УДК 511.2

Кольца целых чисел квадратичных полей

Журавлев Е.В., Токарев В.Н.
Алтайский государственный университет,
Алтайский государственный технический университет
evzhuravlev@mail.ru, tok321.1973@mail.ru

Аннотация

В работе рассматривается кольцо $\mathbb{Z}[\sqrt{n}] = \{a+b\sqrt{n}|a,b \in \mathbb{Z}\}$, где n – простое число. Указывается разложение элементов кольца $\mathbb{Z}[\sqrt{n}]$ на простые множители, строение его идеалов и фактор-колец.

1. Введение

Рассмотрим квадратичное поле

$$\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n}|a,b \in \mathbb{Q}\},$$

где n – свободное от квадратов целое число. Если n сравнимо с 2 или 3 по модулю 4, то кольцо целых квадратичного поля $\mathbb{Q}[\sqrt{n}]$ это множество линейных комбинаций вида $a + b\sqrt{n}$, где $a,b \in \mathbb{Z}$. Если же $n \equiv 1 \pmod 4$, то кольцо целых состоит из чисел вида $a+b\cdot\frac{1+\sqrt{n}}{2}$, $a,b \in \mathbb{Z}$. Наша цель – изучить свойства колец вида $\mathbb{Z}[\sqrt{n}] = \{a+b\sqrt{n}|a,b \in \mathbb{Z}\}$, где n - простое положительное целое число.

Определение 1. *Сопряженным элементом к* $z = a+b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ *называется элемент* $\bar{z} = a - b\sqrt{n}$.

Определение 2. *Нормой элемента* $z = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ *называется целое число* $N(z) = a^2 - nb^2$.

Заметим что:

1. $N(z) = 0 \Leftrightarrow z = 0$,
2. $\forall z \in \mathbb{Z}[\sqrt{n}]\ N(z) = N(\bar{z})$,
3. $\forall z \in \mathbb{Z} \quad N(z) = z^2$,
4. $\forall z_1, z_2 \in \mathbb{Z}[\sqrt{n}]\ N(z_1z_2) = N(z_1)N(z_2)$.

Очевидно, что обратимыми элементами кольца $\mathbb{Z}[\sqrt{n}]$ являются элементы с нормой ± 1.

Определение 3. *Пусть* $u, v, q \in \mathbb{Z}[\sqrt{n}]$. *Будем говорить, что число* u *делится (нацело) на число* v, *если существует число* q *такое, что* $u = vq$.

Определение 4. *Число из* $\mathbb{Z}[\sqrt{n}]$ *называется составным, если оно является произведением двух необратимых чисел из* $\mathbb{Z}[\sqrt{n}]$. *Иначе, число называется неразложимым.*

Определение 5. *Число из* $\alpha \in \mathbb{Z}[\sqrt{n}]$ *называется простым, если* α *– необратимое число и если* $\alpha \mid (uv)$ *для некоторых* u *и* v, *то* $\alpha \mid u$ *или* $\alpha \mid v$ *(см. [1, 2]).*

Понятие нормы и обратимого элемента тесно связано с проблемой разрешимости уравнений Пелля вида $x^2 - ny^2 = \pm 1$ (n – свободное от квадратов натуральное число), являющихся частным случаем нелинейных диофантовых уравнений.

Уравнение Пелля вида $x^2 - ny^2 = 1$ всегда имеет тривиальные решения $(1; 0)$ и $(-1; 0)$ и бесконечное множество нетривиальных (существование которых следует из теоремы Дирихле о единицах). В тоже время, для отрицательного уравнение Пелля $x^2 - ny^2 = -1$ до сих пор не существует простого алгоритма решения и не определены необходимые и достаточные условия его существования.

Предложение 1. *(Теорема Дирихле). Пусть $K = \mathbb{Q}(\alpha)$ – поле степени $m = r_1 + 2r_2$, где r_1 – число вещественных корней неприводимого многочлена α, $2r_2$ – число комплексных корней этого многочлена. Тогда группа единиц (группа обратимых элементов) кольца целых алгебраических чисел является прямым произведением $A \times \langle\varepsilon_1\rangle \times ... \times \langle\varepsilon_r\rangle$, где $r = r_1 + r_2 - 1$, $A = \langle\zeta\rangle$ – конечная циклическая группа и $\langle\varepsilon_i\rangle$ – бесконечные циклические группы.*

Евклидово кольцо это область целостности R, для которой определена евклидова функция (евклидова норма) $N : R \setminus \{0\} \to \mathbb{N}_0$, такая, что возможно деление с остатком по норме меньшей нормы делителя, то есть для любых $a, b \in R, b \neq 0$ имеется представление $a = bq + r$, для которого $N(r) < N(b)$ или $r = 0$. Кольца $\mathbb{Z}[\sqrt{m}]$, где m – положительное, но не обязательно простое число, являются евклидовыми только при $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97$ (см. [3]).

