Math-Net.Ru
Общероссийский математический портал

М. М. Глухов, Использование колец вычетов целых алгебраических чисел для построения криптографических систем с открытым ключом,
Тр. по дискр. матем., 2007, том 10, 47–72

https://www.mathnet.ru/tdm160

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.9.173
14 июля 2025 г., 02:17:24

Труды по дискретной математике
Том 10, с. 47–72
М.: ФИЗМАТЛИТ, 2007

ИСПОЛЬЗОВАНИЕ КОЛЕЦ ВЫЧЕТОВ ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ ДЛЯ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ

М. М. ГЛУХОВ

Описывается кольцо целых алгебраических чисел поля $\mathbf{Q}\left(\sqrt[4]{D}\right)$, где D — натуральное число, свободное от квадратов и отличное от 1. Изучаются свойства его факторкольца по идеалу (m), где m — простое число или произведение двух простых чисел, и мультипликативной группы этого факторкольца, предлагается криптосхема типа RSA, основанная на использовании кольца $\mathbf{Z}\left(\sqrt[4]{D}\right)/(m)$.

ВВЕДЕНИЕ

В зарубежной литературе широко обсуждаются предложения об использовании для построения схем с открытым ключом (типа Диффи–Хеллмана (DH), Ривеста–Шамира–Адлемана (RSA), Эль–Гамаля (EG)) различных алгебраических структур, производных от колец целых алгебраических чисел, а именно, колец вычетов кольца целых алгебраических чисел и групп классов идеалов (см. [2, 4, 6–24]). Представителями схем, основанных на использовании колец вычетов целых алгебраических чисел, являются схемы типа RSA, предложенные в 1985 г. Н. Вильямсом (см. [24]) и в 1998 г. Р. Шедлером (см. [20]).

В криптосистеме Вильямса используются вычеты по модулю $n = pq$ элементов кольца $\mathbf{Z}[\sqrt{D}]$ (т. е. элементы факторкольца кольца $\mathbf{Z}[\sqrt{D}]$ по его идеалу (pq)), где p, q — различные и достаточно большие простые числа, а D — отличное от 1, свободное от квадратов и взаимно простое с pq целое число, удовлетворяющее следующему условию на символы Лежандра:

$$\left(\frac{D}{p}\right) = \varepsilon_p \equiv -p \pmod 4, \quad \left(\frac{D}{q}\right) = \varepsilon_q \equiv -q \pmod 4.$$

В криптосистеме Шедлера используются вычеты по модулю pq элементов кольца целых алгебраических чисел расширения 6-й степени поля рациональных чисел $\mathbf{Q}$, а именно, поля $\mathbf{Q}(\varepsilon, \delta)$, где ε — первообразный корень

© М. М. Глухов, 2007

3-й степени из 1, а δ — действительный корень 3-й степени из большого свободного от кубов числа D.

Для каждой из этих схем авторы доказывают, что проблема дешифрования информации по сложности эквивалентна проблеме факторизации числа $n = pq$. Доказательства эквивалентности указанных проблем в обоих случаях используют применяемые авторами достаточно специфические и сильно избыточные предварительные кодирования шифруемой информации. Шифрованный текст в этих схемах специально организуется так, чтобы можно было доказать указанную эквивалентность. Однако придуманные для этой цели способы кодирования и организации шифртекста привели к слабости схем по отношению к специально подобранной паре открытого и шифрованного текстов.

Вместе с тем сама идея использования вычетов колец целых алгебраических чисел по составному модулю pq для построения криптосистем с открытым ключом представляется весьма интересной. Такие кольца вычетов допускают при знании чисел p, q представления в виде прямых сумм конечных полей характеристик p и q, что способствует большей прозрачности системы, а потому и более полному анализу ее криптографической стойкости.

Автором в [4] была предложена криптосистема типа RSA, основанная на использовании вычетов по модулю $n = pq$ элементов биквадратичных расширений кольца целых чисел. Предварительный анализ показал, что по ряду методов анализа она является более стойкой по сравнению с первоначальной схемой RSA. Некоторым минусом этой схемы является то, что в отдельных ее вариантах имеется возможность представления используемого кольца в виде прямой суммы колец вычетов по модулю n квадратичных расширений кольца целых чисел при умении решать квадратные сравнения по модулю pq без знания простых чисел p, q. В связи с этим представляет определенный интерес построение и анализ криптосистем с открытым ключом, основанных на расширениях 4-й степени поля $\mathbf{Q}$, не являющихся биквадратичными расширениями (т. е. не являющихся последовательными расширениями 2-й степени).

§ 1. СТРОЕНИЕ КОЛЬЦА ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ ПОЛЯ $\mathbf{Q}(\sqrt[4]{D})$

Зафиксируем произвольное нечетное, свободное от квадратов и отличное от 1, положительное целое число D и обозначим через θ арифметический корень 4-й степени из D. Минимальный многочлен $m(x) = x^4 - D$ числа θ неприводим над $\mathbf{Q}$, и потому поле $\mathbf{Q}(\theta)$ является расширением 4-й степени поля $\mathbf{Q}$. Многочлен $m(x)$ имеет в поле комплексных чисел корни

$$\theta_1 = \theta, \quad \theta_2 = -\theta, \quad \theta_3 = \theta i, \quad \theta_4 = -\theta i.$$

Элементы θ_i, $i = 2, 3, 4$, называют сопряженными с θ. Два из них не содержатся в $\mathbf{Q}(\theta)$. Следовательно, $\mathbf{Q}(\theta)$ не является расширением Галуа.

Каждый элемент поля $\mathbf{Q}(\theta)$ однозначно представляется в виде

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3,$$

где a_0, a_1, a_2, $a_3 \in \mathbf{Q}$. Далее мы этот элемент иногда ради краткости будем обозначать в виде вектора (a_0, a_1, a_2, a_3). Произведение элемента α на $\beta = (b_0, b_1, b_2, b_3)$ равно элементу $\gamma = (c_0, c_1, c_2, c_3)$, где c_0, c_1, c_2, c_3 находятся по формулам

$$c_0 = a_0b_0 + a_1b_3D + a_2b_2D + a_3b_1D,$$

$$c_1 = a_0b_1 + a_1b_0 + a_2b_3D + a_3b_2D,$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0 + a_3b_3D,$$

$$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0.$$

Обозначим через $\mathbf{Q}_0(\theta)$ кольцо целых алгебраических чисел поля $\mathbf{Q}(\theta)$ и опишем его элементы.

Пусть $\alpha \in \mathbf{Q}_0(\theta)$. Число α может быть элементом степени 1, 2, 4. Хорошо известно (см., например, [3]), что элементами степени 1 являются все числа из $\mathbf{Z}$ и только они. Если число α имеет степень 2, то оно совпадает с некоторым из отличных от него и сопряженных с ним чисел, т. е. с числом, полученным заменой в записи α числа θ на некоторое сопряженное с ним число θ_i. Сопряженными с числом α являются оно само, а также числа

$$\begin{gathered}\alpha_1 = a_0 - a_1\theta + a_2\theta^2 - a_3\theta^3, \quad \alpha_2 = a_0 + a_1\theta i - a_2\theta^2 - a_3\theta^3 i, \\ \alpha_3 = a_0 - a_1\theta i - a_2\theta^2 + a_3\theta^3 i.\end{gathered} \tag{1}$$

Так как множество $\mathbf{Q}(\theta)$ состоит лишь из действительных чисел, то α может совпадать только с числом α_1, и, следовательно,

$$\alpha = (a_0, 0, a_2, 0) = a_0 + a_2\theta^2 = a_0 + a_2\sqrt{D}, \quad a_0, a_2 \in \mathbf{Q}.$$

Теперь воспользуемся тем, что α является корнем квадратного уравнения

$$x^2 - 2a_0x + a_0^2 - a_2^2D = 0.$$

Из него видно, что $\alpha \in \mathbf{Q}_0(\theta)$ в том и только том случае, когда $2a_0, a_0^2 - a_2^2D \in \mathbf{Z}$. Легко видеть, что последние условия выполняются тогда и только тогда, когда $a_0, a_2 \in \mathbf{Z}$ или $a_0 = u_0/2$, $a_2 = u_2/2$, где u_0, u_2 — целые нечетные числа и $D \equiv 1 \pmod 4$.

Пусть теперь α — элемент 4-й степени кольца $\mathbf{Q}_0(\theta)$. Найдем сначала минимальный многочлен $f_\alpha(x)$ числа α, воспользовавшись тем, что такой многочлен имеет степень 4 и, кроме корня α, имеет своими корнями и со-

пряженные с ним числа (1). Если $f_\alpha(x) = f_0 + f_1x + f_2x^2 + f_3x^3 + x^4$, то по теореме Виета находим

$$f_0 = (a_0^2 - a_2^2D)^2 - D(a_1^2 - a_3^2D)^2 - 4D(a_0a_1 - a_2a_3D)(a_0a_3 - a_1a_2),$$
$$f_1 = -4(a_0^3 - a_0a_2^2D + a_1^2a_2D + 2a_2a_3^2D^2 - 2a_0a_1a_3D),$$
$$f_2 = 6a_0^2 - 2D(a_2^2 + 2a_1a_3),$$
$$f_4 = -4a_0.$$

Известно [3], что $\alpha \in \mathbf{Q}_0(\theta)$ тогда и только тогда, когда $f_i \in \mathbf{Z}$, $i = 1, 2, 3, 4$. Поэтому из равенства $f_4 = -4a_0$ следует, что число a_0 представляется в виде $u_0/4$, где $u_0 \in \mathbf{Z}$. Так как $\mathbf{Q}_0(\theta)$ — кольцо, то $(\alpha + \alpha_1) - (\alpha_2 + \alpha_3) \in \mathbf{Q}_0(\theta)$, т. е. $4a_2\theta^2 \in \mathbf{Q}_0(\theta)$, а потому и $16a_2^2D \in \mathbf{Q}_0(\theta)$. А так как последнее число рационально, то оно целое. Отсюда, учитывая, что D нечетно, получаем: число a_2 представляется в виде $a_2 = u_2/4$, где $u_2 \in \mathbf{Z}$. Так как $\alpha - \alpha_1$, $\theta \in \mathbf{Q}_0(\theta)$, то $(\alpha - \alpha_1)\theta = 2a_1\theta^2 + 2a_3D \in \mathbf{Q}_0(\theta)$, а потому и сопряженное с ним число $2a_1\theta^2 + 2a_3D$ содержится в $\mathbf{Q}_0(\theta)$. Следовательно, $4a_3D, 4a_1\theta^2 \in \mathbf{Q}_0(\theta)$ и $4a_3D, 4a_1^2D \in \mathbf{Z}$. Отсюда видно, что $a_1 = u_1/4$, $a_3 = u_3/4$, где $u_1, u_3 \in \mathbf{Z}$. Таким образом, установлено, что

$$a_i = u_i/4, \quad u_i \in \mathbf{Z}, \ i = 0, 1, 2, 3.$$

Отсюда и из найденных выше выражений для коэффициентов f_i следует, что $\alpha \in \mathbf{Q}_0(\theta)$ в том и только том случае, когда выполнены условия делимости

$$2^3 \mid A = 3u_0^2 - Du_2^2 - 2Du_1u_3, \tag{2}$$

$$2^4 \mid B = u_0(u_0^2 - u_2^2D) + u_2D(u_1^2 + u_3^2D) - 2u_0u_1u_3D, \tag{3}$$

$$2^8 \mid C = (u_0^2 - u_2^2D)^2 - D(u_1^2 - u_3^2D)^2 - 4D(u_0u_1 - u_2u_3D)(u_0u_3 - u_1u_2). \tag{4}$$

Далее будем считать, что условия (2)–(4) выполнены, и исходя из этого будем искать u_0, u_1, u_2, u_3. При этом условимся о следующих обозначениях. Число D будем записывать в виде

$$D = 2^kt + 1,$$

где $k > 0$, t нечетно.

