, b) сравнения $a^2 + b^2 \equiv 0(mod\ p)$ таких, что $a \equiv 0(mod\ p)$ и $b \equiv 0(mod\ p)$ является очевидным фактом. Например, пара $(0, 0)$ обладает таким свойством. Легко доказывается, что если пара (a, b), в которой $a \equiv 0(mod\ p)$, является решением сравнения $a^2 + b^2 \equiv 0(mod\ p)$, то каждая из пар $(a, b + lp)$, где $l = \overline{1, p^{\alpha-1}}$ также является решением этого сравнения. □

Следствие В кольце $Z_m[I]$, где $m = p^\alpha, p = 4n + 1, \alpha \geqslant 1, n \in N$ число Q обратимых элементов равно $p^{2(\alpha-1)}(p - 1)^2$.

Доказательство. Подсчитаем число необратимых элементов. Число значений a, удовлетворяющих условию $(a, p^\alpha) = 1$, равно значению $\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$ функции Эйлера [1, с 89]. В соответствии с теоремой 4, каждое такое значение a определит два необратимых элемента $\bar{a} + \bar{b_1}I$ и $\bar{a} + \bar{b_2}I$, причем таких, что $(b_1, p^\alpha) = 1$ и $(b_2, p^\alpha) = 1$. Действительно, в противном случае пары (a, b_1) и (a, b_2) не будут решениями сравнения $a^2 + b^2 \equiv 0(mod\ p)$. Далее, если пара (a, b), где $(a, p^\alpha) = 1$, является решением сравнения $a^2 + b^2 \equiv 0(mod\ p)$, то каждая из пар $(a, b + lp), l = \overline{1, p^{\alpha-1}}$ также является решением этого сравнения, причем для каждого $l = \overline{1, p^{\alpha-1}}$ по свойству НОД имеем $(b + lp, p) = 1$. Согласно теореме 5, в случае $(a, p^\alpha) = 1$, получаем еще $p^{\alpha-1} \cdot p^{\alpha-1}$ необратимых элементов. Других пар (a, b), удовлетворяющих сравнению $a^2 + b^2 \equiv 0(mod\ p)$, нет. Таким образом, число $\bar{Q}$ необратимых элементов в этом кольце вычисляется по формуле

$$\bar{Q} = 2p^\alpha \left(1 - \frac{1}{p}\right) p^{\alpha-1} + (p^{\alpha-1})^2 = p^{2(\alpha-1)}(2p - 1),$$

а число Q обратимых элементов равно разности $p^{2\alpha} - \bar{Q} = p^{2(\alpha-1)}(p - 1)^2$, что и требовалось доказать. □

Теорема 6. *Кольцо $Z_m[I]$ при простом модуле m вида $m = 4n + 3, n \in N$ является полем.*

Доказательство. Докажем, что при любых $a = 0$, $b = 0$ сравнение $a^2 + b^2 \equiv 0(mod\ p)$ не имеет решений. Так как m простое, то $(a, m) = 1$. Тогда, для каждого фиксированного a имеем

$$(-a^2)^{\frac{m-1}{2}} = (-a^2)^{\frac{4n+3-1}{2}} = (-a^2)^{2n+1} = (-1)^{2n+1} \cdot a^{2n+1} = (-1)a^{4n+2} =$$
$$= (-1)a^{4n+3-1} = (-1)a^{m-1} \equiv -1(mod\ m),$$

то есть $-a^2$ является квадратичным невычетом по простому модулю $m = 4n+3$. Аналогично, $-b^2$ является квадратичным невычетом для сравнения $a^2 + b^2 \equiv 0(mod\ p)$ при любом фиксированном b. Единственным решением этого сравнения является нулевой элемент кольца $Z_{4n+3}[I]$. Таким образом, в этом кольце любой ненулевой элемент обратим, то есть кольцо является полем. □

