НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики
им. А.Н. Тихонова

НЕСТЕРЕНКО АЛЕКСЕЙ ЮРЬЕВИЧ

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Избранные вопросы алгоритмической теории чисел

редакция от 21 февраля 2022 г.

Оглавление

Часть I

Введение в теорию чисел

глава 1

Множества и операции

1.1 Множества

Начнем с того, что напомним базовое определение понятия «множество».

Определение 1.1. *Мы будем называть множеством совокупность объектов, обладающих некоторым одинаковым свойством, например, множество букв или цифр.*

1. *Если все элементы некоторого множества* $\mathbb{U}$ *также принадлежат другому множеству* $\mathbb{V}$*, то будем говорить, что* $\mathbb{U}$ *является подмножеством множества* $\mathbb{V}$ *и использовать запись* $\mathbb{U} \subseteq \mathbb{V}$.

2. *Будем говорить, что два множества равны и использовать запись* $\mathbb{U} = \mathbb{V}$*, если одновременно выполнено* $\mathbb{U} \subseteq \mathbb{V}$ *и* $\mathbb{V} \subseteq \mathbb{U}$.

3. *Если выполнено* $\mathbb{U} \subseteq \mathbb{V}$ *и множество* $\mathbb{V}$ *содержит элементы, которые не принадлежат* $\mathbb{U}$*, то будем называть* $\mathbb{U}$ *собственным подмножеством и использовать обозначение* $\mathbb{U} \subset \mathbb{V}$.

4. *Если множество не содержит ни одного элемента, то будем говорить, что оно содержится в любом другом множестве. Такое множество мы будем называть пустым и обозначать его символом* $\emptyset$.

5. *Если множество* $\mathbb{U}$ *не пусто, то в нем содержится хотя бы один элемент* a*; будем обозначать символом* $a \in \mathbb{U}$ *принадлежность элемента* a *множеству* $\mathbb{U}$.

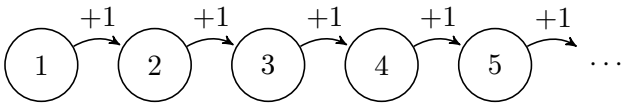
6. *Если множество* $\mathbb{W}$ *состоит из элементов двух множеств* $\mathbb{U}$ *и* $\mathbb{V}$*, то такое множество называется объединением множеств* $\mathbb{U}$ *и* $\mathbb{V}$ *и обозначается символом* $\mathbb{U} \cup \mathbb{V}$.

Определение 1.2. *Будем называть множеством натуральных чисел*

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

множество образованное фиксированным элементом 1*, которое вместе с элементом* n *содержит и элемент* $n+1$*.*

Схематично, процесс построения множества натуральных чисел изображен на следующем рисунке.



Определение 1.3. *Мы будем называть множество конечным, если количество его элементов может быть записано натуральным числом.*

Теорема 1.1. *Множество натуральных чисел бесконечно.*

Доказательство. Предположим, что множество $\mathbb{N}$ конечно. Тогда число его элементов записывается некоторым натуральным числом n, а само множество $\mathbb{N}$ состоит только из элементов

$$\{1, 2, \ldots, n\}.$$

Поскольку n принадлежит $\mathbb{N}$ то, в силу определения 1.2, множество $\mathbb{N}$ содержит в себе еще один элемент $n+1$, который не содержится среди указанных элементов. Таким образом наше предположение не верно. Лемма доказана. □

Определение 1.4. *Сопоставим каждому натуральному числу* n *формальный символ* $-n$*, который мы будем называть «обратным» к* n*, а множество таких символов обозначим* $-\mathbb{N}$*. Тогда множество целых чисел может быть определено как объединение*

$$\mathbb{Z} = -\mathbb{N} \cup 0 \cup \mathbb{N} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$$

где символ 0 *принято называть нулем. Множество*

$$0 \cup \mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$$

мы будем обозначать символом $\mathbb{N}_0$*.*

Отметим, что множество целых чисел обладает одним важным свойством, а именно, свойством упорядоченности.

Определение 1.5. *Будем говорить, что для всех* $n \in \mathbb{N}_0$ *число* $n+1$ *«больше»* n *и записывать* $n+1 > n$*, а число* $-n$ *«больше»* $-(n+1)$ *и записывать* $-n > -(n+1)$*. Относительно введенной операции*

«>» множество целых чисел может быть упорядочено следующим образом

$$\ldots 5 > 4 > 3 > 2 > 1 > 0 > -1 > -2 > -3 > -4 > -5 \ldots$$

Также введем операцию «меньше», обозначаемую символом «<», которая является отрицанием операции «больше». Относительно операции «меньше», множество целых чисел может быть упорядочено следующим образом

$$\ldots < -5 < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < 5 < \ldots .$$

Приведенные множества натуральных и целых чисел можно считать элементарными, поскольку с их помощью могут быть сконструированы более сложные множества. Приведем несколько простых примеров.

Определение 1.6. *Пусть n произвольное натуральное число и $\mathbb{U}$ – произвольное непустое множество. Будем называть вектором упорядоченный набор из n произвольных элементов множества $\mathbb{U}$, записанный в виде*

$$(a_1, \ldots, a_n).$$

Тогда множество $\mathbb{V}_n(\mathbb{U})$ всех возможных векторов, называется n-мерным векторным пространством над множеством $\mathbb{U}$.

Легко видеть, что при $n = 1$ векторное пространство над множеством $\mathbb{U}$ совпадает с самим множеством $\mathbb{U}$.

Определение 1.7. *Пусть n, m произвольные натуральные числа и $\mathbb{U}$ – произвольное непустое множество. Будем называть матрицей размера $m \times n$ прямоугольную таблицу, состоящую из nm упорядоченных произвольных элементов множества $\mathbb{U}$, записанных в виде*

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ & & \cdots & \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}.$$

Тогда множество $\mathbb{L}_{n,m}(\mathbb{U})$ всех возможных матриц называется пространством матриц размера $m \times n$ над множеством $\mathbb{U}$.

Если $n = m$, то для пространства матриц $\mathbb{L}_{n,n}(\mathbb{U})$ мы также будем использовать обозначение $GL_n(\mathbb{U})$, а для сокращенной записи матриц из $GL_n(\mathbb{U})$ – обозначение $(a_{i,j})_{i,j=1}^n$.

1.2 Операции на множествах

Какой-либо содержательный смысл перечисленные выше множества приобретают только после того, как на них будут определены операции – произвольные отображения множества в себя.

Определение 1.8. *Пусть* $\mathbb{U}$ *– произвольное непустое множество. Мы будем говорить, что на множестве* $\mathbb{U}$ *задана:*

- *унарная операция* $\delta : \mathbb{U} \to \mathbb{U}$*, если любому элементу* a *множества* $\mathbb{U}$ *может быть сопоставлен элемент* $\delta(a)$ *множества* $\mathbb{U}$*;*
- *бинарная операция* $* : \mathbb{U} \times \mathbb{U} \to \mathbb{U}$*, если любым двум упорядоченным, то есть записанным в определенном порядке, элементам* a, b *множества* $\mathbb{U}$ *можно сопоставить элемент множества* $\mathbb{U}$*, обозначаемый символом* $a * b$*.*

Для наиболее распространенных операций используются специальные обозначения, например, обозначения

$$\begin{aligned} \delta(a) &= -a, \\ \delta(a) &= \overline{a}, \\ \delta(a) &= a^{-1}, \end{aligned}$$

используются для записи унарной операции «обращения». Для бинарных операций, традиционно называемых «сложением» и «умножением» элементов, используются привычные обозначения $a+b$ и, соответственно, $a \cdot b$ или, просто, ab.

Определим два типа бинарных операций, играющих важнейшую роль для всего дальнейшего изложения.

Определение 1.9. *Бинарная операция* $*$ *называется ассоциативной, если для любых трех элементов* a, b, c *множества* $\mathbb{U}$ *выполнено равенство*

$$(a * b) * c = a * (b * c).$$

Определение 1.10. *Бинарная операция* $*$ *называется коммутативной, если для любых двух элементов* a, b *множества* $\mathbb{U}$ *выполнено равенство*

$$a * b = b * a.$$

Операции сложения и умножения, определенные для множества целых чисел $\mathbb{Z}$, являются ассоциативными и коммутативными. В общем случае, на одном и том же множестве могут быть определены как коммутативные, так и не коммутативные операции. Приведем следующий простой пример.

Пример 1.1. Рассмотрим множество

$$GL_n(\mathbb{Z}) = \left\{(a_{i,j})_{i,j=1}^n, \quad \text{где } a_{i,j} \in \mathbb{Z}, \quad i,j \in \{0,\dots,n\}\right\}$$

квадратных матриц размера $n \times n$ с целыми коэффициентами.
Рассмотрим квадратные матрицы $A = (a_{i,j})_{i,j=1}^n$ и $B = (b_{i,j})_{i,j=1}^n$ и определим операции

- сложения, равенством $C = A + B$, где

$$C = (c_{i,j})_{i,j=1}^n, \quad c_{i,j} = a_{i,j} + b_{i,j},$$

- и умножения, равенством $D = A * B$, где

$$D = (d_{i,j})_{i,j=1}^n, \quad d_{i,j} = \sum_{k=1}^n a_{i,k} b_{k,j}.$$

В силу коммутативности операции сложения целых чисел операция сложения матриц в $GL_n(\mathbb{Z})$ также коммутативна. В то же время выполнено равенство

$$B * A = (e_{i,j})_{i,j=1}^n, \quad \text{где} \quad e_{i,j} = \sum_{k=1}^n b_{i,k} a_{k,j},$$

из которого следует, что найдется такие целые числа $a_{i,j}$ и $b_{i,j}$, при $i,j \in \{1,\dots,n\}$, что

$$A * B \neq B * A.$$

Сказанное легко проверить при помощи численных вычислений, например,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} * \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 8 \\ 13 & 20 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 15 & 22 \\ 7 & 10 \end{pmatrix}.$$

Определение 1.11. *Элемент e множества $\mathbb{U}$ называется нейтральным элементом относительно бинарной операции $*$ если для любого элемента $a \in \mathbb{U}$ выполнено равенство*

$$e * a = a * e = a.$$

Теперь мы можем дать одно из важнейших определений.

Определение 1.12. *Непустое множество $\mathbb{U}$ называется группой, если*

1. *на множестве $\mathbb{U}$ задана ассоциативная бинарная операция $*$;*
2. *относительно операции $*$ во множестве $\mathbb{U}$ существует нейтральный элемент e;*
3. *для любого элемента a множества $\mathbb{U}$ найдется элемент $a^{-1} \in \mathbb{U}$ такой, что $a * a^{-1} = e$.*

Элемент a^{-1} принято называть обратным элементом к элементу a.

Если операция $*$ коммутативна, то группа называется коммутативной или абелевой.

Если в качестве бинарной операции $*$ используется операция сложения «+», то группа называется аддитивной, если же используется операция умножения «·», то группа называется мультипликативной.

Из данного определения вытекает, что для любой группы бинарная операция $*$ порождает унарную операцию δ — операцию обращения, определяемую следующим условием

$$\delta(a) = a^{-1}, \quad \text{если} \quad a * a^{-1} = e,$$

при этом, в силу определения нейтрального элемента, $e^{-1} = e$.

Пример 1.2.

1. Множество $\mathbb{Z}$ целых чисел образует коммутативную группу относительно операции сложения с нейтральным элементом 0. Действительно, в силу определения множества целых чисел, для любого натурального числа n найдется его обратный $-n$ такой, что $n + (-n) = 0$.

2. Множество квадратных матриц $GL_n(\mathbb{Z})$ размера $n \times n$ образует коммутативную группу относительно операции сложения, в которой нейтральным элементом является матрица, состоящая из одних нулей.

Приведем менее тривиальный пример и определим группу перестановок $\mathbb{S}_n$.

Определение 1.13. *Зафиксируем натуральное число $n > 1$. Мы будем называть перестановкой отображение π, ставящее в соответствие вектору $(1, 2, \ldots, n)$ вектор $(\pi_1, \pi_2, \ldots, \pi_n)$, в котором величины $\pi_1, \ldots, \pi_n$ различны и принимают все возможные значения от 1 до n.*

Если мы рассмотрим некоторое множество $\mathbb{U}$ и выберем в нем n произвольных элементов $a_1, \ldots, a_n$, то отображение π определяет способ перестановки выбранных элементов, то есть реализует отображение

$$\pi : \ (a_1, \ldots, a_n) \to (a_{\pi_1}, \ldots, a_{\pi_n})$$

или, в более простой форме $\pi(a_1, \ldots, a_n) = (a_{\pi_1}, \ldots, a_{\pi_n})$.

В наглядной форме перестановку π принято изображать следующим образом

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi_1 & \pi_2 & \ldots & \pi_n \end{pmatrix} \quad \text{или} \quad \pi = (\pi_1, \ \ldots, \ \pi_n).$$

Пусть π и ϕ две перестановки, действующие на некоторый вектор $a_1, \ldots, a_n$. Определим операцию композиции перестановок $\phi * \pi$ путем последовательного применения к вектору $a_1, \ldots, a_n$ сначала перестановки π, а потом и перестановки ϕ, то есть

$$(a_1, \ldots, a_n) \xrightarrow{\pi} (a_{\pi_1}, \ldots, a_{\pi_n}) \xrightarrow{\phi} (a_{\phi_{\pi_1}}, \ldots, a_{\phi_{\pi_n}}).$$

Таким образом, композиция перестановок также является перестановкой и может быть использована для определения бинарной операции на множестве перестановок, которое мы обозначаем символом $\mathbb{S}_n$.

Легко видеть, что перестановка $\varepsilon = (1, 2, \ldots, n)$ оставляет вектор $a_1, \ldots, a_n$ без изменений. Такую перестановку принято называть единичной и она является нейтральным элементом группы $\mathbb{S}_n$. Действительно, для любой перестановки π выполнено

$$\pi * \varepsilon = \varepsilon * \pi = \pi.$$

Более того, перестановка $\phi = (\phi_1, \ldots, \phi_n)$, определяемая условием

$$\phi_{\pi_k} = k, \quad k = 1, \ldots, n,$$

является обратной к перестановке π, то есть $\phi * \pi = \varepsilon$.

Пример 1.3. Легко видеть, что группа перестановок $\mathbb{S}_n$ является некоммутативной группой. Пусть $n = 3$ и заданы две перестановки

$$\pi = (3, 2, 1), \quad \phi = (1, 3, 2),$$

тогда для произвольного вектора $a = (a_1, a_2, a_3)$ выполнены равенства

$$\pi(a_1, a_2, a_3) = (a_3, a_2, a_1), \quad \phi(a_1, a_2, a_3) = (a_1, a_3, a_2).$$

Следовательно, выполнены равенства

$$\begin{aligned} \phi * \pi(a) &= \phi(a_3, a_2, a_1) = (a_3, a_1, a_2) \\ \pi * \phi(a) &= \pi(a_1, a_3, a_2) = (a_2, a_3, a_1) \end{aligned}$$

из которых следует, что $(3, 1, 2) = \phi * \pi \neq \pi * \phi = (2, 3, 1)$.

Определение 1.14. *Пусть U группа с заданной бинарной операцией $*$. Операцией возведения в степень или операцией вычисления кратного элемента называется отображение $a^n : \mathbb{U} \times \mathbb{N}_0 \to \mathbb{U}$, если для любого $a \in \mathbb{U}$ выполнено:*

1. *$a^0 = e$, где e нейтральный элемент группы,*

2. $a^1 = a$, *и*

3. $a^n = a^{n-1} * a$ *для всех* $n > 1$.

Теорема 1.2. *Для операции возведения в степень выполнены равенства*

$$a^n = a * a^{n-1} \tag{1.1}$$

и

$$a^{n+m} = a^n * a^m, \quad a^{nm} = (a^n)^m \tag{1.2}$$

для любых значений индексов $n, m \in \mathbb{N}_0$.

Доказательство. Докажем равенство (1.1) по индукции. При $n = 1, 2$ данное равенство, очевидно, выполнено. Теперь предположим, что оно выполнено для всех индексов, меньших чем n, тогда

$$a^n = a^{n-1} * a = (a * a^{n-2}) * a = a * (a^{n-2} * a) = a * a^{n-1}.$$

Теперь докажем равенство (1.2) и, в начале, рассмотрим случай, когда один из индексов n или m равен нулю. Пусть $n = 0$, тогда

$$a^{0+m} = a^m = e{*}a^m = a^0{*}a^m, \quad a^{0\cdot m} = a^0 = e = e{*}e = e^2{*}e = \cdots = e^m = (a^0)^m.$$

Аналогично, пусть $m = 0$, тогда

$$a^{n+0} = a^n = a^n * e = a^n * a^0, \quad a^{n\cdot 0} = a^0 = e = (a^n)^0.$$

Далее сделаем индуктивный переход и будем считать, что для некоторого натурального k и всех индексов $n + m < k$ утверждение теоремы выполнено. Тогда, при $n + m = k$ выполнены равенства

$$a^{n+m} = a^{n+m-1} * a = \left(a^n * a^{m-1}\right) * a = a^n * \left(a^{m-1} * a\right) = a^n * a^m.$$

Если $n = 1$, то $a^m = (a^1)^m$. Если же $m = 1$, то $a^n = (a^n)^1$. Таким образом, при $n = 1$ или $m = 1$ утверждение теоремы выполнено. Далее будем считать, что $n > 1$ и $m > 1$, тогда, воспользовавшись индуктивным предположением, запишем равенства

$$a^{nm} = a^{nm-1} * a = (a^{nm-2} * a) * a = a^{mn-2} * (a * a) = a^{mn-2} * a^2 = \cdots$$
$$\cdots = a^{mn-n} * a^n = a^{n(m-1)} * a^n = (a^n)^{m-1} * a^n = (a^n)^m,$$

которые завершают доказательство теоремы. □

Согласно данному определению значение a^n может быть вычислено с использованием $n - 1$ групповой операции $*$. В следующей главе мы введем понятие операции деления с остатком, которая позволит определить двоичный алгоритм возведения в степень, с помощью которого можно вычислить значение a^n существенно быстрее.

1.3 Множества с двумя операциями

Определение 1.15. *Непустое множество* $\mathbb{U}$ *называется кольцом, если*

1. *на множестве* $\mathbb{U}$ *заданы две ассоциативные бинарные операции «*$+$*» и «*$\cdot$*»;*
2. *операция «*$+$*» коммутативна;*
3. *относительно операции «*$+$*» множество* $\mathbb{U}$ *является группой;*
4. *выполнены законы дистрибутивности*

$$a(b+c) = ab + bc \quad \text{и} \quad (b+c)a = ba + ca.$$

Группа, образованная элементами кольца $\mathbb{U}$ *относительно операции «*$+$*», называется аддитивной группой кольца. Нейтральный элемент аддитивной группы называется нулевым элементом кольца* $\mathbb{U}$ *и обозначается, как правило, символом* 0*.*

Если операция «$\cdot$*» коммутативна, то кольцо называется коммутативным.*

Если кольцо $\mathbb{U}$ *содержит нейтральный элемент, относительно операции «*$\cdot$*», то такой элемент называется единичным элементом, а кольцо* $\mathbb{U}$ *– кольцом с единицей. Единичный элемент, как правило, обозначают символом* 1*.*

Пример 1.4. Множество целых чисел $\mathbb{Z}$ образует кольцо с единицей относительно операций сложения и умножения. Кроме того, можно предъявить несколько собственных подмножеств в $\mathbb{Z}$, которые также являются кольцами.

1. Множество $\{0\}$, состоящее из одного нулевого элемента, образует кольцо. Данное кольцо принято называть «нулевым» кольцом.
2. Пусть $k > 1$ произвольное натуральное число. Тогда множество

$$\{\ldots, -3k, -2k, -k, 0, k, 2k, 3k, \ldots\}$$

целых, делящихся на k чисел, образует кольцо без единицы.

3. Пусть i символ, определяемый равенством $i^2 = -1$. Рассмотрим множество

$$\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\}$$

и определим на нем операции сложения и умножения следующими равенствами

$$\begin{aligned} (a+bi) + (c+di) &= (a+c) + (b+d)i, \\ (a+bi) \cdot (c+di) &= (ac-bd) + (bc+ad)i. \end{aligned}$$

Множество $\mathbb{Z}[i]$ содержит в себе кольцо целых чисел $\mathbb{Z}$, т.е. $\mathbb{Z} \subset \mathbb{Z}[i]$, и также является кольцом; его принято называть кольцом целых гауссовых[a] чисел.

4. Множество квадратных матриц $GL_n(\mathbb{Z})$ размера $n \times n$ образует некоммутативное кольцо относительно введенных ранее операций сложения и умножения матриц.

[a]Данное множество чисел ввел в обращение великий немецкий математик Иоганн Карл Фридрих Гаусс (1777 – 1855). С помощью таких чисел он доказал ряд результатов, например, о том, что любое простое натуральное число вида $4n + 1$ можно представить в виде суммы квадратов двух натуральных чисел, причём единственным способом. (лучше дать ссылку на доказавыемую позже лемму см. Zinotes.pdf) В последствии гауссовы целые привели к появлению комплексных чисел.

Определение 1.16. *Пусть $\mathbb{U}$ кольцо, $a, b \in \mathbb{U}$ и $a \neq 0$. Мы будем говорить, что a делит b и записывать $a|b$, если найдется элемент $c \in \mathbb{U}$ такой, что $b = ac$. Элемент a будем называть левым делителем элемента b, элемент c – правым делителем. Если кольцо коммутативно, то любой делитель элемента b является одновременно и правым, и левым, т.е. просто делителем.*

Пример 1.5. В кольце целых чисел выполнено равенство $12 = 3 \cdot 4$, из которого следует, что $3|12$ и $4|12$. Аналогично, в кольце целых гауссовых чисел $\mathbb{Z}[i]$ из равенства

$$5 = (1 + 2i)(1 - 2i)$$

следует, что $1 - 2i|5$ и $1 + 2i|5$.

Лемма 1.1. *Пусть задано кольцо $\mathbb{U}$ и элементы $a, b \in \mathbb{U}$. Для операции деления выполнены следующие утверждения.*

1. *Выполнено условие $1|a$.*
2. *Если $a \neq 0$, то выполнено $a|a$ и $a|0$.*
3. *Если $a \neq 0$ и $a|b$, то $a|bc$ для любого $c \in \mathbb{U}$.*
4. *Если для $a \neq 0$, $b \neq 0$ выполнено условие $a|b$, $b|c$, то $a|c$.*
5. *Если $a \neq 0$ и $a|b$, то $a^n|b^n$ для любого значения $n \in \mathbb{N}_0$.*

Доказательство. Первые три утверждения леммы сразу следуют из определения операции деления. Докажем оставшиеся.

Пусть $a|b$ и $b|c$, тогда $c = bu$, $b = av$ для некоторых $u, v \in \mathbb{U}$. Тогда $c = bu = auv$ и $a|c$. Для доказательства последнего утверждения, используя свойство ассоциативности операции умножения, запишем равенство

$$b^n = \underbrace{b \cdot b \cdot \ldots \cdot b \cdot b}_{n \text{ раз}} = \underbrace{a \cdot u \cdot \ldots \cdot a \cdot u}_{n \text{ раз}} = a^n u^n,$$

из которого следует, что $a^n|b^n$. □

Определение 1.17. *Если кольцо* $\mathbb{U}$ *содержит элементы* $a, b \in \mathbb{U}$ *такие, что*

$$a \cdot b = 0, \quad a \neq 0, \quad b \neq 0, \tag{1.3}$$

то такое кольцо называется кольцом с делителями нуля. В противном случае, кольцо называется кольцом без делителей нуля.

Элемент a*, удовлетворяющий (1.3) называется левым делителем нуля, а элемент* b *– правым делителем нуля (для коммутативных колец эти понятия совпадают).*

Коммутативное кольцо $\mathbb{U}$ *без делителей нуля называется целостным кольцом.*

Заметим, что все приведенные в примере 1.3 кольца являются кольцами без делителей нуля. Позднее, в главе XXX, мы приведем пример кольца, удовлетворяющего определению 1.17.

Пусть $\mathbb{U}$ произвольное кольцо. Ранее мы показали, как можно расширить $\mathbb{U}$ и построить новые множества – векторное пространство, пространство прямоугольных матриц и множество перестановок. Сейчас мы приведем еще один способ построения нового множества.

Определение 1.18. *Пусть* $\mathbb{U}$ *кольцо и* x *некоторый формальный символ, тогда мы будет называть многочленом формальную сумму*

$$a(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + \cdots + a_1 x + a_0, \quad n \in \mathbb{N}_0, \quad a_0, \ldots, a_n \in \mathbb{U},$$

где $a_n \neq 0$*, если* $n > 0$*.*

Множество всех возможных многочленов будем обозначать символом $\mathbb{U}[x]$*.*

Величины $a_0, \ldots, a_n$ *мы будем называть коэффициентами, коэффициент* a_n *– старшим коэффициентом, а* x *– переменной. Величину* n *будем называть степенью многочлена и обозначать символом* $\deg a(x)$*.*

Многочлен со старшим коэффициентом, равным единичному элементу кольца $\mathbb{U}$*, будем называть унитарным многочленом.*

Определим на множестве $\mathbb{U}[x]$ *операции сложения и умножения полагая, что символ* x *перестановочный с элементами кольца* $\mathbb{U}$*, то есть* $ax = xa$ *для любого* $a \in \mathbb{U}$*. Пусть* $b(x) = \sum_{k=0}^{m} b_k x^k$ *и, без ограничения общности, будем считать, что* $m \geqslant n$*, тогда*

$$\begin{aligned} a(x)+b(x) &= \sum_{k=0}^{n}(a_k+b_k)x^k+\sum_{k=n+1}^{m} b_k x^k, \\ a(x)b(x) &= \sum_{k=0}^{n+m} c_k x^k, \quad \text{где} \quad c_k=\sum_{i+j=k} a_i b_j. \end{aligned} \tag{1.4}$$

Пример 1.6. Рассмотрим многочлены

$$\begin{aligned} a(x) &= x^3+2x^2+3x+1 \\ b(x) &= 4x^2+5x+2 \end{aligned}$$

с целыми коэффициентами, тогда их сумма определяется равенством

$$a(x)+b(x)=x^3+(2+4)x^2+(3+5)x+(1+2)=x^3+6x^2+8x+3.$$

Произведение многочленов определяется, согласно (1.4), равенством

$$\begin{aligned} a(x)b(x) &= 4x^5+(1\cdot 5+2\cdot 4)x^4+ \\ &+(1\cdot 2+2\cdot 5+3\cdot 4)x^3+(2\cdot 2+3\cdot 5+1\cdot 4)x^2+(3\cdot 2+1\cdot 5)x+1\cdot 2= \\ &= 4x^5+13x^4+24x^3+23x^2+11x+2 \end{aligned}$$

и представляет собой попарное произведение всех слагаемых многочленов $a(x)$ и $b(x)$.

Описанный нами процесс построения кольца многочленов может быть повторен еще раз и применен к кольцу $\mathbb{U}[x]$.

Рассмотрим формальный символ y, для которого выполнено равенство $xy=yx$. Применяя определение 1.18 к кольцу $\mathbb{U}[x]$, мы можем определить кольцо многочленов $\mathbb{U}[x,y]$ от двух неизвестных x,y. Тогда элементами кольца $\mathbb{U}[x,y]$ будут формальные суммы

$$a(x,y)=\sum_{k=0}^{n} a_k(x)y^k=a_n(x)y^n+\cdots+a_1(x)y+a_0=\sum_{k=0}^{n}\sum_{j=0}^{m} a_{k,j}x^k y^j,$$

где $n\in\mathbb{N}_0$, $a_0(x),\ldots,a_n(x)\in\mathbb{U}[x]$, $a_n(x)\neq 0$, если $n>0$, и $m=\max_{k=0,\ldots,n}\{\deg a_k(x)\}$.

Продолжая так дальше, мы можем определить кольцо $\mathbb{U}[x_1,\ldots,x_n]$ от n неизвестных, элементами которого являются формальные суммы вида

$$a(x_1,\ldots,x_n)=\sum_{i_1}\cdots\sum_{i_n} a_{i_1,\ldots,i_n}x_1^{i_1}\cdots x_n^{i_n}.$$

Лемма 1.2. *Если $\mathbb{U}$ целостное кольцо, то $\mathbb{U}[x]$ также является целостным кольцом.*

Доказательство. Пусть $a(x), b(x) \in \mathbb{U}[x]$ два отличных от нуля многочлена со старшими коэффициентами a_n и b_m соответственно. Тогда $a_n \neq 0$, $b_m \neq 0$ и, в силу целостности кольца $\mathbb{U}$, выполнено $a_n b_m \neq 0$. Таким образом, хотя бы один коэффициент многочлена $a(x)b(x)$, а следовательно и сам многочлен $a(x)b(x)$, отличен от нуля. □

Определение 1.19. *Пусть $\mathbb{U}$ кольцо. Если множество ненулевых элементов кольца $\mathbb{U}$ образует группу относительно операции «$\cdot$», то $\mathbb{U}$ называется телом. Если данная группа – коммутативна, то такое тело называется полем.*

Группа, образованная ненулевыми элементами тела (поля) $\mathbb{U}$ называется мультипликативной группой тела (поля).

Пример 1.7. Рассмотрим состоящее из трех элементов множество $\{-1, 0, 1\}$ и зададим на нем операции сложения и умножения следующим образом.

Сложение

	-1	0	1
-1	0	-1	0
0	-1	0	1
1	0	1	0

Умножение

	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

Рассмотренное нами множество является полем. Действительно, операции вводят на множестве $\{-1, 0, 1\}$ структуру аддитивной группы, а на множестве $\{-1, 1\}$ – структуру мультипликативной группы. Нейтральным элементом относительно операции сложения является 0, а нейтральным элементом относительно операции умножения — 1.

Для того, чтобы предъявить менее тривиальный способ построения полей, нам потребуется понятие эквивалентности элементов множества.

Определение 1.20. *Мы будем говорить, что на множестве $\mathbb{U}$ задано отношение эквивалентности $\sim$, если оно*

- *рефлексивно, то есть $a \sim a$;*
- *симметрично, то есть из $a \sim b$ следует $b \sim a$;*
- *транзитивно, то есть из $a \sim b$ и $b \sim c$ следует $a \sim c$.*

Пример 1.8. Рассмотрим кольцо целых чисел $\mathbb{Z}$ и будем говорить, что два целых числа эквивалентны, если их разность делится на 2. Легко видеть, что для данного определения эквивалентности все перечисленные свойства выполнены, а само определение разбивает целые числа на два класса эквивалентности – четные и нечетные числа.

Отношение эквивалентности может быть использовано для построения новых множеств, отличных от описанных нами ранее. Представляется естественным обозначить все эквивалентные между собой элементы множества $\mathbb{U}$ за новый элемент, определить новое множество, состоящее из указанных элементов, и определить на новом множестве элементарные операции сложения и умножения.

Именно такая последовательность действий используется в ходе доказательства следующей теоремы.

Теорема 1.3. *Пусть $\mathbb{U}$ целостное кольцо с единицей. Тогда найдется поле $\mathbb{F}$ такое, что $\mathbb{F} \supset \mathbb{U}$.*

Доказательство. Пусть $\mathbb{U}$ целостное кольцо, т.е. коммутативное кольцо с единицей. Рассмотрим множество упорядоченных пар (a, b) элементов из $\mathbb{U}$ таких, что $b \neq 0$ и введем отношение эквивалентности двух пар

$$(a, b) \sim (c, d), \quad \text{если} \quad ad = bc.$$

Данное отношение:

- рефлексивно, поскольку из коммутативности кольца $\mathbb{U}$ и равенства $ab = ba$ следует, что $(a, b) \sim (a, b)$;
- симметрично, поскольку из равенства $ad = bc$ следует равенство $bc = ad$ и условие $(c, d) \sim (a, d)$;
- транзитивно, поскольку из $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$ следуют равенства

  $$ad = bc, \quad cf = ed.$$

  Тогда

  $$adf = bcf = bed \quad \text{и} \quad af = be,$$

  следовательно, $(a, b) \sim (e, f)$ и отношение $\sim$ задает отношение эквивалентности на множестве пар (a, b).

Выберем произвольную пару (a, b) и рассмотрим множество пар, эквивалентных паре (a, b). Будем называть это множество классом эквивалентности и обозначать символом $\dfrac{a}{b}$. Тогда равенство $\dfrac{a}{b} = \dfrac{c}{d}$ означает, что $(a, b) \sim (c, d)$ или $ad = bc$.

Множество классов будем обозначать символом $\mathbb{F}$.

Определим операции сложения и умножения новых символов (классов эквивалентности) равенствами

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

и

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Приведенные определения корректно определены, поскольку для $b \neq 0$, $d \neq 0$ кольцо $\mathbb{U}$ не содержит делителей нуля и величина $bd \neq 0$, и не зависят от выбора представителей классов.

Действительно, пусть $(a_1, b_1) \sim (a, b)$, тогда

$$a_1 b = a b_1, \quad \text{или} \quad a_1 bd = a d b_1,$$

для любого $d \in \mathbb{U}$, $d \neq 0$, следовательно,

$$\frac{a_1}{b_1} + \frac{c}{d} = \frac{a_1 d + b_1 c}{b_1 d} = \frac{(a_1 d + b_1 c)b}{b_1 db} = \frac{a d b_1 + b_1 cb}{b_1 db} = \frac{ad + bc}{bd} = \frac{a}{b} + \frac{c}{d}.$$

Аналогично,

$$\frac{a_1}{b_1} \times \frac{c}{d} = \frac{a_1 d}{b_1 d} = \frac{a_1 db}{b_1 db} = \frac{a_1 d b_1}{b_1 db} = \frac{a}{b} \times \frac{c}{d}.$$

Легко проверить, что нейтральными элементами для введенных операций являются классы

$$\frac{0}{b} \quad \text{и} \quad \frac{1}{1},$$

а сами операции определяют на множестве классов $\mathbb{F}$ структуру поля.

Покажем, что $\mathbb{U} \subset \mathbb{F}$. Сопоставим элементу $c \in \mathbb{U}$ все дроби вида $\frac{cb}{b}$. Тогда, из равенства

$$(cb)b_1 = b(cb_1)$$

следует, что элементу c сопоставлен только один класс эквивалентности в $\mathbb{F}$. При этом, различным элементам $c_1 \neq c$ сопоставляются различные классы. В противном случае выполнены равенства

$$\frac{cb}{b} = \frac{c_1 b_1}{b_1}$$

или

$$cbb_1 = c_1 b_1 b.$$

Так как $b \neq 0$, $b_1 \neq 0$, то, сокращая, получим $c = c_1$. Следовательно, элементам кольца $\mathbb{U}$ однозначно сопоставляются дроби вида $\frac{cb}{b} \in \mathbb{F}$.

Поскольку

$$\frac{c_1 b_1}{b_1} + \frac{c_2 b_2}{b_2} = \frac{(c_1 + c_2)b_1 b_2}{b_1 b_2}$$

и

$$\frac{c_1 b_1}{b_1} \times \frac{c_2 b_2}{b_2} = \frac{(c_1 c_2)b_1 b_2}{b_1 b_2}$$

то операции сложения и умножения в $\mathbb{F}$ оставляют множество дробей $\left\{\frac{cb}{b}\right\}$ замкнутым, т.е не выводят за его пределы, и индуцируют на нем структуру коммутативного кольца $\mathbb{U}$. □

Определение 1.21. *Построенное в теореме поле* $\mathbb{F}$ *принято называть полем частных целостного кольца* $\mathbb{U}$. *Процесс построения поля* $\mathbb{F}$ *называют погружением кольца* $\mathbb{U}$ *в поле* $\mathbb{F}$.

Из доказанной теоремы следуют следующие определения.

Определение 1.22. *Кольцо целых чисел* $\mathbb{Z}$ *может быть погружено в поле частных, которое принято называть полем рациональных чисел и обозначать символом* $\mathbb{Q}$.

Определение 1.23. *Кольцо многочленов* $\mathbb{Z}[x]$ *может быть погружено в поле частных, которое принято называть полем рациональных функций и обозначать символом* $\mathbb{Z}(x)$.

Задачи и упражнения

1. Для множества $\{1, 7, 11, 29\}$ найдите все его собственные подмножества.

2. Покажите, как из определения натуральных чисел следует общепринятое определение операций сложения и умножения на множестве целых чисел.

3. Докажите, что операции сложения и умножения на множестве целых чисел удовлетворяют как свойству ассоциативности, так и свойству коммутативности.

4. Найдите сумму и произведение матриц

$$A = \begin{pmatrix} -2 & 4 & 3 \\ 1 & 4 & 5 \\ 7 & -6 & 0 \end{pmatrix} \quad \text{и} \quad B = \begin{pmatrix} 5 & 2 & 11 \\ 4 & 0 & 3 \\ 5 & 9 & 2 \end{pmatrix}.$$

5. Докажите ассоциативность введенной операции композиции перестановок и, тем самым, завершите доказательство утверждения о том, что множество $\mathbb{S}_n$ группа.

6. Для перестановок $\pi = (1, 5, 2, 3, 4)$ и $\varphi = (5, 4, 1, 2, 3)$ найдите их композицию, а также обратные перестановки π^{-1} и φ^{-1}.

7. Докажите самостоятельно первые три утверждения леммы 1.1 о свойствах операции деления.