Если u_i — отличное от нуля четное число или отличное от единицы нечетное число, то будем соответственно писать $u_i = 2^{k_i}v_i$, $k_i > 0$, v_i нечетно; $u_i = 2^{r_i}t_i + 1$, $r_i > 0$, t_i нечетно; $i = 0, 1, 2, 3$.

Ради единообразия записей в случаях $u_i = 0$ или $u_i = 1$ будем использовать те же обозначения, полагая k_i, r_i как угодно большими натуральными числами, а v_i, t_i — равными нулю.

Из условия (2) видно, что u_0, u_2 — числа одной четности, а тогда, в силу условия (4), u_1, u_3 — также числа одной четности.

I. u_0, u_2 четны.

Тогда число $3u_0^2 - Du_2^2$ кратно четырем. Отсюда и из (2) следует, что число u_1u_3 является четным, а потому и u_1, u_3 также четны. Следовательно, число $2Du_1u_3$ кратно 8 и условие (2) равносильно сравнению

$$3 \cdot 2^{2k_0}v_0^2 - D2^{2k_2}v_2^2 \equiv 0 \pmod 8.$$

Так как D нечетно, то это сравнение выполняется лишь в случаях:

$$\text{a)}\ \ k_0 > 1,\ k_2 > 1; \quad \text{b)}\ \ k_0 = 1,\ k_2 = 1.$$

II. u_0, u_2 нечетны.

Так как $a^2 - b^2$ кратно 8 при любых нечетных a, b, то в рассматриваемом случае условие (2) равносильно сравнению

$$1 - 2^{k-1}t - (2^k t + 1)u_1u_3 \equiv 0 \pmod 4. \tag{5}$$

Если $k = 1$, то $1 - 2^{k-1}t = 1 - t$ четно и сравнение (5) выполняется лишь при условии

$$\text{c)}\ \ u_1,\ u_3 \text{ четны} \quad \text{и} \quad t \equiv 1 \pmod 4, \quad \text{т. е.} \quad D \equiv 3 \pmod 8.$$

Если $k > 1$, то сравнение (5) равносильно сравнению

$$1 - 2^{k-1}t - u_1u_3 \equiv 0 \pmod 4,$$

которое выполняется лишь при нечетных u_1, u_3, причем в этом случае должно выполняться сравнение $u_1u_3 \equiv 1 - 2^{k-1}t \pmod 4$. Так как

$$u_1u_3 - 1 \equiv 2^{r_1}t_1 + 2^{r_3}t_3 \pmod 4,$$

то последнее сравнение можно записать в виде

$$2^{r_1}t_1 + 2^{r_3}t_3 \equiv -2^{k-1}t \pmod 4.$$

Легко видеть, что это сравнение выполняется лишь при наборах чисел k, r_1, r_3, выписанных в таблице 1.

Таблица 1

	k	r_1	r_3
d_1)	2	1	> 1
d_2)	2	> 1	1
d_3)	> 2	1	1
d_4)	> 2	> 1	> 1

В итоге нами найдены все случаи, в которых выполняется условие (2).

Выясним теперь, в каких из этих случаев выполняется условие (3). Обозначим: $B = B_1 + B_2 - B_3$, где

$$B_1 = u_0(u_0^2 - u_2^2 D), \quad B_2 = u_2 D(u_1^2 + u_3^2 D), \quad B_3 = 2u_{20}u_1u_3D.$$

Введем еще обозначение $\exp_2(a)$ для максимального числа k, при котором отличное от нуля целое число a делится на 2^k. Положим также $\exp_2(0) = \infty > > n$ при любом целом n. Далее в данном параграфе вместо $\exp_2(a)$ будем писать $\exp(a)$ и называть это число экспонентой числа a.

I. u_0, u_2 четны.

В случаях a), b) числа u_1, u_3 также четны и каждое из чисел B_1, B_3 кратно 16. Следовательно, условие (3) выполняется тогда и только тогда, когда B_2 кратно 16. Так как числа u_1, u_3 четны, то число $u_1^2 + u_3^2 D$ кратно четырем. Следовательно, в случае a) число B_2 кратно 16 и условие (3) выполнено. В случае b) оно будет выполняться тогда и только тогда, когда $8 \mid u_1^2 + u_3^2 D$. Последнее же условие выполняется лишь при $k_1 > 1$, $k_3 > 1$ или $k_1 = 1$, $k_3 = 1$.

Таким образом, при четных u_0, u_2 условия (2), (3) выполняются лишь при четных же u_1, u_3, любом нечетном D и наборах показателей k_i выписанных в таблице 2.

Таблица 2

	k_0	k_1	k_2	k_3
i_1)	> 1	> 0	> 1	> 0
i_2)	1	> 1	1	> 1
i_3)	1	1	1	1

II. u_0, u_2 нечетны.

Рассмотрим случай c). Здесь, как было доказано выше, u_1, u_3 четны, и очевидно, что B_2 кратно 4 и B_3 кратно 8. Найдем B_1 в общем случае при любых нечетных u_0, u_2:

$$B_1 = u_0[(2^{2r_0}t_0^2 + 2^{r_0+1}t_0 + 1) - (2^{2r_2}t_2^2 + 2^{r_2+1}t_2 + 1)(2^k t + 1)]. \tag{6}$$

Следовательно, B_1 имеет вид: $B_1 = u_0[(8m + 1) - (8n + 1)(8l + 3)] = = 8w - 2$, где $w \in \mathbf{Z}$. Таким образом, $\exp B = 2$, и условие (3) не выполняется.

В случаях d_1)–d_4) числа u_1, u_3 также нечетны и $k > 1$. Для проверки условия (3) в этих случаях распишем сначала подробно числа B_i, $i = 1, 2, 3$, используя введенные выше обозначения для D и для нечетных u_i. Учитывая требование условия (3), мы сразу будем отбрасывать слагаемые, кратные 16. При этом неоднократно будет использоваться легко проверяемый факт

о делимости числа вида $2^{2s}m + 2^{s+1}n$ на 8 при любом натуральном s и любых нечетных натуральных m, n. В итоге получим:

$$B_1 \equiv (2^{2r_0}t_0^2 + 2^{r_0+1}t_0) - (2^{2r_2}t_2^2 + 2^{r_2+1}t_2) - 2^k t - 2^{k+r_0}t_0 t \pmod{16},$$

$$B_2 = (2^{k+1}t + 2^{k+r_2}t_2 t) + (2^{2r_1}t_1^2 + 2^{r_1+1}t_1) + (2^{2r_3}t_3^2 + 2^{r_3+1}t_3) + 2^k t + 2 + \\ + 2^{r_2+1}t_2 + 2^{2k}t^2 \pmod{16},$$

$$B_3 \equiv 2^{r_0+r_1+1}t_0 t_1 + 2^{r_0+r_3+1}t_0 t_3 + 2^{r_1+r_3+1}t_3 t_1 + 2^{r_0+1}t_0 + 2^{r_1+1}t_1 + 2^{r_3+1}t_3 + \\ + 2^{k+1}t + 2 \pmod{16}.$$

Отсюда следует, что

$$B = B_1 + B_2 - B_3 \equiv (2^{2r_0}t_0^2 - 2^{2r_2}t_2^2) + (2^{2r_1}t_1^2 + 2^{2r_3}t_3^2) - \\ - (2^{r_0+k}t_0 t - 2^{k+r_2}t_2 t) - (2^{r_0+r_1+1}t_0 t_1 + 2^{r_0+r_3+1}t_0 t_3 + 2^{r_1+r_3+1}t_3 t_1) \pmod{16}. \tag{7}$$

Слагаемые, взятые в скобки в левой части последнего сравнения, обозначим через S_1, S_2, S_3, S_4 соответственно и найдем точные значения или оценки величин $\exp(S_i)$:

$\exp(S_1) = 2$, если $\{r_0, r_2\} = \{1, b\}$, где $b > 1$, $\exp(S_1) = 4$ в противном случае;

$\exp(S_2) = 2$, если $\{r_1, r_3\} = \{1, b\}$, где $b > 1$, $\exp(S_2) = 3$, если $r_1 = r_3 = 1$, и $\exp(S_2) = 4$ в остальных случаях;

$\exp(S_3) = 3$, если $k = 2$ и $\{r_0, r_2\} = \{1, b\}$, где $b > 1$, $\exp(S_3) = 4$ в противном случае;

$\exp(S_3) = 3$, если среди чисел r_0, r_1, r_3 есть две единицы, $\exp(S_3) = 4$ в противном случае.

Теперь для нахождения экспоненты числа B воспользуемся следующими очевидными или легко проверяемыми фактами:

1) $\exp(a^2 - b^2) \geqslant 3$, $\exp(a^2 + b^2) = 1$ для любых нечетных чисел a, b;

2) если $\exp(a) \neq \exp(b)$, то $\exp(a + b) = \min\{\exp(a), \exp(b))$;

3) если $\exp(a) = \exp(b) = c$, то $\exp(a + b) > c$.

В итоге получим следующие результаты.