Теорема 7. *В кольце $Z_m[I]$, где $m = p^\alpha, p = 4n + 3, \alpha \geqslant 1, n \in N$ для каждого $a \equiv 0(mod\ p)$ существует $p^{\alpha-1}$ значений $b \equiv 0(mod\ p)$ таких, что $a^2 + b^2 \equiv 0(mod\ p)$.*

Доказательство. В теореме 6 доказано, что в кольце $Z_{4n+3}[I]$ единственным решением сравнения $a^2 + b^2 \equiv 0(mod\ p)$ является пара $(0, 0)$. Очевидно, что в кольце $Z_{p^\alpha}[I], p = 4n + 3, \alpha \geqslant 1, n \in N$ пары $(0 + kp, 0 + lp)$, где $k, l = \overline{1, p^{\alpha-1}}$, также являются решениями этого сравнения. □

Следствие В кольце $Z_m[I]$, где $m = p^\alpha, p = 4n + 3, \alpha \geqslant 1, n \in N$ число Q обратимых элементов равно $p^{2(\alpha-1)}(p^2 - 1)$.

Доказательство. Из теоремы 7 следует, что элементы $\bar{a} + \bar{b}I$, для которых $a \equiv 0(mod\ p)$ и $a \equiv 0(mod\ p)$, являются необратимыми в этом кольце. Число $\bar{Q}$ таких элементов равно $p^{2(\alpha-1)}$. Тот факт, что пары (a, b), в которых либо $(a, p^\alpha) = 1$, либо $(p^\alpha, b) = 1$, не удовлетворяют сравнению $a^2 + b^2 \equiv 0(mod\ p)$, доказывается точно так же, как и в теореме 6. Таким образом, получаем следующую формулу для числа Q обратимых элементов в этом кольце

$$Q = p^{2\alpha} - p^{2(\alpha-1)} = p^{2(\alpha-1)}(p^2 - 1),$$

что и требовалось доказать. □

Теорема 8. *В кольце $Z_m[I]$, где $m = 2^\alpha, \alpha \geqslant 1$ число Q обратимых элементов равно числу $\bar{Q}$ необратимых элементов.*

Доказательство. Необратимые элементы определим из сравнения $a^2 + b^2 \equiv 0(mod\ 2)$. Пары $(0, 0)$ и $(1, 1)$ являются, очевидно, решениями этого сравнения. Но тогда любая из пар $(0 + 2k, 0 + 2l)$ и $(1 + 2k, 1 + 2l)$, где $k, l = \overline{1, 2^{\alpha-1}}$ также является решением этого сравнения. Общее число необратимых элементов в этом кольце равно $2 \cdot \left(2^{\alpha-1}\right)^2 = 2^{2\alpha-1}$, то есть равно числу обратимых элементов. □

Перейдем к подсчету числа обратимых элементов в кольцах $Z_m[I]$ при непростом модуле вида $m = p_1^{\alpha_1} p_2^{\alpha_2}$. Рассмотрим 3 случая:
1) $p_1 = 4n + 3, \alpha_1 \geqslant 1, n \in N$ и $p_2 = 4k + 3, \alpha_2 \geqslant 1, k \in N$;
2) $p_1 = 4n + 1, \alpha_1 \geqslant 1, n \in N$ и $p_2 = 4k + 1, \alpha_2 \geqslant 1, k \in N$;
3) $p_1 = 4n + 1, \alpha_1 \geqslant 1, n \in N$ и $p_2 = 4k + 3, \alpha_2 \geqslant 1, k \in N$.

Теорема 9. *В кольце $Z_m[I]$, где $m = p_1^{\alpha_1} p_2^{\alpha_2}$, $p_1 = 4n + 3, \alpha_1 \geqslant 1, n \in N$ и $p_2 = 4k + 3, \alpha_2 \geqslant 1, k \in N$ число необратимых элементов вычисляется по формуле* $m^2 - \left(\frac{m}{p_1}\right)^2 - \left(\frac{m}{p_2}\right)^2 + \left(\frac{m}{p_1 p_2}\right)^2$.