8. Докажите, что кольцо $\mathbb{Z}[i]$ не содержит делителей нуля. Для этого рассмотрите решение системы уравнений

$$\begin{cases} ac - bd = 0, \\ dc + ad = 0 \end{cases}$$

для произвольных $a, b, c, d \in \mathbb{Z}$.

9. Найдите произведение следующих трех гауссовых чисел $1 + 2i$, $2 + i$, $5 + i$.

10. Попробуйте заменить в определении кольца гауссовых чисел величину i, удовлетворяющую равенству $i^2 = -1$, на величину j, удовлетворяющую равенству $j^2 + j + 1 = 0$. Определите операции сложения и умножения для полученного множества.

11. По аналогии с кольцом целых гауссовых чисел определите кольцо, содержащее корень многочлена $f(x) = x^3 + 2x - 1$.

12. Пусть $\mathbb{U}$ произвольное кольцо. Покажите, что $\mathbb{U} \subset \mathbb{U}[x]$ и докажите, что множество $\mathbb{U}[x]$ образует кольцо.

13. Найдите произведение двух многочленов $a(x) = 7x^3 + 2x + 1$ и $b(x) = 6x^2 + 2x + 9$ с целыми коэффициентами.

14. Найдите сумму и произведение двух многочленов $a(x) = x^2y^3 + 2x + 12y^2$ и $b(x) = x^3 + xy + 6x + 1$ с целыми коэффициентами.

15. Докажите, что тело (поле) не имеет делителей нуля.

16. Вычислите значение суммы и произведения двух элементов поля рациональных функций $\frac{1}{2x+1}$ и $\frac{x}{x^3-3}$.

17. Покажите, что кольцо многочленов $\mathbb{Z}[x, y]$ от двух переменных является целостным кольцом и погрузите его в поле частных $\mathbb{Z}(x, y)$.

18. Введите понятие упорядоченности для следующих множеств $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}[x, y]$.

Рекомендации к сдаче экзамена

Схематично, последовательность определения рассматриваемых в настоящей главе множеств изображена на рисунке 1.1.

Определения рассматриваемых множеств и их свойств в обязательном порядке входят в перечень вопросов устного экзамена по курсам

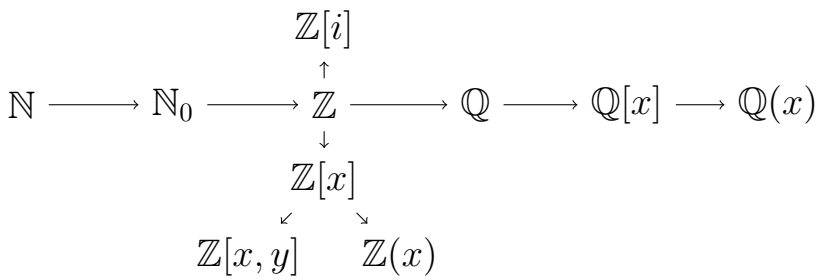


Рис. 1.1: Схема элементарных числовых множеств.

«Введение в теорию чисел» и «Теоретико-числовые методы в криптографии». В экзаменационные билеты по курсу «Введение в теорию чисел» входят следующие вопросы.

- Основные множества. Понятия группы, кольца и поля.
- Теорема о погружении целостного кольца в поле (теорема 1.3).

  Доказательство теоремы 1.3 состоит из нескольких шагов. На первом шаге строится множество пар элементов целостного кольца $\mathbb{U}$ и на этом множестве вводится понятие эквивалентности. Множество эквивалентных пар образует один класс, а множество классов – поле $\mathbb{F}$.

  На втором шаге определяются операции сложения и умножения элементов поля $\mathbb{F}$ (классов эквивалентности) и показывается, что введенные операции не зависят от выбора представителей классов эквивалентности. На третьем шаге доказательства предъявляются классы эквивалентности, содержащие элементы кольца $\mathbb{U}$. Множество таких классов содержит в себе кольцо $\mathbb{U}$. Показывается, что введенные в поле $\mathbb{F}$ операции не выводят за пределы кольца $\mathbb{U}$, т.е. результатом сложения и умножения классов эквивалентности, содержащих элементы кольца $\mathbb{U}$, также являются классы эквивалентности, содержащие элементы кольца $\mathbb{U}$.

Дополнительная литература к 1-й главе

1. ван дер Варден Б. Л. *Алгебра.* – М.: Мир, 1976. – 648 с.
2. Зарисский О., Самуэль П. Коммутативная алгебра. Том 1. –
3. Кострикин А.И. Введение в алгебру. – М.:Наука, 1972.

глава 2

Теория делимости

В этой главе, если не оговорено особо, мы будем рассматривать только коммутативные кольца, без делителей нуля.

Определение 2.1. *Мы будем говорить, что элемент $\varepsilon \in \mathbb{U}$ обратим, если он делит единичный элемент кольца, то есть найдется такой элемент $\varepsilon^{-1} \in \mathbb{U}$ такой, что $\varepsilon\varepsilon^{-1} = 1$. Мы будем обозначать множество обратимых элементов кольца $\mathbb{U}$ символом $\mathbb{U}^*$.*

Лемма 2.1. *Множество $\mathbb{U}^*$ обратимых элементов кольца $\mathbb{U}$ образует мультипликативную группу.*

Доказательство. Пусть $\varepsilon \in \mathbb{U}^*$, тогда, по определению, найдется элемент $\varepsilon^{-1} \in \mathbb{U}^*$ такой, что $\varepsilon\varepsilon^{-1} = 1$.

Аналогично, для $\rho \in \mathbb{U}^*$ найдется $\rho^{-1} \in \mathbb{U}^*$ такой, что $\rho\rho^{-1} = 1$. Поскольку кольцо $\mathbb{U}$ коммутативно, то из равенства

$$\varepsilon\varepsilon^{-1} \cdot \rho\rho^{-1} = \varepsilon\rho \cdot \varepsilon^{-1}\rho^{-1} = 1$$

следует, что элемент $\varepsilon\rho \in \mathbb{U}^*$. Таким образом множество $\mathbb{U}^*$ замкнуто относительно операции умножения, определенной для кольца $\mathbb{U}$, и наследует ее свойство ассоциативности, т.е. $\mathbb{U}^*$ – группа. Лемма доказана. □

Пример 2.1. Рассмотрим группы обратимых элементов для нескольких колец.

1. В кольце целых чисел $\mathbb{Z}$ группу обратимых элементов образуют числа
$$\mathbb{Z}^* = \{1, -1\}.$$
2. В кольце целых гауссовых чисел $\mathbb{Z}[i]$ группу обратимых элементов образуют числа
$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$
Для доказательства этого факта смотри лемму 2.4.
3. Группа обратимых элементов кольца многочленов от одной переменной $\mathbb{U}[x]$ состоит из обратимых элементов кольца $\mathbb{U}$.
4. В любом поле $\mathbb{F}$ группа обратимых элементов совпадает с мультипликативной группой поля.

2.1 Норма и операция деления с остатком

Определение 2.2. *Отображение* $N : \mathbb{U} \to \mathbb{N}_0$ *называется нормой, если выполнены следующие условия:*

1. $N(0) = 0$,
2. *отображение* N *не вырождено, т.е. найдется элемент* $a \in \mathbb{U}$ *такой, что* $N(a) \neq 0$,
3. *пусть* $a \neq 0$ *и* $a|b$, *то* $N(a) \leqslant N(b)$.

Пусть приводимые ниже равенства выполнены для любых двух элементов $a, b \in \mathbb{U}$, *тогда будем называть норму:*

- *«аддитивной», если* $N(ab) = N(a) + N(b)$,
- *«мультипликативной», если* $N(ab) = N(a)N(b)$,

Докажем следующее утверждение.

Лемма 2.2. *Пусть* $\mathbb{U}^*$ *группа обратимых элементов кольца* $\mathbb{U}$. *Тогда для любого* $\varepsilon \in \mathbb{U}^*$ *выполнены условия:*

1. *если норма мультипликативна, то* $N(\varepsilon) = 1$,
2. *если норма аддитивна, то* $N(\varepsilon) = 0$.

Доказательство. В начале предположим, что норма N – мультипликативна. Тогда, в силу равенства $\varepsilon\varepsilon^{-1} = 1$, выполнено

$$N(1) = N(\varepsilon\varepsilon^{-1}) = N(\varepsilon)N(\varepsilon^{-1}). \tag{2.1}$$

Поскольку $1 \in \mathbb{U}^*$, т.е. также является обратимым элементом, то из (2.1) получаем равенство

$$N(1) = N(1)N(1),$$

которое может выполняться только в двух случаях – когда $N(1)$ равно 0 или 1. Предположим, что $N(1) = 0$, тогда для любого элемента $a \in \mathbb{U}$ выполнено

$$N(a) = N(a \cdot 1 \cdot 1^{-1}) = N(a \cdot 1^{-1})N(1) = 0$$

и мы получаем противоречие с тем, что норма не вырождена. Следовательно, выполнено равенство $N(1) = 1$. Теперь из (2.1) следует условие $N(\varepsilon)|1$, которое дает равенство $N(\varepsilon) = 1$. Первое утверждение леммы доказано.

Теперь рассмотрим случай, когда норма в кольце $\mathbb{U}$ аддитивна. Тогда

$$N(1) = N(\varepsilon\varepsilon^{-1}) = N(\varepsilon) + N(\varepsilon^{-1}).$$

Полагая $\varepsilon = 1$, получаем равенство

$$N(1) = N(1) + N(1) \quad \text{или} \quad N(1) = 0,$$

которое завершает доказательство леммы. □

Доказанная лемма послужила причиной появления следующего определения.

Определение 2.3. *Пусть $\mathbb{U}$ кольцо, а котором задана мультипликативная норма. Тогда группу $\mathbb{U}^*$ обратимых элементов кольца $\mathbb{U}$ принято называть группой единиц.*

Теперь мы явно определим отображения, удовлетворяющие определению нормы.

Лемма 2.3. *Выполнены следующие утверждения.*

1. *Отображение $N : \mathbb{Z} \to \mathbb{N}_0$ определяемое равенством $N(a) = |a|$ задает мультипликативную норму в кольце целых чисел $\mathbb{Z}$.*

2. *Пусть $\mathbb{U}$ кольцо без делителей нуля. Отображение $N : \mathbb{U}[x] \to \mathbb{N}_0$ определяемое равенством $N(a(x)) = \deg a(x)$, $a(x) \in \mathbb{U}[x]$, задает аддитивную норму в кольце многочленов $\mathbb{U}[x]$.*

3. *Отображение $N : \mathbb{Z}[i] \to \mathbb{N}_0$ определяемое равенством*

$$N(a + bi) = a^2 + b^2,\ a + bi \in \mathbb{Z}[i],$$

задает мультипликативную норму в кольце целых гауссовых чисел $\mathbb{Z}[i]$.

Доказательство. Для кольца целых чисел выполнены равенства

$$\begin{array}{rcccl} N(0) & = & |0| & = & 0, \\ N(1) & = & |1| & = & 1, \\ N(ab) & = & |ab| & = & |a| \cdot |b| = N(a) \cdot N(b) \end{array}$$

из которых следует, что все свойства нормы, введенные ранее в определении 2.2, выполнены.

Рассмотрим кольцо многочленов $\mathbb{U}[x]$ и пусть $a(x), b(x) \in \mathbb{U}[x]$

$$a(x) = \sum_{k=0}^{n} a_k x^k, \quad b(x) = \sum_{k=0}^{m} b_k x^k.$$

Тогда $\deg a(x) = n$, если $a_n \neq 0$, и $\deg b(x) = m$, если $b_m \neq 0$. Поскольку кольцо $\mathbb{U}$ без делителей нуля, то $a_n b_m \neq 0$ и, согласно определению операции умножения многочленов, см. (1.4), выполнено равенство

$$\deg\left(a(x)b(x)\right) = \deg\left(a_n b_m x^{n+m} + \cdots\right) = n + m.$$

Следовательно, выполнено

$$N(a(x)b(x)) = \deg\left(a(x)b(x)\right) = n + m = \\ = \deg a(x) + \deg b(x) = N(a(x)) + N(b(x)),$$

и норма в кольце многочленов – аддитивна.

В завершение доказательства рассмотрим кольцо целых гауссовых чисел $\mathbb{Z}[i] = \{a + bi,\ i^2 = -1,\ a, b \in \mathbb{Z}\}$. Пусть $\alpha = a + bi$, $\gamma = c + di$, тогда

$$N(\alpha\gamma) = N\left((ac - bd) + (ad + bc)i\right) = (ac - bd)^2 + (ad + bc)^2 = \\ = (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\gamma).$$

Полученное равенство позволяет говорить о том, что в кольце гауссовых целых введенная норма мультипликативна. □

Пример 2.2. Выполнены следующие равенства.

1. В кольце целых чисел $N(-5) = N(5) = 5$.
2. В кольце многочленов $\mathbb{Q}[x]$

$$N\left(\frac{x^4}{5} + 2x^2 + 1\right) = 4, \quad N(2x^4 + x^3 + x + 1) = 4.$$

3. В кольце целых гауссовых чисел

$$N(2 + 3i) = N(3 - 2i) = 13, \quad N(-5) = N(5) = 25.$$

Простым следствием доказанной ранее леммы 2.3 служит следующее утверждение.

Лемма 2.4. *Группу обратимых элементов кольца целых гауссовых чисел* $\mathbb{Z}[i]$ *образуют элементы* $\{1, -1, i, -i\}$.

Доказательство. Пусть α, γ обратимые элементы кольца $\mathbb{Z}[i]$ такие, что $\alpha\gamma = 1$. Тогда

$$N(\alpha)N(\gamma) = N(1) = 1^2 + 0^2 = 1.$$

Поскольку значение нормы является целым числом, то из полученного равенства следует, что

$$N(\alpha) = \pm 1, \quad N(\gamma) = \pm 1.$$

С другой стороны равенство

$$N(\alpha) = N(a + bi) = a^2 + b^2 = 1$$

выполнено только в том случае, когда одно из целых чисел a, b равно нулю, а второе равно ± 1. Таким образом мы получаем, что множество всех обратимых элементов кольца $\mathbb{Z}[i]$ состоит из чисел

$$1, -1, i, -i.$$

□

Определение 2.4. *Кольцо $\mathbb{U}$ называется эвклидовым,*[1] *если на нем задана норма $N : \mathbb{U} \to \mathbb{N}_0$ такая, что для любых двух элементов $a, b \in \mathbb{U}$, где $a \neq 0$, найдутся элементы $q, r \in \mathbb{U}$ удовлетворяющие условию*

$$b = qa + r, \quad \text{где} \quad N(r) < N(a) \quad \text{или} \quad r = 0. \tag{2.2}$$

Мы будем называть операцию вычисления пары q, r, удовлетворяющей (2.2), операцией деления с остатком, величину r – остатком от деления, или просто, остатком, а величину q – частным.

Стоит отметить, что из данного нами определения следует, что отличный от нуля элемент a эвклидового кольца $\mathbb{U}$, удовлетворяющий условию $N(a) = 0$, должен делить любой элемент b этого кольца.

Способ определения нормы существенно влияет на определение операции деления с остатком. Проиллюстрируем это на примере введенных ранее колец.

2.1.1 Кольцо целых чисел

Теорема 2.1. *Кольцо целых чисел $\mathbb{Z}$ является эвклидовым кольцом, то есть для любой пары целых чисел a, b таких, что $a \neq 0$, найдутся целые q, r такие, что*

$$b = qa + r, \quad |a| > r \geqslant 0$$

и такая пара чисел q, r — единственна.

[1] Эвклид или Евклид (ок. 325 г. до н.э. - до 265 г.до н.э.) — древнегреческий математик, автор первого из дошедших до нас теоретических трактатов по математике. Его главная работа «Начала» содержит в себе изложение планиметрии, стереометрии, а также начал теории чисел. Кроме того, Эвклид автор работ по оптике и астрономии.

Для доказательства теоремы 2.1 нам необходимо постулировать ряд аксиом, выполненных для кольца целых чисел.

Аксиома 1 (Архимеда)**.** *Для любых целых чисел a, b найдется такое целое число, что $ac > b$. Данную аксиому принято называть аксиомой Архимеда.*

Аксиома 2. *Пусть $M \subset \mathbb{Z}$ конечное, непустое подмножество во множестве целых чисел, тогда M содержит минимальный и максимальный элементы, т.е. такие элементы a и b, что*

$$a \leqslant c \leqslant b, \quad \text{для всех} \quad c \in M.$$

Следует отметить, что указанные аксиомы тесно связаны с введенным нами ранее свойством упорядоченности множества целых чисел, см. определение 1.5. Приводимое далее доказательство теоремы 2.1 также использует свойства введенных на множестве целых чисел операций «больше», «меньше».

Доказательство теоремы 2.1. В начале предположим, что a, b неотрицательные целые числа и $a \neq 0$. Тогда, в силу аксиомы Архимеда найдется такое целое число c, что $ac > b$.

Множество чисел, удовлетворяющих указанному неравенству, – конечно. Действительно из неравенства $ac > b \geqslant 0$ следует, что выполнено неравенство $c \geqslant 0$. Тогда, из второй аксиомы следует, что рассматриваемое множество содержит минимальный элемент и для этого элемента выполнены неравенства

$$ac > b \geqslant a(c-1). \tag{2.3}$$

Обозначим $q = c - 1$ и $r = b - a(c-1)$, тогда из (2.3) следует оценка (2.2), т.е. неравенство

$$a = ac - a(c-1) > b - a(c-1) = r \geqslant 0.$$

Докажем, что полученное представление единственно. Если это не так, то найдутся целые q_1, r_1 такие, что

$$aq + r = b = aq_1 + r_1, \quad a > r_1 \geqslant 0.$$

или

$$a(q - q_1) = r_1 - r.$$

Поскольку правая часть равенства удовлетворяет неравенствам $a > |r_1 - r| \geqslant 0$, а левая всегда кратна a, то равенство возможно только

в случае, когда $r_1 - r = 0$, следовательно, $r_1 = r$, $q_1 = q$ и для случая $b > a > 0$ теорема доказана.

Пусть теперь выполнено равенство для абсолютных значений $|b| = q|a| + r$. Тогда остальные возможные варианты описываются равенствами

$$\begin{aligned} |b| &= (-q)(-|a|) + r, \\ -|b| &= (-q-1)|a| + (|a| - r), \\ -|b| &= (q+1)(-|a|) + (|a| - r). \end{aligned}$$

□

Заметим, что в формулировке теоремы фигурирует условие $r \geqslant 0$, являющееся более жестким, чем условие $N(r) \geqslant 0$. Именно это условие определяет единственность остатка от деления.

Способ определения остатка от деления, приведенный в ходе доказательства теоремы, не является единственным, который удовлетворяет определению 2.4. Пусть $b > a > 0$ и выполнено равенство (2.2) с условием $r > 0$, тогда

$$b = (q+1)a + (r-a) = q_1 a + r_1, \quad 0 < |r_1| = N(r_1) < N(a) = a.$$

Если $r > \frac{a}{2}$, то $-\frac{a}{2} < r_1 < 0$, если же $r \leqslant \frac{a}{2}$, то $r_1 \leqslant -\frac{a}{2} < 0$. Таким образом, если $r \neq 0$, то всегда найдутся два остатка r и r_1 – один положительный, другой отрицательный, удовлетворяющих определению 2.4.

Пример 2.3. Для целых чисел 23 и 6 выполнены равенства

$$23 = 3 \cdot 6 + 5, \quad \text{и} \quad 6 > 5 > 0, \quad \text{или} \quad 23 = 4 \cdot 6 - 1, \quad \text{и} \quad 6 \geqslant |-1| > 0,$$

которые иллюстрируют оба способа определения операции деления с остатком, для которых выполнено $|a| > |r| \geqslant 0$. Такая двойственность, очевидно, выполнена в силу того, что функция нормы допускает возникновение коллизии, т.е. выполнимость равенства $N(r) = N(-r)$ для любого целого r.

2.1.2 Кольцо многочленов

Пусть $\mathbb{F}$ – произвольное поле, например, поле рациональных чисел $\mathbb{Q}$. Рассмотрим кольцо многочленов $\mathbb{F}[x]$ и произвольный, отличный от нуля элемент $a \in \mathbb{F}$. Тогда, $a \in \mathbb{F}[x]$, $\deg a = 0$ и, кроме того, найдется элемент $a^{-1} \in \mathbb{F}$ такой, что для любого многочлена $b(x) = \sum_{k=0}^{m} b_k x^k$ выполнено равенство

$$b(x) = \sum_{k=0}^{m} b_k \cdot a a^{-1} x^k = a \left(\sum_{k=0}^{m} b_k a^{-1} x^k \right) = aq(x). \tag{2.4}$$

Поскольку $N(a) = \deg a = 0$, то любой элемент кольца $\mathbb{F}[x]$ может быть разделен нацело на отличный от нуля элемент a кольца $\mathbb{F}[x]$ с условием $N(a) = 0$. Для многочленов степени большей нуля может быть определена операция деления с остатком.

Теорема 2.2. *Пусть $\mathbb{F}$ – поле, тогда кольцо многочленов $\mathbb{F}[x]$ является эвклидовым кольцом, то есть для любой пары многочленов $a(x), b(x) \in \mathbb{F}[x]$ таких, что $a(x) \neq 0$, найдутся такие многочлены $q(x), r(x)$, что выполнено равенство*

$$b(x) = q(x)a(x) + r(x), \quad \deg a(x) > \deg r(x) \geqslant 0 \tag{2.5}$$

и пара многочленов $q(x), r(x) \in \mathbb{F}[x]$ — единственна.

Доказательство. Пусть $a(x) = \sum_{k=0}^{n} a_k x^k$, $b(x) = \sum_{k=0}^{m} b_k x^k$ два многочлена из кольца $\mathbb{F}[x]$ и $a_n \neq 0$.

Если $N(a(x)) = 0$, то многочлен $a(x)$ является элементом поля $\mathbb{F}$. Тогда искомое равенство выполнено для многочленов $r(x) = 0$ и $q(x)$, определяемого соотношением (2.4). Далее будем считать, что $N(a(x)) > 0$.

Если $b(x) = 0$, то легко заметить, что многочлены $q(x) = r(x) = 0$ удовлетворяют утверждению теоремы. Далее будем считать, что $b_m \neq 0$.

Если $\deg b(x) < \deg a(x)$, то многочлены $q(x) = 0$, $r(x) = b(x)$ удовлетворяют утверждению теоремы. Далее будем считать, что $\deg b(x) \geqslant \deg a(x)$ или, что равносильно, $m \geqslant n$.

Поскольку $a_n \in \mathbb{F}$ отлично от нуля, а $\mathbb{F}$ – поле, то найдется $a_n^{-1} \in \mathbb{F}$ такой, что $a_n a_n^{-1} = 1$. Тогда определим многочлены

$$q_1(x) = b_m a_n^{-1} x^{m-n}$$

и

$$r_1(x) = b(x) - q_1(x)a(x) = \sum_{k=0}^{m} b_k x^k - b_m a_n^{-1} x^{m-n} \left(\sum_{k=0}^{n} a_k x^k \right) =$$

$$= b_m x^m + \sum_{k=0}^{m-1} b_k x^k - b_m a_n^{-1} x^{m-n} a_n x^n - b_m a_n^{-1} x^{m-n} \left(\sum_{k=0}^{n-1} a_k x^k \right) = \sum_{k=0}^{m-1} r_{1,k} x^k,$$

где $\deg r_1(x) < \deg b(x)$. Если $\deg r_1(x) < \deg a(x)$, то мы получили искомое представление. В противном случае для $i = 2, 3, \ldots$, определим

$$q_i(x) = r_{i-1,s} a_n^{-1} x^{s-n},$$

где $s = \deg r_{i-1}(x)$ и

$$r_i(x) = r_{i-1}(x) - q_i(x)a(x), \quad \deg r_i(x) < \deg r_{i-1}(x).$$

Поскольку с каждым шагом степень многочлена $r_i(x)$ уменьшается, то найдется такой индекс i, что $\deg r_i(x) < \deg a(x)$. Тогда выполнено равенство

$$b(x) = a(x)\sum_{k=1}^{i} q_k(x) + r_i(x), \quad \deg r_i(x) < \deg a(x)$$

и условие (2.2). Покажем, что полученное равенство единственно.

Пусть найдется другая пара многочленов $s(x), t(x) \in \mathbb{F}[x]$ такая, что

$$b(x) = s(x)a(x) + t(x), \quad \deg t(x) < \deg(a),$$

тогда выполнено равенство для многочленов

$$a(x)(q(x) - s(x)) = t(x) - r(x).$$

Степень многочлена, стоящего в правой части равенства, удовлетворяет неравенству

$$\deg(t(x) - r(x)) \leqslant \max\{\deg t(x), \deg r(x)\} < \deg a(x).$$

С другой стороны, степень многочлена, стоящего в левой части, удовлетворяет неравенству

$$\deg(a(x)(q(x) - s(x))) \geqslant \deg a(x) + \deg(q(x) - s(x)) \geqslant \deg a(x).$$

Полученное противоречие разрешимо только в случае, когда выполнены равенства $s(x) = q(x)$ и $t(x) = r(x)$. Теорема доказана. □

Отметим, что принципиальным моментом приведенного доказательство является существование элемента $a_n^{-1} \in \mathbb{F}$. Поскольку $\mathbb{F}$ поле, то его группа обратимых элементов совпадает с множеством ненулевых элементов поля и определенная равенством (2.5) операция деления с остатком корректно определена.

Однако, если мы рассмотрим кольцо многочленов $\mathbb{U}[x]$, где $\mathbb{U}$ произвольное кольцо, а не поле, то операция деления с остатком может быть корректно определена только для $a(x) \in \mathbb{U}[x]$ такого, что $a_n \in \mathbb{U}^*$, т.е. принадлежит группе обратимых элементов кольца $\mathbb{U}$.

Пример 2.4. Пусть $a(x), b(x) \in \mathbb{Q}[x]$ – многочлены с рациональными коэффициентами и

$$b(x) = x^5 + x^3 + 11x^2 + 1 \quad \text{и} \quad a(x) = 2x^3 + x + 3.$$

Тогда выполнено равенство

$$\begin{aligned} x^5 + x^3 + 11x^2 + 1 = \\ = \frac{1}{2}x^2(2x^3 + x + 3) + \frac{1}{2}x^3 - \frac{3}{2}x^2 + 11x + 1 = \\ = \left(\frac{1}{2}x^2 + \frac{1}{4}\right)(2x^3 + x + 3) - \frac{3}{2}x^2 + \frac{43}{4}x + \frac{1}{4}, \end{aligned}$$

из которого определяется частное $q(x) = \frac{1}{4}(2x^2 + 1)$ и остаток $r(x) = \frac{1}{4}(-6x^2 + 43x + 1)$. Легко видеть, что если мы рассмотрим операцию деления с остатком многочленов $b(x), a(x)$ над кольцом $\mathbb{Z}[x]$, то данная операция не сможет быть корректно определена, поскольку величина $\frac{1}{4}$ не является целым числом.

2.1.3 Кольцо целых гауссовых чисел

Теорема 2.3. *Кольцо целых гауссовых чисел $\mathbb{Z}[i]$ является эвклидовым кольцом, т.е. для любых элементов $\alpha = a_0 + a_1 i$, $\beta = b_0 + b_1 i$ таких, что $N(\alpha) \neq 0$, найдутся элементы $\gamma = q_0 + q_1 i$ и $\rho = r_0 + r_1 i$ такие, что*

$$\beta = \gamma\alpha + \rho, \quad N(\alpha) > N(\rho) \geqslant 0.$$

Доказательство. В начале мы рассмотрим частный случай, когда $\alpha = a_0 \in \mathbb{Z}$. Разделим b_0, b_1 с остатком на a_0

$$b_0 = q_0 a_0 + r_0, \quad b_1 = q_1 a_0 + r_1 \tag{2.6}$$

и запишем равенство

$$(b_0 + b_1 i) = (q_0 a_0 + r_0) + (q_1 a_0 + r_1)i = (q_0 + q_1 i)a_0 + (r_0 + r_1 i) = \gamma\alpha + \rho, \tag{2.7}$$

которое и дает нам искомое соотношение. При этом остатки r_0, r_1 должны принадлежать интервалу $\left[-\frac{1}{2}a_0, \frac{1}{2}a_0\right]$. Тогда

$$N(\rho) = r_0^2 + r_1^2 \leqslant \frac{1}{4}a_0^2 + \frac{1}{4}a_0^2 < a_0^2 = N(\alpha)$$

и утверждение теоремы выполнено.

Отметим, что среди целых гауссовых чисел, соответствующих другим возможным значениям пар остатков r_0, r_1, могут найтись числа, норма которых также не превосходит величины $N(\alpha)$. □

Пример 2.5. Рассмотрим простой пример деления с остатком в кольце гауссовых чисел. Пусть $\beta = 2 + 7i$ и $\alpha = -3$, тогда воспользуемся равенствами (2.6) и запишем равенство

$$2 = -3 \cdot \underbrace{-1}_{q_0} + \underbrace{-1}_{r_0}, \quad 7 = -3 \cdot \underbrace{-2}_{q_1} + \underbrace{1}_{r_1},$$

в котором остатки от деления принадлежат заданному множеству значений $[-1, 0, 1]$. Легко видеть, что $(-1)^2 + 1^2 = 2 < 9 = N(-3)$ и мы можем записать искомое равенство

$$(2 + 7i) = (-3 \cdot -1 - 1) + (-3 \cdot -2 + 1)i = (-1 - 2i) \cdot -3 + (-1 + i).$$

Однако данное представление не единственно. Выполняя деление коэффициентов числа β на $\alpha = -3$, мы можем получить также равенства

$$\begin{array}{rclrcl} 2 &=& -3 \cdot 0 + 2, & 7 &=& -3 \cdot -2 + 1, \\ 2 &=& -3 \cdot -1 - 1, & 7 &=& -3 \cdot -3 - 2, \\ 2 &=& -3 \cdot 0 + 2, & 7 &=& -3 \cdot -3 - 2. \end{array}$$

Каждая из указанных пар равенств дает нам еще одно искомое соотношение

$$\begin{array}{rcll} 2 + 7i &=& -3 \cdot -2i + (2 + i), & N(2 + i) = 5 < N(-3), \\ 2 + 7i &=& -3 \cdot (-1 - 3i) + (-1 - 2i), & N(-1 - 2i) = 5 < N(-3), \\ 2 + 7i &=& -3 \cdot -3i + (2 - 2i), & N(2 - 2i) = 8 < N(-3). \end{array}$$

Итак, мы получили, что $2 + 7i$ при делении на -3 имеет следующие остатки

$$-1 + i, \quad 2 + i, \quad -1 - 2i, \quad 2 - 2i.$$

Окончание доказательства теоремы 2.3. Идея вывода соотношений, определяющих операцию деления с остатком в кольце целых гауссовых чисел, основывается на равенстве (2.7). Выходя за пределы кольца целых чисел, которому принадлежит величина $\alpha = a_0$, мы можем записать (2.7) в виде

$$\frac{\beta}{\alpha} = \frac{b_0}{a_0} + \frac{b_1}{a_0} i = (q_0 + q_1 i) + \frac{1}{a_0}(r_0 + r_1 i) = \gamma + \frac{\rho}{\alpha},$$

который позволяет определить величины γ и ρ.

Теперь рассмотрим $\alpha = a_0 + a_1 i$ в общем виде и снова запишем отношение

$$\frac{\beta}{\alpha} = \frac{b_0 + b_1 i}{a_0 + a_1 i} = \frac{(b_0 + b_1 i)(a_0 - a_1 i)}{(a_0 + a_1 i)(a_0 - a_1 i)} = \frac{(a_0 b_0 + a_1 b_1) + (a_0 b_1 - a_1 b_0)i}{N(\alpha)} = \gamma + \frac{\rho}{\alpha},$$

из которого можно определить величины γ и ρ.

Дадим формальное определение. Используя операцию деления с остатком для целых чисел, запишем

$$\begin{array}{rcl} a_0 b_0 + a_1 b_1 &=& q_0 N(\alpha) + l_0, \\ a_0 b_1 - a_1 b_0 &=& q_1 N(\alpha) + l_1, \end{array} \tag{2.8}$$

где

$$-\frac{1}{2}N(\alpha) < l_0 \leqslant \frac{1}{2}N(\alpha), \quad -\frac{1}{2}N(\alpha) < l_1 \leqslant \frac{1}{2}N(\alpha),$$

и определим

$$\begin{aligned} r_0 &= b_0 - a_0q_0 + a_1q_1, \\ r_1 &= b_1 - a_0q_1 - a_1q_0. \end{aligned} \tag{2.9}$$

Теперь надо проверить, что величины $\gamma = q_0 + q_1 i$ и $\rho = r_0 + r_1 i$ удовлетворяют утверждению теоремы. Легко видеть, что

$$\begin{aligned} \gamma\alpha + \rho = (q_0 + q_1 i)(a_0 + a_1 i) + (r_0 + r_1 i) = \\ = (a_0q_0 - a_1q_1) + (a_0q_1 + a_1q_0)i + (b_0 - a_0q_0 + a_1q_1) + (b_1 - a_0q_1 - a_1q_0)i = \\ = b_0 + b_1 i = \beta. \end{aligned}$$

Покажем, что $N(\alpha) > N(\rho)$. Из условия $N(\alpha) = a_0^2 + a_1^2$ и (2.8), (2.9) следуют равенства

$$\begin{aligned} r_0a_0 + r_1a_1 = a_0b_0 - a_0^2q_0 + a_0a_1q_1 + a_1b_1 - a_0a_1q_1 - a_1^2q_0 = \\ = a_0b_0 + a_1b_1 - q_0(a_0^2 + a_1^2) = l_0, \end{aligned}$$

и

$$\begin{aligned} r_0a_1 - r_1a_0 = b_0a_1 - a_0a_1q_0 + a_1^2q_1 - b_1a_0 + a_0^2q_1 + a_0a_1q_0 = \\ = a_1b_0 - a_0b_1 - q_1(a_0^2 + q_1^2) = l_1. \end{aligned}$$

Определим $\lambda = l_0 + l_1 i$, тогда

$$N(\lambda) = l_0^2 + l_1^2 = (r_0a_0 + r_1a_1)^2 + (r_0a_1 - r_1a_0)^2 = (a_0^2 + a_1^2)(r_0^2 + r_1^2) = N(\alpha)N(\rho).$$

В силу построения мы получаем

$$N(\alpha)N(\rho) = N(\lambda) = l_0^2 + l_1^2 \leqslant \left(\frac{N(\alpha)}{2}\right)^2 + \left(\frac{N(\alpha)}{2}\right)^2 = \frac{N(\alpha)^2}{2}$$

и $N(\rho) < N(\alpha)$. Теорема доказана. □

Заметим, что для доказательства теоремы достаточно выполнимости условия

$$N(\lambda) = l_0^2 + l_1^2 < N(\alpha)^2.$$

Выбранные нами в ходе доказательства теоремы ограничения на величины l_0, l_1 позволяют гарантировать выполнение неравенства $0 \leqslant N(\rho) < N(\alpha)$. Однако единственность величин γ и ρ, определяемых равенствами (2.8),(2.9), не обеспечивается.

Пример 2.6. Пусть $\beta = 7 + 2i$ и $\alpha = 3 - i$, тогда

$$\begin{aligned} a_0 &= 3, \quad a_1 = -1, \\ b_0 &= 7, \quad b_1 = 2 \end{aligned}$$

и

$$N(\alpha) = a_0^2 + a_1^2 = 10.$$

Равенства (2.8) могут быть записаны в виде

$$\begin{aligned} 3 \cdot 7 + (-1) \cdot 2 &= 19 = 1 \cdot 10 + 9 = 2 \cdot 10 - 1, \\ 3 \cdot 2 - (-1) \cdot 7 &= 13 = 1 \cdot 10 + 3 = 2 \cdot 10 - 7, \end{aligned}$$

что дает нам четыре пары значений l_0, l_1

$$(9, 3), \quad (9, -7), \quad (-1, 3), \quad (-1, -7).$$

Легко видеть, что только три из приведенных пар удовлетворяют необходимому неравенству $N(\lambda) < N(\alpha)^2$

$$\begin{aligned} 9^2 + 3^2 &= 90 < 100, \\ (-1)^2 + 3^2 &= 10 < 100, \\ (-1)^2 + (-7)^2 &= 50 < 50. \end{aligned}$$

Каждая из таких пар дает нам равенство $\beta = \gamma\alpha + \rho$ с условием $N(\rho) < N(\alpha)$. Действительно, выполнены равенства

$$\begin{aligned} 7 + 2i &= (3 - i)(1 + i) + 3, \quad \text{и} \quad N(3) = 9 < 10, \\ 7 + 2i &= (3 - i)(2 + i) + i, \quad \text{и} \quad N(i) = 1 < 10, \\ 7 + 2i &= (3 - i)(2 + 2i) + (-1 - 2i), \quad \text{и} \quad N(-1 - 2i) = 5 < 10. \end{aligned}$$

Также можно заметить, что разности между остатками от деления кратны величине α

$$i - 3 = -1(3 - i), \quad i - (-1 - 2i) = i(3 - i), \quad 3 - (-1 - 2i) = (1 + i)(3 - i).$$

2.2 Наибольший общий делитель

Пусть ε – обратимый элемент кольца $\mathbb{U}$, а a, b два произвольных элемента кольца $\mathbb{U}$ такие, что $b = \varepsilon a$ тогда, в силу определения операции деления, $a|b$. С другой стороны, $b\varepsilon^{-1} = \varepsilon a \varepsilon^{-1} = a$, и мы получаем, что $b|a$.