2. Арифметика кольца $\mathbb{Z}[\sqrt{n}]$

Рассмотрим кольцо $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} | a, b \in \mathbb{Z}\}$, где n – простое число. Пусть $\mathbb{Z}^*[\sqrt{n}]$ – группа обратимых чисел кольца $\mathbb{Z}[\sqrt{n}]$. Всюду далее будем полагать n таким простым целым числом, что $\mathbb{Z}[\sqrt{n}]$ – евклидово кольцо, относительно нормы $N(a + b\sqrt{n}) = a^2 - b^2 n$, и в кольце $\mathbb{Z}$ разрешимо отрицательное уравнение Пелля $x^2 - y^2 n = -1$, то есть существует обратимое число $\mu + \eta\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ с нормой $N(\mu + \eta\sqrt{n}) = -1$. Если $N(a + b\sqrt{n}) = -m$ и $N(\mu + \eta\sqrt{n}) = -1$, то $N((a + b\sqrt{n})(\mu + \eta\sqrt{n})) = m$, то есть при умножении числа с отрицательной нормой на обратимое число с нормой -1 мы получаем число с положительной нормой.

Теорема 1. *Пусть p – натуральное число. Тогда*

$$\mathbb{Z}[\sqrt{n}] / \langle p\rangle \cong \mathbb{Z}_p[\sqrt{n}],$$

где $\mathbb{Z}_p[\sqrt{n}] = \mathbb{Z}_p[x] / \langle x^2 - n\rangle$.

Доказательство. Определим отображение

$$\varphi : \mathbb{Z}[\sqrt{n}] \to Z_p[\sqrt{n}]$$

по правилу $\varphi(x + y\sqrt{n}) = [x]_p + [y]_p\sqrt{n}$, где $[\cdot]_p$ – представитель класса эквивалентности по модулю p. Это отображение, очевидно, является сюръективным кольцевым гомоморфизмом.

Докажем, что $\ker\varphi = \langle p\rangle$. Так как $\varphi(p) = [p]_p = [0]_p$, то $\langle p\rangle \subseteq \ker\varphi$. С другой стороны, если $x + y\sqrt{n} \in \ker\varphi$, то $\varphi(x + y\sqrt{n}) = [x]_p + [y]_p\sqrt{n} = [0]_p$. Следовательно, $x \equiv 0 \pmod p$ и $y \equiv 0 \pmod p$. Значит, $x = px'$ и $y = py'$ для некоторых целых чисел x' и y'. Поэтому $x + y\sqrt{n} = px' + py'\sqrt{n} = p(x' + y'\sqrt{n}) \in \langle p\rangle$. Следовательно, $\ker\varphi \subseteq \langle p\rangle$. В силу теоремы о гомоморфизмах $\mathbb{Z}[\sqrt{n}] / \langle p\rangle \cong \mathbb{Z}_p[\sqrt{n}]$. □

Теорема 2. *Пусть p – натуральное число, $p \neq 2$. Кольцо $\mathbb{Z}_p[\sqrt{n}]$ является полем тогда и только тогда, когда p – простое число, $p \neq n$ и*

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Доказательство. Предположим, что $\mathbb{Z}_p[\sqrt{n}]$ – поле. Если p – составное число, то $\mathbb{Z}_p$ содержит делители нуля, что невозможно. Значит, p - простое число.

Если $p = n$, то $(\sqrt{n})^2 = p$, $(\sqrt{n})^2 \equiv 0 \pmod{p}$, а, значит, $\mathbb{Z}_p[\sqrt{n}]$ содержит делители нуля, что невозможно.