Доказательство. Как и в теореме 7 получим $\left(\frac{m}{p_1}\right)^2$ решений $(0 + kp_1, 0 + lp_1), k, l = \overline{1, \frac{m}{p_1}}$ сравнения $a^2 + b^2 \equiv 0(mod\ p_1)$ и $\left(\frac{m}{p_2}\right)^2$ решений $(0 + kp_2, 0 + lp_2), k, l = \overline{1, \frac{m}{p_2}}$ сравнения $a^2 + b^2 \equiv 0(mod\ p_2)$. Каждое из этих решений дает необратимый элемент рассматриваемого кольца. При этом пары $(0 + kp_1p_2, 0 + lp_1p_2)$ учитываются дважды, а число таких пар равно $\left(\frac{m}{p_1 p_2}\right)^2$. Поэтому, искомое число всех необратимых элементов рассматриваемого кольца равно $\left(\frac{m}{p_1}\right)^2 + \left(\frac{m}{p_2}\right)^2 - \left(\frac{m}{p_1 p_2}\right)^2$, а число Q обратимых элементов равно $Q = m^2 - \left(\frac{m}{p_1}\right)^2 - \left(\frac{m}{p_2}\right)^2 + \left(\frac{m}{p_1 p_2}\right)^2$. □

Пример. Пусть $m = 3 \cdot 7$. Тогда $Q = (21)^2 - (3^2 + 7^2 - 1) = 21^2 - 57$. Если же $m = 3^2 \cdot 7^2$, то $Q = (21)^4 - ((3 \cdot 7^2)^2 + (7 \cdot 3^2)^2 - (21)^2) = (21)^4 - 25137$. **Замечание**. В теории чисел числа вида $m = pq$, где p, q различные простые числа, причем $p \equiv 3(mod\ 4)$ и $q \equiv 3(mod\ 4)$, называются числами Блюма. Эти числа широко применяются при построении криптосистем.

Теорема 10. *В кольце $Z_m[I]$, где $m = p_1^{\alpha_1} p_2^{\alpha_2}, p_1 = 4n + 1, \alpha_1 \geqslant 1, n \in N$, и $p_2 = 4n + 3, \alpha_2 \geqslant 1, k \in N$ число необратимых элементов вычисляется по формуле* $2\varphi(m)\left(\frac{m}{p_1} + \frac{m}{p_1 p_2}\right) + \left(\frac{m}{p_1}\right)^2 + \left(\frac{m}{p_2}\right)^2 - \left(\frac{m}{p_1 p_2}\right)^2$.

Доказательство. В соответствии с теоремой 4, в этом кольце необратимыми будут элементы $\bar{a}+\bar{b}I$, для которых пары (a,b) удовлетворяют сравнению $a^2+b^2 \equiv 0(mod\ p_1)$, причем $(a,m)=1$, а вместе с ними и элементы, соответствующие парам $(a, b+kp_1)$, где $k = \overline{1, \frac{m}{p_1}}$. Количество таких элементов равно $2\varphi(m)\frac{m}{p_1}$. Среди этих пар есть такие, вторая компонента которых не взаимно проста с модулем. Очевидно, таких пар $2\varphi(m)\frac{m}{p_1p_2}$. Каждая из них определит пару с другим порядком компонент. Этим парам соответствуют в силу леммы 2 необратимые элементы, которые еще не учтены. В этом кольце для каждого $a \equiv 0(mod\ p_1)$ существует $\left(\frac{m}{p_1}\right)$ значений $b \equiv 0(mod\ p_1)$ таких, что $a^2+b^2 \equiv 0(mod\ p_1)$. Этот факт доказывается так же, как и в теореме 5. И, аналогично, для каждого $a \equiv 0(mod\ p_2)$ существует $\frac{m}{p_2}$ значений $b \equiv 0(mod\ p_2)$ таких, что $a^2+b^2 \equiv 0(mod\ p_2)$. При этом дважды учитываются пары (a,b), для которых $a \equiv 0(mod\ p_1p_2)$ и $b \equiv 0(mod\ p_1p_2)$. Для каждого фиксированного a такого, что $a \equiv 0(mod\ p_1)$, число таких пар равно $\frac{m}{p_1p_2}$. Учтем еще, что число решений сравнения $a \equiv 0(mod\ p_1)$ равно $\frac{m}{p_1}$, а число решений сравнения $a \equiv 0(mod\ p_2)$ равно $\frac{m}{p_2}$. Таким образом, число необратимых элементов в этом кольце равно $2\varphi(m)\left(\frac{m}{p_1}+\frac{m}{p_1p_2}+\left(\frac{m}{p_1}\right)^2+\left(\frac{m}{p_2}\right)^2-\left(\frac{m}{p_1p_2}\right)^2\right)$. □