Определение 2.5. *Мы будем называть два элемента $a, b \in \mathbb{U}$ ассоциированными, если $a|b$ и $b|a$. Ассоциированные элементы обозначаются символом $a \sim b$.*

Из данного определения сразу следует, что

$$a \sim a\varepsilon, \quad \text{для любого} \quad \varepsilon \in \mathbb{U}^*.$$

Пример 2.7. В кольце целых чисел с каждым числом ассоциировано только одно значение, например, ассоциированными являются числа 3 и -3.
В кольце многочленов $\mathbb{Q}[x]$ с каждым многочленом $a(x)$ ассоциировано множество многочленов, удовлетворяющее условию

$$\{c \cdot a(x),\ c \in \mathbb{Q},\ c \neq 0\}.$$

Данное множество, очевидно, бесконечно. В то же время в кольце $\mathbb{Z}[x]$ с каждым многочленом $a(x)$ ассоциирован только один многочлен $-a(x)$.
В кольце целых гауссовых чисел с каждым числом ассоциировано три числа, например,

$$2+i \sim -2-i, \quad 2+i \sim -1+2i, \quad 2+i \sim 1-2i.$$

Лемма 2.5. *Понятие ассоциированности задает отношение эквивалентности на множестве ненулевых элементов кольца* $\mathbb{U}$.

Доказательство. Для доказательства леммы необходимо проверить выполнимость трех свойств, введенных ранее в определении 1.20.

1. Рефлексивность $a \sim a$ следует из второго утверждения леммы 1.1, поскольку $a|a$ для любого $a \neq 0$.

2. Симметричность выполняется по определению понятия ассоциированности.

3. Пусть $a \sim b$ и $b \sim c$, тогда для доказательства транзитивности, необходимо показать, что $a \sim c$. Это свойство очевидным образом следует из пятого утверждения леммы 1.1. Если $a|b$ и $b|c$, то $a|c$. Аналогично, если $c|b$ и $b|a$, то $c|a$, т.е. $a \sim c$. □

Определение 2.6. *Пусть* a, b *элементы эвклидового кольца* $\mathbb{U}$. *Элемент* $d \in \mathbb{U}$, $d \neq 0$, *называется наибольшим общим делителем, если*

1. $d|a$ *и* $d|b$,
2. *для любого общего делителя* $\delta \neq 0$ *такого, что* $\delta|a$ *и* $\delta|b$ *выполнено* $\delta|d$.

Далее мы будем обозначать наибольший общий делитель символом $\mathbf{НОД}(a,\ b)$.

Из данного определения, а также из определения нормы, см. определение 2.2, следует, что для любого общего делителя δ такого, что $\delta|\,\mathbf{НОД}(a,\ b)$ выполнено

$$N(\delta) \leqslant N\left(\mathbf{НОД}(a,\ b)\right),$$

т.е. наибольший общий делитель обладает максимальной нормой из всех общих делителей элементов a, b.

Покажем, что определение 2.6 позволяет определить наибольший общий делитель с точностью до ассоциированных значений.

Теорема 2.4. *Пусть* $\mathbb{U}$ *эвклидово кольцо и* $a, b \in \mathbb{U}$*, одновременно не равные нулю. Тогда наибольший общий делитель* $\mathbf{НОД}(a,\ b)$ *существует и, с точностью до ассоциированных значений, единственен.*

Доказательство. Рассмотрим множество

$$\mathcal{D} = \{au + bv,\ u, v \in \mathbb{U}\},$$

образованное всеми возможными линейными комбинациями элементов a, b с коэффициентами $u, v \in \mathbb{U}$. Выберем в этом множестве отличный от нуля элемент d такой, что его норма $N(d)$ минимальна (поскольку хотя бы один из элементов a, b отличен от нуля, то найдется хотя бы один отличный от нуля элемент d; поскольку множество $\mathbb{N}_0$, которому принадлежат значения нормы, ограничено снизу, то среди всех ненулевых элементов d найдется элемент с минимальной нормой).

Предположим, что d не делит a. Тогда найдутся такие $q, r \in \mathbb{U}$, что

$$a = dq + r, \quad N(r) < N(d), \quad r \neq 0.$$

Тогда r удовлетворяет равенству

$$r = a - dq = a - (au + bv)q = a(1 - u) + bvq$$

и, следовательно, принадлежит множеству $\mathcal{D}$. Однако, это противоречит тому, что d имеет наименьшую норму среди элементов множества $\mathcal{D}$. Таким образом, предположение не верно, $r = 0$ и $d|a$. Аналогичными рассуждениями получаем, что $d|b$, следовательно, d – общий делитель.

Пусть теперь δ другой общий делитель a и b. Обозначим $a = c\delta$, $b = s\delta$, тогда из равенства

$$d = au + bv = c\delta u + s\delta v = \delta(cu + sv)$$

следует, что δ делит d.

Теперь покажем, что выбранный таким образом элемент d единственен. Пусть найдется d_2 – второй, отличный от d, наибольший общий делитель элементов a и b.

Поскольку d_2 общий делитель, а d – наибольший общий делитель, то $d_2|d$. Аналогично, поскольку d общий делитель, а d_2 – наибольший общий делитель, то $d|d_2$, и мы получили, что $d \sim d_2$. □

Из доказательства теоремы вытекает следующее следствие.

Следствие 2.4.A (соотношение Безу[2]). *Пусть a, b элементы эвклидового кольца $\mathbb{U}$. Тогда найдутся элементы $u, v \in \mathbb{U}$ такие, что*

$$au + bv \sim \mathbf{НОД}(a,\ b)\,.$$

Для определения наибольшего общего делителя как единственного элемента эвклидового кольца необходимо ввести дополнительное ограничение и указать способ выбора одного значения $\mathbf{НОД}(a,\ b)$ из множества ассоциированных элементов.

- В кольце целых чисел $\mathbb{Z}$ мы накладываем условие $\mathbf{НОД}(a,\ b) > 0$.
- В кольце многочленов от одной переменной $\mathbb{Q}[x]$ мы накладываем условие унитарности многочлена $d(x) = \mathbf{НОД}(a(x),\ b(x))$, то есть $d(x) = x^n + d_{n-1}x^{n-1} + \cdots d_0 \in \mathbb{Q}[x]$.
- В кольце целых гауссовых чисел из четырех ассоциированных друг с другом чисел

  $$a + bi, \quad -a - bi, \quad -b + ai, \quad b - ai$$

  всегда можно выбрать такой, что $0 < a \leqslant |b|$.

Пример 2.8. Приведем несколько простых примеров.

1. Рассмотрим целые числа 30 и 42. Перебирая все возможные делители числа 30 легко обнаружить, что общими делителями являются

   $$\pm 1, \pm 2, \pm 3 \quad \text{и} \quad \pm\, 6.$$

   Поскольку $N(\pm 1) < N(\pm 2) < N(\pm 3) < N(\pm 6)$ мы заключаем, что именно 6, поскольку $6 > 0$, является наибольшим общим делителем, т.е.

   $$\mathbf{НОД}(30,\ 42) = 6.$$

   Более того, мы можем записать соотношение Безу

   $$3 \cdot 30 + (-2) \cdot 42 = 6 = \mathbf{НОД}(30,\ 42)\,.$$

2. Рассмотрим целые гауссовы числа $2i$ и $1 - 3i$. Замечая, что

   $$\begin{array}{lcll} (1+i)^2 & = & 1 + 2i - 1 & = \quad 2i, \\ (1+i)(1+2i) & = & 1 + i + 2i + 2i^2 & = \quad -1(1-3i), \end{array}$$

[2]Этьен Безу (1730 – 1783) – французский математик, член Французской академии наук, основные труды относятся к алгебре. Автор шеститомного «Курса математики» (1764—1769). Безу обобщил рассматриваемое соотношение на случай кольца многочленов от одной переменной. Доказательство соотношения для кольца целых чисел принадлежит французу Клоду Гаспару Башэ (1581 – 1638).

получим, что общими делителями являются ± 1, $\pm i$ (как обратимые элементы кольца целых гауссовых чисел) и нетривиальные $\pm(1+i)$, $\pm(-1+i)$. Поскольку нормы найденных делителей удовлетворяют неравенству

$$N(\pm(-1+i)) = N(\pm(1+i)) = 2 > 1 = N(\pm 1) = N(\pm i),$$

то

$$\mathbf{НОД}\,(2i,\ 1-3i) = 1+i.$$

Поиск всех возможных общих делителей двух элементов a, b и выбор из найденного множества элемента с максимальной нормой может быть весьма трудоемким. Кроме того, знание общих делителей не позволяет составить соотношение Безу.

Для того, чтобы описать эффективный алгоритм вычисления наибольшего общего делителя, нам потребуется доказать ряд вспомогательных утверждений.

Определение 2.7. *Мы будем называть два элемента a, b эвклидова кольца $\mathbb{U}$ взаимно простыми, если* $\mathbf{НОД}\,(a,\ b) \in \mathbb{U}^*$ *или, что равносильно,* $\mathbf{НОД}\,(a,\ b) \sim 1$.

Лемма 2.6. *Пусть a, b взаимно простые элементы эвклидового кольца $\mathbb{U}$ такие, что выполнено равенство $au = bv$. Тогда, $a|v$ и $b|u$.*

Доказательство. Поскольку $\mathbf{НОД}\,(a,\ b) \sim 1$ то, согласно соотношению Безу, найдутся элементы $s, t \in \mathbb{U}$ такие, что $as + bt = \varepsilon$ для некоторого $\varepsilon \in \mathbb{U}^*$. Тогда из равенства $au = bv$ следует

$$aut = bvt = v(\varepsilon - as)$$

или

$$a(ut + as)\varepsilon^{-1} = v,$$

следовательно, в силу определения операции деления, $a|v$.

Аналогично, подставляя в равенство $aus = bvs$ выражение $as = \varepsilon - bt$, получим

$$u(\varepsilon - bt) = bvs$$

или

$$u = b(vs + tu)\varepsilon^{-1}.$$

Тогда, в силу определения операции деления, $b|v$ и лемма доказана. □

Далее нам понадобится следующая техническая лемма, описывающая свойства ассоциированных элементов.

Лемма 2.7. *Верны следующие утверждения.*

1. *Пусть $\mathbb{U}$ эвклидово кольцо и элементы $a, b \in \mathbb{U}$. Тогда $a \sim b$ тогда и только тогда, когда $N(a) = N(b)$ и $a|b$.*

2. *Утверждение леммы 2.2 обратимо, т.е если норма в кольце $\mathbb{U}$ мультипликативна (соответственно, аддитивна), то из равенства $N(\varepsilon) = 1$ (соответственно, $N(\varepsilon) = 0$) следует, что элемент ε обратим.*

Доказательство. Пусть элементы a, b ассоциированы. Тогда, в силу определения ассоциированности элементов и понятия нормы, получаем

$$a|b, \quad \text{и} \quad N(a) \leqslant N(b), \quad \text{а также} \quad b|a, \quad \text{и} \quad N(b) \leqslant N(a),$$

следовательно, $N(b) \leqslant N(a) \leqslant N(b)$ и мы заключаем, что $N(a) = N(b)$.

Для доказательства утверждения в обратную сторону достаточно показать, что $b|a$. Предположим, что это не так, тогда найдутся такие q, r, что

$$a = qb + r, \quad N(r) < N(b) \quad \text{и} \quad r \neq 0.$$

Поскольку, по условию леммы, $N(a) = N(b)$, то выполнено $N(r) < N(a)$.

С другой стороны, поскольку $a|b$ можно записать равенства $b = ac$, для некоторого $c \in \mathbb{U}$, и

$$r = a - bq = a - acq = a(1 - cq).$$

Из последнего равенства следует, что $a|r$ и, в силу определения нормы, $N(a) \leqslant N(r)$, т.е. выполнено противоречивое неравенство

$$N(a) \leqslant N(r) < N(a).$$

Полученное противоречие позволяет говорить о том, что $r = 0$ или, что равносильно, $b|a$. Первое утверждение леммы доказано.

Для доказательства второго утверждения предположим, что норма в кольце $\mathbb{U}$ мультипликативна и рассмотрим элемент $\varepsilon \in \mathbb{U}$ такой, что $N(\varepsilon) = 1$. Пусть a элемент с отличной от нуля нормой, тогда из условий

$$N(a\varepsilon) = N(a)N(\varepsilon) = N(a) \quad \text{и} \quad a|a\varepsilon \tag{2.10}$$

а также первого утверждения леммы следует, что $av \sim a$ и $av|a$. Тогда найдется элемент $\mu \in \mathbb{U}$ такой, что

$$a\varepsilon\mu = a \quad \text{или} \quad \varepsilon\mu = 1,$$

т.е. элемент ε обратим. В случае аддитивной нормы условия (2.10) заменяются условиями

$$N(a\varepsilon) = N(a) + N(\varepsilon) = N(a),\ N(\varepsilon) = 0 \quad \text{и} \quad a|a\varepsilon$$

Лемма доказана. □

Теперь докажем теорему, утверждения которой позволяют построить несколько различных алгоритмов вычисления наибольшего общего делителя.

Теорема 2.5 (о свойствах НОД)**.** *Пусть* $\mathbb{U}$ *эвклидово кольцо и* $a, b \in \mathbb{U}$*, тогда выполнены следующие утверждения.*

1. $\mathbf{НОД}(a,\ b) \sim \mathbf{НОД}(b,\ a)$.
2. *Если* $a \neq 0$*, то* $\mathbf{НОД}(a,\ 0) \sim a$.
3. *Если* $\varepsilon \in \mathbb{U}^*$ *обратимый элемент кольца, то* $\mathbf{НОД}(a,\ \varepsilon) \sim \varepsilon$.
4. $\mathbf{НОД}(ac,\ bc) \sim c\,\mathbf{НОД}(a,\ b)$ *для любого, отличного от нуля* $c \in \mathbb{U}$.
5. $\mathbf{НОД}(a,\ b) \sim \mathbf{НОД}(a,\ a \pm b)$.
6. *Пусть* $b = aq + r$*, где* $N(r) < N(a)$ *или* $r = 0$*, тогда* $\mathbf{НОД}(a,\ b) \sim \mathbf{НОД}(a,\ r)$.
7. *Пусть для некоторого элемента* $c \neq 0$ *и* $\varepsilon \in \mathbb{U}^*$ *выполнено* $\mathbf{НОД}(a,\ c) \sim \varepsilon$*, тогда* $\mathbf{НОД}(a,\ bc) \sim \mathbf{НОД}(a,\ b)$.
8. *Если* $\varepsilon \in \mathbb{U}^*$ *обратимый элемент кольца, то* $\mathbf{НОД}(a,\ b\varepsilon) \sim \mathbf{НОД}(a,\ b)$.

Доказательство. Первое утверждение теоремы следует из определения наибольшего общего делителя.

Для доказательства второго утверждения леммы заметим, что, согласно соотношению Безу, для некоторого отличного от нуля элемента $u \in \mathbb{U}$ выполнено равенство

$$\mathbf{НОД}(a,\ 0) = au.$$

Поскольку $a|au$, то $N(a) \leqslant N(au)$ для любого, отличного от нуля $u \in \mathbb{U}$. Таким образом, a имеет минимальную норму из элементов вида au и является наибольшим общим делителем элементов a и 0.

Для доказательства третьего утверждения достаточно заметить, что выполнено условие $\mathbf{НОД}(a,\ \varepsilon)\,|\varepsilon$, тогда учитывая, что ε делит любой элемент кольца $\mathbb{U}$ и, в том числе, элемент $\mathbf{НОД}(a,\ \varepsilon)$, получаем $\mathbf{НОД}(a,\ \varepsilon) \sim \varepsilon$.

Для доказательства четвертого утверждения обозначим

$$d = \mathbf{НОД}(a,\ b) \quad \text{и} \quad \delta = \mathbf{НОД}(ac,\ bc)\,.$$

Тогда $d|a$ и мы получаем, что $dc|ac$. Аналогично, $d|b$ и $dc|bc$, следовательно, $dc|\,\mathbf{НОД}\,(ac,\ bc) = \delta$ или $dcs = \delta$ для некоторого $s \in \mathbb{U}$. Если $N(s) = N(1)$, то s обратимый элемент кольца $\mathbb{U}$ и выполнено условие $dc \sim \delta$, из которого следует четвертое утверждение леммы.

Предположим, что $N(s) > 1$. Поскольку $\delta|ac$, то найдется такой элемент $t \in \mathbb{U}$, что

$$\delta t = ac,$$

тогда, записывая $a = dl$,

$$dcs \cdot t = dl \cdot c.$$

Сокращая на $c \neq 0$ и $d \neq 0$, получим $st = l$, откуда $a = dl = dst$ и $ds|a$. Аналогично получаем, что $ds|b$, следовательно $ds|d$ или

$$dsv = d$$

для некоторого v. Сокращая на d получаем $sv = 1$ и s – обратимый элемент.

Для доказательства пятого и шестого утверждений леммы обозначим

$$d = \mathbf{НОД}\,(a,\ b)\,, \quad s = \begin{cases} a \pm b, \\ b - aq, \end{cases} \text{ или, } \quad \delta = \mathbf{НОД}\,(a,\ s)\,.$$

Тогда $d|a$, $d|b$, следовательно, $d|s$ и тогда $d|\delta$. С другой стороны, $\delta|a$, $\delta|s$ следовательно

$$\delta|b = \pm(a - s), \quad \text{и} \quad \delta|b = aq + s,$$

и мы получаем, что $\delta|d$ и тогда $d \sim \delta$.

Для доказательства седьмого утверждения леммы обозначим $d = \mathbf{НОД}\,(a,\ b)$. Легко видеть, что $d|\,\mathbf{НОД}\,(a,\ bc)$.

Обозначим $\delta = \mathbf{НОД}\,(a,\ bc)$. Тогда $\delta|bc$ и найдется некоторый элемент $u \in \mathbb{U}$ такой, что $\delta u = bc$. Если $\mathbf{НОД}\,(\delta,\ c) \sim 1$, то воспользовавшись утверждением леммы 2.6 получаем, что $\delta|b$ и $\delta|d$, откуда сразу вытекает условие $\delta \sim d$.

Таким образом, для доказательства седьмого утверждения леммы осталось показать, что $\mathbf{НОД}\,(\delta,\ c) \sim 1$. Пусть это не так, тогда обозначим $\mathbf{НОД}\,(\delta,\ c) = l$ и $N(l) > 1$. Тогда $l|\delta|a$, откуда следует, что $l|\,\mathbf{НОД}\,(a,\ c) \sim 1$ и $l \sim 1$. Полученное условие, вместе со вторым утверждением леммы 2.7, опровергает предположение $N(l) > 1$ и завершает доказательство седьмого утверждения.

Поскольку восьмое утверждение является прямым следствием третьего и седьмого утверждений, то теорема доказана. □

2.3 Алгоритм Эвклида

Теперь мы должны ответить на вопрос: как найти наибольший общий делитель?

Если нам известны все общие делители элементов a и b, то вычисление наибольшего общего делителя не представляет труда: мы можем перебрать все делители и выбрать делитель с максимальной нормой. Однако на практике нам неизвестны все общие делители. Более того, как мы покажем далее, задача поиска всех делителей значительно сложнее, чем вычисление наибольшего общего делителя. Наиболее известный алгоритм нахождения наибольшего общего делителя называется алгоритмом Эвклида.

Пусть $\mathbb{U}$ эвклидово кольцо и $a, b \in \mathbb{U}$ – отличные от нуля элементы этого кольца. Используя операцию деления с остатком, см. равенство (2.2), определим $r_{-1} = b$, $r_0 = a$ и последовательность

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\dots \\ r_{k-1} &= r_k q_{k+1} + r_{k+1}, \\ &\dots \\ r_{n-1} &= r_n q_{n+1}, \quad r_{n+1} = 0, \quad n \in \mathbb{N}_0. \end{aligned} \tag{2.11}$$

Теорема 2.6. *Пусть a, b отличные от нуля элементы эвклидового кольца $\mathbb{U}$. Определим величины $r_{-1}, r_0, \dots, r_{n+1}, q_1, \dots, q_{n+1} \in \mathbb{U}$ равенствами (2.11). Тогда найдется такой индекс $n \in \mathbb{N}_0$, что $r_{n+1} = 0$ и*

$$r_n \sim \mathbf{НОД}(a,\ b).$$

Доказательство. В силу определения операции деления с остатком для всех $n = 0,\ 1,\ \dots$ выполнено равенство $N(r_{n+1}) < N(r_n)$ или $r_{n+1} = 0$. Тогда, последовательность величин $N(r_1), N(r_2), \dots$ является убывающей последовательностью целых чисел, ограниченных, в силу определения нормы, снизу нулем. Следовательно, найдется индекс, для которого будет выполнено условие $N(r_{n+1}) = 0$. Тогда, либо $r_{n+1} = 0$, либо r_{n+1} нацело делит r_n и уже элемент $r_{n+2} = 0$.

Теперь, из второго и шестого утверждения теоремы 2.5, получаем соотношения

$$\mathbf{НОД}(a,\ b) \sim \mathbf{НОД}(r_1,\ a) \sim \dots \sim \mathbf{НОД}(r_n,\ 0) \sim r_n,$$

если $r_{n+1} = 0$, или $\mathbf{НОД}(a,\ b) \sim \dots \sim \mathbf{НОД}(r_{n+1},\ 0) \sim r_{n+1}$, если $r_{n+2} = 0$. Теорема доказана. □

Пример 2.9. Приведем несколько примеров, иллюстрирующих доказанную теорему.

1. Для целых чисел -45 и 24 выполнены равенства

$$\begin{aligned} \underbrace{-45}_{r_{-1}} &= \underbrace{24}_{r_0}\cdot\underbrace{(-2)}_{q_1}+\underbrace{3}_{r_1}, \\ \underbrace{24}_{r_0} &= \underbrace{3}_{r_1}\cdot\underbrace{8}_{q_2}+\underbrace{0}_{r_2} \end{aligned}$$

   из которых следует, что $\mathbf{НОД}(-45,\ 24) \sim 3$.

2. Для многочленов $a(x) = 2x^2+3x+1$, $b(x) = x^3+3x^2+3x+1$, $a(x), b(x) \in \mathbb{Q}[x]$, выполнены равенства

$$\begin{aligned} x^3+3x^2+3x+1 &= (2x^2+3x+1)\cdot\left(\tfrac{1}{2}x+\tfrac{3}{4}\right)+\tfrac{1}{4}(x+1), \\ 2x^2+3x+1 &= \tfrac{1}{4}(x+1)\cdot 4(2x+1), \end{aligned}$$

   из которых следует, что

$$\mathbf{НОД}\left(x^3+3x^2+3x+1,\ 2x^2+3x+1\right) \sim \frac{1}{4}(x+1) \sim x+1.$$

3. Для гауссовых целых $b = 126-148i$, $a = 5+19i$ выполнены равенства

$$\begin{aligned} 126-148i &= -(6+8i)(5+19i) &+ (4+6i), \\ 5+19i &= (3+i)(4+6i) &+ (-1-3i), \\ 4+6i &= (-2+i)(-1-3i) &+ (-1+i), \\ -1-3i &= (-1+2i)(-1+i) &+ 0. \end{aligned}$$

   При этом, как легко проверить

$$386 = N(5+19i) > 52 = N(4+6i) > 10 = N(-1-3i) > 2 = N(-1+i).$$

   Мы получили, что $\mathbf{НОД}(126-148i,\ 5+19i) \sim (-1+i) \sim (1+i)$. Как легко проверить

$$\begin{aligned} 126-148i &= (1+i)(-11-137i), \\ 5+19i &= (1+i)(12+7i). \end{aligned}$$

Вычисление последовательности остатков $r_{-1}, r_0, \ \ldots, \ r_{n+1}$, определенных равенствами (2.11), называется алгоритмом Эвклида. Можно минимизировать количество используемых вспомогательных переменных и переписать алгоритм Эвклида в виде, который может быть легко запрограммирован, например, следующим образом.

Алгоритм 2.1 (Алгоритм Эвклида)

Вход: натуральные числа a и b.
Выход: $\mathbf{НОД}(a,\ b)$ – наибольший общий делитель чисел a и b.

```
1 def gcd_z( a, b ):
2         if a.is_integer() != True:
3                 print("Неверный тип первого аргумента");
4                 return 0;
```

```
5         if b.is_integer() != True:
6                 print("Неверный тип второго аргумента");
7                 return 0;
8         # приводим числа к их абсолютному значению
9         if a < 0: a = -a;
10        if b < 0: b = -b;
11        # при необходимости, меняем местами аргументы функции
12        if a > b:
13                r = b; b = a; a = r;
14        # запускаем основной цикл вычисления остатков от деления
15        while a > 0:
16                (q,r) = b.quo_rem(a);
17                b = a; a = r;
18        return b;
```

Алгоритм 2.1 реализован в рамках системы компьютерной алгебры Sage и может быть применен, как видно из строк 2 и 5, только для поиска наибольшего общего делителя в кольце целых чисел. Для других эвклидовых колец реализация алгоритма Эвклида аналогична.

2.4 Теорема Ламе

Представляет интерес вопрос о том, насколько быстро работает алгоритм 2.1 или, более формально, какое количество операций деления с остатком нужно выполнить для того, чтобы найти наибольший общий делитель. Следующая теорема позволяет оценить число шагов алгоритма Эвклида.

Теорема 2.7 (Ламе[3], 1844). *Пусть a, b целые числа и $b > a > 0$. Количество операций деления с остатком в алгоритме 2.1 может быть оценено сверху величиной $1 + c \log_2 b$, где c положительная, эффективно вычислимая константа.*

Для доказательства этой теоремы нам потребуется сделать небольшое отступление и доказать лемму о свойствах элементов последовательности Фибоначчи. В утверждении леммы и при ее доказательстве используется понятие поля «действительных» чисел, которое известно из школьной программы, однако, формально, будет определено только в XXX-й главе.

Определение 2.8. *Мы будем называть рекуррентную последовательность целых чисел*

$$\begin{aligned} &A_0 = 0, \quad A_1 = 1, \\ &A_{n+1} = A_n + A_{n-1}, \quad \textit{при} \quad n = 1,\ 2,\ \ldots \end{aligned} \tag{2.12}$$

[3]Габриель Ламе (Gabriel Lame) — французский математик, физик и инженер. В 1820—1832 гг. работал в Институте корпуса инженеров путей сообщения в Петербурге.

последовательностью Фибоначчи.[4]

Лемма 2.8. *Пусть* $z = \frac{1+\sqrt{5}}{2}$ *действительный, положительный корень уравнения* $z^2 = z + 1$. *Тогда для последовательности Фибоначчи при всех натуральных* n *выполнено неравенство*

$$A_{n+1} \geqslant z^{n-1}. \tag{2.13}$$

Доказательство леммы 2.8. При $n = 1$, очевидно, $A_2 = 1 > 0$ и утверждение леммы выполнено. Далее проведем доказательство по индукции. Пусть условие леммы выполнено для всех индексов, меньших либо равных n. Тогда, в силу выбора z, выполнено неравенство

$$A_{n+1} = A_n + A_{n-1} \geqslant z^{n-2} + z^{n-3} = z^{n-3}(z+1) = z^{n-1}.$$

□

Доказательство теоремы Ламе. Вначале мы докажем неравенство

$$r_{k-1} \geqslant A_{n+1-k}, \quad \text{при} \quad k = 0,\ 1,\ \ldots,\ n, \tag{2.14}$$

где последовательность $r_{-1},\ r_0,\ \ldots r_n$ определена равенством (2.11), а последовательность Фибоначчи $A_1,\ A_2,\ \ldots$ равенством (2.12).

При $k = n$ выполнено $r_{n-1} = r_n q_{n+1} \geqslant 1 = A_1$. Далее по индукции. Пусть для всех $n, n-1, \ldots, k$ неравенство (2.14) выполнено. Тогда

$$r_{k-1} = r_k q_{k+1} + r_{k+1} \geqslant r_k + r_{k+1} \geqslant A_{n-k} + A_{n-(k+1)} = A_{n+1-k}.$$

Из неравенства (2.14) и леммы 2.8 при $k = 0$ получаем

$$b = r_{-1} \geqslant A_{n+1} \geqslant z^{n-1} \quad \text{или} \quad n \leqslant 1 + \log_z b.$$

Учитывая значение $z = \dfrac{1+\sqrt{5}}{2}$, мы получаем неравенство

$$n \leqslant 1 + \frac{\log_2 b}{\log_2(1+\sqrt{5})},$$

которое завершает доказательство теоремы. □

Теорема Ламе является одной из первых теорем, утверждение которой позволяет получить оценку трудоемкости некоторого алгоритма. Получение оценок трудоемкости является важным с точки зрения защиты информации, поскольку позволяет сравнивать алгоритмы между собой и выбирать, в случае существования нескольких альтернативных путей решений, алгоритм, имеющий наименьшую трудоемкость.

[4]Леонардо Пизанский (ок. 1170 - ок. 1250) — один из известнейших математиков Средневековья, известен под псевдонимом Фибоначчи. Автор работ по теории диофантовых уравнений, т.е. уравнений, решения которых ищутся в целых числах.

Задачи и упражнения

1. Докажите, что в любом поле $\mathbb{F}$ группа обратимых элементов совпадает с мультипликативной группой поля.

2. Докажите, что обратимый элемент делит любой элемент кольца.

3. Найдите норму чисел -13, $2-7i$, а также произведений $3\cdot 7\cdot 19$, $2i(3+6i)$ и $(x^2+1)(x^7+13x+2)$.

4. Найдите остатки от деления:

   - целых чисел 11, -393, 571 на 5, 19 и -11,
   - многочленов с рациональными коэффициентами $x^5+\frac{x}{2}+1$, $2x^2-14x+3$ на x, $2x^2+\frac{1}{3}$, x^3+x+2,
   - целых гауссовых чисел $-7+6i$, $3+i$ на $2i$, $1+3i$, $5i-1$.

5. Может ли поле, например, рациональных чисел быть евклидовым кольцом? Ответ обоснуйте.

6. Пусть a произвольный элемент кольца $\mathbb{U}$. Докажите, что $a\sim a\varepsilon$ для любого обратимого элемента $\varepsilon\in\mathbb{U}^*$.

7. В кольце целых гауссовых чисел найдите все числа, ассоциированные с 11, $-4i$ и $3+9i$.

8. Докажите, что числа 3 и $2+i$ не являются ассоциированными в кольце гауссовых чисел.

9. Вычислите значения наибольшего общего делителя

   $$\textbf{НОД}\,(13,\ 39)\,,\quad \textbf{НОД}\,\left(32x^5-1,\ 4x^2-1\right)\quad\text{и}\quad \textbf{НОД}\,(15,\ 2+i)\,.$$

   Найдите все значения, ассоциированные с вычисленными.

10. Используя утверждения теоремы 2.5 предъявите «двоичный» алгоритм вычисления НОД, использующий в качестве операции деления только операцию деления на два.

11. Укажите, какие из чисел $\{i,\ 5,\ 1+2i,\ 1+7i,\ 12,\ 6+3i\}$ являются взаимно простыми в кольце целых гауссовых чисел.

12. Покажите, почему изложенное выше доказательство теоремы Ламе не может быть использовано для оценки трудоемкости алгоритма Эвклида в кольцах многочленов и целых гауссовых чисел. Указание: попробуйте использовать неравенство $N(a+b)\leqslant N(a)+N(b)$.

13. Получите оценку трудоемкости алгоритма Эвклида для колец многочленов и целых гауссовых чисел.

Рекомендации к сдаче экзамена

В экзаменационные билеты по курсу «Введение в теорию чисел» входят следующие вопросы.

- Группа обратимых элементов кольца. Понятие нормы и ее связь с обратимыми элементами.

  При изложении данного билета необходимо сформулировать и доказать леммы 2.1, 2.2, 2.3 и 2.4.

- Понятие эвклидового кольца. Теорема об эвклидовости кольца целых чисел (теорема 2.1).

  Доказательство теоремы 2.1 существенным образом использует свойство упорядоченности кольца целых чисел, а также связанные с этим свойством аксиомы – аксиому Архимеда и аксиому о существовании минимального элемента в конечном подмножестве кольца целых чисел.

  Подробное доказательство теоремы проводится для случая $b > a > 0$. В начале доказывается существование пары целых чисел q, r, удовлетворяющих условию теоремы, потом – единственность найденной пары. В заключение, рассматриваются случаи, когда числа a, b принимают отрицательные значения.

- Понятие кольца многочленов. Теорема об эвклидовости кольца многочленов от одной переменной (теорема 2.2).

  В начале доказательства теоремы рассматриваются частные случаи $b(x) = 0$, $\deg b(x) < \deg a(x)$ и $N(a(x)) = 0$. Для каждого из указанных случаев, в явном виде, предъявляется представление $b(x) = a(x)q(x) + r(x)$. После этого приводится алгоритм построения необходимого представления в общем случае. В заключение, методом «от противного» приводится доказательство единственности построенного представления.

- Понятие кольца целых гауссовых чисел. Теорема об эвклидовости кольца целых гауссовых чисел (теорема 2.3).

  Доказательство теоремы разделено на две части. В первой части рассматривается случай, в котором в качестве делителя α выступает целое число. Данный случай иллюстрирует идею вывода соотношений для частного и остатка от деления.

Во второй части доказательства рассматривается общий случай – в явном виде определяются коэффициенты частного γ и остатка от деления ρ, после чего проверяется, что норма полученного остатка удовлетворяет неравенству $N(\alpha) > N(\rho)$.

- Понятие наибольшего общего делителя и теорема о его существовании (теорема 2.4). Соотношение Безу.

  Доказательство теоремы состоит из двух частей – доказательство «существования» и «единственности». В начале, для доказательства «существования», предъявляется элемент вида $d = au + bv$ с минимальной нормой и показывается, что он является наибольшим общим делителем. Для доказательства «единственности» показывается, что любой наибольший делитель ассоциирован с предъявленным ранее делителем d.

- Теорема о свойствах наибольшего общего делителя (теорема 2.5) и алгоритм Эвклида (теорема 2.6).

  Теорема 2.5 носит технический характер и может быть использована для построения нескольких алгоритмов вычисления наибольшего общего делителя. Наиболее известным алгоритмом является алгоритм Эвклида. В ходе доказательства теоремы 2.6 необходимо проверить, что последний ненулевой остаток от деления является наибольшим общим делителем, а также доказать, что число шагов алгоритма конечно.

- Теорема Ламе (теорема 2.7).

  При доказательстве теоремы Ламэ необходимо начать с леммы, позволяющей получить экспоненциальное неравенство (2.13), которое связывает количество элементов последовательности Фибоначчи n, значение элемента этой последовательности A_{n+1} и z – корень многочлена второй степени $z^2 - z - 1$.

  При доказательстве теоремы, максимальное из чисел для которых вычисляется наибольший общий делитель, т.е. b, оценивается элементом последовательности Фибоначчи A_{n+1}, индекс которого определяет количество шагов алгоритма Эвклида. Далее, оценивая элемент A_{n+1} степенью корня многочлена, выводится неравенство $b \geqslant z^{n-1}$ из которого следует оценка величины n.

Схема зависимостей между утверждениями, доказанными во 2-й главе, изображена на рисунке 2.1.

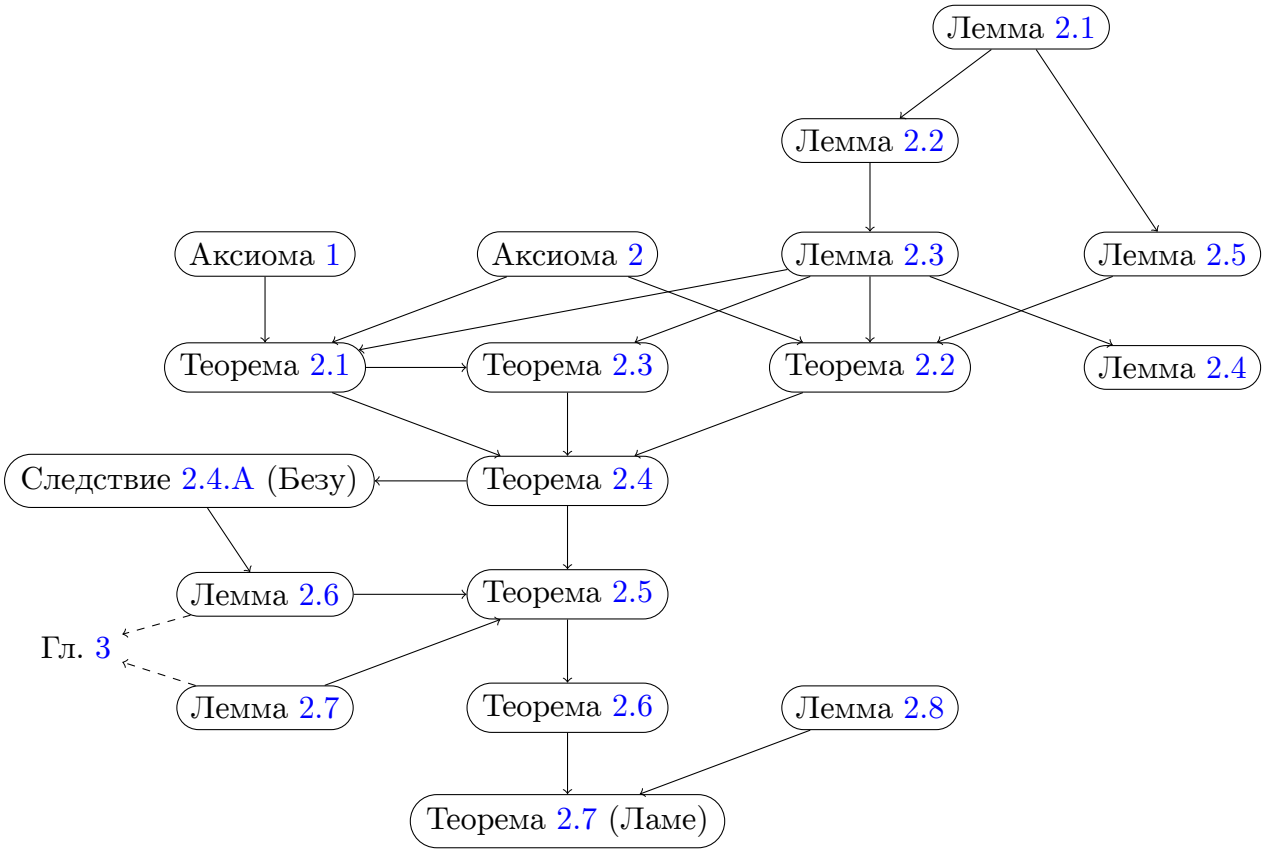


Рис. 2.1: Схема зависимостей между утверждениями 2-й главы.