Рассмотрим кольцевой гомоморфизм

$$\varphi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[\sqrt{n}],$$

определенный по правилу $\varphi(f(x)) = f(\sqrt{n})$, $f(x) \in \mathbb{Z}_p[x]$. Так как $\ker\varphi = \langle x^2 - n\rangle$, то по теореме о гомоморфизмах $\mathbb{Z}_p[\sqrt{n}] \cong \mathbb{Z}_p[x]/\langle x^2 - n\rangle$. Следовательно, $\mathbb{Z}_p[\sqrt{n}]$ является полем тогда и только тогда, когда многочлен $x^2 - n$ является неприводимым по модулю p, то есть уравнение $x^2 \equiv n \pmod{p}$ не имеет решений. Итак, n не делится на p, $p \neq 2$ и n не является квадратичным вычетом по модулю p, следовательно, в силу критерия Эйлера $n^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$ (символ Лежандра $\left(\frac{n}{p}\right)$ должен быть равен -1).

Для доказательства обратного утверждения достаточно повторить все рассуждения в обратном порядке. □

Заметим, что если $p = 2$ и $n \neq 2$, то кольцо $\mathbb{Z}_2[\sqrt{n}]$ не является полем, так как содержит делители нуля: $(1 + \sqrt{n})^2 = 1 + n + 2\sqrt{n} \equiv 0 \pmod{2}$.

Теорема 3. *Если p – натуральное число, $p \neq 2$, то p – простое число в $\mathbb{Z}[\sqrt{n}]$ тогда и только тогда, когда p – простое число в $\mathbb{Z}$, $p \neq n$ и*

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Доказательство. Если p – простое число в $\mathbb{Z}[\sqrt{n}]$, то идеал $\langle p\rangle$ является максимальным в $\mathbb{Z}[\sqrt{n}]$, а, значит, фактор-кольцо $\mathbb{Z}[\sqrt{n}]/\langle p\rangle$ – поле. В силу теоремы 2, p – простое число в $\mathbb{Z}$, $p \neq n$ и $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Для доказательства обратного утверждения достаточно повторить все рассуждения в обратном порядке. □

В работе [4] указано, что уравнение $x^2 - y^2 n = 2$ разрешимо в $\mathbb{Z}$ тогда и только тогда, когда $n \equiv -1 \pmod{8}$. Следовательно, при $n \neq 2$ число 2 является составным в $\mathbb{Z}[\sqrt{n}]$ тогда и только тогда, когда $n \equiv -1 \pmod{8}$. В случае $n = 2$ число $2 = \sqrt{2} \cdot \sqrt{2}$ также составное.

Заметим, что для любых $a + b\sqrt{n}, c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ справедливо равенство

$$\frac{c + d\sqrt{n}}{a + b\sqrt{n}} = \frac{(c + d\sqrt{n})(a - b\sqrt{n})}{a^2 - b^2 n} = \frac{ac - bdn}{a^2 - b^2 n} + \frac{ad - bc}{a^2 - b^2 n}\sqrt{n}.$$

Если a и b – взаимно простые целые числа, то $c + d\sqrt{n}$ содержится в идеале $\langle ak + bk\sqrt{n}\rangle$ тогда и только тогда, когда $k(a^2 - b^2 n)$ делит $ac - bdn$ и $ad - bc$ ($k \in \mathbb{Z}$).

Теорема 4. *Если a, b – взаимно простые целые числа и $a^2 - b^2 n > 0$, то*

$$\mathbb{Z}[\sqrt{n}]/\langle a + b\sqrt{n}\rangle \cong \mathbb{Z}_{a^2 - b^2 n}.$$

Доказательство. Пусть $m = a^2 - b^2 n$. Так как a и b – взаимно простые целые числа, то b – взаимно просто с числом $a^2 - b^2 n$ и поэтому элемент $[b]_m$ обратим в $\mathbb{Z}_{a^2-b^2n}$ ($[\cdot]_m$ – представитель класса эквивалентности по модулю m). Так как $a^2 - b^2 n \equiv 0 \pmod m$, то $a^2 \equiv b^2 n \pmod m$, $(ab^{-1})^2 \equiv n \pmod m$.