Например, в кольце $Z_m[I]$ при $m = 3\cdot 5$ число необратимых элементов равно $2\cdot 8(3+1)+5^2+3^2-1=97$, при $m=3^2\cdot 5$ получим $\bar{Q}=873$, а при $m=4^3\cdot 5$ - $\bar{Q}=7857$.

Теорема 11. *В кольце $Z_m[I]$, где $m=p_1^{\alpha_1}p_2^{\alpha_2}, p_1=4n+1, \alpha_1 \geqslant 1, n \in N$, и $p_2=4k+1, \alpha_2 \geqslant 1, k \in N$ число необратимых элементов вычисляется по формуле $\bar{Q}=2\varphi(m)\left(\frac{m}{p_1}+\frac{m}{p_2}+\left(\frac{m}{p_1}\right)^2+\left(\frac{m}{p_2}\right)^2-\left(\frac{m}{p_1p_2}\right)^2\right)$.*

Доказательство. Как и в предыдущей теореме, нам нужно подсчитать элементы $\bar{a}+\bar{b}I$, для которых пары (a,b) удовлетворяют сравнению $a^2+b^2 \equiv 0(mod\ p_1)$ и $(a,m)=1$. Кроме того, элементы, соответствующие парам $(a, b+kp_1)$, где $k = \overline{1, \frac{m}{p_1}}$, также необратимы. Те из таких пар, для которых $b \equiv 0(mod\ p_2)$, определяют необратимые элементы вида $\bar{b}+\bar{a}I$, их число равно $2\varphi(m)\frac{m}{p_1p_2}$. Точно так же получим число $2\varphi(m)\left(\frac{m}{p_2}+\frac{m}{p_1p_2}\right)$ необратимых элементов, определяемых из сравнения $a^2+b^2 \equiv 0(mod\ p_2)$. При этом нужно учесть, что для каждого a такого, что $(a,m)=1$, есть пары, являющиеся одновременно решениями системы сравнений $\begin{cases} a^2+b^2 \equiv 0(mod\ p_1), \\ a^2+b^2 \equiv 0(mod\ p_2). \end{cases}$ Таких пар будет $\frac{4m}{p_1p_2}$ [1, с 135] для каждого фиксированного a и они учтены дважды. Итак, на этом этапе для числа необратимых элементов получим формулу $2\varphi(m)\left(\frac{m}{p_1}+\frac{m}{p_1p_2}\right)+2\varphi(m)\left(\frac{m}{p_2}+\frac{m}{p_1p_2}\right)-4\varphi(m)\left(\frac{m}{p_1p_2}\right)$. Число необратимых элементов, удовлетворяющих условиям:

$$a \equiv 0(mod\ p_1), b \equiv 0(mod\ p_1), a^2+b^2 \equiv 0(mod\ p_1)$$

или

$$a \equiv 0(mod\ p_2), b \equiv 0(mod\ p_2), a^2+b^2 \equiv 0(mod\ p_2)$$

определяется так же, как и в теореме 9. Таким образом,

$$\bar{Q} = 2\varphi(m) \left(\frac{m}{p_1} + \frac{m}{p_2} \right) + \left(\frac{m}{p_1} \right)^2 + \left(\frac{m}{p_2} \right)^2 - \left(\frac{m}{p_1 p_2} \right)^2 .$$