В случаях d_1), d_2) $\exp(B) = 2$ (и, значит, условие (3) не выполняется) при всех значениях параметров r_i, кроме

$$\{r_0, r_2\} = \{1, b\}, \quad \{r_1, r_3\} = \{1, c\}, \quad \text{где} \quad b > 1, \ c > 1. \tag{8}$$

Покажем, что при выполнении условия (8) $\exp(B) = 3$ и условие (3) также не выполняется. Пусть, например, в условии (8) $r_0 = 1$, $r_1 = 1$, $r_2 > 1$, $r_3 > 1$ (это относится к случаю d_1), в котором $k = 2$). Тогда

$$B \equiv 2^2 t_0^2 + 2^2 t_2^2 - 2^3 t_0 t - 2^3 t_0 t_1 \equiv 2^2 t_0^2 + 2^2 t_2^2 \pmod{16}.$$

Отсюда, учитывая, что $\exp(t_0^2 + t_1^2) = 1$, получаем: $\exp(B) = 3$, и, значит, условие (3) не выполняется. Аналогично к такому же результату приходим и в других вариантах условия (8).

Таким образом, в случаях d_1), d_2) условие (3) не выполняется.

В случаях d_3), d_4) $\exp(B) = 2$ при всех значениях параметров r_0, r_2, кроме вариантов

$$r_0 = 1, \quad r_2 = 1 \quad \text{или} \quad r_0 > 1, \quad r_2 > 1.$$

В этих условиях $\exp(S_1) = \exp(S_3) = 4$, $\exp(S_2) = \exp(S_4) = 3$. Поэтому $\exp(B) = 4$ и условие (3) выполняется.

Таким образом, при нечетных u_0, u_2 условия (2), (3) выполняются лишь при нечетных же u_1, u_3, и соответствующие наборы параметров k и r_i выписаны в таблице 3.

Таблица 3

	k	r_0	r_1	r_2	r_3
j_1)	> 2	1	1	1	1
j_2)	> 2	> 1	> 1	> 1	> 1
j_3)	> 2	1	> 1	1	> 1
j_4)	> 2	> 1	1	> 1	1

Выясним теперь, в каких случаях из оставшихся выполняется условие (4), т. е. $\exp(C) \geqslant 8$. Обозначим: $C = C_1 - C_2 - C_3$, где

$$C_1 = (u_0^2 - u_2^2 D)^2, \quad C_2 = D(u_1^2 - u_3^2 D)^2,$$

$$C_3 = 4D(u_0 u_1 - u_2 u_3 D)(u_0 u_3 - u_1 u_2).$$

Рассмотрим отдельно два случая.

I. Все числа u_i четны. Требуется рассмотреть варианты i_1)–i_3).

В случае i_1) числа C_1 и C_3 кратны 2^8, и потому условие (4) выполнено тогда и только тогда, когда $16 \mid u_1^2 - u_3^2 D$. Так как $u_1^2 - u_3^2 D = u_1^2 - u_3^2 - u_3^2 2^k t$, то $16 \mid u_1^2 - u_3^2 D$ лишь при условиях

$$k_1 > 1, \quad k_3 > 1 \quad \text{или} \quad k_1 = 1, \quad k_3 = 1 \text{ и } D \equiv 1 \pmod 4.$$

В случае i_2) числа C_2 и C_3 кратны 2^8, и потому условие (4) выполнено тогда и только тогда, когда $16 \mid u_0^2 - u_2^2 D$. Здесь, как и в предыдущем случае, условие $16 \mid u_0^2 - u_2^2 D$ выполняется лишь при условиях

$$k_0 > 1, \quad k_2 > 1 \quad \text{или} \quad k_0 = 1, \quad k_2 = 1 \text{ и } D \equiv 1 \pmod 4.$$

Отсюда следует, что в случае i_2) условие (4) выполняется лишь при $D \equiv$ $\equiv 1 \pmod 4$.

В случае i_3) число C_3 кратно 2^8. Кроме того, как показано выше, C_1 и C_2 также кратны 2^8, если $D \equiv 1 \pmod 4$. Значит, в этом случае условие (4) выполняется. Остается найти экспоненту числа $C_1 - C_2$ при $D \equiv -1 \pmod 4$, т. е. при $k = 1$. Имеем

$$C_1 = ((2v_0)^2 - (2v_2)^2(2t+1))^2 = ((2v_0)^2 - (2v_2)^2 - (2v_2)^2 2t)^2,$$

где v_0, v_2, t нечетны.

Так как $v_0^2 - v_2^2$ кратно 8, то C_1 можно представить в виде $C_1 = (2^5 m - 2^3 r)^2$, где r нечетно. Отсюда видно, что $C_1 \equiv 2^6 r^2 \pmod{2^8}$. Аналогично, $C_2 \equiv (u_1^2 - u_3^2 D)^2 s^2$, где s нечетно. Следовательно, $C_1 - C_2 \equiv 2^6 r^2 - 2^6 s^2 - 2^7 s^2 t \pmod{2^8}$. Так как $r^2 - s^2$ кратно 8, то $\exp(C_1 - C_2) = 7$, и условие (4) не выполняется.

Таким образом, при четных u_0, u_1, u_2, u_3 условия (2)–(4) выполняются лишь при наборах показателей k, k_i, выписанных в таблице 4.

Таблица 4

	k	k_0	k_1	k_2	k_3
1	>0	>1	>1	>1	>1
2	>1	>1	1	>1	1
3	>1	1	>1	1	>1
4	>1	1	1	1	1

Заметим, что набором 1 из табл. 4 определяются все числа из $\mathbf{Z}[\theta]$; набором 2 — все числа вида $a_0 + a_1\theta/2 + a_2\theta^2 + a_3\theta^3/2$, где $a_0, a_1, a_2, a_3 \in \mathbf{Z}$ и a_1, a_3 нечетны, т. е. множество чисел

$$\mathbf{Z}[\theta] + \alpha_1 \quad \text{при} \quad \alpha_1 = \frac{\theta + \theta^3}{2};$$

набором 3 — множество чисел

$$\mathbf{Z}[\theta] + \alpha_2 \quad \text{при} \quad \alpha_2 = \frac{1 + \theta^2}{2};$$

набором 4 — множество чисел

$$\mathbf{Z}[\theta] + \alpha_3 \quad \text{при} \quad \alpha_3 = \frac{1 + \theta + \theta^2 + \theta^3}{2}.$$

II. Все u_i нечетны, $k > 2$. Требуется рассмотреть варианты j_1)–j_4).

Заметим сначала, что числа u_i нас интересуют лишь по модулю 4, поскольку $\mathbf{Z}[\theta] \subset \mathbf{Q}_0(\theta)$. Кроме того, из указанной в начале параграфа связи чисел u_i с числами t_i и r_i следует, что условия $r_i > 1$ и $r_i = 1$ равносильны условиям $u_i \equiv 1 \pmod 4$ и $u_i \equiv -1 \pmod 4$ соответственно. Следовательно,

наборы чисел r_i из строк с номерами j_1)–j_4) определяют соответственно множества чисел $\mathbf{Z}[\theta] + \alpha_i$, $i = 4, 5, 6, 7$, где

$$\alpha_4 = \frac{3 + 3\theta + 3\theta^2 + 3\theta^3}{4}, \quad \alpha_5 = \frac{1 + \theta + \theta^2 + \theta^3}{4},$$

$$\alpha_6 = \frac{3 + \theta + 3\theta^2 + \theta^3}{4}, \quad \alpha_7 = \frac{1 + 3\theta + \theta^2 + 3\theta^3}{4}.$$

Значит, в данном пункте нам достаточно выяснить, какие из чисел α_i, $i = 4, 5, 6, 7$, содержатся в $\mathbf{Q}_0(\theta)$. А так как $\alpha_4 = 3\alpha_5$, $\alpha_6 = \alpha_5 + \alpha_2$, $\alpha_7 = \alpha_5 + \alpha_1$ и $\alpha_1, \alpha_2 \in \mathbf{Q}_0(\theta)$, то достаточно лишь решить вопрос о принадлежности α_5 к $\mathbf{Q}_0(\theta)$, т. е. рассмотреть случай j_2), все $k_i > 1$, $k > 2$.

С этой целью выпишем сначала в общем случае подробно числа C_1, C_2, C_3 по модулю 2^8, заменив в их выражениях из (4) u_i на $2^{r_i}t_i + 1$, $i = 0, 1, 2, 3$, $r_i > 0$:

$$C_1 \equiv [(2^{2r_0}t_0^2 + 2^{r_0+1}t_0) - (2^{2r_2}t_2^2 + 2^{r_2+1}t_2) - 2^k t - 2^{k+2r_2}t_2^2 t - \\ - 2^{k+r_2+1}t_2 t]^2 \pmod{2^8};$$

$$C_2 \equiv (2^k t + 1)[(2^{2r_1}t_1^2 + 2^{r_1+1}t_1) - (2^{2r_3}t_3^2 + 2^{r_3+1}t_3) - 2^k t - 2^{k+2r_3}t_3^2 t) - \\ - 2^{k+r_2+1}t_3 t]^2 \pmod{2^8};$$

$$C_3 \equiv 4(2^k t + 1)[(2^{k_0+k_1}t_0 t_1 + 2^{k_0}t_0 + 2^{k_1}t_1) - \\ - (2^{k_2+k_3}t_2 t_3 + 2^{k_2}t_2 + 2^{k_3}t_3) - (2^{k_2+k_3}t_2 t_3 + 2^{k_2}t_2 + 2^{k_3}t_3)2^k t - 2^k t] \times \\ \times [(2^{k_0+k_3}t_0 t_3 + 2^{k_0}t_0 + 2^{k_3}t_3) - (2^{k_1+k_2}t_1 t_2 + 2^{k_1}t_1 + 2^{k_2}t_2)] \pmod{2^8}.$$

Отсюда в рассматриваемом случае j_2) получим

$$C_1 \equiv (2^{2r_0+2}t_0^2 + 2^{2r_2+2}t_2^2) + 2^{2k}t^2 - (2^{k+r_0+2}t_0 t - 2^{k+r_2+2}t_2 t) - \\ - 2^{r_0+r_2+3}t_0 t_2 \pmod{2^8};$$

$$C_2 \equiv (2^{2r_1+2}t_1^2 + 2^{2r_3+2}t_3^2) + 2^{2k}t^2 - (2^{k+r_1+2}t_1 t - 2^{k+r_3+2}t_3 t) - \\ - 2^{r_1+r_3+3}t_1 t_3 \pmod{2^8};$$

$$C_3 \equiv 2^2[(2^{2r_0}t_0^2 + 2^{2r_2}t_2^2 - 2^{2r_1}t_1^2 - 2^{2r_3}t_3^2) - (2^{r_0+r_2+1}t_0 t_2 - 2^{r_1+r_3+1}t_1 t_3) - \\ - 2^k t(2^{r_0}t_0 + 2^{k_3}t_3 - 2^{r_1}t_1 - 2^{k_2}t_2)] \pmod{2^8}.$$

Из этих сравнений, учитывая, что $C = C_1 - C_2 - C_3$, находим: $C \equiv 0 \pmod{2^8}$, и условие (4) выполнено.