Определим отображение $\varphi : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z}_{a^2-b^2n}$ по правилу $\varphi(x + y\sqrt{n}) = [x - y(ab^{-1})]_m$. Очевидно, что φ является сюръективным. Пусть $\alpha = x + y\sqrt{n}$ и $\beta = z + t\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$. Тогда

$$\varphi(\alpha)\varphi(\beta) = \varphi(x + y\sqrt{n})\varphi(z + t\sqrt{n}) = [(x - yab^{-1})(z - tab^{-1})]_m =$$
$$= [xz + a^2 b^{-2} yt - (xt + yz)ab^{-1}]_m = [(xz + ytn) - (xt + yz)ab^{-1}]_m =$$
$$= \varphi((xz + ytn) + (xt + yz)\sqrt{n}) = \varphi((x + y\sqrt{n})(z + t\sqrt{n})) = \varphi(\alpha\beta).$$

Так как $\varphi(a + b\sqrt{n}) = [a - ab^{-1}b]_m = [0]_m$, то $\langle a + b\sqrt{n}\rangle \subseteq \ker\varphi$. Пусть $c + d\sqrt{n} \in \ker\varphi$ и $c + d\sqrt{n} = (a + b\sqrt{n})(x + y\sqrt{n})$, где $x, y \in \mathbb{Q}$. Так как $\varphi(c + d\sqrt{n}) = [c - ab^{-1}d]_m = [0]_m$, то $[c]_m = [ab^{-1}d]_m$, $[bc]_m = [ad]_m$, $[ad - bc]_m = [0]_m$, а, следовательно, $ad - bc = k(a^2 - b^2 n)$ для некоторого $k \in \mathbb{Z}$. Тогда из равенства

$$\frac{c + d\sqrt{n}}{a + b\sqrt{n}} = \frac{ac - bdn}{a^2 - b^2 n} + \frac{ad - bc}{a^2 - b^2 n}\sqrt{n} = x + y\sqrt{n},$$

получаем

$$y = \frac{ad - bc}{a^2 - b^2 n} = \frac{k(a^2 - b^2 n)}{a^2 - b^2 n} = k \in \mathbb{Z}.$$

Умножая равенство $[ad - bc]_m = [0]_m$ на ab, получаем $[a^2 bd - ab^2 c]_m = [a^2 b^{-2} bd - ac]_m = [0]_m$. Так как $(ab^{-1})^2 = n$, то $[ac - bdn]_m = [0]_m$, а, следовательно, $ac - bdn = k(a^2 - b^2 n)$, для некоторого $k \in \mathbb{Z}$, и

$$x = \frac{ac - bdn}{a^2 - b^2 n} = \frac{k(a^2 - b^2 n)}{a^2 - b^2 n} = k \in \mathbb{Z}.$$

Итак, x и y - целые числа, $c + d\sqrt{n} \in \langle a + b\sqrt{n}\rangle$ и $\ker\varphi \subseteq \langle a + b\sqrt{n}\rangle$. Таким образом, $\ker\varphi = \langle a + b\sqrt{n}\rangle$ и $\mathbb{Z}[\sqrt{n}] / \langle a + b\sqrt{n}\rangle \cong \mathbb{Z}_{a^2-b^2n}$. □

Теорема 5. *Если a и b – взаимно простые целые числа и $a^2 - b^2 n > 0$, то $a + b\sqrt{n}$ – простое число в $\mathbb{Z}[\sqrt{n}]$ тогда и только тогда, когда $p = a^2 - b^2 n$ – простое число в $\mathbb{Z}$.*

Доказательство. Пусть $z = a + b\sqrt{n}$ – простое число в $\mathbb{Z}[\sqrt{n}]$, тогда $\mathbb{Z}[\sqrt{n}] / \langle a + b\sqrt{n}\rangle \cong \mathbb{Z}_{a^2-b^2n}$ – поле и $a^2 - b^2 n$ – простое целое число. В обратную сторону доказательство аналогично. □

Если $p = a^2 - b^2 n$ – простое число в $\mathbb{Z}$ ($a, b \in \mathbb{Z}$) и $p \neq 2$, $p \neq n$, то

$$n^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Действительно, так как $p = a^2 - b^2 n = N(a + b\sqrt{n})$, то p – составное число в $\mathbb{Z}[\sqrt{n}]$, а, следовательно, в силу теоремы 3, $n^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Теорема 6. *Число π – простое в $\mathbb{Z}[\sqrt{n}]$ тогда и только тогда, когда оно имеет один из следующих видов:*