□

Например, для $m = 5 \cdot 13$ получаем $\bar{Q} = 2 \cdot 48(13+5) + 5^2 + 13^2 - 1 = 1921$, а для $m = 5^2 \cdot 13$ эта формула дает $\bar{Q} = 2 \cdot 240(65+25) + 65^2 + 25^2 - 25 = 48025$. Непосредственный подсчет (с использованием математических пакетов) дает те же результаты.

ВЫВОДЫ И ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

В статье исследован вопрос об обратимости элемента в конечном кольце $Z_m[I]$ элементов вида $\bar{x} + \bar{y}I$, где $\bar{x}, \bar{y}$ - классы вычетов по модулю m, а $I^2 = \overline{m-1}$. Получены необходимые и достаточные условия обратимости элемента при простом и непростом модулях. Решены комбинаторные задачи перечисления и подсчета обратимых элементов при простых модулях и непростых модулях, каноническое разложение которых имеет вид $m = p_1^{\alpha_1} p_2^{\alpha_2}$. Частным случаем чисел такого вида являются числа Блюма, которые используются при построении криптосистем. Дальнейшие исследования можно направить на рассмотрение вопросов простоты, ассоциированости элементов кольца $Z_m[I]$ и поиск приложений.

СПИСОК ЛИТЕРАТУРЫ

1. Бухштаб А.А. Теория чисел / А.А. Бухштаб. — М.: Просвещение, 1966. — 384 с.

2. Виноградов И.М. Основы теории чисел / И.М. Виноградов. — М.: Наука, 1981. — 181 с.

3. Гаусс К.Ф. Труды по теории чисел / К.Ф. Гаусс. — М.: Изд-во АН СССР, 1959. — 979 с.

4. Нестеренко Ю.В. Теория чисел: учебник для студ. высш. учеб. заведений / Ю.В. Нестеренко. — М.: Издательский центр «Академия», 2008. — 272 с.

5. Окунев Л.Я. Целые комплексные числа / Л.Я. Окунев. — М.: УЧПЕДГИЗ, 1941. — 55 с.

REFERENCES

1. Buhshtab A.A. The number theory. [Buxshtab A.A. Teoriya chisel]. M.: Prosveshenie, 1966, 384 p.

2. Vinogradov I.M. The basics of number theory. [Vinogradov I.M. Osnovy teorii chisel]. Moscow: Nauka, 1981, 181 p.

3. Gauss K.F. The writings on the number theory. [Gauss K.F. Trudy po teorii chisel]. Moscow: Publishing house AS USSR, 1959, 979 p.

4. Nesterenko U.V. Number theory: the textbook for the students of the higher school. [Nesterenko Yu.V. Teoriya chisel: uchebnik dlya stud. vyssh. ucheb. zavedenij]. Moscow.: Publishing centre “Academy”, 2008, 272 p.

5. Okunev L.I. Complex integers. [Okunev L.Ya. Celye kompleksnye chisla]. Moscow: Uchpedgiz, 1941, 55 p.

Стеганцева П. Г., к.ф.-м.н., доцент кафедры алгебры и геометрии, Запорожский национальный университет, г. Запорожье, Украина
E-mail: steg_pol@mail.ru
Тел.: +380676849973

Steganceva P. G., associate professor, department of algebra and geometry, Zaporizhzhya National University, Zaporizhzhya, Ukraine
E-mail: steg_pol@mail.ru
Tel.: +380676849973

Белая Н. В., магистр кафедры алгебры и геометрии, Запорожский национальный университет, г. Запорожье, Украина
E-mail: natali_zoryana@inbox.ru

Belay N. V., magister, department of algebra and geometry, Zaporizhzhya National University, Zaporizhzhya, Ukraine
E-mail: natali_zoryana@inbox.ru