Дополнительная литература к 2-й главе

1. Бухштаб А.А. Теория чисел. – М.:Просвещение. – 1966. — 384 с.
2. Зарисский О., Самуэль П. Коммутативная алгебра. Том 1. – М.:Изд-во иностранной литературы, 1963. — 374 с.
3. Воробьев Н.Н. Числа Фибоначчи. – М.:Наука. – 1978.

глава 3

Основная теорема арифметики

Несобственные делители и неразложимые элементы - Теорема о существовании неразложимых элементов - Теорема Эвклида о бесконечности множества неразложимых элементов - Основная теорема арифметики - Решето Эратосфена и построение таблиц неразложимых элементов.

В этой главе мы будем считать, что $\mathbb{U}$ – евклидово кольцо, содержащее в себе хотя бы один необратимый элемент, в частности, это означает, что $\mathbb{U}$ не является полем.

3.1 Несобственные делители

Для любого элемента $a \in \mathbb{U}$ и для любого обратимого элемента ε выполнено равенство

$$a = a \cdot \varepsilon \cdot \varepsilon^{-1}, \quad \varepsilon \in \mathbb{U}^*,$$

из которого следует, что $\varepsilon | a$ или, другими словами, любой элемент кольца можно разделить на любой обратимый элемент того же кольца.

Определение 3.1. *Множество делителей элемента $a \in \mathbb{U}$*

$$\{\varepsilon,\ a\varepsilon : \quad \varepsilon \in \mathbb{U}^*\},$$

определенное для всех возможных обратимых элементов кольца $\mathbb{U}$, называется множеством несобственных делителей элемента a, а сами делители из указанного множества – несобственными делителями.

Делители элемента a, отличные от указанных, называются собственными делителями элемента a.

Пример 3.1.

1. Поскольку в кольце целых чисел $\mathbb{Z}$ обратимыми элементами являются $\{1, -1\}$, то для любого отличного от нуля элемента n его несобственными делителями являются $1, -1, n, -n$. В частности, несобственными делителями числа 6 являются числа $-1, 1, 6, -6$, а числа $2, 3, -2, -3$ являются собственными делителями.

2. В кольце многочленов $\mathbb{Q}[x]$ от одной переменной x все элементы поля $\mathbb{Q}$ являются обратимыми элементами, следовательно, для любого многочлена $f(x)$ его несобственными делителями являются многочлены вида

$$\{\varepsilon,\ \varepsilon f(x) : \text{ для всех } \varepsilon \in \mathbb{Q}\},$$

например, несобственными делителями многочлена $x+1$ являются многочлены 3, $\frac{1}{2}$, $5x+5$, $\frac{1}{2}x+\frac{1}{2}$ и т.п.

3. Поскольку в кольце целых гауссовых чисел обратимыми элементами являются $\{1,-1,i,-i\}$, то для любого $a+bi \in \mathbb{Z}[i]$ его несобственными делителями являются
$$\{1,-1,i,-i,a+bi,-a-bi,-b+ai,b-ai\}$$

Определение 3.2. *Если необратимый элемент $a \in \mathbb{U}$ обладает только несобственными делителями, то такой элемент будем называть неразложимым.*

В кольце целых чисел положительные неразложимые элементы принято называть простыми числами.

Используя знания, полученные в ходе изучения школьной программы, легко выписать несколько неразложимых элементов кольца целых чисел

$$\ldots,\ -13,\ -11,\ -7,\ -5,\ ,-3,\ ,-2,\ \underbrace{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ \ldots}_{\text{простые числа}}$$

среди которых положительные элементы – простые числа. Однако нам необходимо формально доказать существование неразложимых элементов для произвольного евклидового кольца $\mathbb{U}$, включая кольцо целых чисел, а также предложить алгоритм поиска неразложимых элементов.

Определение 3.3. *Если необратимый элемент $a \in \mathbb{U}$ обладает собственным делителем $v \in \mathbb{U}$, то такой элемент принято называть разложимым или составным элементом.*

Лемма 3.1. *Пусть $a \in \mathbb{U}$ отличный от нуля, разложимый элемент и $a = uv$, где v – собственный делитель элемента a. Тогда выполнены следующие утверждения.*

1. *Элемент $u \in \mathbb{U}$ также является собственным делителем элемента a.*

2. *Выполнено строгое неравенство $N(v) < N(a)$.*

Доказательство. Рассмотрим элемент $a = uv$ и предположим, что элемент u является несобственным делителем элемента a. Тогда, в силу определения несобственного делителя, либо $u \in \mathbb{U}^*$ — обратимый элемент кольца, либо $u = \varepsilon a$, где ε обратимый элемент кольца.

Если u обратим, то найдется $u^{-1} \in \mathbb{U}^*$ такой, что $uu^{-1} = 1$. Тогда

$$au^{-1} = uvu^{-1} \quad \text{или} \quad v = au^{-1}.$$

Последнее равенство противоречит тому, что v несобственный делитель элемента a. Если же делитель u имеет вид $u = \varepsilon a$, то из равенства

$$a = uv = \varepsilon av$$

и того факта, что a отличен от нуля, следует, что $\varepsilon v = 1$, т.е. элемент v обратим. Это также противоречит тому, что v несобственный делитель. Из полученных противоречий следует доказательство первого утверждения леммы.

Перед доказательством второго утверждения заметим, что в силу определения нормы выполнено неравенство $N(v) \leqslant N(a)$, таким образом нам достаточно доказать, что $N(v) \neq N(a)$. Предположим, что это не так и $N(v) = N(a)$. Если норма мультипликативна, то из равенств

$$N(v) = N(a) = N(uv) = N(u)N(v), \quad N(v) \neq 0$$

следует, что $N(u) = 1$. Тогда, из второго утверждения леммы 2.7 вытекает, что v обратим, а это противоречит доказанному выше первому утверждению леммы. В случае аддитивной нормы, из равенств

$$N(v) = N(a) = N(uv) = N(u) + N(v)$$

получаем, что $N(u) = 0$ и опять, из леммы 2.7 следует противоречие с тем, что u собственный делитель. □

Теперь мы можем строго доказать, что неразложимые элементы существуют.

Теорема 3.1 (Теорема о существовании)**.** *Пусть $\mathbb{U}$ – евклидово кольцо, содержащее хотя бы один необратимый элемент a. Тогда в кольце $\mathbb{U}$ найдется хотя бы один неразложимый элемент p и $p|a$.*

Доказательство. Пусть $a \in \mathbb{U}$ – отличный от нуля, необратимый элемент кольца и элементы $p_1, \ldots, p_k$ образуют множество всех возможных делителей элемента a. Вычислим значения нормы и упорядочим элементы $p_1, \ldots, p_k$ так, что

$$N(p_1) \leqslant N(p_2) \leqslant \cdots \leqslant N(p_k).$$

Без ограничения общности считаем, что элемент $p = p_1$ имеет минимальное значение нормы, тогда этот элемент является неразложимым.

Предположим обратное, тогда найдется элемент $v \in \mathbb{U}$, являющийся собственным делителем элемента p_1. Следовательно $v|p_1|a$ и v также является делителем элемента a, т.е. должен быть среди элементов $p_2, \ldots, p_k$ и удовлетворять неравенству $N(v) \geqslant N(p_1)$. Вместе с тем, из утверждения леммы 3.1 следует, что $N(v) < N(p_1)$. Полученное противоречие позволяет говорить, что у p_1 имеются только несобственные делители, т.е. он неразложим. Теорема доказана. □

Пример 3.2. Приведем ряд численных примеров, иллюстрирующих доказательство теоремы 3.1.

1. В кольце целых чисел выполнено

$$-15 = -3 \cdot 5 \quad \text{и} \quad N(-3) < N(5).$$

2. В кольце многочленов

$$x^2 - 1 = (x-1)(x+1), \quad N(x+1) = N(x-1) = 1$$

3. В кольце целых гауссовых чисел

$$15 = 3(1-2i)(1+2i), \quad N(1-2i) = 5 < 9 = N(3)$$

В каждом случае мы разложили элемент в произведение множителей и предъявили множитель с наименьшей нормой – данный делитель является неразложимым.

Согласно теореме 3.1, мы можем рассматривать не являющееся полем кольцо $\mathbb{U}$ как объединение следующих сущностей:

$$\mathbb{U} = \begin{cases} 0 \text{ (ноль)}, \\ \mathbb{U}^* \text{ (обратимые элементы)}, \\ \text{неразложимые элементы}, \\ \text{разложимые элементы}. \end{cases}$$

Если же $\mathbb{U}$ поле, то $\mathbb{U} = \{0\} \cup \mathbb{U}^*$.

В случае, когда кольцо $\mathbb{U}$ содержит бесконечное число элементов, а именно примеры таких колец мы рассматривали ранее, можно показать, что число неразложимых элементов бесконечно. Доказательство этого утверждения для кольца целых чисел принадлежит Эвклиду.

Теорема 3.2. *Пусть евклидово кольцо $\mathbb{U}$ удовлетворяет условиям теоремы 3.1. Тогда множество неразложимых элементов кольца $\mathbb{U}$ бесконечно.*

Доказательство. Предположим, что утверждение теоремы не выполнено. Тогда в кольце $\mathbb{U}$ найдется лишь конечное число неразложимых элементов, которые мы обозначим $p_1, \ldots, p_k$ для некоторого натурального k.

Определим элемент

$$p = p_1 \cdots p_k + \varepsilon, \quad \varepsilon \in \mathbb{U}^*, \tag{3.1}$$

являющийся произведением всех неразложимых элементов кольца, к которому прибавлен произвольный обратимый элемент кольца $\mathbb{U}$. Поскольку операции сложения и умножения не выводят за пределы кольца, то построенный элемент $p \in \mathbb{U}$.

Легко проверить, что $p \neq 0$. Действительно, если выполнено равенство $p_1 \cdot p_2 \cdots p_k + \varepsilon = 0$, то

$$-p_1 \cdot p_2 \cdots p_k \varepsilon^{-1} = 1.$$

Поскольку p_i неразложимые элементы, то они не могут быть обратимыми элементами кольца и, следовательно, равенство $p = 0$ не выполнено.

Теперь предположим, что найдется индекс i такой, что $i \in \{1, 2, \ldots, k\}$ и $p = p_i$, тогда выполнено равенство

$$p_1 \cdots p_k + \varepsilon = p_i, \quad \text{или} \quad p_i \left(1 - p_1 \cdots p_{i-1} p_{i+1} \cdots p_k\right) \varepsilon^{-1} = 1,$$

из которого вытекает противоречие с тем, что элементы $p_1, \ldots, p_k$ необратимы, следовательно, мы делаем заключение, что все элементы p_1, $\ldots$, p_k отличны от элемента p.

Если элемент p неразложим, то мы в явном виде предъявили неразложимый элемент, отличный от $p_1, \ldots, p_k$ и, тем самым, опровергли исходное предположение.

Если же элемент p разложим, то, основываясь на доказательстве теоремы 3.1, будем считать, что существует элемент v – неразложимый собственный делитель элемента p.

Поскольку для любого индекса $i \in \{1, 2, \ldots, k\}$ выполнено равенство

$$p = q_i p_i + \varepsilon, \quad q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k, \quad \varepsilon \neq 0,$$

то ни один из неразложимых элементов $p_1, \ldots, p_k$ не делит элемент p и, следовательно, отличен от элемента v. Теорема доказана. □

Для внимательного читателя сделаем следующее замечание. В ходе доказательства теоремы мы не рассмотрели случай, когда построенный элемент p является обратимым элементом кольца. В кольце целых чисел, для которого изначально Эвклидом был предложен изложенный путь доказательства, случай $p = \pm 1$ не возможен. Однако для произвольного эвклидового кольца пропущенный случай необходимо рассмотреть и дополнить доказательство.

3.2 Основная теорема

Прежде, чем доказывать основной результат настоящей главы, докажем пару вспомогательных лемм.

Лемма 3.2. *Пусть $a, b \in \mathbb{U}$ не ассоциированные друг с другом, неразложимые элементы кольца $\mathbb{U}$. Тогда* $\mathbf{НОД}(a,\ b) \sim 1$.

Доказательство. Поскольку a неразложимый элемент кольца $\mathbb{U}$, то его делителями являются элементы $\{\varepsilon, \varepsilon a : \varepsilon \in \mathbb{U}^*\}$. Аналогично, делителями b являются элементы $\{\varepsilon, \varepsilon b :\ \varepsilon \in \mathbb{U}^*\}$. Поскольку $a \neq \varepsilon b$ для некоторого $\varepsilon \in \mathbb{U}^*$, то общими делителями элементов a, b являются обратимые элементы кольца $\mathbb{U}$, тогда $\mathbf{НОД}(a,\ b) \sim 1$. □

Лемма 3.3. *Пусть a, b взаимно простые элементы эвклидового кольца $\mathbb{U}$. Если p неразложимый элемент кольца и $p|ab$, тогда либо $p|a$, либо $p|b$.*

Доказательство. Если элемент $p|a$, то утверждение леммы выполнено. Будем считать, что это не так. Тогда p не делит a и, поскольку p неразложим, выполнено $\mathbf{НОД}(a,\ p) \sim 1$ (иначе существовал бы необратимый элемент d, который делил p, что противоречит тому, что p неразложим).

Поскольку $p|ab$, то существует элемент u такой, что $ab = pu$, тогда, из утверждения леммы 2.6 следует, что $p|b$. Лемма доказана. □

Теперь мы можем доказать основную теорему этой главы.

Теорема 3.3 (Основная теорема арифметики)**.** *Пусть a произвольный, отличный от нуля элемент евклидового кольца $\mathbb{U}$, тогда его можно представить в виде произведения*

$$a = \varepsilon \cdot p_1 \cdots p_k$$

где $\varepsilon \in \mathbb{U}^*$, а $p_1, \ldots, p_k$ неразложимые элементы кольца $\mathbb{U}$. Данное представление единственно, с точностью до перестановки элементов $p_1, \ldots, p_k$ и обратимых сомножителей кольца $\mathbb{U}$.

Доказательство. Начнем с доказательства существования указанного представления.

Если a обратимый элемент, то выполнено равенство $n = \varepsilon$ для некоторого $\varepsilon \in \mathbb{U}^*$. Если a неразложимый элемент, что выполнено равенство $a = p_1$ для некоторого неразложимого элемента $p_1 \in \mathbb{U}$. Осталось рассмотреть случай, когда a разложимый элемент.

В этом случае, согласно утверждению теоремы 3.1, найдется неразложимый элемент $p_1 \in \mathbb{U}$ такой, что $p_1|a$ и $a = p_1 a_1$ для некоторого $a_1 \in \mathbb{U}$. При этом, согласно лемме 3.1, будет выполнено $N(a_1) < N(a)$.

Применяя к элементу a_1 рассуждения, аналогичные тем, что мы применили к элементу a, получим цепочку равенств

$$\begin{aligned} a &= p_1 a_1, && N(a_1) < N(a), \\ a &= p_1 p_2 a_2, && N(a_2) < N(a_1), \\ &\cdots \\ a &= p_1 p_2 \cdots p_k a_k, && N(a_k) < N(a_{k-1}). \end{aligned}$$

Поскольку величины $N(a_k) < \cdots < N(a_1) < N(a)$ принимают неотрицательные целые значения и убывают, то процесс не сможет длиться бесконечно (см. вторую аксиому Архимеда) и оборвется на некотором шаге k. Это означает, что величина a_k окажется неразложимым элементом и, обозначая $p_{k+1} = a_k$, мы получим искомое равенство.

Зафиксируем некоторый индекс $i \in \{1, \ldots, k\}$ и рассмотрим ассоциированный с p_i элемент π_i. Тогда π_i также неразложим, кроме того выполнены равенства $p_i = \varepsilon\pi_i$, где $\varepsilon \in \mathbb{U}^*$, и

$$a = p_1 \cdots p_{i-1} \cdot \varepsilon\pi_i \cdot p_{i_1} \cdots p_k.$$

Существование доказано.

Для доказательства единственности предположим, что существует другое представление элемента a в виде произведения и выполнено равенство

$$\varepsilon p_1 \cdots p_k = a = \gamma q_1 \cdots q_s, \tag{3.2}$$

где $k, s \in \mathbb{N}_0$, а $p_1, \ldots, p_k, q_1, \ldots, q_s$ неразложимые элементы кольца $\mathbb{U}$. Кроме того, без ограничения общности, будем считать, что выполнено условие $k \leqslant s$.

Рассмотрим p_1 и предположим, что среди $q_1, \ldots, q_s$ найдется элемент, ассоциированный с p_1. Изменяя очередность записи множителей, будем считать, что это q_1, тогда $p_1 = q_1\gamma_1$ для некоторого $\gamma_1 \in \mathbb{U}^*$, а равенство (3.2) принимает вид

$$\varepsilon\gamma_1 p_2 \cdots p_k = \gamma q_2 \cdots q_s. \tag{3.3}$$

Если же мы предположим, что среди элементов $q_1, \ldots, q_s$ не найдется элемента ассоциированного с p_1, то выбрав один из неассоциированных элементов, скажем q_s, получим, согласно утверждению леммы 3.2, условие $\mathbf{НОД}(p_1,\ q_s) \sim 1$. Теперь, воспользовавшись утверждением леммы 2.6, мы можем сказать, что $p_1 | q_1 \cdots q_{s-1}$. Поскольку p_1 неразложим, то согласно лемме 3.3 найдется такой индекс, скажем единица, что $p_1 | q_1$. Поскольку q_1 также неразложим, то последнее условие возможно, если p_1 ассоциирован с q_1, т.е. $p_1 = q_1\gamma_1$ для некоторого $\gamma_1 \in \mathbb{U}^*$. Это снова приводит нас к равенству (3.3).

Продолжая рассуждения аналогичным образом для всех индексов $i = 2, \ldots, k$ получим равенство

$$\varepsilon\gamma_1 \cdots \gamma_k = \gamma$$

в случае, когда $k = s$, или равенство

$$\varepsilon\gamma_1 \cdots \gamma_k = \gamma q_{k+1} \cdots q_s$$

при $k < s$.

В первом случае, мы получили условие $p_i \sim q_i$ для всех $i = 1, \ldots k$, которое эквивалентно утверждению теоремы. Во втором случае мы можем записать равенство

$$1 = \varepsilon^{-1}\gamma_1^{-1} \cdots \gamma_k^{-1}\gamma q_{k+1} \cdots q_s$$

из которого сразу следует, что величины $q_{k+1}, \ldots, q_s$ являются обратимыми элементами кольца $\mathbb{U}$. Теорема доказана. □

Пусть a произвольный, отличный от нуля элемент кольца $\mathbb{U}$ и задано его разложение на неразложимые множители $a = \varepsilon p_1 \cdots p_k$. Пусть среди элементов $p_1, \ldots, p_k$ найдется α_1 элементов, ассоциированных с p_1, найдется α_2 элементов, ассоциированных с p_2 и так далее. Тогда, мы можем записать равенство

$$a = \gamma p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \tag{3.4}$$

где $\alpha_1 + \cdots + \alpha_s = k$ и $\gamma \in \mathbb{U}^*$. Представление (3.4) принято называть каноническим разложением элемента a на неразложимые сомножители.

Пример 3.3. Приведем примеры, иллюстрирующие единственность разложения на множители с точностью до перестановки и обратимых сомножителей в различных кольцах.

1. В кольце целых чисел выполнены равенства

$$-75 = (-1) \cdot 3 \cdot 5^2 = -3 \cdot 5^2 = -5 \cdot 3 \cdot 5.$$

2. В кольце многочленов от одной переменной $\mathbb{Q}[x]$ выполнены равенства

$$x^2 - 1 = (x - 1)(x + 1) = \frac{2}{3}\left(\frac{x}{2} - \frac{1}{2}\right)(3x + 3).$$

3. В кольце целых гауссовых чисел выполнены равенства

$$-15 = -3 \cdot (1 + 2i) \cdot (1 - 2i) = i^3 \cdot 3 \cdot (1 + 2i) \cdot (2 + i).$$

Если у кого-то из читателей сложилось впечатление, что свойство единственности разложения присуще всем кольцам, то сейчас самое время его разрушить. Приведем еще один пример.

Пример 3.4. По аналогии с кольцом целых гауссовых чисел определим кольцо $\mathbb{Z}[\theta]$ следующим образом. Будем считать, что θ – формальный символ, удовлетворяющий равенству $\theta^2 = -5$. Рассмотрим множество

$$\mathbb{Z}[\theta] = \{a + b\theta,\ a, b \in \mathbb{Z}\}$$

и определим на нем операции сложения и умножения равенствами

$$\begin{aligned}(a + b\theta) + (c + d\theta) &= (a + c) + (b + d\theta),\\ (a + b\theta) \cdot (c + d\theta) &= (ac - 5bd) + (ad + bc\theta),\end{aligned}$$

Ноль и группа единиц (обратимых элементов) кольца $\mathbb{Z}[\theta]$ совпадают с нулем и группой единиц кольца целых чисел $\mathbb{Z}$, кроме того $\mathbb{Z} \subset \mathbb{Z}[\theta]$. Следующие равенства показывают, что в отличие от колец $\mathbb{Z}$ и $\mathbb{Z}[i]$, в кольце $\mathbb{Z}[\theta]$ утверждение теоремы 3.3 оказывается неверным

$$\begin{aligned}(1 + \theta) \cdot (1 - \theta) &= 6 &&= 2 \cdot 3,\\ (-1) \cdot (1 + \theta)^2 &= 4 - 2\theta &&= 2 \cdot (2 - \theta),\end{aligned}$$

поскольку элементы $1 - \theta, 1 + \theta, 2, 3, 2 - \theta$ не являются ассоциированными между собой. Если мы определим в кольце $\mathbb{Z}[\theta]$ норму равенством $N(a + b\theta) = a^2 + 5b^2$, то из приведенных выше равенств следует равенство норм

$$\begin{aligned}36 = 6 \cdot 6 = N(1 + \theta)N(1 - \theta) &= N(6) &&= N(2)N(3) = 4 \cdot 9 = 36,\\ 36 = 1 \cdot 6 \cdot 6 = N(-1)N(1 + \theta)N(1 + \theta) &= N(4 - 2a) &&= N(2)N(2 - \theta) = 4 \cdot 9 = 36,\end{aligned}$$

т.е. норма в кольце $\mathbb{Z}[\theta]$ мультипликативна. Вместе с тем, она не удовлетворяет определению 2.4, а кольцо $\mathbb{Z}[\theta]$ не является эвклидовым.

3.3 Элементарные методы поиска неразложимых элементов

Нам потребуется следующая лемма об оценке нормы делителя разложимого (составного) элемента кольца.

Лемма 3.4. *Пусть a разложимый элемент эвклидового кольца $\mathbb{U}$ и p его неразложимый делитель с наименьшей нормой.*

Если норма мультипликативна, то $N(p) \leqslant \sqrt{N(a)}$. Если же норма аддитивна, то $N(p) \leqslant \frac{N(a)}{2}$.

Доказательство. Предположим, что норма в кольце $\mathbb{U}$ мультипликативна и утверждение леммы не выполнено. Обозначим $p_1, \ldots, p_k$ неразложимые делители элемента a и $k \geqslant 2$. Тогда выполнены неравенства

$$\sqrt{N(a)} < N(p_1) \leqslant \cdots \leqslant N(p_k),$$

а также

$$N(a) = N(p_1 \cdots p_k) = N(p_1) \cdots N(p_k) > \left(\sqrt{N(a)}\right)^k.$$

Поскольку $N(a) > 0$, то последнее неравенство ложно при $k \geqslant 2$.

Аналогично, если норма в кольце $\mathbb{U}$ аддитивна, то отрицание утверждения леммы сводится к выполнению неравенств

$$\frac{N(a)}{2} < N(p_1) \leqslant \cdots \leqslant N(p_k),$$

и

$$N(a) = N(p_1 \cdots p_k) = N(p_1) + \cdots + N(p_k) > \frac{k}{2} N(a).$$

Последнее неравенство, очевидно, не выполнено при $k \geqslant 2$. □

Пример 3.5. Проиллюстрируем утверждение леммы численными примерами. В кольце целых чисел выполнено равенство

$$135 = 3^3 \cdot 5, \quad 3 = N(3) < \sqrt{N(135)} = \sqrt{135} = 11.618,$$

а в кольце целых гауссовых чисел равенство

$$15 = 3i(1+2i)(2+i), \quad N(1+2i) = 5 < \sqrt{N(15)} = \sqrt{15^2} = 15.$$

В кольце многочленов от одной переменной $\mathbb{Q}[x]$ норма аддитивна, что дает равенство

$$x^3 + 3x^2 + 3x + 1 = (x+1)^3, \quad 1 = N(x+1) < \frac{N(x^3 + 3x^2 + 3x + 1)}{2} = \frac{3}{2}.$$

3.3.1 Решето Эратосфена

Из утверждения леммы 3.4 следует, что у разложимого элемента a всегда найдется неразложимый делитель p, норма которого ограничена значением, зависящим от нормы элемента a. Если же такого делителя не существует, то элемент a – неразложимый.

Сформулированная идея легла в основу решета Эратосфена[1] — алгоритма поиска всех неразложимых элементов кольца $\mathbb{U}$, норма которых ограничена сверху некоторым натуральным значением b. Данный алгоритм может быть реализован только в тех эвклидовых кольцах, в которых число элементов, имеющих заданное значение нормы, конечно.

Для кольца целых чисел решето Эратосфена состоит в следующем. Выпишем все натуральные, необратимые целые числа от 2 до максимального значения b, упорядочив их по возрастанию нормы, т.е.

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ \cdots,\ b-1,\ b.$$

[1] Эратосфен Киренский (276 год до н. э.—194 год до н. э.) – древнегреческий математик, астроном, географ, филолог и поэт. Глава Александрийской библиотеки, первый известный учёный, вычисливший размеры Земли.

Первое число в этой последовательности будет иметь минимально возможную норму для необратимого элемента, поэтому оно не может быть разделено на какой-либо другой обратимый элемент с меньшей нормой. Следовательно, данное число является неразложимым элементом.

Отметим двойку в качестве неразложимого элемента, вычеркнем из рассматриваемой последовательности все элементы, которые делятся на двойку, и получим следующую последовательность чисел

$$\textcircled{2},\ 3,\qquad 5,\qquad 7,\qquad 9,\qquad 11,\qquad 13,\qquad 15,\qquad \cdots,\qquad b.$$

Рассмотрим среди оставшихся чисел первое неотмеченное число с наименьшей нормой, т.е. тройку. Данное число не делится на отмеченный ранее неразложимый элемент с меньшей нормой и, следовательно, само является неразложимым элементом кольца. Тогда, отметим тройку в качестве неразложимого элемента, вычеркнем из рассматриваемой последовательности все элементы, которые делятся на тройку, и получим следующую последовательность чисел

$$\textcircled{2},\ \textcircled{3},\qquad 5,\qquad 7,\qquad 11,\qquad 13,\qquad \cdots,\qquad b.$$

Далее, мы повторим эту процедуру применительно к первому неотмеченному элементу с минимальной нормой, т.е. пятерке, потом к семерке и так далее, до тех пор, пока мы не отметим элемент p такой, что $N(p) > \sqrt{N(b)}$ (при этом может оказаться, что число b будет вычеркнуто ранее). Все оставшиеся числа, согласно утверждению леммы 3.4, будут положительными неразложимыми элементами кольца целых чисел, т.е. простыми числами. Добавляя к ним ассоциированные элементы, мы получим множество всех неразложимых элементов кольца целых чисел, норма которых не превосходит заданной величины

$$\pm 2,\ \pm 3,\ \pm 5,\ \pm 7,\ \pm 11,\ \pm 13,\ \ldots.$$

При практической реализации решета Эратосфена на ЭВМ выписывание всех целых чисел от 2 до b оказывается неэффективным как с точки зрения использования оперативной памяти, так и с точки быстродействия алгоритма. Числа, которые должны быть выписаны, можно вычислять в ходе выполнения алгоритма и хранить в памяти только найденные простые числа. С учетом этого замечания, решето Эратосфена может быть немного модифицировано и реализовано в виде следующего алгоритма для системы компьютерной алгебры Sage.

Алгоритм 3.1 (Алгоритм построения таблицы простых чисел)

Вход: Натуральное число b, где $b > 3$.
Выход: Таблица простых чисел, не превосходящих b.

```
1  def primes_z( b ):
2          if b.is_integer() != True:
3                  print("Неверный тип входных данных");
4                  return [];
5          if b <= 3:
6                  print("Граница для простых чисел слишком мала");
7                  return [];
8          # явно определяем первые элементы таблицы
9          v=[2,3];
10         n=3;
11         # опробуем все натуральные числа n ⩽ b,
12         # выполняя пробное деление на простые, удовлетворяющие неравенству r ⩽ √n
13         while n < b:
14                 n=n+1;
15                 i=0;
16                 r = ceil(sqrt(n));
17                 while i < len(v) and v[i] <= r:
18                         if n%v[i] == 0: break;
19                         i=i+1;
20                 if i == len(v):
21                         v.append(n);
22                 else:
23                         if v[i] > r: v.append(n);
24         return v;
```

Основываясь на аналогичных идеях, решето Эратосфена может быть реализовано в кольце целых гауссовых чисел. Для начала сведём в одну таблицу, см. таблицу 3.1 на стр. 63, необратимые числа с минимальной нормой. В первом столбце приведём значение нормы, во втором – число α с указанной нормой, где $\alpha = a + bi$ и a, b неотрицательные целые числа, а в остальных столбцах – числа, ассоциированные с α. При этом, как можно заметить, не каждое из натуральных чисел является нормой целого гауссового числа.

Рассматривая второй столбец в качестве исходной последовательности для решета Эратосфена мы видим, что число $1 + i$ имеет минимальную норму и, следовательно, неразложимо. Теперь, вычеркивая в первом столбце числа, делящиеся на $1+i$, получим последовательность

$$1 + i,\ 1 + 2i,\ 2 + i,\ 3,\ 2 + 3i,\ 3 + 2i,\ 1 + 4i,\ 4 + i,\ 5,\ 3 + 4i,\ 4 + 3i,\ \ldots$$

Рассмотрим среди оставшихся чисел число с минимальной нормой, т.е. $1 + 2i$. Выделим его, вычеркнем все числа, делящиеся на $1 + 2i$, и получим последовательность

$$1 + i,\ 1 + 2i,\ 2 + i,\ 3,\ 2 + 3i,\ 3 + 2i,\ 1 + 4i,\ 4 + i,\quad 3 + 4i,\qquad \ldots$$

$N(\alpha)$	α	$-\alpha$	$i\alpha$	$-i\alpha$
2	$1+i$	$-1-i$	$-1+i$	$1-i$
3				
4	2	-2	$2i$	$-2i$
5	$1+2i$	$-1-2i$	$-2+i$	$2-i$
5	$2+i$	$-2-i$	$-1+2i$	$1-2i$
6				
7				
8	$2+2i$	$-2-2i$	$-2+2i$	$2-2i$
9	3	-3	$3i$	$-3i$
10	$1+3i$	$-1-3i$	$-3+i$	$3-i$
10	$3+i$	$-3-i$	$-1+3i$	$1-3i$
11				
12				
13	$2+3i$	$-2-3i$	$-3+2i$	$3-2i$
13	$3+2i$	$-3-2i$	$-2+3i$	$2-3i$
14				
14				

$N(\alpha)$	α	$-\alpha$	$i\alpha$	$-i\alpha$
15				
16	4	-4	$4i$	$-4i$
17	$1+4i$	$-1-4i$	$-4+i$	$4-i$
17	$4+i$	$-4-i$	$-1+4i$	$1-4i$
18	$3+3i$	$-3-3i$	$-3+3i$	$3-3i$
19				
20	$2+4i$	$-2-4i$	$-4+2i$	$4-2i$
20	$4+2i$	$-4-2i$	$-2+4i$	$2-4i$
21				
22				
23				
24				
25	5	-5	$5i$	$-5i$
25	$3+4i$	$-3-4i$	$-4+3i$	$4-3i$
25	$4+3i$	$-4-3i$	$-3+4i$	$3-4i$
26	$1+5i$	$-1-5i$	$-5+i$	$5-i$
26	$5+i$	$-5-i$	$-1+5i$	$1-5i$

Таблица 3.1: Элементы кольца $\mathbb{Z}[i]$ с минимальной нормой.

Поскольку $2+i=(1+2i)+(1-i)$, т.е. не делится на $1+2i$ нацело, то число $2+i$ также является неразложимым элементом кольца, норма которого совпадает с нормой $1+2i$. Выделяя $2+i$ и вычеркивая все числа, делящиеся на $2+i$, получим последовательность

$$1+i,\ 1+2i,\ 2+i,\ 3,\ 2+3i,\ 3+2i,\ 1+4i,\ 4+i,\ \ldots \tag{3.5}$$

Добавляя к последовательности (3.5) ассоциированные элементы получим множество всех неразложимых элементов кольца целых гауссовых чисел, норма которых не превосходит 17.

Стоит также отметить, что при вычеркивании элементов, делящихся на неразложимые элементы, мы неявно использовали свойство мультипликативности нормы в кольце целых гауссовых чисел. Действительно, рассматривая число $4+3i$, легко заметить, что из равенства норм

$$N(4+3i)=25=5\cdot 5=N(1+2i)\cdot N(2-i)$$

следует равенство целых гауссовых чисел $4+3i=(1+2i)(2-i)$.

3.3.2 Решето Сундарама

Задачи и упражнения

1. Найдите все несобственные делители чисел $7-2i$ и $2+3i$ в кольце целых гауссовых чисел.

2. Докажите, что целые гауссовы числа $3+4i$ и 5 не являются ассоциированными, хоть и имеют одинаковую норму. Указание: для доказательства рассмотрите уравнения $(3+4i)(x+yi)=5$ и $5(x+yi)=3+4i$ и покажите, что они не имеют решений в целых числах.

3. Найдите наименьшие неразложимые делители целых чисел 192 и 3789, а также целых гауссовых чисел $5-7i$ и $9+2i$.

4. Доведите до конца доказательство Эвклида теоремы о бесконечности множества неразложимых элементов. Для этого используйте тот факт, что множество элементов α, для которых выполнено неравенство $N(\alpha+\varepsilon)\leqslant N(\varepsilon)$, конечно.

5. Выпишите все возможные варианты разложения чисел 10, 12, $5+3i$ на неприводимые сомножители в кольце целых гауссовых чисел.

6. Постройте таблицу всех простых чисел, не превосходящих 75.

7. Постройте таблицу всех неразложимых элементов кольца целых гауссовых чисел, норма которых меньше 82.

8. Поясните, почему решето Эратосфена не может быть применено для построения неразложимых элементов кольца многочленов от одной переменной.

9. Используя свойство мультипликативности нормы в кольце целых гауссовых чисел, разложите на множители числа $1-5i$, 15, а также $-13+65i$.

10. Постройте кольцо, отличное от колец целых и целых гауссовых чисел, а также кольца многочленов, удовлетворяющее утверждению основной теоремы арифметики.

Рекомендации к сдаче экзамена

В экзаменационные билеты по курсу «Введение в теорию чисел» входят следующие вопросы.

- Теоремы о существовании и бесконечности множества неразложимых элементов.

  При изложении данного билета необходимо сформулировать и доказать вспомогательную лемму 3.1, теорему о существовании неразложимых элементов (теорема 3.1), а также теорему о бесконечности множества неразложимых элементов (теорема 3.2).

  При доказательстве теоремы 3.1 необходимо упорядочить делители необратимого элемента во возрастанию нормы, тогда делитель с наименьшей нормой будет неразложимым элементом. При доказательстве теоремы 3.2 необходимо зафиксировать конечное множество неразложимых элементов $p_1, \ldots, p_k$ и определить новый элемент кольца вида $p = p_1 \cdots p_k + \varepsilon$, где $\varepsilon \in \mathbb{U}^*$. Тогда новым неразложимым элементом кольца будет либо элемент p, либо делитель элемента p с наименьшей нормой.