Таким образом, $\alpha_5 \in \mathbf{Q}_0(\theta)$, а потому и $\alpha_4, \alpha_6, \alpha_7 \in \mathbf{Q}_0(\theta)$.

В итоге нами описаны все элементы кольца $\mathbf{Q}_0(\theta)$. Результат можно сформулировать в виде следующей теоремы. Для ее формулировки введем еще обозначение $\alpha_0 = 0$.

ТЕОРЕМА 1. 1. *Если* $D \equiv -1 \pmod 4$, *то* $[\mathbf{Q}_0(\theta) : \mathbf{Z}[\theta]] = 1$, *т.е.* $\mathbf{Q}_0(\theta) = \mathbf{Z}[\theta]$.

2. *Если* $D \equiv 1 \pmod 4$, *но* $D \not\equiv 1 \pmod 8$, *то* $[\mathbf{Q}_0(\theta) : \mathbf{Z}[\theta]] = 4$, *и кольцо* $\mathbf{Q}_0(\theta)$ *имеет следующее разложение в смежные классы по подкольцу* $\mathbf{Z}[\theta]$:

$$\mathbf{Q}_0(\theta) = \bigcup_{i=0}^{3} (\mathbf{Z}[\theta] + \alpha_i).$$

3. *Если* $D \equiv 1 \pmod 8$, *то* $[\mathbf{Q}_0(\theta) : \mathbf{Z}[\theta]] = 8$, *и кольцо* $\mathbf{Q}_0(\theta)$ *имеет следующее разложение в смежные классы по подкольцу* $\mathbf{Z}[\theta]$:

$$\mathbf{Q}_0(\theta) = \bigcup_{i=0}^{7} (\mathbf{Z}[\theta] + \alpha_i).$$

Для доказательства теоремы остается лишь заметить, что смежные классы $\mathbf{Z}[\theta] + \alpha_i$, $i \in \{0, \dots, 7\}$, попарно различны.

На основании этой теоремы укажем общий вид элементов кольца $\mathbf{Q}_0(\theta)$.

В случаях 1, 2, 3 кольцо $\mathbf{Q}_0(\theta)$ состоит соответственно из элементов вида

$$a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3,$$

где $a_0, a_1, a_2, a_3 \in \mathbf{Z}$;

$$\frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3}{2},$$

где $a_0, a_1, a_2, a_3 \in \mathbf{Z}$ и либо a_0, a_1, a_2, a_3 нечетны, либо a_0, a_2 нечетны, a_1, a_3 четны, либо a_0, a_2 четны, a_1, a_3 нечетны;

$$\frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3}{4},$$

где a_0, a_1, a_2, a_3 — целые нечетные числа, $a_0 \equiv a_2 \pmod 4$, $a_1 \equiv a_3 \pmod 4$.

§ 2. СТРОЕНИЕ КОЛЕЦ ВЫЧЕТОВ $\mathbf{Q}_0(\theta)/p$ И $\mathbf{Z}[\theta]/p$

Обозначим через $\mathbf{Q}_0(\theta)/m$ и $\mathbf{Z}[\theta]/m$ факторкольца колец $\mathbf{Q}_0(\theta)$ и $\mathbf{Z}[\theta]$ по главному идеалу, порожденному натуральным числом m соответственно в кольцах $\mathbf{Q}_0(\theta)$ и $\mathbf{Z}[\theta]$. Их элементами являются классы чисел вида $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$ из $\mathbf{Q}_0(\theta)$ и $\mathbf{Z}[\theta]$ соответственно, где в качестве коэффициентов a_i выступают элементы из $\mathbf{Z}/m$, а все операции над ними осуществляются по модулю m. Указанные классы элементов из $\mathbf{Q}_0(\theta)$ и $\mathbf{Z}[\theta]$, содержащие элемент α, будем обозначать через $[[\alpha]]_m$ и $[\alpha]_m$ соответственно. Легко доказать, что при нечетном m отображение $f\colon \mathbf{Q}_0(\theta)/m \to \mathbf{Z}[\theta]/m$,

определенное для любого $[[\alpha]]_m$ правилом $f([[\alpha]]_m) = [\beta]_m$, где β — любой элемент из $[[\alpha]]_m \cap \mathbf{Z}[\theta]$, является изоморфизмом колец. Для доказательства этого утверждения достаточно показать, что каждый из классов $[[\alpha]]_m$ содержит хотя бы один элемент из $\mathbf{Z}[\theta]$. Как следует из теоремы 1, этот факт достаточно установить лишь для классов $[[\alpha_i]]_m$, где α_i — элементы, фигурирующие в формулировке теоремы, $i = 1, \ldots, 7$. Докажем это, например, для элемента

$$\alpha_5 = \frac{1 + \theta + \theta^2 + \theta^3}{4}.$$

Так как m нечетно, то сравнение $4x \equiv 1 \pmod{m}$ разрешимо. Пусть x_0 — любое его решение, т. е. $4x_0 - 1 = mt$ при некотором целом t. Тогда число $4x_0\alpha_5$ будет содержаться в $\mathbf{Z}[\theta]$, а разность $4x_0\alpha_5 - \alpha_5 = mt\alpha_5$ — в идеале (m). Следовательно, $4x_0\alpha_5 \in \mathbf{Z}[\theta] \cap [[\alpha]]_m$, и для α_5 требуемое утверждение доказано. Аналогично оно доказывается и для других α_i.

Таким образом, структуры колец $\mathbf{Q}_0(\theta)/m$ и $\mathbf{Z}[\theta]/m$ совпадают, и потому достаточно изучить структуру кольца $\mathbf{Q}_0(\theta)/m$.

Ограничимся сначала рассмотрением кольца $\mathbf{Q}_0(\theta)/p$ при нечетном простом p.

Строение кольца $\mathbf{Q}_0(\theta)/p$ определяется разложением идеала (p) в произведение простых идеалов кольца $\mathbf{Q}_0(\theta)$, которое, в свою очередь, зависит от разложения на неприводимые множители над полем $\mathbf{Z}/p$ многочлена $(m(x))_p$, полученного из $m(x)$ заменой коэффициентов из $\mathbf{Z}$ их вычетами по модулю p. А именно, если

$$(m(x))_p = \prod_{i=1}^{s} a_i(x)^{k_i}$$

есть каноническое разложение многочлена $(m(x))_p$ над полем $\mathbf{Z}/p$, то

$$(p) = \prod_{i=1}^{s} P_i^{k_i}$$

— разложение идеала (p) в произведение простых идеалов, где P_i — идеал, порожденный элементами p и $a_i(\theta)$, при этом $a_i(x)$ рассматривается как многочлен над $\mathbf{Z}$ (см, например, [5, с. 196]). Как следует из теоремы 1, в рассматриваемом нами случае p не делит индекс $[\mathbf{Q}_0(\theta) : \mathbf{Z}[\theta]]$ и указанное утверждение имеет место.

Рассмотрим вопрос о разложении многочлена $(m(x))_p$, т. е. $(x^4 - D)_p$, на неприводимые множители над полем $\mathbf{Z}/p$.

Если D — квадратичный вычет по модулю p, d — некоторое фиксированное решение сравнения $x^2 \equiv D \pmod{p}$, то многочлен $(x^4 - D)_p$ над $\mathbf{Z}/p$ разлагается в произведение $(x^2 - d)(x^2 + d)$. Ниже число d будет обозначаться также через $(\sqrt{D}\,)_p$.

Дальнейшее разложение зависит уже от d. Если d — квадратичный вычет по модулю p и $d \equiv d_1^2 \pmod p$, то многочлен $x^2 - d$ разлагается над $\mathbf{Z}/p$ в произведение $(x - d_1)(x + d_1)$. Если при этом $p \equiv 1 \pmod 4$, то $-d$ — также квадратичный вычет по модулю p, т. е. $-d \equiv d_2^2 \pmod p$ при некотором d_2, и многочлен $x^2 + d$ разлагается в произведение $(x - d_2)(x + d_2)$. Если же $p \equiv -1 \pmod 4$, то $-d$ — квадратичный невычет по модулю p, и многочлен $x^2 + d$ неприводим над $\mathbf{Z}/p$.

Пусть теперь D — квадратичный невычет по модулю p. Тогда многочлен $(x^4 - D)_p$ не имеет корней в $\mathbf{Z}/p$ и, значит, либо неприводим, либо разлагается в произведение двух многочленов степени 2 над $\mathbf{Z}/p$. Допустим, что

$$(x^4 - D)_p = (x^2 + ax + b)(x^2 + rx + s).$$

Тогда в $\mathbf{Z}/p$ выполнены равенства:

$$a + r = 0, \quad b + s + ar = 0, \quad as + br = 0, \quad bs = -D.$$

Из них получаем: $r = -a$, $b + s = a^2$, $a(s - b) = 0$. Следовательно, $s = -b$ и $D = b^2$, что противоречит условию. Значит, в рассматриваемом случае многочлен $(x^4 - D)_p$ неприводим над $\mathbf{Z}/p$.

В итоге доказана следующая теорема.

Теорема 2. 1) *Если D — квадратичный невычет по модулю p, то многочлен $(x^4 - D)_p$ неприводим над $\mathbf{Z}/p$.*

2) *Если D — квадратичный вычет, а $(\sqrt{D})_p$ — квадратичный невычет по модулю p и $p \equiv 1 \pmod 4$, то многочлен $(x^4 - D)_p$ разлагается над $\mathbf{Z}/p$ в произведение двух многочленов 2-й степени:*

$$(x^4 - D)_p = (x^2 - d)(x^2 + d), d^2 \equiv D \pmod p.$$

3) *Если D и $d = (\sqrt{D})_p$ — квадратичные вычеты по модулю p и $p \equiv -1 \pmod 4$, то многочлен $(x^4 - D)_p$ разлагается над $\mathbf{Z}/p$ в произведение двух многочленов 1-й степени и одного неприводимого многочлена 2-й степени:*

$$(x^4 - D)_p = (x - d_1)(x + d_1)(x^2 + d), \quad d_1^2 \equiv d \pmod p.$$

4) *Если D — квадратичный вычет, а $(\sqrt{D})_p$ — квадратичный невычет по модулю p и $p \equiv -1 \pmod 4$, то многочлен $(x^4 - D)_p$ разлагается над $\mathbf{Z}/p$ в произведение двух многочленов 1-й степени и одного неприводимого многочлена 2-й степени:*

$$(x^4 - D)_p = (x^2 - d)(x - d_2)(x + d_2), \quad d_2^2 \equiv -d \pmod p.$$

5) *Если числа D и $(\sqrt{D})_p$ — квадратичные вычеты по модулю p и $p \equiv 1 \pmod 4$, то многочлен $(x^4 - D)_p$ разлагается над $\mathbf{Z}/p$ в произведение линейных множителей:*

$$(x^4 - D)_p = (x - d_1)(x + d_1)(x - d_2)(x + d_2).$$

Теперь, пользуясь результатами теоремы 2, опишем строение колец $\mathbf{Q}_0(\theta)/p$ и $\mathbf{Z}[\theta]/p$.