1. *$\pi = p\varepsilon$, где p – простое число в $\mathbb{Z}$, $p \neq 2$ и $n^{\frac{p-1}{2}} \equiv -1 \pmod p$, $\varepsilon \in \mathbb{Z}^*[\sqrt{n}]$;*
2. *$\pi = 2\varepsilon$, $\varepsilon \in \mathbb{Z}^*[\sqrt{n}]$ (только если $n \not\equiv -1 \pmod 8$ и $n \neq 2$);*
3. *$\pi = (a + b\sqrt{n})\varepsilon$, где $a^2 - b^2 n = p$ – простое число в $\mathbb{Z}$, $p \neq 2$, $n^{\frac{p-1}{2}} \equiv 1 \pmod p$, $\varepsilon \in \mathbb{Z}^*[\sqrt{n}]$;*

4. $\pi = (c + d\sqrt{n})\varepsilon$, *где* $c^2 - d^2 n = 2$, $\varepsilon \in \mathbb{Z}^*[\sqrt{n}]$ *(только если* $n \equiv -1 \pmod 8$*);*

5. $\pi = \sqrt{n}\,\varepsilon$, *где* $\varepsilon \in \mathbb{Z}^*[\sqrt{n}]$.

Доказательство. Утверждение является следствием вышеуказанных теорем. Заметим лишь, что если $a^2 - b^2 n = n$ – простое число, то a^2 делится на n и, следовательно, $a = kn$, для некоторого $k \in \mathbb{Z}$. Тогда $a^2 - b^2 n = k^2 n^2 - b^2 n = n$, $k^2 n - b^2 = 1$, $b^2 - k^2 n = -1$ и $b - k\sqrt{n}, b + k\sqrt{n} \in \mathbb{Z}^*[\sqrt{n}]$. Таким образом, $a - b\sqrt{n} = kn - b\sqrt{n} = -\sqrt{n}(b - k\sqrt{n})$ и $a + b\sqrt{n} = kn + b\sqrt{n} = -\sqrt{n}(b + k\sqrt{n})$, то есть числа $a \pm b\sqrt{n}$ имеют вид, указанный в пункте 5 условия теоремы. □

Так как мы изначально полагаем, что $\mathbb{Z}[\sqrt{n}]$ – евклидово кольцо, то $\mathbb{Z}[\sqrt{n}]$ – кольцо главных идеалов и для всякого числа $\sigma \in \mathbb{Z}[\sqrt{n}]$ единственным образом определено разложение на простые множители:

1. если $n \not\equiv -1 \pmod 8$ и $n \neq 2$, то

$$\sigma = \prod_{i=1}^{k_1} p_i^{u_i} \cdot \prod_{i=1}^{k_2} \left(a_i + b_i\sqrt{n}\right)^{v_i} \cdot 2^m \cdot \left(\sqrt{n}\right)^l \cdot \varepsilon,$$

2. если $n \equiv -1 \pmod 8$ или $n = 2$, то

$$\sigma = \prod_{i=1}^{k_1} p_i^{u_i} \cdot \prod_{i=1}^{k_2} \left(a_i + b_i\sqrt{n}\right)^{v_i} \cdot \prod_{i=1}^{k_3} \left(c_i + d_i\sqrt{n}\right)^{w_i} \cdot \left(\sqrt{n}\right)^l \cdot \varepsilon,$$

где $\varepsilon \in \mathbb{Z}^*[\sqrt{n}]$, $k_1, k_2, k_3, u_i, v_i, w_i, l, m \in \mathbb{N} \cup \{0\}$, $a_i, b_i, c_i, d_i \in \mathbb{Z}$, p_i – некоторые простые целые числа, $p_i \neq 2$, $n^{\frac{p_i - 1}{2}} \equiv -1 \pmod{p_i}$, $a_i^2 - b_i^2 n = q_i$ – простые целые числа, $q_i \neq 2$, $n^{\frac{q_i - 1}{2}} \equiv 1 \pmod{q_i}$, $c_i^2 - d_i^2 n = 2$.

Рассмотрим фактор-кольца по различным идеалам кольца $\mathbb{Z}[\sqrt{n}]$.

Случай 1. Пусть p – простое целое число, $p \neq 2$, $n^{\frac{p-1}{2}} \equiv -1 \pmod p$ и $\alpha \in \mathbb{N}$. Тогда

$$\mathbb{Z}\left[\sqrt{n}\right] / \langle p^\alpha \rangle \cong \mathbb{Z}_{p^\alpha}\left[\sqrt{n}\right] = \mathbb{Z}_{p^\alpha}[x] / \left\langle x^2 - n \right\rangle.$$

Многочлен $x^2 - [n]_p$ неприводим в $\mathbb{Z}_p$, следовательно, $S = \mathbb{Z}_{p^\alpha}[x] / \langle x^2 - n \rangle$ – локальное кольцо, которое также называют кольцом Галуа. Радикал Джекобсона $J(S) = \langle \overline{p} \rangle$, $J(S)^\alpha = 0$ и $S/J(S) = GF(p^2)$.