- Основная теорема арифметики.

  Перед доказательством основной теоремы (теорема 3.3) необходимо напомнить вспомогательные утверждения, которые будут использованы в дальнейшем (леммы 2.7, 2.6, 3.2 и 3.3).

  Доказательство теоремы состоит из двух последовательных частей – доказательства существования и доказательства единственности. При доказательстве существования мы последовательно делим элемент на неразложимые сомножители. Согласно утверждению леммы 3.1 норма делимого уменьшается, что позволяет сделать вывод о конечности данной процедуры.

  Доказательство единственности проводится от противного. Рассматриваются два различных представления одного и того же элемента, после чего, с помощью леммы 2.6, производится сокращение общих множителей в правой и левой частях. После сокращения показывается, что оставшиеся множители являются обратимыми элементами кольца.

- Решето Эратосфена в кольцах целых и целых гауссовых чисел.

  Перед изложением алгоритма, который принято называть решетом Эратосфена, необходимо доказать лемму 3.4. Оценка нормы наименьшего делителя должна быть использована для определения числа шагов излагаемого алгоритма. В заключение необходимо показать как классическое решето Эратосфена применяется в кольце целых гауссовых чисел.

Схема зависимостей между утверждениями, доказанными в 3-й главе, изображена на рисунке 3.1.

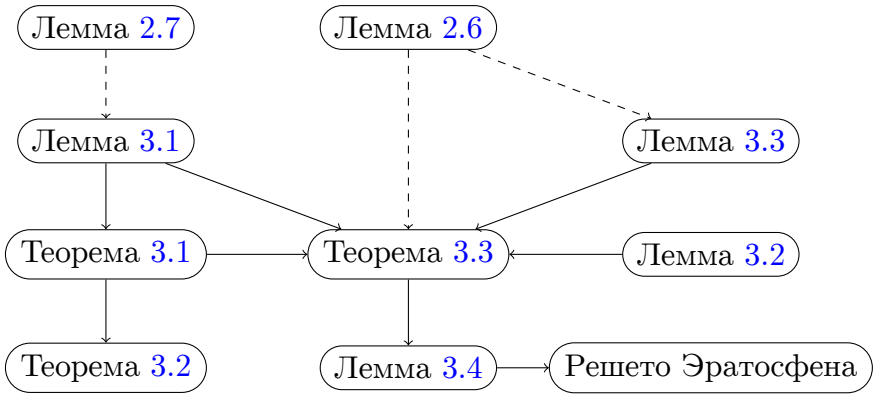


Рис. 3.1: Схема зависимостей между утверждениями 3-й главы.

Дополнительная литература к 3-й главе

1. Девенпорт Г. Высшая арифметика. Введение в теорию чисел. – М.:Наука. – 1965.

2. Кордемский Б.А. Математическая смекалка. – М.: ГИФМЛ, 1958.

глава 4

Элементы теории сравнений

Определение классов вычетов, их свойства – Теорема о кольце классов вычетов – Теорема о конечности классов вычетов.

Прежде, чем дать определение, играющее важную роль в излагаемом далее теоретическом материале, напомним, что согласно определению 1.17, см. главу 1, коммутативное кольцо $\mathbb{U}$ называется целостным кольцом, если в нем нет делителей нуля, т.е. отличных от нуля элементов a, b таких, что $ab = 0$.

Определение 4.1. *Пусть $\mathbb{U}$ целостное кольцо, $a, b, m \in \mathbb{U}$ элементы этого кольца и $m \neq 0$. Мы будем говорить, что элементы a и b сравнимы по модулю m и записывать $b \equiv a \pmod{m}$, если $m|(b-a)$, т.е. элемент m делит разность $b - a$.*

Данное нами определение понятия сравнимости элементов кольца обладает следующими арифметическими свойствами.

Лемма 4.1. *Пусть $\mathbb{U}$ целостное кольцо, $a, b, m \in \mathbb{U}$ элементы этого кольца и $m \neq 0$. Если $b \equiv a \pmod{m}$, то*

1. *сравнение симметрично, т.е. $a \equiv b \pmod{m}$,*
2. *для любого $c \in \mathbb{U}$ выполнено*

$$b + c \equiv a + c \pmod{m},$$

   в частности $a \equiv a + 0 \pmod{m}$ и $a + (-a) \equiv 0 \pmod{m}$, а также $a \equiv a + m \pmod{m}$,
3. *для любого $c \in \mathbb{U}$ выполнено $ac \equiv bc \pmod{m}$,*
4. *если $\mathbf{НОД}(a,\ b) = d$ и $d|m$, тогда $\dfrac{a}{d} \equiv \dfrac{b}{d} \left(mod\, \dfrac{m}{d}\right)$,*
5. *если $\mathbf{НОД}(a,\ b) = d$ и $\mathbf{НОД}(d,\ m) \sim 1$, тогда $\dfrac{a}{d} \equiv \dfrac{b}{d} \pmod{m}$.*
6. *если существует элемент $c \in \mathbb{U}$ такой, что $c|a$ и $c|m$, тогда $c|b$.*

Доказательство. Содержательный интерес представляет доказательство трех последних утверждений. Доказательство остальных утверждений оставляются читателю в качестве упражнения.

Рассмотрим четвертое утверждение. Если $m|(b-a)$, то найдется элемент $k \in \mathbb{U}$ такой, что $mk = b - a$. Далее, если $\mathbf{НОД}(a,\ b) = d$ и $d|m$, то можно записать

$$a = da_1, \quad b = db_1, \quad m = dm_1,$$

для некоторых $a_1, b_1, m_1 \in \mathbb{U}$. Тогда

$$dm_1k = mk = b - a = db_1 - da_1 = d(b_1 - a_1).$$

Сокращая на d получим, что $m_1k = b_1 - a_1$ или $b_1 \equiv a_1 \pmod{m_1}$. Равенства $m_1 = \frac{m}{d}$, $a_1 = \frac{a}{d}$ и $b_1 = \frac{b}{d}$ завершают доказательство четвертого утверждения.

Для доказательства пятого утверждения, аналогично, запишем равенство

$$mk = b - a = d(b_1 - a_1), \quad k \in \mathbb{U},$$

из которого следует, что $d|mk$. Поскольку $\mathbf{НОД}(d,\ m) \sim 1$, то $d|k$, что равносильно равенству $k = dk_1$, выполненному для некоторого $k_1 \in \mathbb{U}$. Теперь можно записать равенство

$$mdk_1 = mk = b - a = d(b_1 - a_1).$$

Сокращая правую и левую части полученного равенства на d, получаем сравнение $a_1 \equiv b_1 \pmod{m}$ и доказательство пятого утверждения.

Рассмотрим шестое утверждение. Поскольку $a \equiv b \pmod{m}$, то, как и ранее, для некоторого $k \in \mathbb{U}$ будет выполнено равенство $mk = b - a$. Из условия леммы следует, что $a = ca_1$ и $m = cm_1$ для некоторых $a_1, m_1 \in \mathbb{U}$. Тогда выполнено равенство

$$b = mk + a = cm_1k + ca_1 = c(m_1k + a_1),$$

из которого следует доказательство последнего утверждения леммы. □

Пример 4.1.

1. В кольце целых чисел $\mathbb{Z}$ выполнено сравнение $33 \equiv 3 \pmod{6}$, поскольку $6|(33-3)$. Кроме того, $43 = 33 + 10 \equiv 13 = 3 + 10 \pmod{6}$.

   Поскольку $\mathbf{НОД}(3,\ 33) = 3$ и $3|6$, то выполнено сравнение $11 \equiv 1 \pmod{2}$.

2. В кольце многочленов $\mathbb{Q}[x]$ выполнено сравнение

$$1 - x^2 \equiv x^3 - x^2 \pmod{x^3 - 1},$$

поскольку многочлен $x^3 - 1$ делит многочлен $1 - x^3 = (1 - x^2) - (x^3 - x^2)$.

Поскольку выполнено условие $\mathbf{НОД}(1 - x^2,\ x^3 - x^2) = 1 - x$ и $1 - x | x^3 - 1$, то выполнено сравнение

$$1 + x \equiv -x^2 \pmod{x^2 + x + 1}.$$

3. В кольце целых гауссовых чисел выполнено сравнение $3 \equiv -i \pmod{1 + i}$, поскольку $1 + i$ делит $3 + i = (1 + i)(2 - i)$.

Легко показать, что введенное нами понятие сравнимости элементов кольца $\mathbb{U}$ задает отношение эквивалентности в смысле определения 1.20, данного нами ранее в главе 1.

Лемма 4.2. *Отношение $a \equiv b \pmod m$ есть отношение эквивалентности в кольце $\mathbb{U}$.*

Доказательство. Нам необходимо показать выполнимость свойств, указанных в определении 1.20. Свойства рефлексивности $a \equiv a \pmod m$ и симметричности $a + b \equiv b + a \pmod m$ следуют из утверждений леммы 4.1. Для доказательства выполнимости свойства транзитивности заметим следующее.

Пусть $b \equiv a \pmod m$ и $c \equiv b \pmod m$, тогда выполнены равенства

$$c = b + lm = a + km + lm = a + (k + l)m,$$

для некоторых элементов $k, l \in \mathbb{U}$, и $m|(c - a)$. Мы получили сравнение $a \equiv c \pmod m$, которое завершает доказательство леммы. □

Отношение эквивалентности позволяет рассматривать множество сравнимых между собой элементов кольца $\mathbb{U}$ как некоторый новый элемент, который может быть использован, в дальнейшем, для построения нового множества.

Строение множества сравнимых между собой элементов кольца $\mathbb{U}$ описывается следующей леммой.

Лемма 4.3. *Пусть $\mathbb{U}$ целостное кольцо, m – отличный от нуля элемент кольца $\mathbb{U}$ и a – произвольный элемент кольца $\mathbb{U}$. Рассмотрим множество*

$$\overline{a}_m = \{a + km,\ k \in \mathbb{U}\} \tag{4.1}$$

в котором элемент k пробегает все возможные значения из кольца $\mathbb{U}$. Элемент $b \in \mathbb{U}$ сравним с a тогда и только тогда, когда $b \in \overline{a}_m$.

Доказательство. Если $b \in \overline{a}_m$, то, в силу определения 4.1, найдется такой элемент $k \in \mathbb{U}$, что $b = a + km$ или $b - a = km$. Отсюда следует, что $m|(b-a)$ и $a \equiv b \pmod m$.

Теперь обратное утверждение. Пусть элемент $b \in \mathbb{U}$ сравним с элементом a по модулю m. Тогда $m|(b-a)$ и найдется элемент k кольца $\mathbb{U}$ такой, что $b - a = km$ или $b = a + km$. Последнее равенство говорит о том, что $b \in \overline{a}_m$. □

Определение 4.2. *Пусть m – отличный от нуля элемент целостного кольца $\mathbb{U}$. Множество $\overline{a}_m$, определяемое равенством (4.1), будем называть классом вычетов по модулю m, элементы множества $\overline{a}_m$ — вычетами по модулю m или, просто, вычетами, а элемент $a \in \mathbb{U}$ из равенства (4.1) будем называть представителем класса вычетов $\overline{a}_m$.*

Пример 4.2. Рассмотрим кольцо целых чисел $\mathbb{Z}$ и зафиксируем $m = 15$. Тогда все целые числа вида $3 + 15k$, $k \in \mathbb{Z}$, образуют класс вычетов $\overline{3}_{15}$, представляющий собой бесконечное множество чисел

$$\ldots, -27, -12, 3, 18, 33, \ldots$$

каждое из которых сравнимо с 3 по модулю 15. Легко видеть, что

$$\begin{aligned} -27 &= 3 + 15 \cdot (-2), \\ -12 &= 3 + 15 \cdot (-1), \\ 3 &= 3 + 15 \cdot 0, \\ 18 &= 3 + 15 \cdot 1, \\ 33 &= 3 + 15 \cdot 2, \ldots \end{aligned}$$

Как можно заметить, 3 не является единственным представителем класса вычетов $\overline{3}_{15}$. Действительно, равенства

$$\begin{aligned} -27 &= -12 + 15 \cdot (-1), \\ -12 &= -12 + 15 \cdot 0, \\ 3 &= -12 + 15 \cdot 1, \\ 18 &= -12 + 15 \cdot 2, \ldots \end{aligned}$$

позволяют говорить о том, что $\overline{3}_{15} = \overline{-12}_{15}$.

Наблюдение, сделанное в рамках приведенного примера, может быть оформлено в виде формального утверждения.

Лемма 4.4. *Пусть $\overline{a}_m$ класс вычетов по модулю m, тогда для любого $b \in \overline{a}_m$ выполнено равенство $\overline{b}_m = \overline{a}_m$, т.е. класс вычетов не зависит от выбора своего представителя.*

Доказательство. Пусть $\overline{a}_m = \{a + km,\ k \in \mathbb{U}\}$ и $b = a + km \in \overline{a}_m$.

Рассмотрим произвольный элемент $c \in \overline{a}_m$. Тогда найдется элемент $l \in \mathbb{U}$ такой, что

$$c = a + lm = b - km + lm = b + (k - l)m, \quad k - l \in \mathbb{U}.$$

Из данного равенства следует, что элемент $c \in \overline{b}_m$, следовательно, в силу того, что элемент c был выбран произвольно, множество $\overline{a}_m$ содержится во множестве $\overline{b}_m$.

Аналогично, выбирая произвольный элемент $c \in \overline{b}_m$, $c = b + lm$, где $l \in \mathbb{U}$, получим равенство

$$c = b + lm = a + km + lm = a + (k + l)m, \quad k + l \in \mathbb{U},$$

из которого следует, что $c \in \overline{a}_m$ и включение $\overline{b}_m \subset \overline{a}_m$, следовательно, $\overline{b}_m = \overline{a}_m$. Лемма доказана. □

Из утверждения леммы следует, что любой элемент класса вычетов $\overline{a}_m$ является его представителем.

Определение 4.3. *В кольце целых чисел $\mathbb{Z}$, традиционно, выделяют два вида представителей. Пусть $\overline{a}_m$ – класс вычетов, тогда*

- *если $0 \leqslant a < |m|$, то вычет a называется наименьшим вычетом,*
- *если $-\frac{|m|}{2} < a \leqslant \frac{|m|}{2}$, то вычет a называется абсолютно-наименьшим вычетом.*

Далее, для упрощения используемых обозначений, мы иногда будем опускать нижний индекс, указывающий на значение модуля m, и использовать обозначение $\overline{a}$ вместо $\overline{a}_m$.

Пример 4.3.

1. Рассмотрим кольцо многочленов $\mathbb{Q}[x]$ и зафиксируем многочлен $m(x) = x^2 + 1$. Тогда множество многочленов

$$\overline{x^2} = \{x^2 + k(x)(x^2 + 1),\ k(x) \in \mathbb{Q}[x]\}$$

образует класс вычетов, сравнимых с многочленом x^2 по модулю многочлена $x^2 + 1$. Легко проверить, что многочлены

$$\begin{aligned} -1 &= x^2 + (x^2 + 1) \cdot (-1), \\ x^2 &= x^2 + (x^2 + 1) \cdot 0, \\ \tfrac{3}{2}x^2 + \tfrac{1}{2} &= x^2 + (x^2 + 1) \cdot \tfrac{1}{2}, \\ x^3 + x^2 + x &= x^2 + (x^2 + 1) \cdot x, \end{aligned}$$

принадлежат классу вычетов $\overline{x^2}$.

2. Рассмотрим кольцо целых гауссовых чисел $\mathbb{Z}[i]$ и зафиксируем элемент $m = 1+i$, тогда множество
$$\overline{5} = \{5 + (1+i)k,\ k \in \mathbb{Z}[i]\}$$
образует класс вычетов, сравнимых с 5. Легко видеть, что следующие элементы принадлежат классу вычетов $\overline{5}$ в кольце $\mathbb{Z}[i]$:
$$\begin{aligned} 1 &= 5 + (1+i)\cdot 2(i-1), \\ 4-i &= 5 + (1+i)\cdot(-1). \end{aligned}$$

Как видно из приведенных примеров, существует тесная связь между отношением сравнения двух элементов и операцией деления с остатком в кольце $\mathbb{U}$. Далее будем считать, что кольцо $\mathbb{U}$ – эвклидово.

Лемма 4.5. *Пусть m отличный от нуля элемент эвклидового кольца $\mathbb{U}$. Пусть $a \in \mathbb{U}$ произвольный элемент, а r – остаток от деления элемента a на m, тогда*

1. *элемент a принадлежит классу вычетов $\overline{r}$,*
2. *в случае, если остатков от деления несколько, то все они принадлежат одному классу вычетов.*

Доказательство. Запишем равенство
$$a = qm + r, \quad 0 \leqslant N(r) < N(m),$$
тогда a принадлежит классу $\overline{r}$ в силу определения класса вычетов, как множества элементов кольца $\mathbb{U}$, удовлетворяющих условию (4.1). Из леммы 4.3 также следует, что $a \equiv r \pmod m$.

Пусть в результате деления с остатком были получены два остатка r_1 и r_2, удовлетворяющие равенствам
$$a = q_1 m + r_1, \quad a = q_2 m + r_2,$$
тогда выполнено $r_2 - r_1 = (q_1 - q_2)m$ и мы получаем, что $m|(r_2 - r_1)$. Таким образом выполнено сравнение $r_1 \equiv r_2 \pmod m$ которое, с учетом леммы 4.3, завершает доказательство. □

Утверждение доказанной леммы позволяет предложить способ проверки, принадлежат ли два заданных элемента кольца одному классу вычетов.

Пример 4.4.

1. В кольце целых чисел выполнены равенства

$$\begin{aligned} 37 &= 2 \cdot 14 + 9, \\ -33 &= -3 \cdot 14 + 9, \end{aligned}$$

из которых следует, что $-33, 37 \in \overline{9}_{14}$ и $37 \equiv -33 \pmod{14}$.

2. Рассмотрим кольцо целых гауссовых чисел и элементы $m = 3 - i$ и $\alpha = 2 + 7i$. Из равенств

$$\begin{aligned} 7 + 2i &= (3 - i)(1 + i) + 3, \\ 7 + 2i &= (3 - i)(2 + i) + i, \\ 7 + 2i &= (3 - i)(2 + 2i) + (-1 - 2i). \end{aligned}$$

и утверждения леммы 4.5 следует, что величины $3, i$ и $-1-2i$ принадлежат одному классу вычетов. Это также следует из равенств

$$\begin{aligned} 3 - i &= 1 \cdot (3 - i), \\ -1 - 2i - i &= -i \cdot (3 - i). \end{aligned}$$

Вернемся к вопросу о построении нового множества, состоящего из классов вычетов. Нам потребуется следующая лемма.

Лемма 4.6. *Пусть $\mathbb{U}$ эвклидово кольцо и $m \in \mathbb{U}$ отличный от нуля элемент. Тогда каждый элемент кольца $\mathbb{U}$ принадлежит только одному классу вычетов по модулю m.*

Доказательство. Пусть элемент c принадлежит двум классам вычетов $\overline{a}$ и $\overline{b}$. Тогда найдутся такие $k, l \in \mathbb{U}$, что $c = a + km = b + lm$, следовательно $b - a = (k - l)m$ и $m|(b - a)$. Таким образом мы получили, что $a \equiv b \pmod{m}$ и, согласно первому утверждению леммы 4.1 и утверждению леммы 4.3, классы вычетов $\overline{a}$ и $\overline{b}$ совпадают. □

Из утверждения леммы следует, что классы вычетов образуют непересекающиеся подмножества кольца $\mathbb{U}$, объединение которых образует все кольцо $\mathbb{U}$.

Определение 4.4. *Пусть $\mathbb{U}$ эвклидово кольцо и $m \in \mathbb{U}$ отличный от нуля элемент. Мы будем обозначать множество классов вычетов кольца $\mathbb{U}$ по модулю m символом $\mathbb{U}/(m)$, например*

$$\mathbb{Z}/(15), \quad \mathbb{Q}[x]/(x^2 + 1), \quad \mathbb{Z}[i]/(1 + 2i).$$

В ряде случаев, для упрощения записи, мы будем использовать символ $\mathbb{U}_m$, в частности, для множества классов вычетов по модулю целого числа m будем использовать обозначение $\mathbb{Z}_m$.

Пусть $a, b \in \mathbb{U}$ два элемента, не сравнимые между собой по модулю m. Из леммы 4.3 следует, что классы вычетов $\overline{a}, \overline{b} \in \mathbb{U}/(m)$ различны. Определим для данных классов операции сложения и умножения

$$\overline{c} = \overline{a} + \overline{b}, \quad \overline{d} = \overline{a} \cdot \overline{b}, \tag{4.2}$$

где представители классов $\overline{c}$, $\overline{d}$ определяются условиями

$$c \equiv a + b \pmod{m}, \quad d \equiv ab \pmod{m}.$$

Теорема 4.1. *Пусть $\mathbb{U}$ эвклидово кольцо и $m \in \mathbb{U}$ отличный от нуля элемент. Множество классов вычетов $\mathbb{U}/(m)$ образует кольцо, относительно операций сложения и умножения, определенных равенствами (4.2).*

Доказательство. Для доказательства теоремы нам необходимо проверить выполнимость всех свойств определения 1.15. Начнем с операции сложения и рассмотрим два класса $\overline{a}$, $\overline{b}$, заданных своими представителями a, b и, используя операцию деления с остатком, определим элемент c равенством

$$a + b = qm + c.$$

Тогда $c \equiv a + b \pmod{m}$ и класс вычетов $\overline{c}$ является суммой классов $\overline{a}$ и $\overline{b}$. В силу коммутативности кольца $\mathbb{U}$ получаем равенства $b + a = a + b = qm + c$ и

$$\overline{a} + \overline{b} = \overline{b} + \overline{a},$$

т.е. коммутативность введенной нами операции сложения.

Пусть 0 – нейтральный элемент кольца $\mathbb{U}$ относительно операции сложения. Рассмотрим класс вычетов $\overline{0} = \{c \cdot m,\ c \in \mathbb{U}\}$, состоящий из всех элементов кольца, делящихся на m. Тогда $a \equiv a + 0 \pmod{m}$ и мы получаем, что класс $\overline{0}$ является нейтральным классом, относительно введенной нами операции сложения в $\mathbb{U}/(m)$.

Аналогично, из равенства $0 \equiv a + (-a) \pmod{m}$, выполненного для любого отличного от нуля $m \in \mathbb{U}$, мы получаем, что класс $\overline{-a}$ является обратным к классу $\overline{a}_m$, относительно введенной нами операции сложения в $\mathbb{U}/(m)$.

Теперь рассмотрим операцию умножения классов и определим элемент d равенством

$$ab = s \cdot m + d$$

для некоторого $s \in \mathbb{U}$. Выполнено равенство $d \equiv ab \pmod{m}$ из которого следует, что $\overline{a} \cdot \overline{b} = \overline{d}$. Из коммутативности операции умножения в кольце $\mathbb{U}$ следует коммутативность операции умножения в $\mathbb{U}/(m)$.

Пусть 1 – нейтральный элемент кольца $\mathbb{U}$ относительно операции умножения, тогда из сравнения $a \cdot 1 \equiv a \pmod m$ следует, что класс вычетов $\overline{1} = \{1 + k \cdot m,\ k \in \mathbb{U}\}$, является нейтральным классом, относительно введенной нами операции умножения в $\mathbb{U}/(m)$.

Нам осталось проверить дистрибутивность введенных операций сложения и умножения. В силу дистрибутивности кольца $\mathbb{U}$ мы можем записать равенства

$$c(a+b) = ca + cb = qm + r$$

из которых следуют сравнения $c(a+b) \equiv r \pmod m$ и $ca+cb \equiv r \pmod m$, следовательно, класс вычетов $\overline{r}$ совпадает как с классом $\overline{c}(\overline{a}+\overline{b})$, так и с классом $\overline{c}\cdot\overline{a} + \overline{c}\cdot\overline{b}$. Теорема доказана. □

Проиллюстрируем утверждение теоремы численным примером.

Пример 4.5. Рассмотрим кольцо вычетов $\mathbb{Z}/(12)$ и выберем в нем два класса

$$\begin{array}{rcccl} \overline{1} & = & \{\ldots, -11, 1, 13, 25, \ldots\} & = & \{1 + 12k,\ k \in \mathbb{Z}\}, \\ \overline{-2} & = & \{\ldots, -14, -2, 10, 22, \ldots\} & = & \{-2 + 12k,\ k \in \mathbb{Z}\}, \end{array}$$

тогда $1 + (-2) \equiv 11 \pmod{12}$ и сумма рассмотренных классов есть

$$\overline{11} \quad = \quad \{\ldots, -13, -1, 11, 23, \ldots\} \quad = \quad \{11 + 12k,\ k \in \mathbb{Z}\}.$$

Аналогично, $1 \cdot (-2) \equiv 10 \pmod{12}$ и произведение рассмотренных классов есть

$$\overline{10} \quad = \quad \{\ldots, -14, -2, 10, 22, \ldots\} \quad = \quad \{-2 + 12k,\ k \in \mathbb{Z}\},$$

Докажем несколько дополнительных утверждений, описывающих свойства построенного кольца вычетов.

Теорема 4.2. *Пусть $\mathbb{U}$ эвклидово кольцо и $m \in \mathbb{U}$ отличный от нуля, неразложимый элемент кольца. Тогда, множество классов вычетов $\mathbb{U}/(m)$ образует поле.*

Доказательство. Пусть $\overline{a} = \{a + km,\ k \in \mathbb{U}\}$ произвольный класс вычетов. Из утверждения теоремы 4.1 следует, что $\mathbb{U}/(m)$ – кольцо, поэтому нам осталось показать, что найдется класс вычетов $(\overline{a})^{-1}$ такой, что $\overline{a} \cdot (\overline{a})^{-1} = \overline{1}$ относительно операции умножения, определенной равенством (4.2).

Поскольку m неразложимый элемент кольца, то из утверждения леммы 3.2 следует, что $\mathbf{НОД}(a,\ m) \sim 1$. Тогда, согласно соотношению Безу, см. соотношение 2.4.A, найдутся элементы $u, v \in \mathbb{U}$ такие, что

$$au + mv = \varepsilon, \quad \varepsilon \in \mathbb{U}^*.$$

Домножая правую и левую части на ε^{-1} получим равенства

$$au\varepsilon^{-1} + mv\varepsilon^{-1} = 1 \quad \text{или} \quad mv\varepsilon^{-1} = 1 - au\varepsilon^{-1}.$$

Таким образом, $m|(1 - au\varepsilon^{-1})$ и, согласно определению 4.1, выполнено $au\varepsilon^{-1} \equiv 1 \pmod m$. Из данного сравнения следует, что элемент $u\varepsilon^{-1}$ является представителем класса вычетов $(\overline{a})^{-1}$ и $\overline{a} \cdot (\overline{a})^{-1} = \overline{1}$. Теорема доказана. □

В случае, когда m – разложимый элемент кольца $\mathbb{U}$, кольцо классов вычетов $\mathbb{U}/(m)$ не является целостным кольцом, т.е. содержит в себе делители нуля. Действительно, пусть $p \in \mathbb{U}$ – собственный делитель элемента m, тогда $m = pq$ и, согласно первому утверждению леммы 3.1, q также является собственным делителем элемента m.

Рассмотрим два класса вычетов

$$\overline{p}_m = \{p + km,\ k \in \mathbb{U}\}, \quad \overline{q}_m = \{q + lm,\ l \in \mathbb{U}\}.$$

Тогда, воспользовавшись равенствами (4.2), определим класс $\overline{p}_m \cdot \overline{q}_m$, для которого выполнено равенство

$$\overline{p}_m \cdot \overline{q}_m = \{pq + km,\ k \in \mathbb{U}\} = \{km,\ k \in \mathbb{U}\} = \overline{0}.$$

Таким образом, классы $\overline{p}_m$ и $\overline{q}_m$ являются делителями нуля.

Нам также потребуется теорема, которая описывает случаи, в которых кольцо $\mathbb{U}/(m)$ конечно, т.е. содержит в себе лишь конечное число классов вычетов.

Теорема 4.3. *Пусть $\mathbb{U}$ эвклидово кольцо и $m \in \mathbb{U}$ отличный от нуля элемент. Если в кольце $\mathbb{U}$ найдется лишь конечное число элементов r, удовлетворяющих условию $0 \leqslant N(r) < N(m)$, то кольцо $\mathbb{U}/(m)$ также конечно.*

Доказательство. Рассмотрим произвольный элемент кольца $a \in \mathbb{U}$. Используя операцию деления с остатком запишем равенство

$$a = qm + r, \quad 0 \leqslant N(r) < N(m).$$

Тогда, из первого утверждения леммы 4.5 следует, что $a \equiv r \pmod m$, и элемент a содержится в классе вычетов, представителем которого является элемент r. Поскольку количество элементов с ограниченной нормой конечно, то конечно и число классов вычетов кольца $\mathbb{U}/(m)$ также конечно. □

Пример 4.6. Легко заметить, что в кольце целых чисел $\mathbb{Z}$ лишь конечное число целых чисел r удовлетворяют неравенству $0 \leqslant N(r) < N(m)$. Этими числами являются:

$$-m+1, \ldots, -1, 0, 1, \ldots, m-1.$$

В кольце целых гауссовых чисел $\mathbb{Z}[i]$ также найдется лишь конечное число элементов $r = a + bi$ таких, что $N(r) = a^2 + b^2 < N(m)$. Вместе с тем, в кольце многочленов от одной переменной $\mathbb{Q}[x]$ существует бесконечное число элементов, удовлетворяющих неравенству $0 \leqslant N(r) < N(m)$. Действительно, такими элементами являются многочлены $r(x) = \sum_{k=0}^{n} a_k x^k$, определяемые для любого целого n такого что $0 \leqslant n < N(m)$ и произвольных элементов $a_k \in \mathbb{Q}$.

Пусть n – натуральное число и $r_1, \ldots, r_n$ различные элементы кольца $\mathbb{U}$, удовлетворяющие неравенству $0 \leqslant N(r_n) < N(m)$. Из утверждения теоремы следует, что найдется не более n различных классов вычетов по модулю m. Действительно, из условия $r_i \equiv r_j \pmod m$, $i, j \in \{1, \ldots, n\}$, будет следовать, что r_i, r_j являются представителями одного и того же класса вычетов.

Следствие 4.3.А. *Пусть m отличное от нуля целое число, тогда число классов вычетов в $\mathbb{Z}/(m)$ в точности равно $N(m)$.*

Доказательство. Из теоремы 2.1 следует, что для каждого целого числа a найдется остаток r от деления на m такой, что $0 \leqslant r < |m| = N(m)$. Тогда, мы можем в явном виде выписать m целых чисел

$$0, 1, \ldots, m-1,$$

которые являются различными элементами кольца $\mathbb{Z}$ и, следовательно, представителями различных классов вычетов. Предположим, что это не так, тогда найдутся индексы i и j такие, что $0 \leqslant j \leqslant i < |m|$ и

$$i \equiv j \pmod m.$$

Тогда, в силу определения отношения сравнимости, $m|(j-i)$, т.е. выполнено равенство $mk = i - j$ для некоторого целого k. Поскольку в правой части равенства находится неотрицательное целое число $i - j$, меньшее m, то равенство возможно только в случае, когда $i = j$. □

Отметим, что в кольце целых гауссовых чисел аналогичное утверждение неверно.

Пример 4.7. Рассмотрим кольцо $\mathbb{Z}[i]$ и элемент $m = 2 - 2i$, норма которого удовлетворяет равенству $N(2-2i) = 8$. Согласно таблице 3.1 элементами кольца, имеющими меньшую норму, являются

$$0,\ 1,\ 1+i,\ 2,\ 1+2i,\ 2+i,$$

а также ассоциированные с ними – всего 21 элемент кольца $\mathbb{Z}[i]$. Все остальные элементы при делении на $2-2i$ должны давать в остатке одно из перечисленных значений, например, из равенств

$$1+3i = i(2-2i) - 1 + i, \quad 3+4i = 2i(2-2i) - 1$$

следует, что $1+3i \equiv -1+i \pmod{2-2i}$ и $3+4i \equiv -1 \pmod{2-2i}$. С другой стороны, из равенств

$$\begin{aligned} 2 &\equiv 2i \pmod{2-2i}, \\ -2 &\equiv -2i \pmod{2-2i}, \\ (1+2i)\varepsilon = i\varepsilon(2-2i) - \varepsilon &\equiv -\varepsilon \pmod{2-2i}, \\ (2+i)\varepsilon = i\varepsilon(2-2i) - i\varepsilon &\equiv -i\varepsilon \pmod{2-2i}, \end{aligned}$$

выполненных для любого обратимого элемента $\varepsilon \in \{1, -1, i, -i\}$, следует, что найдется только 11 несравнимых между собой по модулю $2-2i$ элементов кольца $\mathbb{Z}[i]$:

$$0,\ 1,\ -1,\ i,\ -i,\ 1+i,\ -1-i,\ -1+i,\ 1-i,\ 2,\ -2.$$

Таким образом, выполнено равенство $|\mathbb{Z}[i]/(2-2i)| = 11$.

Задачи и упражнения

1. Используя утверждения леммы 4.1, упростите сравнения:

$$148 \equiv -5 \pmod{17}, \ 8a^2 + 10 \equiv 8a + 12 \pmod{11}.$$

2. Принадлежат ли одному классу вычетов по модулю 17 следующие целые числа: 2131, 1197 и 171?

3. Принадлежат ли одному классу вычетов по модулю $3-i$ следующие элементы кольца целых гауссовых чисел $3, i$ и $-1-2i$?

4. Какие из перечисленных множеств являются полем

$$\mathbb{Z}/(119),\ \mathbb{Z}/(2^{16}+1),\ \mathbb{Q}[x]/(x^2+2),\ \mathbb{Z}[i]/(4-i),\ \mathbb{Z}[i]/(17)?$$

5. Вычислите $|\mathbb{Z}/(16)|$, $|\mathbb{Z}[i]/(1+2i)|$ и $|\mathbb{Z}[i]/(3)|$.

Рекомендации к сдаче экзамена

В данной главе мы определили новое множество $\mathbb{U}/(m)$ – кольцо классов вычетов по модулю отличного от нуля элемента m эвклидового кольца $\mathbb{U}$. Это позволяет нам дополнить схему, изображенную на рисунке 1.1, следующим образом.

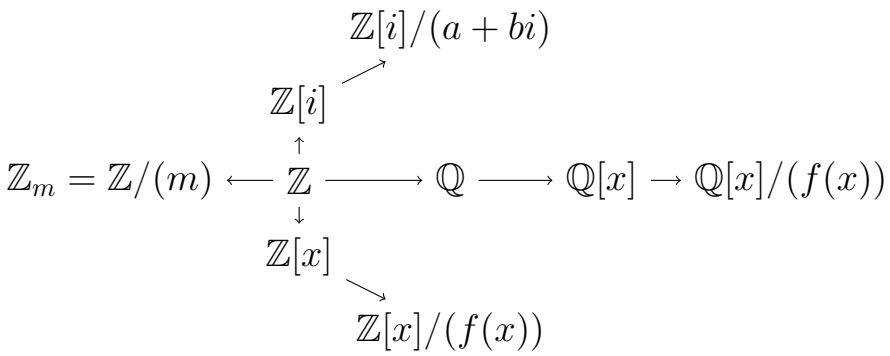


Рис. 4.1: Зависимости основных классов вычетов.

В экзаменационные билеты по курсу «Введение в теорию чисел» входят следующие вопросы.

- Лемма об арифметических свойствах операции сравнения (лемма 4.1).

  В рамках ответа на данный вопрос необходимо дать определение операции сравнения двух элементов эвклидового кольца $\mathbb{U}$, а также доказать все утверждения леммы 4.1.

- Понятие класса вычетов, их свойства.

  В ответ на данный вопрос входят формулировки и доказательства лемм 4.2, 4.3 и 4.4.

  В начале рассматривается отношение эквивалентности на некотором подмножестве эвклидового кольца $\mathbb{U}$, см. лемму 4.2, что позволяет рассматривать это помножество как один новый элемент (класс вычетов), потом определяется явный вид данного подмножества элементов, см. лемму 4.3. В заключение доказывается, что любой элемент из рассматриваемого подмножества однозначно определяет это подмножество, т.е. является его представителем, см. лемму 4.4.

- Теорема о кольце классов вычетов (теорема 4.1).

  Перед доказательством основной теоремы необходимо доказать леммы 4.5 и 4.6. После чего, доказательство теоремы 4.1 сводится к проверке выполнения свойств, которым удовлетворяет кольцо, см. определение 1.15.

- Теоремы о свойствах колец классов вычетов.

  В рамках ответа на данный вопрос необходимо сформулировать и доказать теоремы 4.2, 4.3, а также следствие 4.3.A.

Схема зависимостей между утверждениями, доказанными в 4-й главе, изображена на рисунке 4.2.