Теорема 3. *В условиях пп. 1)–5) теоремы 2 справедливы соответственно следующие утверждения:*

1) $\mathbf{Q}_0(\theta)/p$ *есть поле порядка* p^4;

2) $\mathbf{Q}_0(\theta)/p$ *есть прямая сумма двух полей порядка* p^2;

3)–4) $\mathbf{Q}_0(\theta)/p$ *есть прямая сумма одного поля порядка* p^2 *и двух полей порядка* p;

5) $\mathbf{Q}_0(\theta)/p$ *есть прямая сумма четырех полей порядка* p.

При этом изоморфизмы кольца $\mathbf{Q}_0(\theta)/p$ *на соответствующие прямые суммы полей задаются конструктивно с использованием корней 2-й и 4-й степеней из числа* D *в поле* $\mathbf{Z}/p$.

Доказательство. Рассмотрим отдельно 5 случаев, соответствующих условиям теоремы 2.

1) Пусть $(x^4 - D)_p$ неприводим над $\mathbf{Z}/p$. В этом случае (p) является простым, а значит, и максимальным идеалом кольца $\mathbf{Q}_0(\theta)$. Следовательно, $\mathbf{Q}_0(\theta)/p$ есть поле порядка p^4. Оно изоморфно полю $\mathbf{Z}/p[x]/(x^4 - D)_p$, и изоморфизмом является естественное отображение $[f(x)] \to f(\theta)$.

2) Пусть $(x^4 - D)_p = (x^2 - d)(x^2 + d)$ и $x^2 - d$, $x^2 + d$ неприводимы над $\mathbf{Z}/p$. Здесь $(p) = P_1P_2$, где P_1, P_2 — различные простые идеалы, причем в силу теоремы Дедекинда (см., например, [5]) они порождаются соответственно парами элементов $(p, \theta^2 - d)$ и $(p, \theta^2 + d)$. Следовательно, они состоят из элементов вида $X = ((\theta^2 - d)\alpha)_p$ и $Y = ((\theta^2 + d)\alpha)_p$ соответственно, где α — произвольный элемент из $\mathbf{Q}_0(\theta)$, а индекс p означает, что все коэффициенты в соответствующих произведениях приводятся по модулю p. Если $\alpha = (a_0, a_1, a_2, a_3)$, то

$$X = (a_2D - a_0d, a_3D - a_1d, a_0 - a_2d, a_1 - a_3d)_p,$$

$$Y = (a_2D + a_0d, a_3D + a_1d, a_0 + a_2d, a_1 + a_3d)_p.$$

Отсюда находим общий вид элементов X, Y:

$$X = (b_0, b_1, b_2, b_3)_p,$$

где b_2, b_3 — любые элементы из $\mathbf{Z}/p$, $b_0 = -b_2d$, $b_1 = -b_3d$, т. е.

$$X = (-b_2d, -b_3d, b_2, b_3)_p, \quad Y = (c_0, c_1, c_2, c_3)_p,$$

где c_2, c_3 — любые элементы из $\mathbf{Z}/p$, $c_0 = c_2 d$, $c_1 = c_3 d$, т. е.

$$Y = (c_2 d, c_3 d, c_2, c_3)_p.$$

Из полученного описания элементов идеалов P_1, P_2, учитывая условие $(p, 2D) = 1$, легко показать, что $P_1 \cap P_2 = (p)$. Отсюда следует, что кольцо $\mathbf{Q}_0(\theta)/p$ разлагается в прямую сумму:

$$\mathbf{Q}_0(\theta)/p \cong \mathbf{Q}_0(\theta)/P_1 \oplus \mathbf{Q}_0(\theta)/P_2,$$

и, значит, кольцо $\mathbf{Q}_0(\theta)/p$ изоморфно прямой сумме двух полей порядка p^2.

Найдем явный вид соответствующего изоморфизма. Смежные классы $\alpha + P_1$, $\alpha + P_2$ кольца $\mathbf{Q}_0(\theta)$ по идеалам P_1, P_2 содержат также элементы $\alpha - X$, $\alpha - Y$ соответственно. Положив в X, Y $b_2 = c_2 = a_2$, $b_3 = c_3 = a_3$, мы получим следующие представители указанных классов: $(a_0 + a_2 d, a_1 + a_3 d, 0, 0)_p$ и $(a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p$. Представителей с двумя последними нулевыми компонентами назовем особыми. Нетрудно проверить, что особые представители определяются соответствующими классами однозначно. Действительно, если $\alpha = (a_0, a_1, a_2, a_3)$ и $\beta = (b_0, b_1, b_2, b_3)_p$ содержатся в одном смежном классе, например по идеалу P_1, то $\alpha - \beta \in P_1$, и потому $a_0 - b_0 = -(a_2 - b_2)d$, $a_1 - b_1 = -(a_3 - b_3)d$ и $a_0 + a_2 d = b_0 + b_2 d$, $a_1 + a_3 d = b_1 + b_3 d$. Следовательно, особые представители, определенные по элементам α и β, совпадают. К такому же результату придем и для P_2. Поэтому каждое из факторколец $\mathbf{Q}_0(\theta)/P_1$, $\mathbf{Q}_0(\theta)/P_2$ можно отождествить с системой особых представителей соответствующих смежных классов. В связи с этим далее будем считать, что

$$\mathbf{Q}_0(\theta)/P_1 = \{(a_0 + a_2 d, a_1 + a_3 d, 0, 0)_p \colon a_0, a_1, a_2, a_3 \in \mathbf{Z}/p\},$$

$$\mathbf{Q}_0(\theta)/P_2 = \{(a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p \colon a_0, a_1, a_2, a_3 \in \mathbf{Z}/p\}.$$

Теперь непосредственной проверкой нетрудно убедиться, что изоморфизмом $\mathbf{Q}_0(\theta)/p$ на $\mathbf{Q}_0(\theta)/P_1 \oplus \mathbf{Q}_0(\theta)/P_2$ является отображение φ, определенное формулой

$$\varphi(a_0, a_1, a_2, a_3)_p = ((a_0 + a_2 d, a_1 + a_3 d, 0, 0)_p, \quad (a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p). \quad (9)$$

3) Пусть $(x^4 - D)_p = (x^2 - d)(x^2 + d)$, d — квадратичный вычет по модулю p и $p \equiv -1 \pmod 4$. Тогда $-d$ — квадратичный невычет по модулю p, и, значит, многочлен $x^2 + d$ неприводим над $\mathbf{Z}/p$, а $x^2 - d = (x - d_1)(x + d_1)$, где $d_1^2 \equiv \equiv d \pmod p$. Следовательно, в этом случае идеал (p) равен произведению трех попарно различных простых идеалов:

$$(p) = \mathbf{Q}_1 \mathbf{Q}_2 P_2,$$

где P_2 — идеал из п. 2, а $\mathbf{Q}_1$, $\mathbf{Q}_2$ порождаются парами элементов $(p, \theta - d_1)$, $(p, \theta + d_1)$ соответственно. Так как любые два из этих трех идеалов пересекаются по (p), то кольцо $\mathbf{Q}_0(\theta)/p$ разлагается в прямую сумму трех полей:

$$\mathbf{Q}_0(\theta)/p \cong \mathbf{Q}_0(\theta)/\mathbf{Q}_1 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_2 \oplus \mathbf{Q}_0(\theta)/P_2.$$

Как и в предыдущем случае, найдем общий вид элементов из $\mathbf{Q}_1$, $\mathbf{Q}_2$ и особых представителей смежных классов по $\mathbf{Q}_1$, $\mathbf{Q}_2$:

$$\mathbf{Q}_1 = \{(-(b_1 d_1 + b_2 d_1^2 + b_3 d_1^3), b_1, b_2, b_3)_p \colon b_1, b_2, b_3 \in \mathbf{Z}/p\},$$

$$\mathbf{Q}_2 = \{((b_1 d_1 - b_2 d_1^2 + b_3 d_1^3), b_1, b_2, b_3)_p \colon b_1, b_2, b_3 \in \mathbf{Z}/p\},$$

$$(a_0 + a_1 d_1 + a_2 d_1^2 + a_3 d_1^3, 0, 0, 0)_p \in \mathbf{Q}_1 + \alpha,$$

$$(a_0 - a_1 d_1 + a_2 d_1^2 - a_3 d_1^3, 0, 0, 0)_p \in \mathbf{Q}_2 + \alpha.$$

Изоморфизм кольца $\mathbf{Q}_0(\theta)/p$ на кольцо $\mathbf{Q}_0(\theta)/\mathbf{Q}_1 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_2 \oplus \mathbf{Q}_0(\theta)/P_2$ задается отображением

$$\varphi(a_0, a_1, a_2, a_3)_p = ((a_0 + a_1 d_1 + a_2 d_1^2 + a_3 d_1^3, 0, 0, 0)_p,$$
$$(a_0 - a_1 d_1 + a_2 d_1^2 - a_3 d_1^3, 0, 0, 0)_p, (a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p). \quad (10)$$

4) Этот случай симметричен предыдущему, в нем d — квадратичный невычет, а $-d$ — квадратичный вычет по модулю p, кольцо $\mathbf{Q}_0(\theta)/p$ изоморфно кольцу

$$\mathbf{Q}_0(\theta)/P_1 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_3 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_4,$$

где идеалы $\mathbf{Q}_3$, $\mathbf{Q}_4$ порождаются парами $(p, \theta - d_1)$, $(p, \theta + d_1)$ соответственно. При этом изоморфизм задается формулой

$$\varphi(a_0, a_1, a_2, a_3)_p = ((a_0 + a_2 d, a_1 + a_3 d, 0, 0)_p, (a_0 + a_1 d_2 + a_2 d_2^2 + a_3 d_2^3, 0, 0, 0)_p,$$
$$(a_0 - a_1 d_2 + a_2 d_2^2 - a_3 d_2^3, 0, 0, 0)_p).$$