Случай 2. Пусть $a^2 - b^2 n = p$ – простое число в $\mathbb{Z}$, $p \neq 2$, $n^{\frac{p-1}{2}} \equiv 1 \pmod p$ и $\alpha \in \mathbb{N}$. Тогда

$$\mathbb{Z}\left[\sqrt{n}\right] / \left\langle (a + b\sqrt{n})^\alpha \right\rangle \cong \mathbb{Z}_{p^\alpha}.$$

Случай 3. Пусть $c^2 - d^2 n = 2$ и $\alpha \in \mathbb{N}$. Тогда

$$\mathbb{Z}\left[\sqrt{n}\right] / \left\langle (c + d\sqrt{n})^\alpha \right\rangle \cong \mathbb{Z}_{2^\alpha}.$$

Случай 4. Пусть $\alpha \in \mathbb{N}$. Тогда

$$\mathbb{Z}\left[\sqrt{n}\right] / \left\langle (\sqrt{n})^\alpha \right\rangle \cong \mathbb{Z}_{n^{\frac{\alpha}{2}}}\left[\sqrt{n}\right],$$

если α – четное число,

$$\mathbb{Z}\left[\sqrt{n}\right] / \left\langle (\sqrt{n})^\alpha \right\rangle = \mathbb{Z}\left[\sqrt{n}\right] / \left\langle n^k \sqrt{n} \right\rangle \cong \mathbb{Z}[x] / \left\langle x^2 - n, n^k x \right\rangle,$$

если $\alpha = 2k + 1$ – нечетное число, $k \in \mathbb{Z}$.

Теорема 7. *Пусть $\sigma \in \mathbb{Z}\left[\sqrt{n}\right]$. Тогда справедливы следующие разложения*

1. *если $n \not\equiv -1 \pmod 8$ и $n \neq 2$, то*

$$\mathbb{Z}\left[\sqrt{n}\right] / \langle\sigma\rangle \cong \bigoplus_{i=1}^{k_1} \mathbb{Z}_{p_i^{u_i}}\left[\sqrt{n}\right] \bigoplus_{i=1}^{k_2} \mathbb{Z}_{q_i^{v_i}} \bigoplus \mathbb{Z}_{2^m}\left[\sqrt{n}\right] \bigoplus \mathbb{Z}_{n^k}\left[\sqrt{n}\right]$$

или

$$\mathbb{Z}\left[\sqrt{n}\right] / \langle\sigma\rangle \cong \bigoplus_{i=1}^{k_1} \mathbb{Z}_{p_i^{u_i}}\left[\sqrt{n}\right] \bigoplus_{i=1}^{k_2} \mathbb{Z}_{q_i^{v_i}} \bigoplus \mathbb{Z}_{2^m}\left[\sqrt{n}\right] \bigoplus \mathbb{Z}[x] / \left\langle x^2 - n, n^k x\right\rangle$$

2. *если $n \equiv -1 \pmod 8$ или $n = 2$, то*

$$\mathbb{Z}\left[\sqrt{n}\right] / \langle\sigma\rangle \cong \bigoplus_{i=1}^{k_1} \mathbb{Z}_{p_i^{u_i}}\left[\sqrt{n}\right] \bigoplus_{i=1}^{k_2} \mathbb{Z}_{q_i^{v_i}} \bigoplus_{i=1}^{k_3} \mathbb{Z}_{2^{w_i}} \bigoplus \mathbb{Z}_{n^k}\left[\sqrt{n}\right]$$

или

$$\mathbb{Z}\left[\sqrt{n}\right] / \langle\sigma\rangle \cong \bigoplus_{i=1}^{k_1} \mathbb{Z}_{p_i^{u_i}}\left[\sqrt{n}\right] \bigoplus_{i=1}^{k_2} \mathbb{Z}_{q_i^{v_i}} \bigoplus_{i=1}^{k_3} \mathbb{Z}_{2^{w_i}} \bigoplus \mathbb{Z}[x] / \left\langle x^2 - n, n^k x\right\rangle$$

где $k, k_1, k_2, k_3, u_i, v_i, w_i, m \in \mathbb{N} \cup \{0\}$, p_i – простые целые числа, $p_i \neq 2$, $n^{\frac{p_i-1}{2}} \equiv -1 \pmod{p_i}$, $a_i^2 - b_i^2 n = q_i$ – простые целые числа, $a_i, b_i \in \mathbb{Z}$, $q_i \neq 2$, $n^{\frac{q_i-1}{2}} \equiv 1 \pmod{q_i}$.