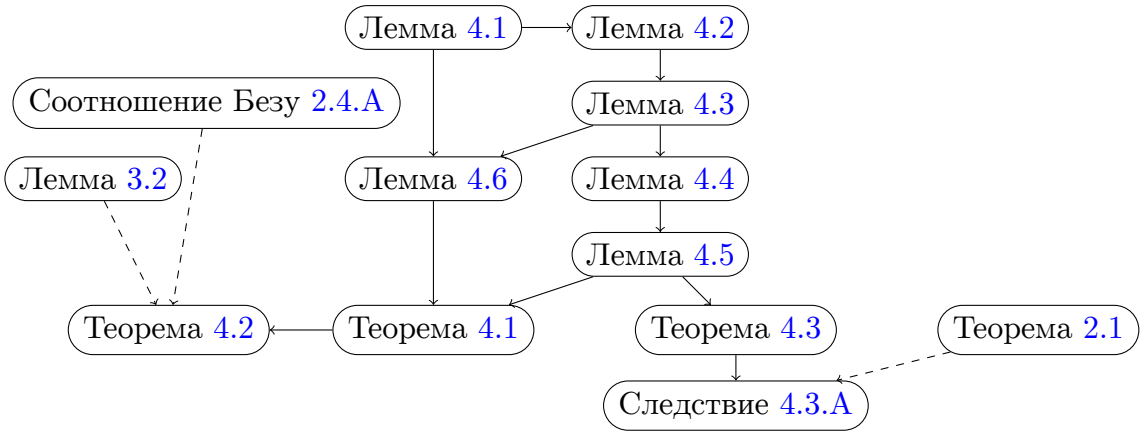


Рис. 4.2: Схема зависимостей между утверждениями 4-й главы.

Дополнительная литература к 4-й главе

1. ван дер Варден Б. Л. *Алгебра*. – М.: Мир, 1976. – 648 с.

глава 5

Полиномиальные сравнения

Кольца многочленов с коэффициентами из классов вычетов – Сравнения первой степени – Китайская теорема об остатках – Алгоритм Гарнера – Сравнения старших степеней – Поиск корней многочленов по составному модулю – Теорема о подъеме решения – Поиск корней многочленов по простому модулю.

Пусть $\mathbb{Z}_m = \mathbb{Z}/(m)$ кольцо вычетов по модулю целого, отличного от нуля числа m. Аналогично тому, как мы делали это в первой главе, см. определение 1.18, рассмотрим кольцо многочленов $\mathbb{Z}_m[x]$ от одной переменной. Предметом нашего дальнейшего исследования будут элементы кольца $\mathbb{Z}_m[x]$, т.е. многочлены

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n, \ldots, a_0 \in \mathbb{Z}_m,$$

коэффициенты которых являются вычетами по модулю m.

Пример 5.1. Рассмотрим многочлен $f(x) = x^3 + 5x^2 + 12x + 18$, принадлежащий кольцу $\mathbb{Z}_4[x]$. Коэффициенты этого многочлена: $1, 5, 12$ и 18 являются различными представителями классов вычетов по модулю 4. Тогда, выбирая в каждом классе вычетов наименьший вычет, см. определение 4.3, можно записать равенство многочленов в кольце $\mathbb{Z}_4[x]$

$$x^3 + 5x^2 + 12x + 18 = x^3 + x^2 + 2.$$

Также мы будем использовать запись в виде сравнения

$$x^3 + 5x^2 + 12x + 18 \equiv x^3 + x^2 + 2 \pmod 4,$$

акцентируя внимание на кольце классов вычетов, которому принадлежат коэффициенты многочлена $f(x)$.

Для сохранения общности мы также будем рассматривать общий случай, т.е. кольцо многочленов $\mathbb{U}_m[x]$, где $\mathbb{U}_m = \mathbb{U}/(m)$ кольцо классов вычетов эвклидового кольца $\mathbb{U}$ по модулю отличного от нуля элемента $m \in \mathbb{U}$.

Пример 5.2. Рассмотрим многочлен

$$f(x) = 2ix^2 + 5x + (-2 + 3i) \in \mathbb{U}_m[x],$$

коэффициенты которого принадлежат кольцу вычетов $\mathbb{U}_m = \mathbb{Z}[i]/(1 + 2i)$.

Учитывая, что выполнены сравнения

$$\begin{aligned} 2i &\equiv -1 = i^2 \pmod{1+2i}, \\ 5 &\equiv 0 \pmod{1+2i}, \\ -2+3i &\equiv 2i = (1+i)^2 \pmod{1+2i}, \end{aligned}$$

можно записать сравнение

$$f(x) = 2ix^2 + 5x + (-2+3i) \equiv i^2x^2 + (1+i)^2 = (1+i-x)(1+i+x) \pmod{1+2i}$$

из которого следует, в частности, что многочлен $f(x)$ является разложимым элементом кольца $\mathbb{U}_m[x]$.

Далее нас будет интересовать вопрос о нахождении корней многочленов с коэффициентами из кольца классов вычетов $\mathbb{U}_m$. В начале дадим формальное определение.

Определение 5.1. *Пусть $\mathbb{U}$ произвольное кольцо. Элемент $e \in \mathbb{U}$ называется корнем или нулем многочлена $f(x) \in \mathbb{U}[x]$, если $f(e) = 0$.*

В интересующем нас случае, нулем многочлена, если он существует, является e – класс вычетов по модулю m, удовлетворяющий сравнению

$$f(e) \equiv 0 \pmod{m}, \text{ где } f(x) \in \mathbb{U}_m[x].$$

5.1 Сравнения первой степени

Начнем с самого простого случая и рассмотрим многочлен $f(x)$ первой степени. Если $f(x) = x - b \in \mathbb{V}[x]$, то сравнение $f(x) \equiv 0 \pmod{m}$ принимает вид

$$x \equiv b \pmod{m},$$

а его решением, т.е. нулем многочлена $f(x)$, является класс $e \in \mathbb{V}$, определяемый равенством

$$e = \overline{b}_m = \{b + km,\ k \in \mathbb{U}\}.$$

Теперь рассмотрим произвольный многочлен первой степени

$$f(x) = ax - b \in \mathbb{V}[x], \quad \text{где} \quad a \not\equiv 0 \pmod{m},$$

и сравнение $f(x) \equiv 0 \pmod{m}$, которое может быть записано в виде

$$ax \equiv b \pmod{m}. \tag{5.1}$$

Верна следующая теорема.

Теорема 5.1. *Пусть* $\mathbb{U}$ *эвклидового кольцо и* a, b, m *элементы кольца* $\mathbb{U}$ *такие, что* a, m *отличны от нуля. Тогда количество классов вычетов, удовлетворяющих сравнению (5.1), равно*

1. *единице, если* $1 \sim \mathbf{НОД}(a,\ m)$,
2. *числу классов вычетов по модулю* $d = \mathbf{НОД}(a,\ m)$, *если* $d|b$,
3. *в противном случае сравнение неразрешимо.*

Доказательство. Начнем с первого утверждения теоремы. Допустим, что выполнено условие $\mathbf{НОД}(a,\ m) \sim 1$ и покажем, что в этом случае найдется класс вычетов по модулю m, удовлетворяющий сравнению (5.1).

Воспользуемся соотношением Безу (см. соотношение 2.4.A) и найдем $u, v \in \mathbb{U}$ такие, что

$$au + mv \sim \mathbf{НОД}(a,\ m)\,.$$

Тогда, учитывая, что $\mathbf{НОД}(a,\ m) \sim 1$, найдется $\varepsilon \in \mathbb{U}^*$ такой, что

$$au + mv = \varepsilon \quad \text{или} \quad au\varepsilon^{-1} = 1 - mv\varepsilon^{-1}.$$

Следовательно, $au\varepsilon^{-1} \equiv 1 \pmod m$ и, домножая правую и левую части последнего сравнения на b, получим, что класс вычетов, представителем которого является $ub\varepsilon^{-1}$, удовлетворяет сравнению (5.1).

Покажем, что такой класс единственен. Для это предположим обратное, т.е. то, что найдутся два различных класса вычетов, удовлетворяющих сравнению (5.1). Обозначим эти классы вычетов следующим образом

$$\overline{x}_1 = \{x_1 + k_1 m,\ k_1 \in \mathbb{U}\}, \quad \overline{x}_2 = \{x_2 + k_2 m,\ k_2 \in \mathbb{U}\}.$$

Поскольку данные классы удовлетворяют сравнению (5.1), то для любых двух представителей x_1, x_2 будет выполнено сравнение

$$ax_1 \equiv b \equiv ax_2 \pmod m\,.$$

Следовательно, в силу определения операции сравнения, выполнено равенство

$$m|ax_1 - ax_2 = a(x_1 - x_2),$$

и найдется такой элемент $u \in \mathbb{U}$, что $mu = a(x_1 - x_2)$. Поскольку $\mathbf{НОД}(a,\ m) \sim 1$, то из утверждения леммы 2.6 следует, что $m|(x_1 - x_2)$, и найдется элемент $v \in \mathbb{U}$ такой, что

$$mv = x_1 - x_2, \quad \text{или} \quad x_1 = x_2 + vm.$$

Тогда x_1 принадлежит классу вычетов $\overline{x}_2$ по модулю m и является его представителем, следовательно, в силу леммы 4.4, классы вычетов совпадают. Первое утверждение доказано.

Пусть $\mathbf{НОД}(a,\ m) = d$, тогда из шестого утверждения леммы 4.1 следует, что элемент d должен делить элемент b. Если это условие не выполнено, то сравнение (5.1) неразрешимо.

Теперь будем считать, что $d|b$. Определим элементы $a_1, b_1, m_1 \in \mathbb{U}$ равенствами

$$a = a_1 d, \quad b = b_1 d, \quad m = m_1 d.$$

Тогда из четвертого утверждения леммы 4.1 следует, что сравнение $a_1 x \equiv b_1 \pmod{m_1}$ разрешимо. Поскольку $\mathbf{НОД}(a_1,\ m_1) \sim 1$, то, в силу первого утверждения теоремы, это сравнение имеет единственное решение $\overline{x}_{m_1}$ – класс вычетов по модулю m_1

$$\overline{x}_{m_1} = \{x + l m_1,\ l \in \mathbb{U}\}. \tag{5.2}$$

Выберем произвольный элемент кольца $l \in \mathbb{U}$ и зафиксируем элемент $x_l = x + lm$ – некоторый представитель класса вычетов $\overline{x}_{m_1}$. Поскольку выполнено сравнение $a_1 x \equiv b_1 \pmod{m_1}$, то найдется элемент $k \in \mathbb{U}$ такой, что $a_1 x_l = b_1 + k m_1$, тогда

$$\begin{aligned} a x_l = a_1 d x_l = a_1 d(x + l m_1) = \\ = d a_1 x + l m_1 d = d(b_1 + k m_1) + l m_1 d = b + (k + l)m, \end{aligned}$$

т.е. выполнено сравнение

$$a x_l \equiv b \pmod{m}$$

и x_l является представителем класса вычетов, удовлетворяющего сравнению (5.1). Нам осталось определить, сколько различных классов вычетов по модулю m содержится в определяемом равенством (5.2) множестве $\overline{x}_{m_1}$.

В силу свойств кольца $\mathbb{U}$ найдется натуральное число n и конечное число элементов $r_1, \ldots, r_n \in \mathbb{U}$, являющихся остатками от деления на d и представителями различных классов вычетов по модулю d, т.е.

$$r_i \not\equiv r_j \pmod{d}, \quad \text{при} \quad i \neq j.$$

Теперь, используя операцию деления с остатком, для любого элемента $l \in \mathbb{U}$ можно определить элементы $q, r_i \in \mathbb{U}$, удовлетворяющие равенству $l = qd + r_i$, $0 \leqslant N(r_i) < N(d)$, для некоторого индекса i. Следовательно, для любого элемента из множества (5.2), выполнено равенство

$$x_l = x + l m_1 = x + (qd + r_i)m_1 = (x + r_i m_1) + qm,$$

т.е.

$$x_l \equiv x + r_i m_1 \pmod{m}.$$

Предположим, что найдутся два различных индекса $i, j \in \{1, \ldots, n\}$ такие, что

$$x + r_i m_1 \equiv x + r_j m_1 \pmod{m},$$

тогда, учитывая второе утверждение леммы 4.1, получим сравнение

$$r_i m_1 \equiv r_j m_1 \pmod{m},$$

что равносильно условию $m | m_1(r_i - r_j)$. Учитывая равенство $m = dm_1$, мы можем считать, что найдется элемент $v \in \mathbb{U}$ такой, что

$$dm_1 v = mv = m_1(r_i - r_j), \quad \text{или} \quad d|(r_i - r_j).$$

Из последнего условия следует, что $r_i \equiv r_j \pmod{d}$, а это противоречит выбору остатков $r_1, \ldots, r_n$. Следовательно, все величины $x + r_i m_1$, $i = 1, \ldots, n$ принадлежат различным классам по модулю m. Что и требовалось доказать. □

Утверждения доказанной теоремы целесообразно проиллюстрировать несколькими примерами.

Пример 5.3.

1. Поскольку в кольце целых чисел выполнено условие $\mathbf{НОД}(5,\ 7) = 1$, то сравнение $5x \equiv 2 \pmod 7$ имеет единственное решение $e \equiv 6 \pmod 7$.

   Легко проверить, что любое целое число из класса вычетов $\overline{6} = \{6 + 7k,\ k \in \mathbb{Z}\}$ удовлетворяет целочисленному равенству

   $$5 \cdot (6 + 7k) = 2 + 7 \cdot (k + 4),$$

   т.е. действительно является решением заданного сравнения.

2. Рассмотрим сравнение $6x \equiv 15 \pmod{21}$, которому удовлетворяет несколько классов вычетов. Действительно, из условий $\mathbf{НОД}(6,\ 21) = 3$ и $3|15$ следует, что найдутся три класса вычетов, удовлетворяющих данному сравнению.

   Разделив $6, 15$ и 21 на величину наибольшего общего делителя, получим сравнение $2x \equiv 5 \pmod 7$, которому удовлетворяет класс вычетов $e \equiv 6 \pmod 7$. Записывая данный класс как множество чисел, получим равенства

   $$x = \{6 + 7k,\ k \in \mathbb{Z}\} = \{6 + 7(3l + r_j)\} = \{6 + 7r_j + 21l,\ l \in \mathbb{Z}\} \text{ и } r_j \in \{0, 1, 2\},$$

   которые дает нам три класса вычетов по модулю 21, удовлетворяющих заданному сравнению, т.е.

   $$\{6 + 21l,\ l \in \mathbb{Z}\}, \quad \{13 + 21l,\ l \in \mathbb{Z}\}, \quad \{20 + 21l,\ l \in \mathbb{Z}\}.$$

Пример 5.4.

1. Рассмотрим сравнение в кольце целых гауссовых чисел $6x \equiv -1+i \pmod{3-i}$. Для поиска классов вычетов, удовлетворяющих данному сравнению заметим, что

$$\begin{aligned} 6 &= (1+i)(1-i)3, \\ -1+i &= (1+i)i, \\ 3-i &= (1+i)(1-2i). \end{aligned}$$

Воспользовавшись таблицей 3.1 заметим, что элементы $1+i, 1-i, 1-2i$ и 3 являются неразложимыми элементами кольца $Z[i]$, следовательно,

$$\textbf{НОД}\,(6,\ 3-i) = 1+i, \quad \text{и} \quad (1+i)|(-1+i).$$

Воспользовавшись утверждением теоремы 5.1 избавимся от общего множителя и запишем сравнение

$$3(1-i)x \equiv i \pmod{1-2i}.$$

Замечая, что выполнено равенство $3-3i = (2+i)(1-2i)-1$, перепишем полученное сравнение, приводя коэффициент при переменной x по модулю $1-2i$,

$$-x \equiv i \pmod{1-2i}.$$

Теперь легко видеть, что классом вычетов, удовлетворяющим полученному сравнению, является класс $e \equiv -i \pmod{1-2i}$.

Записывая данный класс как множество элементов кольца целых гауссовых чисел получим равенства

$$\begin{aligned} e = \{-i+(1-2i)k,\ k \in \mathbb{Z}[i]\} = \{-i+(1-2i)\left((1+i)l+r_j\right),\ l \in \mathbb{Z}[i]\} = \\ = \{(1-2i)r_j - i + (3-3i)l,\ l \in \mathbb{Z}[i]\}, \end{aligned}$$

где $r_j \in \{0,1,i\}$ – остатки от деления на $1+i$, принадлежащие различным классам вычетов по модулю $1+i$. Полученные равенства описывают три класса вычетов, удовлетворяющих исходному сравнению.

2. В заключение, рассмотрим сравнение в кольце многочленов

$$2(x^5-x^2+x-1)e(x) \equiv (x-1)^2 \pmod{x^3-1}.$$

и найдем $e(x)$ — один или несколько классов вычетов кольца $\mathbb{Q}[x]/(x^3-1)$, удовлетворяющих указанному сравнению.

Начнем с того, что воспользуемся равенствами

$$x^5-x^2+x-1 = x^2(x^3-1)+x-1, \quad x^3-1 = (x-1)(x^2+x+1)$$

и запишем исходное сравнение в виде

$$2(x-1)e(x) \equiv (x-1)^2 \pmod{(x-1)(x^2+x+1)}.$$

Сокращая на наибольший общий делитель $d = \textbf{НОД}\,(2(x-1),\ x^3-1) = x-1$ правую, левую части сравнения, а также модуль, получим сравнение

$$2e(x) \equiv (x-1) \pmod{x^2+x+1} \quad \text{и} \quad \textbf{НОД}\,(2,\ x^2+x+1) \sim 1.$$

Для того, чтобы определить класс вычетов $e(x)$, удовлетворяющий приведенному сравнению, заметим, что выполнено соотношение Безу

$$2\left(x^2+x+\frac{3}{2}\right)-2(x^2+x+1)=1.$$

Тогда

$$2\left(x^2+x+\frac{3}{2}\right)\equiv 1 \pmod{x^2+x+1}$$

и

$$2(x-1)\left(x^2+x+\frac{3}{2}\right)\equiv (x-1) \pmod{x^2+x+1}.$$

Из последнего сравнения следует, что

$$e(x)=(x-1)\left(x^2+x+\frac{3}{2}\right)+k(x)(x^2+x+1)=$$
$$=\frac{1}{2}(x-1)+(k(x)+(x-1))(x^2+x+1)$$

для любого $k(x)\in\mathbb{Q}[x]$, т.е

$$e(x)\equiv\frac{1}{2}(x-1) \pmod{x^2+x+1}.$$

Теперь мы можем определить классы вычетов, удовлетворяющие исходному сравнению. Поскольку остатком от деления на многочлен $d(x)=x-1$ может быть любой элемент поля рациональных чисел $\mathbb{Q}$, то класс вычетов по модулю x^3-1, удовлетворяющий исходному сравнению имеет вид

$$e(x)=\frac{1}{2}(x-1)+k(x)(x^2+x+1)=$$
$$=\frac{1}{2}(x-1)+(l(x)(x+1)+q)(x^2+x+1)=$$
$$=\frac{1}{2}(x-1)+q(x^2+x+1)+l(x)(x^3-1)$$

для любого $q\in\mathbb{Q}$. Таким образом, мы получили бесконечное множество классов, удовлетворяющих исходному сравнению, которые, кратко, можно определить сравнением

$$e(x)\equiv\frac{1}{2}(x-1)+q(x^2+x+1) \pmod{x^3-1}, \quad q\in\mathbb{Q}.$$

Многочисленные примеры говорят о том, что можно предъявить простой алгоритм поиска классов вычетов, удовлетворяющих сравнению (5.1)

$$ax\equiv b \pmod{m}.$$

Алгоритм заключается в следующей последовательности шагов.

1. Необходимо вычислить $d=\mathbf{НОД}(a,\ m)$.

2. Если d не делит элемент b, то классов вычетов, удовлетворяющих сравнению (5.1), не существует и алгоритм завершает свою работу.

3. Определить элементы a_1, b_1, m_1 равенствами

$$a = a_1 d, \quad b = b_1 d, \quad m = m_1 d.$$

4. Используя соотношение Безу, см. соотношение 2.4.A, определить элементы $u, v \in \mathbb{U}$ такие, что

$$a_1 u + m_1 v = 1.$$

5. Определить класс вычетов $e \equiv u b_1 \pmod{m_1}$.

6. Если $d \in \mathbb{U}^*$, т.е. элементы a и m являются взаимно-простыми элементами кольца $\mathbb{U}$, то алгоритм завершает свою работу.

7. Необходимо определить $r_1, r_2, \ldots$ – все попарно несравнимые между собой по модулю d остатки от деления на d и определить классы вычетов, удовлетворяющие сравнению (5.1), сравнениями

$$e \equiv u b_1 + r_i m_1 \pmod{m}, \quad i = 1, 2, \ldots$$

Применительно к кольцу целых чисел $\mathbb{Z}$ этот алгоритм может быть реализован на ЭВМ следующим образом.

Алгоритм 5.1 (Алгоритм поиска классов вычетов, удовлетворяющих сравнению $ax \equiv b \pmod{m}$)

Вход: Целые числа a, b, m такие, что $m \neq 0$.
Выход: Таблица представителей классов вычетов по модулю m.

```
1  def axmod( a, b, m ):
2          if a == 0:                      # Если a ≡ 0 (mod m), то решение
3                  if b != 0: return []; # может существовать только в случае, когда
4                  return [infinity]      # b ≡ 0 (mod m).
5          d=gcd(a,m);              # вычисляем НОД(a, m)
6          (b1,r) = b.quo_rem(d); # делим с остатком b = b1*d + r
7          if r != 0: return [];   # если d не делит b нацело, то решений нет
8          a1 = a/d; m1 = m/d;     # определяем a1, m1 равенствами a = a1*d, m = m1*d
9          # используем соотношение Безу и находим обратный для a1 по модулю m
10         (v,u,d1) = xgcd(a1, m1);
11         x = (u*b1)%m1; # определяем решение сравнения a1*x ≡ b1 (mod m1)
12         # вырабатываем все возможные классы вычетов по модулю m
13         v=[x];
14         for i in [1..d-1]: v.append(x+m1*i);
15         return v;
```

В приведенном алгоритме стоит отметить строчку 12, в которой используется соотношение Безу (см. соотношение 2.4.A) для поиска обратного элемента в кольце классов вычетов по модулю m_1. Алгоритм 5.1 реализуется в кольце целых чисел и мы знаем, что функция `gcd()` возвращает целое, положительное число d. В произвольном эвклидовом кольце величина $d = \mathbf{НОД}(a_1,\ m_1)$ может быть обратимым элементом кольца, не обязательно равным единице, что потребует незначительной модификации приведенного алгоритма.

Также отметим, что в строке 16 мы используем тот факт, что согласно следствию 4.3.A в кольце целых чисел $\mathbb{Z}$ остатками $r_1, \ldots, r_n$ являются все целые числа от 0 до $d-1$.

5.2 Расширенный алгоритм Эвклида

Пусть, как и ранее, $\mathbb{U}$ эвклидового кольцо, a, b, m элементы этого кольца и $m \neq 0$. Как мы показали выше, поиск классов вычетов, удовлетворяющих сравнению $ax \equiv b \pmod m$ сводится к соотношению Безу, т.е. поиску элементов $u, v \in \mathbb{U}$ таких, что

$$a_1 u + m_1 v \sim \mathbf{НОД}(a_1,\ m_1)\,,$$

и

$$a_1 = \frac{a}{d}, \quad m_1 = \frac{m}{d}, \quad d = \mathbf{НОД}(a,\ m)\,.$$

Данное нами ранее во второй главе доказательство теоремы 2.4, следствием которой является соотношение Безу, не было конструктивным и не содержало в себе каких-либо рекомендаций по поиску неизвестных значений u, v. Сейчас мы исправим эту ситуацию и опишем алгоритм, базирующийся на алгоритме Эвклида вычисления наибольшего общего делителя.

Пусть a, m произвольные элементы эвклидового кольца и $r_{-1}, r_0, \ldots$ последовательность элементов, удовлетворяющих равенствам $r_{-1} = m$, $r_0 = a$ и

$$\begin{aligned} r_{-1} &= r_0 q_1 + r_1, \\ r_0 &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\ldots \\ r_{n-1} &= r_n q_{n+1}, \quad r_{n+1} = 0, \quad n \in \mathbb{N}_0. \end{aligned} \tag{5.3}$$

В силу утверждения теоремы 2.6 величина r_n является наибольшим общим делителем элементов a и m. Тогда, определим две последова-

тельности элементов $u_{-1}, u_0, \ldots$ и $v_{-1}, v_0, \ldots$ равенствами

$$\begin{aligned} u_{-1} &= 0, \\ u_0 &= 1, \\ v_{-1} &= 1, \\ v_0 &= 0, \\ u_{k+1} &= u_{k-1} - q_k u_k, \\ v_{k+1} &= v_{k-1} - q_k v_k. \end{aligned} \tag{5.4}$$

Теорема 5.2. *Пусть a, m элементы эвклидового кольца $\mathbb{U}$, последовательность элементов кольца $r_{-1}, r_0, \ldots r_n$ определена равенствами (5.3) и представляет собой последовательность остатков в алгоритме Эвклида, а последовательности $u_{-1}, u_0, \ldots$ и $v_{-1}, v_0, \ldots$ определены равенствами (5.4). Тогда, выполнено равенство*

$$au_k + mv_k = r_k, \quad k = -1, 0, \ldots, n, \tag{5.5}$$

в частности $au_n + mv_n \sim \mathbf{НОД}(a,\ m)$.

Доказательство. Легко видеть, что при $k = -1, 0$ равенство (5.5) выполнено в силу выбора элементов u_{-1}, v_{-1} и u_0, v_0. Теперь предположим, что равенство (5.5) выполнено для всех значений $-1, 0, 1, \ldots, k$ и покажем, что оно выполнено и для индекса $k+1$. С учетом равенств (5.3) и (5.4) получаем

$$\begin{aligned} au_{k+1} + mv_{k+1} &= a(u_{k-1} - q_k u_k) + m(v_{k-1} - q_k v_k) = \\ &= au_{k-1} + mv_{k-1} - q(au_k + mv_k) = r_{k-1} - qr_k = r_{k+1}. \end{aligned}$$

Теорема доказана. □

Пример 5.5.

1. Найдем решение уравнения $156u + 148v = \mathbf{НОД}(156,\ 148)$ относительно неизвестных u, v. Для этого, определим начальные значения

   $$u_{-1} = 1, u_0 = 0, v_{-1} = 0, v_0 = 1, r_{-1} = 156, r_0 = 148$$

   и применим соотношения (5.3) и (5.4). Тогда мы получим следующую последовательность равенств

$r_{k+1} = r_{k-1} - q_{k+1} r_k,$	$u_{k+1} = u_{k-1} - q_{k+1} u_k,$	$v_{k+1} = v_{k-1} - q_{k+1} v_k,$
$8 = 156 - 1 \cdot 148,$	$1 = 1 - 1 \cdot 0,$	$-1 = 0 - 1 \cdot 1,$
$4 = 148 - 18 \cdot 8,$	$-18 = 0 - 18 \cdot 1.$	$19 = 1 - 18 \cdot (-1).$
$0 = 8 - 2 \cdot 4.$		

   Теперь, из предпоследней строки, получаем искомое равенство

   $$156 \cdot -18 + 148 \cdot 19 = 4.$$

2. Пусть $f(x) = x^3 + 3x^2 - x - 3$, $g(x) = x^3 - x^2 + x - 1$ и $f(x), g(x) \in \mathbb{Q}[x]$. Найдем решение уравнения $f(x)u(x) + g(x)v(x) = d(x)$ относительно неизвестных многочленов $u(x), v(x)$ и $d(x) = \mathbf{НОД}\,(f(x),\ g(x))$. Для этого, определим начальные значения

$$u_{-1} = 1, u_0 = 0, v_{-1} = 0, v_0 = 1, r_{-1} = f(x), r_0 = g(x)$$

и применим соотношения (5.3). Тогда мы получим следующую последовательность равенств

	r_{k+1}	$= r_{k-1} - q_{k+1}r_k,$
$4x^2 - 2x - 2$		$= (x^3 + 3x^2 - x - 3) - 1 \cdot (x^3 - x^2 + x - 1),$
$\frac{5}{4}(x-1)$		$= (x^3 - x^2 + x - 1) - \left(\frac{1}{4}x - \frac{1}{8}\right)(4x^2 - 2x - 2)$
0		$= 4x^2 - 2x - 2 - \frac{4}{5}(4x+2) \cdot \frac{5}{4}(x-1),$

из которых следует, что

$$\mathbf{НОД}\,(f(x),\ g(x)) = \frac{5}{4}(x-1) \sim x - 1.$$

Применяя последовательность равенств (5.4) получим выражения для разыскиваемых многочленов

u_{k+1}	$=$	$u_{k-1} - q_{k+1}u_k,$	v_{k+1}	$=$	$v_{k-1} - q_{k+1}v_k,$
1	$=$	$1 - 1 \cdot 0,$	-1	$=$	$0 - 1 \cdot 1,$
$-\frac{1}{4}\left(x - \frac{1}{2}\right)$	$=$	$0 - \left(\frac{1}{4}x - \frac{1}{8}\right) \cdot 1,$	$\frac{1}{4}\left(x + \frac{7}{2}\right)$	$=$	$1 - \left(\frac{1}{4}x - \frac{1}{8}\right) \cdot (-1).$

Тогда, выполнено равенство

$$-\frac{1}{4}\left(x - \frac{1}{2}\right)(x^3 + 3x^2 - x - 3) + \frac{1}{4}\left(x + \frac{7}{2}\right)(x^3 - x^2 + x + 1) = \frac{5}{4}(x-1)$$

или, приводя все к коэффициенты к целым числам,

$$-(2x-1)(x^3 + 3x^2 - x - 3) + (2x+7)(x^3 - x^2 + x + 1) = 10(x-1).$$

Используя соотношения (5.3) и (5.4) легко предъявить алгоритм поиска коэффициентов u, v, составляющих соотношение Безу. Для кольца целых чисел такой алгоритм может быть записан следующим образом.

Алгоритм 5.2 (Расширенный алгоритм Эвклида)

Вход: целые числа a и b.
Выход: целые u, v и d такие, что $d = \mathbf{НОД}\,(a,\ b)$ и $au + bv = d$.

```
1  def xgcd_z( a, b ):
2          if a.is_integer() != True:
3                  print("Неверный тип первого аргумента");
4                  return 0;
5          if b.is_integer() != True:
6                  print("Неверный тип второго аргумента");
7                  return 0;
8          # приводим числа к их абсолютному значению
9          ma = 1; mb = 1;
10         if a < 0: a = -a; ma = -1;
```

```
11          else: ma = 1;
12          if b < 0: b = -b; mb = -1;
13          else: mb = 1;
14          # устанавливаем начальные значения для разыскиваемых значений
15          um1 = 0; u0 = 1; vm1 = 1; v0 = 0;
16          # запускаем основной цикл вычисления остатков от деления
17          while a > 0:
18                  (q,r) = b.quo_rem(a);
19                  u = um1-q*u0; um1 = u0; u0 = u;
20                  v = vm1-q*v0; vm1 = v0; v0 = v;
21                  b = a; a = r;
22          # возвращаем значения u,v с учетом знака аргументов функции,
23          # а также значение наибольшего общего делителя
24          return [um1*ma, vm1*mb, b];
```

Предложенный алгоритм является простейшей модификацией алгоритма 2.1, приведенного ранее во второй главе.

В заключение раздела, докажем пару простых свойств, которыми обладает соотношение Безу.

Следствие 5.2.А. *Пусть a, m элементы эвклидового кольца $\mathbb{U}$ и u, v элементы, удовлетворяющие соотношению Безу*

$$au + mv \sim \mathbf{НОД}(a,\ m)\,.$$

Тогда для любого $s \in \mathbb{U}$ элементы

$$u_s = u - \frac{ms}{\mathbf{НОД}(a,\ m)}, \quad v_s = v + \frac{as}{\mathbf{НОД}(a,\ m)}$$

также удовлетворяют соотношению Безу.

Доказательство. Сформулированное утверждение следует из равенства

$$\begin{aligned} au_s + mv_s = \\ = a\left(u - \frac{ms}{\mathbf{НОД}(a,\ m)}\right) + m\left(v + \frac{as}{\mathbf{НОД}(a,\ m)}\right) = \\ = au + mv \sim \mathbf{НОД}(a,\ m)\,. \end{aligned}$$

Кроме того, если $\mathbf{НОД}(a,\ m) \sim 1$, в силу определения операции сравнения получаем, что

$$u_s \equiv u \pmod m\,, \quad v_s \equiv v \pmod a\,.$$

Следствие доказано. □

Следствие 5.2.В. *Пусть $n \geqslant 2$ натуральное число и $a_1, \ldots, a_n$ произвольные элементы эвклидового кольца $\mathbb{U}$. Тогда найдутся такие элементы $z_1, \ldots, z_n \in \mathbb{U}$, что*

$$a_1 z_1 + \cdots + a_n z_n \sim \mathbf{НОД}(a_1, \ldots, a_n).$$

Доказательство. Определим последовательность элементов кольца d_1, $\ldots$, $d_n \in \mathbb{U}$ условиями

$$d_1 = a_1, \quad d_k \sim \mathbf{НОД}(d_{k-1}, \ a_k), \quad \text{для всех} \quad k = 2, \ldots, n.$$

Тогда, последний элемент этой последовательности d_n будет являться наибольшим общим делителем элементов $a_1, \ldots, a_n$. С другой стороны, воспользовавшись утверждением теоремы 5.2, мы можем последовательно найти элементы u_k и v_k, для $k = 1, 2, \ldots, n$, удовлетворяющие равенствам

$$a_k u_k + v_k d_{k-1} = \mathbf{НОД}(a_k, \ d_{k-1}) = d_k, \quad \text{для всех} \quad k = 2, \ldots, n.$$

Тогда

$$\begin{aligned} d_n = u_n a_n + v_n d_{n-1} &= u_n a_n + v_n(u_{n-1} a_{n-1} + v_{n-1} d_{n-2}) = \\ &= u_n a_n + v_n u_{n-1} a_{n-1} + v_n v_{n-1}(u_{n-2} a_{n-2} + v_{n-2} d_{n-3}) = \cdots \\ \cdots &= u_n a_n + v_n u_{n-1} a_{n-1} + v_n v_{n-1} u_{n-2} a_{n-2} + \cdots + v_n v_{n-1} \cdots v_2 u_1 a_1, \end{aligned}$$

и мы получаем точные равенства для неизвестных $z_1, \ldots, z_n$

$$\begin{aligned} z_n &= u_n, \\ z_{n-1} &= v_n u_{n-1}, \\ z_{n-2} &= v_n v_{n-1} u_{n-2}, \\ &\cdots \\ z_2 &= v_n v_{n-1} \cdots v_3 u_2, \\ z_1 &= v_n v_{n-1} \cdots v_2 u_1. \end{aligned}$$

Следствие доказано. □

5.3 Китайская теорема об остатках

Перейдем к рассмотрению систем сравнений и рассмотрим систему

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \qquad \cdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \tag{5.6}$$

где элементы $a_1, \ldots, a_k$ и $m_1, \ldots, m_k$ принадлежат эвклидовому кольцу $\mathbb{U}$, а кроме того,

$$\textbf{НОД}\,(m_i,\ m_j) \sim 1, \quad \text{при} \quad i \neq j,$$

т.е. элементы $m_1, \ldots, m_k$ попарно взаимно-просты. Под решением указанной системы сравнений мы будем подразумевать множество элементов кольца $\mathbb{U}$, удовлетворяющих всем сравнениям, содержащимся в системе 5.6. Строение указанного множества решений дает следующая теорема.

Теорема 5.3 (Китайская теорема об остатках[1], 1247)**.** *Пусть $\mathbb{U}$ эвклидово кольцо и k натуральное число. Пусть m_1, …, m_k попарно взаимно-простые элементы кольца $\mathbb{U}$, произведение которых равно $M = \prod_{j=1}^{k} m_j$. Тогда любого набора элементов a_1, …, $a_k \in \mathbb{U}$ множество решений системы сравнений (5.6)*

$$\begin{cases} x \equiv a_1 \ (mod\, m_1)\,, \\ \qquad \ldots \\ x \equiv a_k \ (mod\, m_k)\,, \end{cases}$$

образует единственный класс вычетов по модулю M и удовлетворяет сравнению

$$x \equiv \sum_{i=1}^{k} a_i b_i c_i \ (mod\, M)\,, \tag{5.7}$$

где $b_i = \frac{1}{m_i}\left(\prod_{j=1}^{k} m_j\right) = \frac{M}{m_i}$ и $c_i \equiv b_i^{-1} \ (mod\, m_i)$.

Доказательство. В силу выбора параметров b_i, c_i для каждого члена суммы, стоящей в правой части сравнения (5.7), выполнены сравнения

$$a_i b_i c_i \equiv a_i \ (\mathrm{mod}\, m_i)\,, \quad a_i b_i c_i \equiv 0 \ (\mathrm{mod}\, m_j)\,, \quad j \neq i,\ i = 1,\ \ldots,\ k,$$

из которых следует, что x удовлетворяет системе уравнений (5.6).

[1]Первое описание метода решения рассматриваемой системы сравнений содержится в сочинении XIII в. «Девять отделов искусства счета» (около 1247 г.), автором которого является выдающийся китайский математик Цинь Цзю-шао. В данном сочинении содержатся комментарии к более древнему трактату VIII в. «Таен лин-шу» и, в частности, к задаче полководца Сунь-цзы, жившего не позднее III в. Эта задача формулируется так «Найти число, которое при делении на 3 даёт остаток 2, при делении на 5 даёт остаток 3 и, наконец, при делении на 7 даёт остаток 2». Решение, предложенное Сунь-цзы, фактически совпадает с тем, что приводится в доказательстве теоремы 5.3. Подробнее, см. статью Юшкевич А.П. «О достижениях китайских ученых в области математики» // Историко-математические исследования. – Вып. VII, – М.:ГИТТЛ, – 1955.