5) Пусть $(x^4 - D)_p = (x - d_1)(x + d_1)(x - d_2)(x + d_2)$, где $d_1^2 = d$, $d_2^2 = -d$, $d^2 = D$. В этом случае идеал (p) разлагается в произведение четырех различных простых идеалов $\mathbf{Q}_1$, $\mathbf{Q}_2$, $\mathbf{Q}_3$, $\mathbf{Q}_4$, и кольцо $\mathbf{Q}_0(\theta)/p$ разлагается в прямую сумму четырех полей порядка p:

$$\mathbf{Q}_0(\theta)/p \cong \mathbf{Q}_0(\theta)/\mathbf{Q}_1 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_2 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_3 \oplus \mathbf{Q}_0(\theta)/\mathbf{Q}_4.$$

При этом изоморфизм задается формулой

$$\varphi(a_0,a_1,a_2,a_3)_p = ((a_0+a_1d_1+a_2d_1^2+a_3d_1^3,0,0,0)_p,$$
$$(a_0-a_1d_1+a_2d_1^2-a_3d_1^3,0,0,0)_p,(a_0+a_1d_2+a_2d_2^2+a_3d_2^3,0,0,0)_p,$$
$$(a_0-a_1d_2+a_2d_2^2-a_3d_2^3,0,0,0)_p). \quad (11)$$

З а м е ч а н и е. Утверждения теоремы 3 сохраняют силу при замене кольца $\mathbf{Q}_0(\theta)/p$ на $\mathbf{Z}[\theta]/p$. При этом в указанных в доказательстве теоремы 3 изоморфизмах под компонентами векторов-чисел следует понимать целые рациональные числа.

§ 3. О МУЛЬТИПЛИКАТИВНОЙ ГРУППЕ КОЛЬЦА $\mathbf{Z}[\theta]/p$

Условимся для краткости обозначать кольцо $\mathbf{Z}[\theta]/m$ через O_m, а его мультипликативную группу — через O_m^*. Из теоремы 3 можно извлечь необходимую информацию о строении, порядке $|O_p^*|$ и экспоненте $\operatorname{Exp} O_p^*$ группы O_p^*. А с помощью указанных в доказательстве теоремы 3 изоморфизмов колец легко получить описание всех элементов группы O_p^*, т. е. всех обратимых и необратимых элементов кольца $\mathbf{Z}[\theta]/p$.

Приведем соответствующие данные в условиях каждого из пунктов теоремы 3.

1) Группа O_p^* является мультипликативной группой конечного поля порядка p^4. Следовательно, она циклическая порядка p^4-1 и $\operatorname{Exp} O_p^* = p^4-1$.

2) Группа O_p^* является прямым произведением двух циклических групп порядка p^2-1. Следовательно, $|O_p^*| = (p^2-1)^2$, $\operatorname{Exp} O_p^* = p^2-1$. Из формулы (9) видно, что $O_p \setminus O_p^*$ состоит из элементов вида $(a_0,a_1,a_2,a_3)_p$, удовлетворяющих хотя бы одному из условий: $a_0 = a_2d$, $a_1 = a_3d$, $a_0 = -a_2d$, $a_1 = -a_3d$ в $\mathbf{Z}/p$, при этом $|O_p \setminus O_p^*| = 2p-1$.

3) Группа O_p^* является прямым произведением двух циклических групп порядка $p-1$ и одной циклической группы порядка p^2-1. Значит, $|O_p^*| = (p-1)^2(p^2-1)$, $\operatorname{Exp} O_p^* = p^2-1$. Из формулы (10) видно, что $O_p \setminus O_p^*$ состоит из элементов вида $(a_0,a_1,a_2,a_3)_p$, удовлетворяющих хотя бы одному из условий: $a_0 = a_2d$, $a_1 = a_3d$, $a_0+a_1d_1+a_2d_1^2+a_3d_1^3 = 0$, $a_0-a_1d_1+a_2d_1^2-a_3d_1^3 = 0$ в $\mathbf{Z}/p$, при этом $|O_p \setminus O_p^*| = 2p^3-2p+1$.

4) В этом случае строение и параметры группы O_p^*, те же, что и в п. 3, а $O_p \setminus O_p^*$ состоит из элементов вида $(a_0,a_1,a_2,a_3)_p$, удовлетворяющих хотя бы одному из условий: $a_0 = -a_2d$, $a_1 = -a_3d$, $a_0+a_1d_2+a_2d_2^2+a_3d_2^3 = 0$, $a_0-a_1d_2+a_2d_2^2-a_3d_2^3 = 0$ в $\mathbf{Z}/p$, при этом $|O_p \setminus O_p^*| = 2p^3-2p+1$.

5) Группа O_p^* есть прямое произведение четырех циклических групп порядка $p-1$. Следовательно, $|O_p^*| = (p-1)^4$, $\operatorname{Exp} O_p^* = p-1$. Из форму-

лы (11) видно, что $O_p \setminus O_p^*$ состоит из элементов вида $(a_0, a_1, a_2, a_3)_p$, где a_0, a_1, a_2, a_3 — элементы из $\mathbf{Z}/p$, удовлетворяющие в $\mathbf{Z}[\theta]/p$ хотя бы одному из следующих четырех равенств:

$$a_0 + a_1 d_1 + a_2 d_1^2 + a_3 d_1^3 = 0, \quad a_0 - a_1 d_1 + a_2 d_1^2 - a_3 d_1^3 = 0,$$
$$a_0 + a_1 d_2 + a_2 d_2^2 + a_3 d_2^3 = 0, \quad a_0 - a_1 d_2 + a_2 d_2^2 - a_3 d_2^3 = 0,$$
$$|O_p \setminus O_p^*| = 4p^3 - 6p^2 + 4p - 1.$$

В дальнейшем нас будут интересовать порядки элементов группы O_p^*. В связи с этим представляет определенный интерес следующее утверждение.

Теорема 4. *Пусть $p - 1 = p_1^{k_1} r$, $p + 1 = p_2^{k_2} s$, где p, p_1, p_2 — нечетные простые числа, $(p_1, r) = 1$, $(p_2, s) = 1$ и $N(m)$ — число элементов группы O_p^*, порядки которых кратны числу m. Тогда в условиях пп. 1)–5) теоремы 2 имеют место следующие утверждения:*

1) a) $N(p_1^{k_1}) = |O_p^*|\left(1 - \frac{1}{p_1}\right)$, b) $N(p_1^{k_1} p_2^{k_2}) = |O_p^*|\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$;

2) a) $N(p_1^{k_1}) = |O_p^*|\left(1 - \frac{1}{p_1^2}\right)$, b) $N(p_1^{k_1} p_2^{k_2}) = |O_p^*|\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right)$;

3)–4) a) $N(p_1^{k_1}) = |O_p^*|\left(1 - \frac{1}{p_1^3}\right)$, b) $N(p_1^{k_1} p_2^{k_2}) = |O_p^*|\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_1^3}\right)$;

5) $N(p_1^{k_1}) = |O_p^*|\left(1 - \frac{1}{p_1^4}\right)$.

Доказательство. Докажем сначала два вспомогательных утверждения общего характера о циклических группах. Обозначим через $N_G(m)$ число элементов в группе G, порядки которых кратны натуральному числу m.

Лемма 1. a) *Если G — циклическая группа порядка mq и $(m, q) = 1$, то*

$$N_G(m) = \varphi(m) q, \tag{12}$$

где φ — функция Эйлера.

b) *Пусть $G = H \cdot K$ — прямое произведение конечных групп H, K, $|H| = mr$, $|K| = ms$, $(m, rs) = 1$.*

Тогда, если m — степень простого числа, то

$$N_G(m) = N_H(m)|K| + N_K(m)|H| - N_H(m) N_K(m). \tag{13}$$

Если же $m = m_1 m_2$, где m_1, m_2 — степени различных простых чисел, то

$$\begin{aligned} N_G(m) = N_H(m)|K| + N_K(m)|H| - \\ - N_H(m) N_K(m) + (N_H(m_1) - N_H(m))(N_K(m_2) - N_K(m)) + \\ + (N_H(m_2) - N_H(m))(N_K(m_1) - N_K(m)). \end{aligned} \tag{14}$$

Доказательство леммы. a) Порядками элементов группы G являются все положительные делители числа mq, и его делители, кратные m, имеют вид md, где d пробегает все положительные делители числа q. Известно, что в конечной циклической группе для любого делителя k ее порядка существует ровно $\varphi(k)$ элементов порядка k. Отсюда, учитывая условие $(m,q)=1$, получим:

$$N_G(m)=\sum_{d|q}\varphi(md)=\varphi(m)\sum_{d|q}\varphi(d)=\varphi(m)q.$$

b) Каждый элемент из G имеет вид (h,k), где $h\in H$, $k\in K$, и порядок элемента (h,k) равен наименьшему общему кратному порядков элементов h, k. Следовательно, в условиях формулы (13) порядок элемента (h,k) кратен m тогда и только тогда, когда этим свойством обладает хотя бы один из элементов h, k. В условиях же формулы (14) порядок элемента (h,k), кроме того, кратен m еще и в тех случаях, когда порядок одного из элементов h, k кратен m_1, а порядок другого кратен m_2. Используя эти факты, мы методом включения и исключения получим формулы (13), (14).

Теперь докажем утверждения теоремы для каждого из пп. 1)–5).

1) В этом случае

$$|O_p^*|=p^4-1=(p-1)(p+1)(p^2+1)=p_1^{k_1}p_2^{k_2}t,$$

где $t=rs(p^2+1)$. Так как

$$(p-1,p+1)=(p-1,p^2+1)=(p+1,p^2+1)=2,$$

а p_1, p_2 нечетны, то $(p_1^{k_1}p_2^{k_2},t)=1$, и утверждения a), b) п. 1) получаются непосредственно по формуле (12).

2) В этом случае группа O_p^* есть прямое произведение двух циклических групп порядка p^2-1, обозначим их через G и H. Из рассуждений п. 1) следует, что

$$N_G(p_1^{k_1})=N_H(p_1^{k_1})=(p^2-1)\Big(1-\frac{1}{p_1}\Big),$$

$$N_G(p_1^{k_1}p_2^{k_2})=N_H(p_1^{k_1}p_2^{k_2})=(p^2-1)\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big).$$

Теперь, воспользовавшись формулами (13), (14) мы после несложных преобразований получим равенства a) и b) п. 1).