Доказательство теоремы следует из китайской теоремы об остатках.

Рассмотрим частный случай – кольцо $\mathbb{Z}\left[\sqrt{2}\right]$. Это кольцо является евклидовым и отрицательное уравнение Пелля $x^2 - y^2 n = -1$ разрешимо при $n = 2$, так как $N(1+\sqrt{2}) = -1$.

Теорема 8. *Число π – простое в $\mathbb{Z}\left[\sqrt{2}\right]$ тогда и только тогда, когда оно имеет один из следующих видов:*

1. *$\pi = p\varepsilon$, где p – простое число в $\mathbb{Z}$, $p = 8k + 3$ или $p = 8k + 5$, для некоторого $k \in \mathbb{Z}$, $\varepsilon \in \mathbb{Z}^*\left[\sqrt{2}\right]$;*
2. *$\pi = (a + b\sqrt{2})\varepsilon$, где $a^2 - 2b^2 = p$ – простое число в $\mathbb{Z}$, $p = 8k + 1$ или $p = 8k + 7$, для некоторого $k \in \mathbb{Z}$, $\varepsilon \in \mathbb{Z}^*\left[\sqrt{2}\right]$;*
3. *$\pi = \sqrt{2}\,\varepsilon$, где $\varepsilon \in \mathbb{Z}^*\left[\sqrt{2}\right]$.*

Доказательство. Доказательство следует из теоремы 6. Заметим, что при $n = 2$ символ Лежандра $\left(\frac{n}{p}\right)$ вычисляется по формуле

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Следовательно, если $p = 8k+1$ или $p = 8k+7$, то число 2 является квадратичным вычетом по модулю p, а если $p = 8k + 3$ или $p = 8k + 5$, то не является ($k \in \mathbb{Z}$). □

Теорема 9. *Пусть $\sigma \in \mathbb{Z}\left[\sqrt{2}\right]$, тогда*

$$\mathbb{Z}\left[\sqrt{2}\right] / \langle\sigma\rangle \cong \bigoplus_{i=1}^{k_1} \mathbb{Z}_{p_i^{u_i}}\left[\sqrt{2}\right] \bigoplus_{i=1}^{k_2} \mathbb{Z}_{q_i^{v_i}} \bigoplus \mathbb{Z}_{2^k}\left[\sqrt{2}\right]$$

или

$$\mathbb{Z}\left[\sqrt{2}\right] / \langle\sigma\rangle \cong \bigoplus_{i=1}^{k_1} \mathbb{Z}_{p_i^{u_i}}\left[\sqrt{2}\right] \bigoplus_{i=1}^{k_2} \mathbb{Z}_{q_i^{v_i}} \bigoplus \mathbb{Z}[x] / \left\langle x^2 - 2, 2^k x\right\rangle$$

где $k, k_1, k_2, u_i, v_i, \in \mathbb{N} \cup \{0\}$, p_i – простые целые числа, $p_i = 8k_i + 3$ или $p_i = 8k_i + 5$, для некоторых $k_i \in \mathbb{Z}$, $a_i^2 - b_i^2 n = q_i$ – простые целые числа, $a_i, b_i \in \mathbb{Z}$, $p_i = 8k_i + 1$ или $p_i = 8k_i + 7$, для некоторых $k_i \in \mathbb{Z}$.

Список литературы

1. Dresden G., Dymacek W.M. Finding factors of factor rings over the Gaussian integers // Amer. Math. Monthly. — 2005. — Vol. 7(112). — P. 602–611.

2. Dekker T.J. Prime numbers in Quadratic fields // CWI Quarterly. — 1994. — no. 7. — P. 367–394.

3. Хассе Г. Лекции по теории чисел. — М. : Наука, 1953.

4. Венков Б.А. Элементарная теория чисел. — М. : Объединенное научно-техническое издательство НКТП СССР, 1937.