Покажем, что данное решение по модулю M единственно. Для этого предположим, что существует другое решение, скажем, y. Тогда выполнены сравнения $x - y \equiv 0 \pmod{m_i}$ для $i = 1, \ldots, k$, или

$$x - y = m_1 c_1 = m_2 c_2 = \cdots = m_k c_k,$$

при некоторых целых значениях $c_1, \ldots, c_k$. Поскольку все числа $m_1, \ldots, m_k$ взаимно просты, то применяя лемму 2.6, получаем, что $m_i | c_j$ при всех $i \neq j$, что равносильно $x - y \equiv 0 \pmod{M}$. Последнее сравнение завершает доказательство теоремы. □

Пример 5.6. Рассмотрим известную задачу Сунь-цзы, в которой надо найти целое число x, удовлеьворяющее системе сравнений

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

где $m_1 = 3$, $m_2 = 5$ и $m_3 = 7$. Тогда, определим $M = 3 \cdot 5 \cdot 7 = 105$ и

$$\begin{aligned} b_1 &= 5 \cdot 7 = 35 = 105/3, \\ b_2 &= 3 \cdot 7 = 21 = 105/5, \\ b_3 &= 3 \cdot 5 = 15 = 105/7. \end{aligned}$$

Используя расширенный алгоритм Эвклида вычислим целочисленные величины u_i, v_i, которые удовлетворяют равенствам $b_i u_i + m_i v_i = 1$ и позволят определить величины c_1, c_2, c_3:

$$\begin{aligned} 35 \cdot 2 - 3 \cdot 23 &= 1, \quad c_1 \equiv 2 \pmod 3, \\ 21 \cdot 1 - 5 \cdot 4 &= 1, \quad c_2 \equiv 1 \pmod 5, \\ 15 \cdot 1 - 7 \cdot 2 &= 1, \quad c_3 \equiv 1 \pmod 7. \end{aligned}$$

Теперь можно определить представитель класса вычетов, удовлетворяющий исходной системе, равенством

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 = 2 \cdot 105 + 23.$$

Выбирая в найденном классе вычетов наименьший неотрицательный вычет, получим что решением исходной системы является класс $x \equiv 23 \pmod{105}$.

Следствие 5.3.А. *Двум различным наборам элементов $a_1, \ldots, a_k$ и $a'_1, \ldots, a'_k$ кольца $\mathbb{U}$ соответствуют два различных класса вычетов x и x' по модулю M, удовлетворяющих системе сравнений (5.6).*

Доказательство. Пусть наборы чисел $a_1, \ldots, a_k$ и $a'_1, \ldots, a'_k$ таковы, что найдется хотя бы один индекс j, $j = 1, \ldots, k$ такой, что выполнено условие $a_j \not\equiv a'_j \pmod{m_i}$.

Определим, согласно (5.7), решения

$$x \equiv \sum_{i=1}^{k} a_i b_i c_i \pmod{M}, \quad x' \equiv \sum_{i=1}^{k} a'_i b_i c_i \pmod{M}$$

и предположим, что $x \equiv x' \pmod{M}$. Тогда для выбранного ранее индекса j будет выполнено $m_j | M$ и, следовательно, $x \equiv x' \pmod{m_j}$. Последнее сравнение равносильно $a_j \equiv a'_j \pmod{m_j}$, что противоречит нашему предположению. □

Рассмотрим частный случай, который будет нам встречаться впоследствии несколько раз.

Следствие 5.3.B. *Пусть для всех индексов $i = 1, \ldots, k$ выполнено неравенство $N(a) < N(m_i)$, тогда системе сравнений*

$$\begin{cases} x \equiv a \ (mod\, m_1), \\ \qquad \ldots \\ x \equiv a \ (mod\, m_k), \end{cases}$$

удовлетворяет единственный класс вычетов $x \equiv a \, (mod\, M = m_1 \cdots m_k)$.

Доказательство. Очевидно, что $x \equiv a \pmod{M}$ удовлетворяет указанной системе сравнений. В силу первого следствия, такое решение единственно. □

Дальнейший текст в этой и следующих главах требует правок.

ПРАВИТЬ ЗДЕСЬ. Формулировка и доказательство последнего следствия требуют уточнения - убрать норму, докво следует из теоремы

Утверждение теоремы 5.3 позволяет предложить следующий алгоритм вычисления вычета $x \pmod M$, удовлетворяющего системе сравнений (5.6).

Алгоритм 5.3 (Решение системы линейных сравнений)

Вход: целые числа k, $m_1, \ldots, m_k$ и $a_1, \ldots, a_k$, удовлетворяющие теореме 5.3.
Выход: вычет x, $0 \leqslant x < M$ – решение системы сравнений (5.6).
1. Определить $x = 0$, $i = 1$ и $M = \prod_{j=1}^{k} m_j$.

□

Остановимся на реализации шага 2.2. Нам надо добавить к текущему значению переменной x произведение $a_i bc$, для которого верна оценка сверху

$$0 \leqslant a_i bc < AM, \quad \text{где} \quad A = \max_{i=1,\ldots,k} a_i.$$

После сложения, нам необходимо произвести операцию деления по модулю числа M и вычислить вычет x.

Поскольку операция приведения по модулю M является достаточно трудоемкой, мы приведем другой алгоритм восстановления значения x по множеству известных остатков $a_1, \ldots, a_k$. Он основывается на следующей теореме.

Теорема 5.4. *Пусть $m_1, \ldots, m_k$ целые, взаимно простые числа, произведение которых равно $M = \prod_{j=1}^{k} m_j$. Пусть $x < M$ целое число, удовлетворяющее системе сравнений (5.6). Тогда найдутся такие целые $x_1, \ldots, x_k$, что $x_i < m_i$ для всех $i = 1, \ldots, k$ и*

$$x = x_1 + x_2 m_1 + x_3 m_1 m_2 + \ldots + x_k m_1 \cdots m_{k-1}. \tag{5.8}$$

Доказательство. Начнем с того, что определим константы $b_1, \ldots, b_k$ равенствами

$$b_1 = 1, \quad b_i = \prod_{j=1}^{i-1} m_j, \quad i = 2, \ldots, k.$$

Теперь мы можем переписать равенство (5.8) в виде $x = \sum_{i=1}^{k-1} x_i b_i$. Введем еще один набор значений $s_1, \ldots, s_k$, зависящий от величины x следующим образом: $s_i = \sum_{j=1}^{i} x_j b_j$, тогда $x = s_k$ и

$$s_1 = x_1, \quad s_i = s_{i-1} + x_i b_i, \quad \text{для всех} \quad i = 2, \ldots, k. \tag{5.9}$$

Теперь мы можем определить величины $x_1, \ldots, x_k$ используя следующее рекуррентное соотношение

$$x_1 = a_1, \quad x_i \equiv b_i^{-1}(a_i - s_{i-1}) \pmod{m_i}, \quad \text{при} \quad i = 2, \ \ldots, \ k, \qquad (5.10)$$

где величина b_i^{-1} определяется из сравнения $b_i b_i^{-1} \equiv 1 \pmod{m_i}$. Поскольку $\mathbf{НОД}(b_i, \ m_i) = 1$, то данное определение величины b_i^{-1} корректно. Заметим, что, в силу определения, для коэффициентов x_i выполнены неравенства $x_i < m_i$ для всех $i = 1, \ldots, k$.

Изучая равенство (5.8), заметим, что для всех индексов $i = 1, \ \ldots, k$ выполнено сравнение $x \equiv s_i \pmod{m_i}$. Тогда из (5.9) и (5.10) получаем

$$x \equiv s_{i-1} + x_i b_i \equiv s_{i-1} + b_i^{-1}(a_i - s_{i-1})b_i \equiv a_i \pmod{m_i},$$

и число x действительно удовлетворяет системе сравнений (5.6).

Нам осталось показать, что выполнено неравенство $x < M$. Для этого докажем, по индукции, что выполнено неравенство $s_i < m_i b_i$ для любого индекса $i = 1, \ldots, k$. Для $s_1 = x_1 < m_1$ неравенство очевидно. Далее, пусть оно выполнено для всех индексов, меньших i. Тогда $s_{i-1} < m_{i-1} b_{i-1} = b_i$ и

$$s_i = s_{i-1} + x_i b_i < b_i + (m_i - 1)b_i < m_i b_i.$$

Применяя полученное неравенство к индексу $i = k$, получаем, что $x = s_k < m_k b_k = M$. Теорема доказана. □

Основываясь на данной теореме, мы можем предложить эффективный алгоритм вычисления значения x. Отметим, что для случая $k = 2$ описание алгоритма может быть найдено в книге Антона Казимировича Сушкевича [?]. Добавим, что в англоязычной и переводной литературе этот алгоритм, применительно к произвольному значению k, носит имя американского математика Харви Гарнера (Harvey L. Garner), см. [?].

Основное преимущество алгоритма Гарнера заключается в том, что в нем вычисления производятся с числами, не превышающими величину модуля M. Более того, не требуется операция приведения по модулю M, которая заменена операциями приведения по модулю множителей m_i, входящих в разложение числа M.

Задачи и упражнения

1. Является ли многочлен $f(x) = 17x^4 + 8x^3 + 6x^2 + 1$ разложимым элементом кольца $\mathbb{Z}_8[x]$?

2. Является ли многочлен $f(x) = 2x^2 - 5ix + 3 + 2i$ разложимым элементом кольца $\mathbb{V}[x]$, где $\mathbb{V} = \mathbb{Z}[i]/(1 + 2i)$?

3. Найдите u, v удовлетворяющие равенствам:

   - $27u + 33v = \mathbf{НОД}\,(27,\ 33)$, где $u, v \in \mathbb{Z}$,
   - $(x^4 - 1)u + (x^2 - 1)v = \mathbf{НОД}\left(x^4 - 1,\ x^2 - 1\right)$, где $u, v \in \mathbb{Q}[x]$,
   - $(-14 + 2i)u + (6i)v = \mathbf{НОД}\,(-14 + 2i,\ 6i)$, где $u, v \in \mathbb{Z}[i]$.

4. Найдите решения следующих сравнений первой степени:

   - в кольце целых чисел:

     $$7x \equiv 13 \pmod{16}, \quad 8x \equiv 14 \pmod{15}, \quad 6x \equiv 27 \pmod{33}.$$

   - в кольце многочленов $\mathbb{Q}[t]$:

     $$(5t^2 + 1)x \equiv 12t - 1 \pmod{t^2 + 2}$$

   - в кольце целых гауссовых чисел:

     $$\begin{aligned} (1+i)x &\equiv 3 \pmod{1+2i}, \\ (1+2i)x &\equiv 5 \pmod{2+3i}, \\ 2x &\equiv 1+3i \pmod{3+3i}. \end{aligned}$$

5. Найдите $z_1, \ldots, z_4$, удовлетворяющие равенствам

   $$2z_1 + 3z_2 + 5z_3 + 7z_4 = 1,$$
   $$(1+i)z_1 + (1+2i)z_2 + 3z_3 + (2+3i)z_4 = 1.$$

6. Найдите решение следующей старинной задачи.

   В одно самое обычное утро погонщик мулов по имени Алибаба гнал своё стадо вдоль отрога старой горы и неожиданно заметил небольшой вход в пещеру. Зайдя внутрь Алибаба обнаружил в углу пещеры множество одинаковых золотых слитков. Обрадовался Алибаба такой находке и решил забрать с собой все найденное золото. Осмотрелся он по сторонам и увидел, что рядом лежат мешки в которых разбойники, а ведь это была их пещера, принесли сюда золотые слитки. Мешки были большие, в которые входит по 11 слитков, также были мешки поменьше, в которые входит по 7 слитков и самые маленькие мешки, в которые помещается уж совсем мало золотых слитков – только три. Алибаба положил все золото в большие мешки, но остался один слиток, тогда он взял средние мешки но и в них не влезло все золото - опять остался один слиток и только взяв маленькие мешки Алибаба смог уложить в них все золото.

   Теперь вопрос, сколько мулов было в стаде у Алибабы, если на каждого мула он повесил по 6 мешков, а на последнем уехал сам?

Рекомендации к сдаче экзамена

Схема зависимостей между утверждениями, доказанными в 5-й главе, изображена на рисунке 5.1.

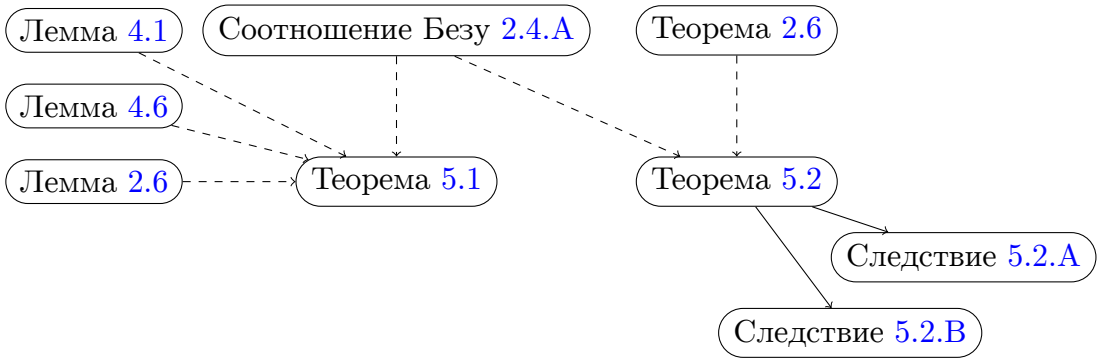


Рис. 5.1: Схема зависимостей между утверждениями 5-й главы.

Дополнительная литература к 5-й главе

Лемма 5.1. *Пусть $b > 1$ натуральное число и $a \in \mathbb{N}_0$ целое число. Тогда найдутся такие целые n, $a_0, \ldots, a_{n-1}$, что*

1. *выполнено равенство*

$$a = a_0 + a_1 b + \cdots + a_{n-1} b^{n-1}, \quad 0 \leqslant a_i < b, \quad i = 0, \ldots, n-1, \quad n \in \mathbb{N}_0, \tag{5.11}$$

2. *для любого $k = n, n+1, \ldots$ выполнено неравенство $b^k > a$,*

3. *равенство (5.11) единственно.*

Доказательство. Используя операцию деления с остатком построим цепочку равенств

$$\begin{aligned} a &= q_0 b + a_0, \\ q_0 &= q_1 b + a_1, \\ q_1 &= q_2 b + a_2, \\ &\cdots \end{aligned}$$

где $0 \leqslant a_n < b$ для $n = 0, 1, \ldots$. Поскольку все используемые нами величины неотрицательны и $a > q_0 > q_1 > \cdots \geqslant q_n = 0$, то цепочка равенств прервется и, обозначая для последнего значения индекса $a_n = q_{n-1}$, получим первое утверждение леммы

$$a = q_0 b + a_0 = (q_1 b + a_1) b + a_0 = \cdots = a_{n-1} b^{n-1} + \cdots a_1 b + a_0.$$

Поскольку операция деления с остатком дает единственное представление, то полученное нами равенство также единственно.

Для доказательства второго утверждения леммы заметим, что выполнена цепочка неравенств

$$\begin{aligned} a = a_0 + a_1 b + a_2 b^2 + \cdots a_{n-1} b^{n-1} < b + a_1 b + a_2 b^2 + \cdots a_{n-1} b^{n-1} \leqslant \\ \leqslant b^2 + a_2 b^2 + \cdots + a_{n-1} b^{n-1} \leqslant \cdots \leqslant b^{n-1} + a_{n-1} b^{n-1} \leqslant b^n < b^{n+1} < \cdots \end{aligned}$$

□

Определение 5.2. *Пусть $b > 1$ натуральное число. Если $a \in \mathbb{N}_0$ записано в виде (5.11), то мы будем говорить, что число a записано в системе счисления по основанию b.*

Пример 5.7. Для целого числа $a = 357$ легко записать его разложение в системе счисления по основанию $b = 11$. Действительно

$$357 = 32 \cdot 11 + 5 = (2 \cdot 11 + 10) \cdot 11 + 5 = 2 \cdot 11^2 + 10 \cdot 11 + 5.$$

Поскольку операция деления с остатком определена для любого евклидого кольца $\mathbb{U}$, то первое и второе утверждения леммы 5.1 также выполнены в любом евклидовом кольце

$\mathbb{U}$. Рассмотрим кольцо многочленов от одной переменной $\mathbb{Q}[x]$ и выберем в нем два многочлена $a(x) = x^5 + 1$ и $b(x) = 2x^2 + x + 1$, тогда

$$\begin{aligned} x^5 + 1 &= \frac{1}{16}(8x^3 - 4x^2 - 2x + 3)(2x^2 + x + 1) - \frac{1}{16}(x - 13) = \\ &= \frac{1}{16}\big((4x - 4)(2x^2 + x + 1) - 2x + 7\big)(2x^2 + x + 1) - \frac{1}{16}(x - 13) = \\ &= \frac{1}{4}(x - 1)(2x^2 + x + 1)^2 + \frac{1}{16}(-2x + 7)(2x^2 + x + 1) - \frac{1}{16}(x - 13). \end{aligned}$$

Аналогичное представление может быть определено и для кольца гауссовых целых чисел $\mathbb{Z}[i]$. Пусть $a = 12 + 7i$ и $b = 3 + 2i$, тогда

$$12+7i = 4\cdot(3+2i)-i = \big((1-i)(3+2i)-1+i\big)(3+2i)-i = (1-i)(3+2i)^2+(i-1)(3+2i)-i.$$

В дальнейшем, на протяжении всей главы, мы будем рассматривать только одно евклидово кольцо – кольцо целых чисел $\mathbb{Z}$. Нам потребуется следующая техническая лемма.

глава 6

Иррациональные числа

6.1 Систематические дроби

Начнем с того, что определим основной объект исследования этой главы – бесконечную систематическую дробь.

Определение 6.1. *Пусть $b > 1$ натуральное число, которое мы будем называть основанием системы счисления. Пусть $\sigma \in \{-1, 1\}$ и m некоторое целое число. Мы будем называть систематической дробью α ряд*

$$\alpha = \sigma \sum_{n=-m}^{\infty} a_n b^{-n} = \sigma \left(a_{-k} b^{-k} + \cdots + a_1 b + a_0 + \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots \right), \quad (6.1)$$

где $a_n \in \mathbb{N}_0$ и $0 \leqslant a_n < b$ для $n = -m, -m+1, \ldots$.

Величину

$$a = \sigma \sum_{k=-m}^{0} a_k b^{-k} = \sigma \left(a_{-k} b^{-k} + \cdots + a_1 b + a_0 \right)$$

мы будем называть целой частью систематической дроби. Для любого $k \in \mathbb{N}_0$ мы будем называть величину

$$s_k(\alpha) = \sigma \sum_{n=-m}^{k} a_n b^{-n} \in \mathbb{Q}, \quad (6.2)$$

конечной суммой систематической дроби (6.1).

Мы будем говорить, что систематическая дробь конечна, если найдется индекс $n_0 \in \mathbb{N}$ такой, что для всех индексов $n \geqslant n_0$ выполнено равенство $a_n = 0$. Это же условие равносильно тому, что

$$s_n(\alpha) = s_{n_0}(\alpha), \quad n \geqslant n_0.$$

Мы будем говорить, что систематическая дробь периодична, если найдется индекс $\lambda \in \mathbb{N}$ и натуральное число $\tau \geqslant 1$ такие, что всех индексов $n \geqslant \lambda$ выполнено равенство

$$a_{n+\tau} = a_n, \quad n = \lambda, \lambda + 1, \ldots.$$

Величину τ мы будем называть периодом систематической дроби, а величину λ – длиной подхода к периоду.

Для записи систематических дробей и их конечных сумм также можно использовать обозначения, более привычные, чем суммы (6.1) или (6.2),

$$\begin{aligned} \alpha &= \pm a_{-m}a_{-m+1}\dots a_0, a_1a_2\dots, \\ s_k(\alpha) &= \pm a_{-m}a_{-m+1}\dots a_0, a_1a_2\dots a_{k_b}. \end{aligned}$$

Для периодических систематических дробей может использоваться обозначение

$$\alpha = \pm a_{-m}a_{-m+1}\dots a_0, a_1a_2\dots(a_\lambda\dots a_{\lambda+\tau-1})_b,$$

в котором элементы $a_\lambda, \dots, a_{\lambda+\tau-1}$ образуют период последовательности коэффициентов систематической дроби. В случаях, когда это ясно из контекста изложения, символ b может быть опущен.

Пример 6.1. Легко привести примеры явно заданных систематических дробей

$$\begin{aligned} & 0,135724680\dots_8, \\ \tfrac{13}{81} &= 0,0111_3, \\ \tfrac{46}{3} &= 15,(3)_{10}. \end{aligned}$$

Стоящие слева в приведенных равенствах числа записаны в десятичной системе счисления. Для чисел, стоящих справа, система счисления указывается явно.

Определение 6.2. *Мы будем говорить, что систематическая дробь сходится к числу α, если сходится последовательность его конечных сумм $(s_k)_{k=0}^{\infty}$, то есть $\alpha = \lim_{k\to\infty} s_k$.*

Любая систематическая дробь сходится к некоторой величине. Для доказательства этого утверждения нам потребуется следующая лемма.

Лемма 6.1. *Пусть $\alpha, \varepsilon \in \mathbb{Q}$ и $\varepsilon > 0$. Пусть $b > 1$ целое число, тогда найдется такое $n \in \mathbb{N}_0$, что*

$$\frac{|\alpha|}{b^n} < \varepsilon.$$

Доказательство. Обозначим $|\alpha| = \frac{p}{q}$ и $\varepsilon = \frac{u}{v}$ так, что все величины p, q, u, v являются неотрицательными целыми числами.

Если $pv < uq$, то положим $n = 0$, иначе, используя операцию деления с остатком, определим $pv = s \cdot uq + a$, где $0 \leqslant a < uq$.

Теперь, представим $s + 1$ в ситеме счисления по основанию b и запишем

$$s + 1 = s_0 + s_1 b + \cdots s_{n-1}b^{n-1}$$

для некоторых $s_0, \ldots, s_{n-1} \in \mathbb{N}_0$. Тогда $b^n > s+1$ и выполнено неравенство

$$pv = s \cdot uq + a < (s+1)uq < uqb^n,$$

из которого следует утверждение леммы. □

Теорема 6.1. *Пусть $b > 1$ и m – целые числа. Для любой последовательности целых чисел $(a_n)_{n=-m}^{\infty}$ такой, что $0 \leqslant a_n < b$ для $n = 1, 2, \ldots$, ряд (6.1) сходится.*

Доказательство. Для начала докажем равенство

$$\frac{b}{b-1} = \sum_{n=0}^{\infty} b^{-n}. \tag{6.3}$$

Введем обозначение $q = \dfrac{1}{b}$, $0 < q < 1$, и рассмотрим частичную сумму, домножая её числитель и знаменатель на $(1-q)$,

$$s_k = \sum_{n=0}^{k} b^{-n} = (1+q+q^2+\cdots+q^k) = \frac{(1+q+q^2+\cdots+q^k)(1-q)}{(1-q)} = \frac{1-q^{k+1}}{1-q}.$$

Обозначим $\alpha = \dfrac{1}{(b-1)}$ и выберем произвольную рациональную величину $\varepsilon > 0$. Тогда, согласно лемме 6.1, найдется такой индекс $n \in \mathbb{N}_0$ такой, что

$$\frac{1}{b^n(b-1)} < \varepsilon.$$

Для данного индекса n выполнено неравенство

$$\left| \frac{1}{1-q} - \frac{1-q^{n+1}}{1-q} \right| = \frac{q^{n+1}}{1-q} = \frac{1}{b^n(b-1)} < \varepsilon.$$

Теперь, воспользовавшись определением предела последовательности, мы делаем вывод, что

$$\lim_{n\to\infty} \frac{1-q^{n+1}}{1-q} = \frac{1}{1-q}$$

и выполнено равенство (6.3), поскольку

$$\frac{1}{1-q} = \frac{b}{b-1}.$$

Теперь вернемся к доказательству утверждения теоремы и рассмотрим произвольную систематическую дробь

$$\alpha = \sigma \sum_{n=-m}^{\infty} a_n b^{-n}.$$

Используя равенство (6.3), получим

$$|\alpha - s_k| = \left|\sigma \sum_{n=-m}^{\infty} a_n b^{-n} - \sigma \sum_{n=-m}^{k} a_n b^{-n}\right| =$$
$$= b^{-k-1}|\sigma| \cdot \left|\sum_{n=0}^{\infty} a_{n+1+k} b^{-n}\right| < b^{-k-1} \left|\sum_{n=0}^{\infty} b^{-n}\right| = \frac{1}{b^k(b-1)}.$$

Выбирая произвольную рациональную величину $0 < \varepsilon < 1$, из леммы 6.1 получаем, что найдется такой индекс k такой, что

$$|\alpha - s_k| < \frac{1}{b^k(b-1)} < \varepsilon,$$

следовательно, $\lim_{k\to\infty} s_k = \alpha$. □

Следствие 6.1.А. *Пусть $b > 1$ целое число, тогда выполнено равенство*

$$1 = (b-1)\sum_{n=1}^{\infty} b^{-n}. \tag{6.4}$$

Доказательство. Доказательство, очевидно, следует из равенства (6.3)

$$(b-1)\sum_{n=1}^{\infty} b^{-n} = (b-1)\left(\sum_{n=0}^{\infty} b^{-n} - 1\right) = (b-1)\left(\frac{b}{b-1} - 1\right) = 1.$$

□

Определение 6.3. *Множество пределов систематических дробей мы будем называть множеством действительных чисел и обозначать символом $\mathbb{R}$.*

Из равенства (6.3) следует, что существуют систематические дроби, пределы которых являются рациональными числами. Из утверждения следующей теоремы будет следовать, что всё множество рациональных чисел является подмножеством действительных чисел.

Теорема 6.2. *Сходящаяся к числу α систематическая дробь конечна или периодична тогда и только тогда, когда α рациональное число.*

Доказательство. Покажем, что всякая конечная или периодическая систематическая дробь определяет рациональное число. Рассмотрим систематическую дробь

$$\alpha = \sigma \sum_{n=0}^{\infty} a_n b^{-n}.$$

Если данная дробь конечна, тогда найдется индекс $k \in \mathbb{N}_0$ такой, что $a_n = 0$ при $n > k$ и

$$\alpha = \sigma \sum_{n=0}^{k} a_n b^{-n} = \frac{\sigma}{b^k}(a_0 b^k + a_1 b^{k-1} + \cdots + a_k) \in \mathbb{Q},$$

т.е. α рациональное число.

Пусть теперь систематическая дробь периодична, тогда найдется натуральное число $\tau \geqslant 1$ и индекс $\lambda \in \mathbb{N}_0$ такой, что $a_{n+\tau} = a_n$ при $n \geqslant \lambda$. Обозначим

$$\begin{aligned} a_\lambda b^{-\lambda} + a_{\lambda+1} b^{-\lambda-1} + \cdots + a_{\lambda+\tau-1} b^{-\lambda-\tau+1} = \\ = b^{-\lambda}\left(a_\lambda + a_{\lambda+1} b^{-1} + \cdots + a_{\lambda+\tau-1} b^{-\tau+1}\right) = \\ = b^{-\lambda} \cdot b^{-\tau+1}\left(a_\lambda b^{\tau-1} + a_{\lambda+1} b^{\tau-2} + \cdots + a_{\lambda+\tau-1}\right) = b^{-\lambda}\frac{A}{b^\tau}, \end{aligned}$$

где $A \in \mathbb{Z}$ и $0 \leqslant A < b^\tau$. Тогда, учитывая (6.2), (6.3), получим равенство

$$\begin{aligned} \alpha\sigma^{-1} = \sum_{n=0}^{\infty} a_n b^{-n} = \\ = \sum_{n=0}^{\lambda-1} a_n b^{-n} + \sum_{n=\lambda}^{\lambda+\tau-1} a_n b^{-n} + \sum_{n=\lambda+\tau}^{\lambda+2\tau-1} a_n b^{-n} + \sum_{n=\lambda+2\tau}^{\lambda+3\tau-1} a_n b^{-n} + \cdots = \\ s_{\lambda-1} + b^{-\lambda}\left(\frac{A}{b^\tau} + \frac{A}{b^{2\tau}} + \frac{A}{b^{3\tau}} + \cdots\right) = s_{\lambda-1} + \frac{A}{b^\lambda}\sum_{n=1}^{\infty}(b^\tau)^{-n} = \\ = s_{\lambda-1} + \frac{A}{b^\lambda} \cdot \frac{1}{b^\tau - 1} \in \mathbb{Q}, \end{aligned}$$

из которого следует, что α является рациональным числом.

Теперь докажем теорему в обратную сторону и рассмотрим произвольное рациональное число $\frac{r}{q}$, где $q > 0$ и $\mathbf{НОД}(r,\ q) = 1$. Используя операцию деления с остатком запишем $|r| = a_0 q + p$, тогда

$$\frac{r}{q} = \sigma\left(a_0 + \frac{p}{q}\right), \quad \text{где} \quad 0 \leqslant p < q, \quad \sigma = \frac{r}{|r|}, \tag{6.5}$$

и нам достаточно в явном виде предъявить систематическую дробь для $\frac{p}{q}$.

Определим $\mathbf{НОД}(q,\ b) = d$ и для $d > 1$ обозначим $\nu_d(b) \in \mathbb{N}_0$ максимальную степень, в которой число d входит в разложение числа b, иначе положим $\nu_1(b) = 0$. Аналогично определим величину $\nu_d(q)$. Тогда

$$q = d^{\nu_d(q)} q_1, \quad b = d^{\nu_d(b)} b_1, \quad \mathbf{НОД}(b,\ b_1) = \mathbf{НОД}(q,\ q_1) = \mathbf{НОД}(b_1,\ q_1) = 1.$$

Определим

$$\nu_d(q) = s\nu_d(b) + t, \quad 0 \leqslant t < \nu_d(b)$$

и запишем равенства

$$q = d^{\nu_d(q)}q_1 = d^t \cdot \left(d^{\nu_d(b)}\right)^s q_1 = d^t \left(\frac{b}{b_1}\right)^s q_1$$

и

$$\frac{p}{q} = \frac{d^t p b_1^s}{b^s q_1} = \frac{1}{b^s} \cdot \left(c_0 + \frac{p_1}{q_1}\right), \tag{6.6}$$

где $d^t p b_1^s = c_0 q_1 + p_1$ и $0 \leqslant p_1 < q_1$. Если $p_1 = 0$, то мы получаем точное равенство

$$\frac{p}{q} = \frac{c_0}{b^s},$$

в противном случае $p_1 > 0$ и $\mathbf{НОД}\,(p_1,\ q_1) = 1$.

Из равенства (6.6) следует, что любая рациональная дробь может быть представлена в виде произведения величины, обратно пропорциональной некоторой степени b и дроби, знаменатель которой взаимно прост с основанием системы счисления b.

Поскольку $p < q$, то $c_0 < b^s$, следовательно, воспользуемся леммой 5.1 и запишем

$$c_0 = a_s + a_{s-1}b + \cdots a_1 b^{s-1}, \tag{6.7}$$

тогда из (6.6) следует равенство

$$\frac{p}{q} = a_1 b^{-1} + a_2 b^{-2} + \cdots + a_s b^{-s} + \frac{1}{b^s} \cdot \frac{p_1}{q_1}.$$

Если $p_1 = 0$, то мы получили конечную систематическую дробь для $\frac{p}{q}$ и утверждение теоремы. Теперь нам осталось построить систематическую дробь для рационального числа $\frac{p_1}{q_1}$ при $0 < p_1 < q_1$. Для этого рассмотрим последовательность целых чисел

$$b, b^2, \ldots, b^\tau, b^{\tau+1}, \ldots$$

и выберем из них то, у которого остаток от деления на q_1 будет равен 1, т.е.

$$b^\tau = cq_1 + 1 \tag{6.8}$$

при некотором натуральном c и минимально возможном значении $\tau > 1$. Поскольку $b^\tau > cq_1 > cp_1$, мы можем снова воспользоваться леммой 5.1 и записать

$$cp_1 = a_{\tau+s} + a_{\tau+s-1}b + \cdots + a_{s+1}b^{\tau-1}, \tag{6.9}$$

тогда

$$\frac{p_1}{q_1} = \frac{cp_1}{cq_1} = cp_1 \cdot \frac{1}{b^\tau - 1} = cp_1 \sum_{n=1}^{\infty} (b^\tau)^{-n} =$$
$$= \left(a_{\tau+s} + a_{\tau+s-1}b + \cdots + a_{s+1}b^{\tau-1}\right) \sum_{n=1}^{\infty} (b^\tau)^{-n} =$$
$$= a_{s+1}b^{-1} + \cdots + a_{s+\tau}b^{-\tau} + a_{s+1}b^{-\tau-1} + \cdots + a_{s+\tau}b^{-2\tau} + \cdots,$$

т.е. дробь $\frac{p_1}{q_1}$ является пределом систематической дроби с периодом $a_{s+1}, \ldots, a_{s+\tau}$. Теперь, учитывая (6.5) и (6.6), запишем окончательное равенство

$$\frac{r}{q} = \sigma\left(a_0 + \frac{p}{q}\right) = \sigma\left(a_0 + \sum_{n=1}^{s} a_n b^{-n} + \frac{1}{b^s} \cdot \frac{p_1}{q_1}\right) =$$
$$= \sigma\left(a_0 + \sum_{n=1}^{s} a_n b^{-n} + \sum_{n=s+1}^{\infty} a_n b^{-n}\right) = \sigma \sum_{n=0}^{\infty} a_n b^{-n},$$

в котором коэффициент a_0 определен равенством (6.5), коэффициенты $a_1, \ldots, a_s$ равенством (6.7), а образующие период коэффициенты $a_{s+1}, \ldots, a_{s+\tau}$ определены равенством (6.9). □

Приведенное доказательство теоремы 6.2 является конструктивным и в явном виде определяет способ представления рационального числа в виде систематической дроби. Покажем, как этот способ может быть применен на практике.

Пример 6.2. Представим рациональное число $\frac{368}{363}$ в виде систематической дроби по основанию $b = 11$. Легко видеть, что

$$\frac{368}{363} = 1 + \frac{5}{3 \cdot 11^2} = 1 + \frac{1}{11^2} \cdot \left(1 + \frac{2}{3}\right).$$

Теперь разложим $\frac{2}{3}$ в систематическую дробь. Для этого рассмотрим последовательность

$$\begin{aligned} 11^1 &= 3 \cdot 3 + 2, \\ 121 = 11^2 &= 40 \cdot 3 + 1, \ldots, \end{aligned}$$

определим $\tau = 2$ и запишем равенство

$$\frac{2}{3} = \frac{2 \cdot 40}{3 \cdot 40} = \frac{80}{11^2 - 1} = 80 \sum_{n=1}^{\infty} \left(11^2\right)^{-n}.$$

Воспользовавшись леммой 5.1, запишем равенство $80 = 3 + 7 \cdot 11$ и окончательное

представление

$$\frac{368}{363} = 1 + \frac{1}{11^2} \cdot \left(1 + \frac{7 \cdot 11 + 3}{11^2} + \frac{7 \cdot 11 + 3}{11^4} + \cdots\right) =$$
$$= 1 + \frac{1}{11^2} \cdot \left(1 + 7 \cdot 11^{-1} + 3 \cdot 11^{-2} + 7 \cdot 11^{-3} + \cdots\right) = 1,017373737373\ldots$$

Последнее равенство можно записать в более короткой форме с явным указанием основания системы счисления

$$\frac{368}{363} = 1,01(73)_{11}.$$

Для реализации описанного способа необходимо вычислить значение τ такое, что $q_1 | b^\tau - 1$. Это вычисление можно производить одновременно с вычислением коэффициентов систематической дроби. Верна следующая лемма.

Лемма 6.2. *Последовательность коэффициентов систематической дроби сходящейся к числу* $\frac{r}{q}$, *где* $q > 0$ *и* $\mathbf{НОД}(r,\ q) = 1$, *удовлетворяет соотношениям*

1. *коэффициент* $a_0 \in \mathbb{N}_0$ *удовлетворяет равенству* $|r| = a_0 q + p$, *где* $0 \leqslant p < q$,
2. *определим* $s \in \mathbb{N}_0$ *равенством* $\frac{p}{q} = \frac{p_1}{q_1 b^s}$; *если* $s \geqslant 1$, *то* $a_1 = \cdots = a_s = 0$,
3. *для индексов* $n = 1, 2, \ldots$ *выполнены равенства* $bp_n = a_{n+s} q_1 + p_{n+1}$.