3)–4) В этом случае группа O_p^* есть прямое произведение циклических групп G, H, K, где $|G|=|H|=p-1$, $|K|=p^2-1$. По формуле (12) получим:

$$N_G(p_1^{k_1})=N_H(p_1^{k_1})=(p-1)\Big(1-\frac{1}{p_1}\Big),$$

$$N_K(p_1^{k_1})=(p^2-1)\Big(1-\frac{1}{p_1}\Big),\quad N_K(p_1^{k_1}p_2^{k_2})=(p^2-1)\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big).$$

Применяя формулу (13) к группе $F = G \cdot H$, получаем

$$N_F(p_1^{k_1}) = (p-1)^2\Big(1 - \frac{1}{p_1^2}\Big).$$

Теперь, применяя формулы (13), (14) к группе $O_p^* = F \cdot K$ и учитывая, что

$$N_F(p_2^{k_2}) = N_F(p_1^{k_1} p_2^{k_2}) = 0,$$

получим равенства a) и b) пп. 3)–4).

5) Здесь $O_p^* = G_1 \cdot G_2 \cdot H_1 \cdot H_2$ — прямое произведение четырех циклических групп порядка $p-1$. Для вычисления величины $N(p_1^{k_1})$ применим формулу (13) сначала к группам $G = G_1 \cdot G_2$, $H = H_1 \cdot H_2$, а затем к группе $O_p^* = G \cdot H$. В итоге получим формулу п. 5). Теорема доказана.

§ 4. О СВОЙСТВАХ КОЛЬЦА $\mathbf{Z}[\theta]/pq$ И ЕГО МУЛЬТИПЛИКАТИВНОЙ ГРУППЫ

Пусть p, q — различные нечетные простые числа, $n = pq$, и, как и выше, D — нечетное, отличное от единицы, свободное от квадратов натуральное число, $(D, pq) = 1$, θ — арифметический корень 4-й степени из D.

Разложение кольца $\mathbf{Z}/n$ в прямую сумму колец $\mathbf{Z}/p$, $\mathbf{Z}/q$ индуцирует разложение кольца O_n в прямую сумму колец O_p, O_q. Поэтому строение кольца O_n полностью определяется строением колец O_p, O_q, и, как следует из теоремы 3, оно разлагается в прямую сумму полей порядков p^4, p^2, p, q^4, q^2, q. Однако соответствующие разложения можно найти, лишь зная числа p, q. В связи с этим возникает вопрос: в каких случаях существуют нетривиальные разложения кольца O_n в прямую сумму колец вида $\mathbf{Z}[w]/n$ при подходящих целых w? Если такое разложение существует, то w должно быть алгебраическим числом 1-й или 2-й степени. В связи с этим кольцо $\mathbf{Z}[w]/n$ будем называть расширением 1-й или 2-й степени по модулю n. Заметим, что кольцо первой степени совпадает с кольцом $\mathbf{Z}/n$. Ответ на поставленный вопрос зависит от указанных в теореме 2 условий 1)–5) на числа D, p и аналогичных условий на числа D, q. Так как D постоянно, то ниже условие i) для p и q будем обозначать через ip) и iq) соответственно, $i = 1, \ldots, 5$.

Теорема 5. a) *Если выполняются условия* 1p) *или* 1q), *то кольцо* O_n *не разлагается в прямую сумму колец меньших степеней по модулю* n.

b) *Если выполняются условия* 5p) *и* 5q), *то кольцо* O_n *разлагается в прямую сумму четырех экземпляров кольца* $\mathbf{Z}/n$.

c) *Если выполняются условия* ip) *и* jq), *где одно из чисел* i, j *равно* 5, *а другое равно* 3 *или* 4, *то кольцо* O_n *разлагается в прямую сумму двух экземпляров кольца* $\mathbf{Z}/n$ *и одного кольца второй степени по модулю* n.

d) *Во всех остальных случаях кольцо O_n разлагается в прямую сумму двух колец 2-й степени по модулю n.*
При этом для явного задания изоморфизмов кольца O_n на соответствующие прямые суммы колец достаточно уметь решать сравнение $x^2 \equiv \equiv D \pmod n$.

Доказательство. a) Если бы кольцо O_n разлагалось в прямую сумму колец меньших степеней по модулю n, то такое разложение индуцировало бы соответствующие разложения колец O_p, O_q, что противоречит условию.

b)–d) Для доказательства остальных утверждений необходимо рассмотреть 16 оставшихся случаев для условий ip), jq). Однако доказательства используют одни и те же идеи, и мы проиллюстрируем их на одном наиболее общем случае, когда выполняются условия 5p) и 3q). Тогда по теореме 3 имеет место изоморфизм $\varphi\colon O_n \to (\mathbf{Z}/p)^4$, определенный формулой (11), которую, используя соотношения $d_1^2 = d$, $d_2^2 = -d$, можно записать в виде

$$\varphi(a_0, a_1, a_2, a_3)_p = ((a_0 + a_2 d + (a_1 + a_3 d)\sqrt{d}, 0, 0, 0)_p,$$
$$(a_0 + a_2 d - (a_1 + a_3 d)\sqrt{d}, 0, 0, 0)_p), (a_0 - a_2 d + (a_1 - a_3 d)\sqrt{-d}, 0, 0, 0)_p,$$
$$(a_0 - a_2 d - (a_1 - a_3 d)\sqrt{-d}, 0, 0, 0)_p).$$

Аналогично, изоморфизм g, определенный для модуля q по формуле, сходной с формулой (10) для модуля p, можно записать в виде

$$g(a_0, a_1, a_2, a_3)_q = ((a_0 + a_2 c + (a_1 + a_3 c)\sqrt{c}, 0, 0, 0)_q,$$
$$(a_0 + a_2 c - (a_1 + a_3 c)\sqrt{c}, 0, 0, 0)_q, (a_0 - a_2 c, a_1 - a_3 c, 0, 0)_q), \quad (15)$$

где $c = (\sqrt{D})_q$. Непосредственной проверкой легко убедиться, что отображение f, определенное формулой

$$f((a_0 - a_2 d + (a_1 - a_3 d)\sqrt{-d}, 0, 0, 0)_p, (a_0 - a_2 d - (a_1 - a_3 d)\sqrt{-d}, 0, 0, 0)_p) =$$
$$= (a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p,$$

является изоморфизмом колец. Используя изоморфизмы φ и f, получим изоморфизм

$$h(a_0, a_1, a_2, a_3)_p = ((a_0 + a_2 d + (a_1 + a_3 d)\sqrt{d}, 0, 0, 0)_p,$$
$$(a_0 + a_2 d - (a_1 + a_3 d)\sqrt{d}, 0, 0, 0)_p), (a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p.$$

Заметим, что множество $\{(a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p\colon a_0, a_1, a_2, a_3 \in \mathbf{Z}/p\}$ является кольцом, изоморфным кольцу $(\mathbf{Z}/p)^2$, поскольку d — квадратичный вычет по модулю p, а множество $\{(a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p\colon a_0, a_1, a_2, a_3 \in \mathbf{Z}/p\}$ является кольцом, изоморфным кольцу $\mathbf{Z}[\sqrt{-d}]/p$ второй степени по модулю p, так как $-d$ — квадратичный невычет по модулю p.

Теперь, используя естественный изоморфизм кольца O_n на кольцо $O_p \oplus O_q$ и изоморфизмы h, g, получим изоморфизм σ:

$$\sigma(a_0, a_1, a_2, a_3)_n = ((a_0 + a_2 d + (a_1 + a_3 d)\sqrt{d}, 0, 0, 0)_p,$$
$$(a_0 + a_2 c + (a_1 + a_3 c)\sqrt{c}, 0, 0, 0)_q, (a_0 + a_2 d - (a_1 + a_3 d)\sqrt{d}, 0, 0, 0)_p,$$
$$(a_0 + a_2 c - (a_1 + a_3 c)\sqrt{c}, 0, 0, 0)_q, (a_0 - a_2 d, a_1 - a_3 d, 0, 0)_p,$$
$$(a_0 - a_2 c, a_1 - a_3 c, 0, 0)_q).$$

Заменив в этом равенстве числа d, c на число w, найденное по китайской теореме об остатках из системы сравнений

$$w \equiv d \pmod p, \quad w \equiv c \pmod q, \tag{16}$$

и учитывая еще раз наличие естественного изоморфизма O_n на кольцо $O_p \oplus O_q$, мы получим изоморфизм кольца O_n:

$$\tau(a_0, a_1, a_2, a_3)_n = ((a_0 + a_2 w + (a_1 + a_3 w)\sqrt{w}, 0, 0, 0)_n,$$
$$(a_0 + a_2 w - (a_1 + a_3 w)\sqrt{w}, 0, 0, 0)_n, (a_0 - a_2 w, a_1 - a_3 w, 0, 0)_n). \tag{17}$$

По условиям 5p), 3q) числа d и $-d$ являются квадратичными вычетами по модулю p, c — квадратичный вычет, а $-c$ — квадратичный невычет по модулю q. Отсюда следует, что w — квадратичный вычет, а $-w$ — квадратичный невычет по модулю n. Следовательно, образом изоморфизма τ является кольцо $(\mathbf{Z}/n)^2 \oplus \mathbf{Z}[w]/n$, и $\mathbf{Z}[w]/n$ есть кольцо второй степени по модулю n.

Из формулы (17) видно, что для получения изоморфизма τ достаточно суметь найти число w. Для его нахождения из системы (16) нужно знать числа p, q. Однако из сравнений (16) и из определения чисел с, d следует, что w есть решение сравнения

$$x^2 \equiv D \pmod n. \tag{18}$$

Поэтому для получения изоморфизма τ достаточно уметь решать сравнение (18). В итоге утверждение теоремы в условиях 5p), 3q) полностью доказано. Аналогично доказывается оно и в остальных случаях.

В связи с заключением теоремы 5 далее наиболее интересными для приложений являются случаи, в которых выполняется хотя бы одно из условий 1p), 1q). Приведем для этих случаев необходимые факты о кольцах O_n и группах O_n^*, которые находятся непосредственно из строения колец O_p, O_q, указанного в теореме 3.

1p), 1q). $O_n \cong \mathbf{GF}(p^4) \oplus \mathbf{GF}(q^4)$,

$$|O_n^*| = (p^4-1)(q^4-1), \quad \operatorname{Exp}(O_n^*) = [p^4-1, q^4-1],$$

$$|O_n \setminus O_n^*| = p^4+q^4-1, \quad |O_n \setminus O_n^*|/|O_n| = \frac{1}{p^4}+\frac{1}{q^4}-\frac{1}{p^4q^4}.$$

1p), 2q). $O_n \cong \mathbf{GF}(p^4) \oplus (\mathbf{GF}(q^2)^2$,

$$|O_n^*| = (p^4-1)(q^2-1)^2, \quad \operatorname{Exp}(O_n^*) = [p^4-1, q^2-1],$$

$$|O_n \setminus O_n^*| = q^4+(p^4-1)(2q^2-1),$$

$$|O_n \setminus O_n^*|/|O_n| = \frac{1}{p^4}+\left(\frac{1}{q^4}-\frac{1}{p^4q^4}\right)(2q^2-1).$$

1p), 3q) или 1p), 4q). $O_n \cong \mathbf{GF}(p^4) \oplus \mathbf{GF}(q^2) \oplus (\mathbf{GF}(q))^2$,

$$|O_n^*| = (p^4-1)(q^2-1)(q-1)^2, \quad \operatorname{Exp}(O_n^*) = [p^4-1, q^2-1],$$

$$|O_n \setminus O_n^*| = q^4+(p^4-1)(2q^3-2q+1),$$

$$|O_n \setminus O_n^*|/|O_n| = \frac{1}{p^4}+\left(\frac{1}{q^4}-\frac{1}{p^4q^4}\right)(2q^3-2q+1).$$

1p), 5q). $O_n \cong \mathbf{GF}(p^4) \oplus (\mathbf{GF}(q)^4$,

$$|O_n^*| = (p^4-1)(q-1)^4, \quad \operatorname{Exp}(O_n^*) = [p^4-1, q-1],$$

$$|O_n \setminus O_n^*| = q^4+(p^4-1)(4q^3-6q^2+4q-1),$$

$$|O_n \setminus O_n^*|/|O_n| = \frac{1}{p^4}+\left(\frac{1}{q^4}-\frac{1}{p^4q^4}\right)(4q^3-6q^2+4q-1).$$

§ 5. ПРИМЕР СХЕМЫ ТИПА RSA, ОСНОВАННОЙ НА ИСПОЛЬЗОВАНИИ КОЛЬЦА $\mathbf{Z}[\theta]/n$

Как следует из теоремы 5, операции в кольце $O_n = \mathbf{Z}[\theta]/n$ не сводятся к операциям в кольцах меньших степеней по модулю n только в тех случаях, когда выполняется хотя бы одно из условий 1p), 1q). Поэтому далее будем считать, что последнее условие выполнено. Точнее, будем рассматривать лишь случаи, когда выполнены условие 1p) и одно из условий 2q), 3q), 4q). Случаи, в которых выполняются условие 1q) и одно из условий 2p), 3p), 4p), симметричны рассматриваемым.

Во всех подлежащих рассмотрению случаях экспонента группы O_n^* равна НОК $\left(p^4-1, q^2-1\right)$. Далее она обозначается буквой m. Таким образом,

$$m = \text{НОК}\left(p^4-1, q^2-1\right).$$

Криптосистему типа RSA, основанную на использовании кольца $\mathbf{Z}_n$, условимся называть стандартной.

В предлагаемой ниже схеме RSA вместо кольца $\mathbf{Z}_n$ используется кольцо O_n. Открытым ключом является тройка чисел (n, D, e), где e — экспонента зашифрования, выбираемая случайно с условием $2 < e < m$ и $(e, m) = 1$, а секретным ключом — тройка чисел (p, q, f), где f — экспонента расшифрования, определяемая из условия

$$ef \equiv 1 \pmod{m}, \quad 0 < f < m.$$

Заметим, что кольцо O_n имеет собственные подкольца. Примерами таких подколец могут служить множества: $\{(a, 0, 0, 0)\colon a \in \mathbf{Z}_n\}$, $\{(a, 0, b, 0)\colon a, b \in \in \mathbf{Z}_n\}$. В связи с этим открытые сообщения желательно кодировать элементами, не содержащими нулевых компонент. Приведем пример такой кодировки.

Представим открытое сообщение в виде $M = (m_1, m_2, m_3, m_4)$, где $0 \leqslant \leqslant m_1, m_2, m_3, m_4 < n - 1$, и закодируем его элементом $C(M) = (m_1 + 1, m_2 + + 1, m_3 + 1, m_4 + 1)$.

Шифрованным текстом будем считать элемент $C(M)^e$ из O_n (записанный в виде четверки целых чисел из промежутка $[0, n - 1]$).

Для расшифрования нужно вычислить $C(M)^{ef} \pmod{n}$. Если элемент M обратим в кольце O_n, то в итоге получим $C(M)$, а после декодирования и открытый текст M. Из теоремы 3 следует, что при случайном и равновероятном выборе элемента $C(M)$ вероятность получить обратимый элемент равна $(2q - 1)/p^4q^4$ в случае $2q$), и $(2q^3 - 2q + 1)/p^4q^4$ в случаях $3q$), $4q$). При реальных значениях p, q указанные вероятности близки к нулю и таким событием можно пренебречь. В действительности, вероятность отличия числа $C(M)^{ef} \pmod{n}$ от $C(M)$ еще меньше, так как существуют и необратимые элементы кольца O_n, удовлетворяющие условию

$$C(M)^{ef} \equiv C(M) \pmod{m}.$$

Вычисление числа $C(M)^e$ можно осуществить известным способом последовательного возведения в квадрат и умножения на число $C(M)$ в кольце O_n. Из правила умножения элементов в кольце O_n следует, что в общем случае для вычисления произведения двух элементов требуется произвести 18 умножений и 12 сложений по модулю n, а для возведения в квадрат — 13 умножений и 12 сложений по модулю n.

Так как абонент связи, осуществляющий расшифрование, обладает секретным ключом, то для упрощения возведения $C(M)^e$ в степень f он может воспользоваться изоморфизмом кольца O_n на прямую сумму полей порядков p^4, q^2, q. Тогда вместо операций над числами по модулю n можно будет производить операции в соответствующих полях.

Таким образом, процессы шифрования и расшифрования в предлагаемой схеме на порядок сложнее по сравнению со стандартной схемой RSA. Частично это усложнение компенсируется тем, что в рассматриваемой схеме вместо одного числа из промежутка $[0, n]$ шифруется сразу четверка чисел из промежутка $[0, n-1]$.

Для решения вопроса о криптографической стойкости предложенной схемы необходимо ее дальнейшее более всестороннее исследование.

СПИСОК ЛИТЕРАТУРЫ

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. — М.: Гелиос АРВ, 2001.
2. *Василенко О.Н.* Применение круговых полей в криптосхемах RSA. — IV Международная конференция «Современные проблемы теории чисел и ее приложения». Тезисы докладов. — Тула, 2001.
3. *Гекке Э.* Лекции по теории алгебраических чисел. — М.-Л.: ГИТТЛ, 1940.
4. *Глухов М.М.* Кольца вычетов биквадратичных расширений кольца целых чисел и криптографические схемы с открытым ключом. — В сб.: Труды по дискретной математике. Т. 7. — М.: ФИЗМАТЛИТ, 2003, с. 31–35.
5. *Cohen H.* A course in computational algebraic number theory. — Berlin: Springer-Verlag, 1993.
6. *Biehl J., Buchmann J.A., Thiel Ch.* Cryptographyc protocol based on discrete logarithms in real quadratic orders. — Lect. Note Comp. Sci., 1994, v. 839, p. 56–60.
7. *Biehl J., Meyer B., Thiel Ch.* Cryptographyc protocol based in real quadratic a fields. — Lect. Note Comp. Sci., 1996, v. 1163, p. 15–25.
8. *Buchmann J., Williams H.C.* A key exchange system based on imaginary quadratic fields. — J. Cryptology, 1988, № 1, p. 107–118.
9. *Buchmann J., Scheidler R., Williams H.C.* A key exchange system based on real quadratic fields. — Lect. Note Comp. Sci., 1989, v. 435, p. 335–343.
10. *Buchmann J., Williams H.C.* A key exchange protocol using real quadratic fields. — J. Cryptology, 1994, № 3, p. 171–199.
11. *Buchmann J., Düllmann S.* On the computation of discrete logarithms in class groups. — Lect. Note Comp. Sci., 1991, v. 537, p. 134–139.
12. *Buchmann J., Düllman S., Williams H.C.* On the complexity and efficiency a new key exchange system. — Lect. Note Comp. Sci., 1990, v. 434, p. 597–616.
13. *Estes D., Adleman L.M., Kompella K., McCurley K., Miller G.L.* Breaking the Ong–Schnorr–Shamir signature scheme for quadratic number fields. — Lect. Note Comp. Sci., 1985, v. 218, p. 3–13.
14. *Hastad J.N.* Using RSA with lowexponent in a public key network. — Lect. Note Comp. Sci., 1986, v. 218, p. 403–408.
15. *Hühnlein D., Jacobson M.J., Paulus S., Takagi T.* A cryptosystem basedon non-maximal quadratic orders with fast decryption. — Lect. Note Comp. Sci., 1998, v. 1403, p. 294–307.
16. *Hühnlein D., Takagi T.* Reduction logarithms in totally non-maximal imaginary quadratic orders to logarithms in finite fields. — Lect. Note Comp. Sci., 1999, v. 1716, p. 219–231.

17. *Jacobson M.J.* (Jr.) Computation of discrete logarithms in quadratic orders. — J. Cryptology. 2000, v. 13, № 4, p. 437–492.

18. *McCurley K.* Cryptographyc key distribution and computation in class groups. — Number Theor. Appl., ser. C, 1989, v. 265, p. 459–479.

19. *Ong H., Schnorr C.P., Shamir A.* An efficient signature scheme based on quadratic equations. — Proceedings of XVIth ACM Symposium on Computation Theory, 1984, p. 208–216.

20. *Scheidler R.* A public-key cryptosystem using purely cubic fields. — J. Cryptology. 1998, v. 11, № 2, p. 109–124.

21. *Scheidler R., Buchmann J., Williams H.C.* Implementation of a key exchange protocol using some real quadratic fields. — Lect. Note Comp. Sci., 1990, v. 473, p. 98–109.

22. *Weber D.* Computing discrete logarithms with quadratic number rings. — Lect. Note Comp. Sci., 1998, v. 1403, p. 171–183.

23. *Williams H.* A modification of the RSA public-key encryption procedure. — IEEE Trans. Inf. Theor., 1980, v. IT-26, p. 726–729.

24. *Williams H.* Some public-key crypto-functions as intractable as factorization. — Cryptologia, 1985, v. 9, № 3, p. 223–237.