Доказательство. Первые два утверждения леммы являются прямым следствием теоремы 6.2 и равенств (6.5) и (6.6). Докажем третье утверждение леммы. Пусть $0 < p_1 < q_1$, тогда домножая каждый раз на b и выполняя деление с остатком, мы получим следующую цепочку равенств

$$\frac{p_1}{q_1} = \frac{1}{b}\left(\frac{p_1 b}{q_1}\right) = \frac{1}{b}\left(a_{s+1} + \frac{p_2}{q_1}\right) =$$
$$= \frac{1}{b}\left(a_{s+1} + \frac{1}{b}\left(\frac{p_2 b}{q_1}\right)\right) = \frac{1}{b}\left(a_{s+1} + \frac{1}{b}\left(a_{s+2} + \frac{p_3}{q_1}\right)\right) = \cdots.$$

С другой стороны, для любого значения индекса $n \geqslant 1$ выполнено равенство

$$\frac{p_1}{q_1} = \frac{a_{s+1} q_1 + p_2}{b q_1} = \frac{b q_1 a_{s+1} + a_{s+2} q_1 + p_3}{b^2 q_1} = \cdots = \frac{b^{n-1} a_{s+1} + \cdots + a_{s+n}}{b^n} + \frac{p_{n+1}}{b^n q_1}.$$

Поскольку для всех возможных значений индекса n величина p_n принимает значения в ограниченном интервале $[0,\ldots,q-1]$, то найдется[1] такой индекс δ, что $p_1 = p_{\delta+1}$. Тогда

$$\frac{p_1}{q_1} = \frac{b^{\delta-1}a_{s+1} + \cdots + a_{s+\delta}}{b^\delta} + \frac{p_1}{b^\delta q_1}$$

и разложение числа $\frac{p_1}{q_1}$ в систематическую дробь зациклится. При этом δ определяет значение периода построенной систематической дроби.

Покажем, что это значение совпадает со значением, определенным в ходе доказательства теоремы 2.4. Обозначим $d = b^{\delta-1}a_{s+1} + \cdots + a_{s+\delta}$ и запишем равенство

$$p_1 b^\delta = dq_1 + p_1. \tag{6.10}$$

С другой стороны, из доказательства теоремы 2.4. см. (6.8), следует, что найдутся величины c и τ такие, что

$$b^\tau = cq_1 + 1 \quad \text{или} \quad p_1 b^\tau = cp_1 q_1 + p_1.$$

Предположим, что $\delta > \tau$ и вычтем полученное равенство из (6.10), тогда

$$p_1 b^\delta - p_1 b^\tau = dq_1 - cp_1 q_1$$

и, учитывая равенство $\mathbf{НОД}\,(b,\ q_1) = 1$, мы заключаем, что $p_1 | d$. Тогда из (6.10) получаем равенство

$$b^\delta - b^\tau = \left(\frac{d}{p_1}q_1 + 1\right) - cq_1 - 1 = q_1\left(\frac{d}{p_1} - c\right),$$

из которого вытекает неосуществимое условие $q_1 | b$. Аналогичное противоречие мы получаем рассматривая разность $b^\tau - b^\delta$ и предполагая, что $\tau > \delta$. Таким образом, равенства (6.8), (6.10) могут выполняться одновременно только при $\delta = \tau$ и $c = dp_1$. Лемма доказана. □

Пример 6.3. Воспользуемся соотношениями, введенными в третьем утверждении доказанной леммы, и представим дробь $\frac{2}{3}$ в виде систематической дроби по основанию $b = 11$

$$\frac{2}{3} = \frac{1}{11}\left(\frac{2\cdot 11}{3}\right) = \frac{1}{11}\left(7 + \frac{1}{3}\right) = \frac{1}{11}\left(7 + \frac{1}{11}\cdot\frac{1\cdot 11}{3}\right) =$$
$$= \frac{1}{11}\left(7 + \frac{1}{11}\cdot\left(3 + \frac{2}{3}\right)\right) = 0,(73)_{11},$$

т.е. то же самое значение, что и в предыдущем примере.

[1] Здесь используется «принцип ящиков» Дирихле.

6.2 Поле действительных чисел

Пусть

$$\alpha = \sum_{n=0}^{\infty} a_n b^{-n}, \quad \gamma = \sum_{n=0}^{\infty} c_n b^{-n}$$

тогда

$$\alpha + \gamma = \sum_{n=0}^{\infty} (a_n + b_n) b^{-n}$$

и

$$\alpha\gamma = \sum_{n=0}^{\infty} u_n b^{-n}, \quad u_n = \sum_{k=0}^{n} a_n c_{n-k}$$

Обратный по сложению – легко, как найти обратный по умножению?

Из условия $\alpha\gamma = 1$ получаем систему уравнений относительно неизвестных $c_0, c_1, \ldots$

$$\begin{aligned} a_0 c_0 &= 1, \\ a_0 c_1 + a_1 c_0 &= 0, \\ a_0 c_2 + a_1 c_1 + a_0 c_2 &= 0, \\ &\ldots \end{aligned}$$

тогда выполнены равенства

$$c_0 = \frac{1}{a_0}, \quad c_1 = -\frac{a_1 c_0}{a_0} = -\frac{a_1}{a_0^2}, \quad \ldots$$

и мы в явном виде получаем рациональные значения $c_0, c_1, \ldots \in \mathbb{Q}$. Раскладывая каждое из полученных значений в систематическую дробь по основанию b, получаем

$$c_n = \sum_{k=0}^{\infty} c_{n,k} b^{-k}, \quad \gamma = \sum_{n=0}^{\infty} c_n b^{-n} = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} c_{n,k} b^{-k-n}.$$

6.3 Критерии иррациональности

Определение 6.4. *Иррациональными числами мы будем называть действительные числа, являющиеся пределами бесконечных непериодичных систематических дробей.*

Пример 6.4. Из данного нами определения следует, что числа

$$\alpha_b = 0,010011000111\ldots\underbrace{0000\ldots0000}_{n\text{ штук}}\underbrace{1111\ldots1111}_{n\text{ штук}}\underbrace{0000\ldots0000}_{n+1\text{ штук}}\underbrace{1111\ldots1111}_{n+1\text{ штук}}\ldots,$$

являются действительными иррациональными числами при любом значении основания системы счисления $b > 1$.

В случае, если действительное число α не определено в явном виде в виде бесконечной непериодичной систематической дроби, мы можем предъявить два критерия, которые позволят определить, что α является иррациональным числом.

Для формулировки первого критерия нам понадобится следующее определение.

Определение 6.5. *Пусть* $a(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}[x]$ *– произвольный многочлен степени* n *от одной неизвестной. Мы будем называть число* α *корнем многочлена* $a(x)$*, если* α *удовлетворяет равенству*

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Теорема 6.3 (1-й критерий иррациональности)**.** *Если действительное число* α *является корнем унитарного многочлена с целыми коэффициентами*

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x],$$

то число α *либо целое, либо иррациональное.*

Доказательство. Поскольку α является корнем многочлена $a(x)$, то выполнено равенство

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha = 0.$$

Предположим, что α рациональное число и запишем $\alpha = \frac{p}{q}$, где $\mathbf{НОД}\,(p,\ \ q) = 1$ и $q > 0$. Тогда

$$a_0 + a_1\frac{p}{q} + \cdots + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \frac{p^n}{q^n} = 0,$$

и, перенося $\frac{p^n}{q^n}$ в правую часть равенства и домножая на q^n,

$$-p^n = a_0 q^n + a_1 q^{n-1} + \cdots + a_{n-1}q = q(a_0 q^{n-1} + a_1 q^{n-2} + \cdots + a_{n-1}).$$

Из последнего равенства следует, что $q|p^n$ и, следовательно, $q|p$. Последнее условие противоречит предположению о том, что p, q взаимно просты. Теорема доказана. □

Упражнение 6.1. Сформулируйте утверждение теоремы 6.3 для случая рациональных коэффициентов $a_0, \ldots, a_{n-1}$. Докажите сформулированное утверждение.

Пример 6.5. Иррацональные числа не образуют поле $\sqrt{2} \cdot \frac{\sqrt{2}}{3} = \frac{2}{3}$ – выводит за пределы множества иррациональных чисел.

Лемма 6.3. *Пусть α рациональное число, тогда существует такое число c, что для любой дроби $\frac{p}{q}$ такой, что $\alpha \neq \frac{p}{q}$, выполнено неравенство*

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{c}{q}.$$

Доказательство. Пусть $\alpha = \frac{a}{b}$ и $b > 0$, тогда для любой несократимой дроби $\frac{p}{q}$, $q > 0$, учитывая, что модуль разности двух целых чисел не менее 1, получаем неравенство

$$\left|\alpha - \frac{p}{q}\right| = \frac{|aq - pb|}{bq} \geqslant \frac{1}{bq}.$$

Следовательно, полагая $c = \frac{1}{b}$, получаем утверждение леммы. □

Теорема 6.4 (2-й критерий иррациональности)**.** *Пусть α действительное число. Если для любого положительного действительного числа c найдется хотя бы одна пара чисел p, q таких, что $\frac{p}{q} \neq \alpha$ и*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q},$$

то число q – иррационально.

Доказательство. Если α рационально, то по лемме найдется такая пара p, q, что $\left|\alpha - \frac{p}{q}\right| \geqslant \frac{c}{q}$, а это противоречит тому, что для этого c найдется хотя бы одна пара чисел p, q таких, что $\frac{p}{q} \neq \alpha$ и $\left|\alpha - \frac{p}{q}\right| < \frac{c}{q}$. Полученное противоречие завершает доказательство теоремы. □

Задачи и упражнения

Для закрепления изложенного теоретического материала предлагается самостоятельно решить следующие задачи и упражнения.

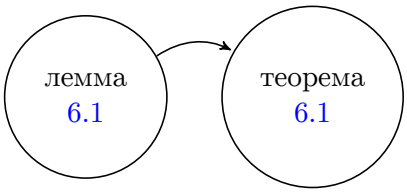
1. Постройте систематическую дробь для рациональных чисел 132, $\frac{11}{13}$ и $\frac{1}{7}$ в нескольких системах счисления с основаниями, равными $2, 3$ и 7.

Рекомендации к сдаче экзамена

Результаты настоящей главы, традиционно, выносятся на теоретический экзамен по курсу «Введение в теорию чисел». В экзаменационные билеты могут входить следующие вопросы.

- Понятие систематической дроби. Теорема о сходимости систематической дроби (теорема 6.1).
- Теорема о периодичности систематической дроби (теорема 6.2).
- Понятия действительного и иррационального числа. Теорема о единственности представления действительного иррационального числа систематической дробью (теорема **??**).
- Первый и второй критерии иррациональности (теоремы 6.3 и 6.4).

При подготовке к экзамену может быть полезным следующий график зависимости утверждений, используемых при доказательстве теорем.



Дополнительная литература

глава 7

Непрерывные дроби

Определение непрерывной дроби - Понятие подходящей дроби - Теорема о наилучшем приближении - Квадратичные иррациональности и их свойства - Иррациональности старших степеней - Эквивалентные числа - Подходящие дроби и наилучшие приближения.

Рассмотрим непрерывные дроби действительных чисел.

Определение 7.1. *Пусть α действительное число. Мы будем называть целой частью α, которую мы обозначаем символом $\lfloor\alpha\rfloor$, наибольшее целое число, меньшее, либо равное α. В частном случае: целая часть целого числа совпадает с ним.*

Отметим, что α может быть как отрицательным, так и положительным числом. Например $\lfloor\sqrt{13}\rfloor = 3$, в то время как $\lfloor-\sqrt{13}\rfloor = -4$. В любом случае выполнено неравенство $\lfloor\alpha\rfloor \leqslant \alpha$.

Пусть α_0 действительное число и $\alpha_0 \neq 0$. Определим последовательность действительных чисел $\alpha_1,\ \alpha_2,\ \ldots$ следующим рекуррентным соотношением

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \quad \text{где} \quad a_n = \lfloor\alpha_n\rfloor. \tag{7.1}$$

В случае, если α_n является целым числом, то есть выполнено равенство $a_n = \alpha_n$, мы будем считать, что последовательность (7.1) обрывается.

Записав равенство (7.1) в виде $\alpha_n = a_n + \dfrac{1}{\alpha_{n+1}}$, мы можем выразить число α_0 в виде

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \cfrac{1}{a_1 + \dfrac{1}{\alpha_2}} = \cdots$$

или, в общем виде,

$$\alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \dfrac{1}{\alpha_n}}}}, \tag{7.2}$$

для произвольного индекса n.

Для упрощенной записи равенства (7.2) мы будем использовать обозначение $\alpha_0 = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$.

Определение 7.2. *Пусть $\alpha_0 \neq 0$ действительное число. Мы будем называть представление (7.2)*

$$\alpha_0 = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{\alpha_n}}}},$$

$n = 1,\ 2,\ \ldots$ непрерывной или цепной дробью числа α_0. Элементы последовательности $a_0,\ a_1,\ \ldots$ мы будем называть неполными частными, а элементы последовательности $\alpha_1,\ \alpha_2,\ \ldots$ полными частными.

Заметим, что из соотношения (7.1) и неравенства $\lfloor \alpha \rfloor \leqslant \alpha$ вытекает выполнимость следующих неравенств

$$0 \leqslant \alpha_n - \lfloor \alpha_n \rfloor < 1 \quad \text{и} \quad \alpha_n > 1, \quad a_n \geqslant 1 \quad \text{при} \quad n \geqslant 1. \tag{7.3}$$

7.1 Конечные непрерывные дроби

Остановимся на частном случае, когда последовательность полных частных $\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_n$ конечна. Верна следующая лемма.

Лемма 7.1. *Пусть $\alpha_0 \neq 0$ действительное число. Последовательность полных частных $\alpha_1,\ \alpha_2,\ \ldots$, определяемая соотношениями (7.1), обрывается тогда и только тогда, когда α_0 рациональное число.*

Доказательство. Если последовательность конечна, то найдется индекс n, такой что α_n целое число и $\alpha_n = a_n$. Тогда $\alpha_{n-1} = a_{n-1} + \frac{1}{a_n}$ является рациональным числом. Выполняя аналогичные рассуждения для всех индексов, меньших n, получаем, что α_0 является рациональным числом.

Если α_0 рациональное число, то оно представимо в виде несократимой дроби $\alpha_0 = \frac{p}{q}$. Применим к числам p, q алгоритм Эвклида, см. алгоритм 2.1, а именно представим

$$p = a_0 q + r_1, \quad \text{где} \quad 0 \leqslant r_1 < q.$$

Тогда $\alpha_0 = \frac{p}{q} = a_0 + \frac{1}{\alpha_1}$, где $\alpha_1 = \frac{q}{r_1}$. Производя деление q на r_1 с остатком, получим

$$q = a_1 r_1 + r_2, \quad \text{где} \quad 0 \leqslant r_2 < r_1,$$

что равносильно $\alpha_1 = \frac{q}{r_1} = a_1 + \frac{1}{\alpha_2}$, где $\alpha_2 = \frac{r_1}{r_2}$.

Продолжая этот процесс, мы получим равенство

$$\alpha_n = \frac{r_{n-1}}{r_n},$$

где

$$\begin{aligned} &r_{-1} = p,\ r_0 = q, \\ &r_{n-1} = a_n r_n + r_{n+1}, \quad 0 \leqslant r_{n+1} < r_n. \end{aligned} \tag{7.4}$$

Последовательность $r_0,\ r_1, \ldots$ образует строго убывающую последовательность неотрицательных целых чисел, следовательно, найдется такой индекс n, что $r_{n+1} = 0$. Из этого равенства следует, что $\alpha_n = a_n = \frac{r_{n-1}}{r_n}$ является целым числом. Последнее рассуждение завершает доказательство леммы. □

Из утверждения доказанной нами леммы следует, что рассматриваемая последовательность $\alpha_1,\ \alpha_2,\ \ldots$ бесконечна, если α_0 является действительной иррациональностью, то есть не может быть представлено в виде несократимой дроби.

7.2 Понятие подходящей дроби

Для каждого индекса n мы можем рассмотреть рациональную дробь $\frac{P_n}{Q_n}$, определяемую равенством

$$\frac{P_n}{Q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} = [a_0, a_1, \ldots, a_{n-1}, a_n]. \tag{7.5}$$

Определение 7.3. *Пусть $\alpha_0 \neq 0$ действительное число. Дробь $\frac{P_n}{Q_n}$, определяемая равенством (7.5), называется подходящей дробью к числу α_0.*

Нам потребуются следующие леммы, описывающие свойства числителей и знаменателей подходящих дробей.

Лемма 7.2. *Пусть $\alpha_0 \neq 0$ действительное число. Для числителей P_n и знаменателей Q_n подходящих дробей числа α_0 выполнены следующие рекуррентные соотношения*

$$\begin{aligned} P_{n+1} &= a_{n+1} P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1} Q_n + Q_{n-1}, \end{aligned} \tag{7.6}$$

где $P_{-1} = 1,\ Q_{-1} = 0,\ P_0 = a_0,\ Q_0 = 1$.

Доказательство. Из определения 7.3 следуют равенства

$$\frac{P_0}{Q_0} = a_0, \quad \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1},$$

которые задают начальные значения для соотношений (7.6).

Проведем доказательство по индукции. Предположим, что утверждение леммы выполнено для всех индексов равных или меньших n, то есть выполнено равенство

$$\frac{P_n}{Q_n} = [a_0, a_1, \ldots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}}.$$

Тогда утверждение леммы следует из следующего равенства

$$\frac{P_{n+1}}{Q_{n+1}} = [a_0, a_1, \ldots, a_n, a_{n+1}] =$$

$$= \left[a_0, a_1, \ldots, a_n + \frac{1}{a_{n+1}}\right] = \frac{\left(a_n + \dfrac{1}{a_{n+1}}\right) P_{n-1} + P_{n-2}}{\left(a_n + \dfrac{1}{a_{n+1}}\right) Q_{n-1} + Q_{n-2}} =$$

$$= \frac{a_{n+1}\left(a_n P_{n-1} + P_{n-2}\right) + P_{n-1}}{a_{n+1}\left(a_n Q_{n-1} + Q_{n-2}\right) + Q_{n-1}} = \frac{a_{n+1} P_n + P_{n-1}}{a_{n+1} Q_n + Q_{n-1}}.$$

□

Основываясь на доказательстве леммы 7.2, легко заметить, что из равенства

$$[a_0, \ldots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}},$$

следует равенство

$$\alpha_0 = [a_0, \ldots, \alpha_{n+1}] = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}. \tag{7.7}$$

Отметим, что неравенство (7.3) и формулы (7.6) позволяют заключить, что числители и знаменатели подходящих дробей удовлетворяют неравенствам

$$P_n > 0, \quad Q_n > 0.$$

Далее мы будем считать, что действительное число α является как рациональным, так и иррациональным.

Лемма 7.3. *При всех индексах $n = 0, 1, \ldots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение*

$$P_{n+1} Q_n - Q_{n+1} P_n = (-1)^n. \tag{7.8}$$

Доказательство. Используя равенства (7.6), получим следующие равенства

$$\begin{aligned} P_{n+1}Q_n - Q_{n+1}P_n &= (a_{n+1}P_n + P_{n-1})Q_n - (a_{n+1}Q_n + Q_{n-1})P_n = \\ &= -(P_nQ_{n-1} - Q_nP_{n-1}) = (-1)^2(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) = \cdots \\ &= (-1)^k(P_{n-k+1}Q_{n-k} - Q_{n-k+1}P_{n-k}), \end{aligned}$$

для любого $k = 1,\ 2,\ \ldots$.

Подставляя в полученные равенства $k = n+1$ и начальные значения $P_{-1} = 1$, $P_0 = a_0$, $Q_{-1} = 0$, $Q_0 = 1$ из (7.6), получим равенство

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^{n+2},$$

которое равносильно утверждению леммы. □

Следствие 7.0.A. *Для любого индекса $n = 0,\ 1, \ldots$ подходящая дробь $\frac{P_n}{Q_n}$ несократима.*

Доказательство. Следствие очевидным образом следует из равенства (7.8). Если предположить обратное, то найдется целое число d_n такое, что $\mathbf{НОД}\,(P_n,\ Q_n) = d_n > 1$ и $d_n|(-1)^{n+1}$. Последнее условие невыполнимо. □

Докажем еще одно следствие, которое может быть использовано для решения сравнений первой степени.

Следствие 7.0.B. *Пусть a и m взаимно простые целые числа и $\frac{P_0}{Q_0},\ \ldots,\ \frac{P_n}{Q_n}$ последовательность подходящих дробей к числу $\alpha = \frac{m}{a}$. Тогда решение уравнения $ax \equiv b\ (mod\, m)$ удовлетворяет сравнению*

$$x \equiv (-1)^n bP_{n-1}\ (mod\, m)$$

для некоторого натурального индекса n.

Доказательство. Разложим число $\alpha = \frac{m}{a}$ в непрерывную дробь и определим последовательность подходящих дробей $\frac{P_0}{Q_0},\ \ldots,\ \frac{P_n}{Q_n}$. Поскольку α рациональное число, то согласно лемме 7.1, непрерывная дробь конечна и найдется индекс n такой, что $\frac{P_n}{Q_n} = \frac{m}{a}$.

Поскольку дробь $\frac{P_n}{Q_n}$ несократима, а числа m, a взаимно просты, то выполнены равенства $P_n = m, Q_n = a$. Тогда, из равенства (7.8) следует, что

$$mQ_{n-1} - aP_{n-1} = (-1)^{n-1}, \quad \text{или} \quad aP_{n-1} = (-1)^n + mQ_{n-1}.$$

Последнее равенство позволяет нам записать сравнение $aP_{n-1} \equiv (-1)^n \pmod m$ или, домножая на $(-1)^n b$, сравнение $a(-1)^n bP_{n-1} \equiv b \pmod m$. Последнее сравнение в явном виде определяет значение неизвестного x, а именно, $x \equiv (-1)^n bP_{n-1} \pmod m$. Следствие доказано. □

Внимательному читателю остается показать, в качестве упражнения, что алгоритм решения сравнения $ax \equiv b \pmod m$, основанный на доказанном следствии, полностью аналогичен расширенному алгоритму Эвклида, см. алгоритм **??**.

Далее нам потребуется следующая лемма.

Лемма 7.4. *При всех индексах $n = 0, 1, \ldots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение*

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(-1)^{n+1}. \tag{7.9}$$

Доказательство. Для доказательства леммы домножим первое равенство в (7.6) на Q_{n-1} и вычтем из полученного второе равенство из (7.6), домноженное на P_{n-1}. Учитывая предыдущую лемму, получаем, с точностью до показателя степени при -1, искомое равенство

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(P_nQ_{n-1} - Q_nP_{n-1}) = a_{n+1}(-1)^{n-1}.$$

□

Доказанные нами леммы 7.3 и 7.4 позволяют получить явное представление о расположении на действительной оси элементов последовательности подходящих дробей. Согласно утверждению леммы 7.3 выполнены неравенства $\frac{P_{2k+1}}{Q_{2k+1}} > \frac{P_{2k}}{Q_{2k}}$ при некотором натуральном k. Далее, из утверждения леммы 7.4 следует, что $\frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}}$ и $\frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}}$ при некотором натуральном k, то есть элементы последовательности с нечетными номерами образуют возрастающую подпоследовательность, а элементы с четными номерами – убывающую. Получаем цепочку неравенств

$$\ldots \frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}} > \ldots > \frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}} > \ldots \tag{7.10}$$

из которой следует, что последовательность подходящих дробей сходится и имеет предел. Чему равен этот предел определяет теорема 7.1, к доказательству которой мы скоро приступим.

Лемма 7.5. *Для всех индексов $n = 1,\ 2,\ \ldots$ знаменатели Q_n подходящих дробей удовлетворяют неравенству $Q_{n+1} > 2^{\lceil \frac{n}{2} \rceil}$ или, что равносильно*

$$\begin{cases} Q_{n+1} \geqslant 2^{\frac{n}{2}}, & \text{при четном } n, \\ Q_{n+1} \geqslant 2^{\frac{n+1}{2}}, & \text{при нечетном } n. \end{cases} \tag{7.11}$$

Доказательство. Из соотношений (7.3) и (7.6) следует неравенство

$$Q_{n+1} = a_{n+1}Q_n + Q_{n-1} \geqslant Q_n + Q_{n-1} \geqslant 2Q_{n-1} + Q_{n-2} \geqslant 2Q_{n-1},$$

из которого следует утверждение леммы – при нечетном n выполнено неравенство $Q_{n+1} \geqslant 2^{\frac{n+1}{2}} Q_0 = 2^{\frac{n+1}{2}}$, а при четном n – выполнено неравенство $Q_{n+1} \geqslant 2^{\frac{n}{2}} Q_1 \geqslant 2^{\frac{n}{2}}$. □

Теперь мы можем доказать теорему о приближении числа α_0 последовательностью подходящих дробей.

Теорема 7.1. *Пусть $\alpha_0 \neq 0$ действительное число. Тогда последовательность подходящих дробей сходится к α_0, то есть выполнено условие*

$$\alpha_0 = \lim_{n\to\infty} \frac{P_n}{Q_n}.$$

Доказательство. Сначала мы покажем, что последовательность подходящих дробей сходится. Действительно, из леммы 7.3 получаем равенство

$$\left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n Q_{n+1}} \left|P_{n+1}Q_n - Q_{n+1}P_n\right| = \frac{1}{Q_n Q_{n+1}}.$$

Из этого равенства и из утверждения леммы 7.5 следует, что последовательность подходящих дробей сходится, то есть

$$\lim_{n\to\infty} \left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = 0.$$

Нам осталось выяснить чему равен предел последовательности подходящих дробей. Учитывая равенство (7.7) и утверждение леммы 7.3, получим следующее равенство

$$\begin{aligned}\alpha_0 - \frac{P_n}{Q_n} = \frac{1}{Q_n}\left(\alpha_0 Q_n - P_n\right) = \\ = \frac{1}{Q_n}\left(Q_n \frac{\alpha_{n+1}P_n + P_{n-1}}{\alpha_{n+1}Q_n + Q_{n-1}} - P_n\right) = \\ = \frac{1}{Q_n}\left(\frac{Q_n P_{n-1} - P_n Q_{n-1}}{\alpha_{n+1}Q_n + Q_{n-1}}\right) = \frac{(-1)^n}{Q_n\left(\alpha_{n+1}Q_n + Q_{n-1}\right)}. \quad (7.12)\end{aligned}$$

Вспоминая, что α_n и Q_n положительны при всех $n \geqslant 1$, получаем неравенство

$$\begin{aligned}\left|\alpha_0 - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n\left(\alpha_{n+1}Q_n + Q_{n-1}\right)} \leqslant \\ \frac{1}{Q_n\left(a_{n+1}Q_n + Q_{n-1}\right)} = \frac{1}{Q_{n+1}Q_n}, \quad (7.13)\end{aligned}$$

из которого вытекает утверждение теоремы. □

Из доказанной нами теоремы следует, что мы можем приблизить действительное число α_0 при помощи рациональной дроби с любой степенью точности. В качестве такой дроби выступает некоторая подходящая дробь. Используя подходящие дроби, можно производить эффективные вычисления с действительными числами, при некотором, заранее заданном, уровне погрешности вычислений.

Пример 7.1. Отойдем от общего случая и рассмотрим частный пример, а именно, разложим $\alpha_0 = \sqrt{29}$ в непрерывную дробь.
Используя равенства (7.1) и (7.6), запишем

$$\alpha_0 = \sqrt{29} \sim 5.3851648, \quad a_0 = \lfloor \sqrt{29} \rfloor = 5, \quad P_0 = 5, Q_0 = 1,$$
$$\alpha_1 = \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{(\sqrt{29} - 5)(\sqrt{29} + 5)} = \frac{\sqrt{29} + 5}{4},$$
$$a_1 = \lfloor \alpha_1 \rfloor = \left\lfloor \frac{\sqrt{29} + 5}{4} \right\rfloor = 2, \quad P_1 = 11, \quad Q_1 = 2, \quad \frac{P_1}{Q_1} = 5.5,$$

аналогично мы получим следующие равенства

$$\alpha_2 = \frac{1}{\frac{\sqrt{29} + 5}{4} - 2} = \frac{\sqrt{29} + 3}{5}, \quad a_2 = 1, \quad \frac{P_2}{Q_2} = \frac{16}{3} = 5.333333,$$
$$\alpha_3 = \frac{1}{\frac{\sqrt{29} + 3}{5} - 1} = \frac{\sqrt{29} + 2}{5}, \quad a_3 = 1, \quad \frac{P_3}{Q_3} = \frac{27}{5} = 5.4,$$
$$\alpha_4 = \frac{1}{\frac{\sqrt{29} + 2}{5} - 1} = \frac{\sqrt{29} + 3}{4}, \quad a_4 = 2, \quad \frac{P_4}{Q_4} = \frac{70}{13} = 5.3846154,$$
$$\alpha_5 = \frac{1}{\frac{\sqrt{29} + 3}{4} - 2} = \sqrt{29} + 5, \quad a_5 = 10, \quad \frac{P_5}{Q_5} = \frac{727}{135} = 5.3851852,$$
$$\alpha_6 = \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{4}, \quad a_6 = 2, \quad \frac{P_6}{Q_6} = \frac{1524}{283} = 5.385159,$$
$$\alpha_7 = \frac{1}{\frac{\sqrt{29} + 5}{4} - 2} = \frac{\sqrt{29} + 3}{5}, \quad a_7 = 1, \quad \frac{P_7}{Q_7} = \frac{2251}{418} = 5.3851675.$$

Мы остановим наши вычисления и заметим, что выполнены равенства

$$\alpha_6 = \alpha_1, \quad \alpha_7 = \alpha_2, \ \ldots,$$

то есть наша последовательность полных частных зациклилась и имеет период равный 5. Мы можем записать непрерывную дробь для $\alpha_0 = \sqrt{29}$ в виде

$$\sqrt{29} = [5; 2, 1, 1, 2, 10, 2, 1, 1, 2, 10, \ldots]$$

или, в еще более короткой форме, $\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$. Отметим, что всего за семь шагов мы получили очень хорошее приближение к α_0. Действительно,

$$\left| \alpha_0 - \frac{P_7}{Q_7} \right| = 0.0000027 < \frac{1}{Q_8 Q_7} = \frac{1}{701 \cdot 418} = 0.0000034.$$

7.3 Квадратичные иррациональности

Напомним, что целое число D называется полным квадратом, если найдется целое число d такое, что $D = d^2$.

Определение 7.4. *Действительное число α называется квадратичной иррациональностью, если найдутся такие целые, взаимно простые числа $u > 0$, v, w, что значение $v^2 - 4uw > 0$ не является полным квадратом, а α является одним из корней многочлена $f(x) = ux^2 + vx + w$, то есть $f(\alpha) = 0$.*

Величина $D = v^2 - 4uw$ называется дискриминантом квадратичной иррациональности α.

Пример 7.2. Проиллюстрируем понятие квадратичной иррациональности. Легко видеть, что значение $\alpha = \sqrt{29}$ является корнем многочлена $f(x) = x^2 - 29$ и, соответственно, квадратичной иррациональностью. Также квадратичной иррациональностью является корень многочлена $f(x) = 3x^2 - 5x - 7$ равный $\alpha = \dfrac{5 + \sqrt{109}}{2}$.

Из определения 7.4 следует, что любая квадратичная иррациональность может быть представлена в виде

$$\alpha = \frac{A + \sqrt{D}}{B}, \tag{7.14}$$

где A, B, D – целые числа, $D = v^2 - 4uw$ не является полным квадратом и

$$\begin{cases} A = -v, B = 2u, & \text{либо} \\ A = v, B = -2u, \end{cases} \tag{7.15}$$

в зависимости от того, какой из двух корней многочлена $f(x)$ выбирается. Если величина D удовлетворяет сравнению $D \equiv 0 \pmod 4$, то из равенства $v^2 = D + 4uv$ следует, что величина v четна. Тогда равенства (7.15) принимают вид

$$A = \mp v, B = \pm u. \tag{7.16}$$

Возникает вопрос: единственно ли указанное представление? Для ответа на него предположим, что равенство (7.14) не единственно, то есть найдется еще одна пара целых чисел C, E таких, что $\alpha = \dfrac{C + \sqrt{D}}{E}$. Тогда выполнено равенство

$$E(A + \sqrt{D}) = B(C + \sqrt{D}),$$

откуда

$$EA - BC = (B - E)\sqrt{D}. \tag{7.17}$$

В левой части равенства (7.17), в силу выбора значений A, B, C, E, находится целое число. В правой части – произведение целого числа на корень из N, не являющегося полным квадратом, то есть действительное число. Таким образом, равенство (7.17) может быть выполнено только в том случае, если в обеих его частях находятся нули. Из этого следует, что $B = E$, $A = C$ и представление (7.17) единственно.

Определение 7.5. *Пусть* $\alpha = \dfrac{A + \sqrt{D}}{B}$ *квадратичная иррациональность – корень многочлена* $f(x) = ux^2 + vx + w$. *Тогда второй корень этого многочлена*

$$\hat{\alpha} = \frac{A - \sqrt{D}}{B}$$

называется квадратичной иррациональностью, сопряженной с α.

Легко показать, что каждое действительное число, представимое в виде (7.14), является квадратичной иррациональностью. Введем многочлен с целыми коэффициентами

$$\begin{aligned} f(x) = B^2(x - \alpha)(x - \hat{\alpha}) = \\ = (Bx - A - \sqrt{D})(Bx - A + \sqrt{D}) = \\ = (Bx - A)^2 - D = B^2x^2 - 2ABx + A^2 - D. \end{aligned} \quad (7.18)$$

Получаем, что α является корнем многочлена $f(x)$ второй степени с целыми коэффициентами. Если $A^2 - D$ делится на B, то коэффициенты многочлена можно сократить на общий множитель.

Используя преобразование (7.1), разложим квадратичную иррациональность $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$, являющуюся корнем многочлена $f(x) = ux^2 + vx + w$, в непрерывную дробь.

Для полного частного α_1 выполнено равенство

$$\begin{aligned} \alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\dfrac{A_0 + \sqrt{D}}{B_0} - a_0} = \frac{B_0}{(A_0 - a_0B_0) + \sqrt{D}} = \\ = \frac{B_0\,(A_0 - a_0B_0) - B_0\sqrt{D}}{(A_0 - a_0B_0)^2 - D}. \end{aligned} \quad (7.19)$$

Обозначим символом $\hat{\alpha}_0 = \dfrac{A_0 - \sqrt{D}}{B_0}$ второй корень многочлена $f(x)$. Тогда, используя теорему Виета, получим равенство

$$\alpha_0\hat{\alpha}_0 = \left(\frac{A_0 + \sqrt{D}}{B_0}\right)\left(\frac{A_0 - \sqrt{D}}{B_0}\right) = \frac{w}{u},$$

откуда $A_0^2 - D = \frac{wB_0^2}{u}$. Обозначим $B_{-1} = -\frac{wB_0}{u}$ и получим необходимое нам равенство $-B_{-1}B_0 = A_0^2 - D$, при этом из (7.15) и (7.16) следует, что B_{-1} является целым числом. Подставляя полученное равенство в (7.19) и сокращая на $-B_0$, получим

$$\alpha_1 = \frac{(a_0B_0 - A_0) + \sqrt{D}}{2a_0A_0 - a_0^2B_0 + B_{-1}} = \frac{A_1 + \sqrt{D}}{B_1},$$

где

$$A_1 = a_0B_0 - A_0,$$
$$B_1 = a_0(2A_0 - a_0B_0) + B_{-1} = a_0(A_0 - A_1) + B_{-1}.$$

Мы получили, что полное частное α_1 имеет такой же вид, как α_0 и также является квадратичной иррациональностью. Более того, значения A_1, B_1 могут быть выражены через значения A_0, B_0 и коэффициенты многочлена $f(x)$. Обобщим полученный результат и докажем следующую лемму.

Лемма 7.6. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *квадратичная иррациональность, являющаяся корнем многочлена* $f(x) = ux^2 + vx + w$, $D = v^2 - 4uw$, *и* $\alpha_0,\ \alpha_1,\ \ldots, \alpha_n, \ldots$ *последовательность полных частных.*

Тогда для каждого полного частного α_{n+1} *выполнено равенство*

$$\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}},$$

где

$$\begin{aligned} A_{n+1} &= a_nB_n - A_n, \\ B_{n+1} &= a_n(A_n - A_{n+1}) + B_{n-1}, \end{aligned} \tag{7.20}$$

при $B_{-1} = -\frac{wB_0}{u}$, *а также выполнено равенство*

$$-B_nB_{n+1} = \left(A_{n+1}^2 - D\right).$$

Доказательство. Мы проведем доказательство по индукции. Выполнимость утверждений леммы для α_1 мы проверили выше. Предположим, что для всех индексов $1, \ldots, n$ утверждение леммы выполнено, тогда, аналогично (7.19), получаем

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{B_n}{(A_n - a_nB_n) + \sqrt{D}} = \\ = \frac{-B_n\left(A_{n+1} + \sqrt{D}\right)}{A_{n+1}^2 - D}, \tag{7.21}$$

где $A_{n+1} = (a_n B_n - A_n)$.

Покажем, что $B_n | \left(A_{n+1}^2 - D\right)$. В силу предположения индукции выполнено $B_n | \left(A_n^2 - D\right)$. Тогда из (7.21) и следующего равенства

$$A_{n+1}^2 - D = (a_n B_n - A_n)^2 - D = a_n^2 B_n^2 - 2a_n A_n B_n + A_n^2 - D$$

следует, что $B_n | \left(A_{n+1}^2 - D\right)$. Обозначим $B_{n+1} = \dfrac{A_{n+1}^2 - D}{-B_n}$, тогда

$$-B_n B_{n+1} = \left(A_{n+1}^2 - D\right). \tag{7.22}$$

Подставляя (7.22) в (7.21), получим приведенное в утверждении леммы равенство $\alpha_{n+1} = \dfrac{A_{n+1} + \sqrt{D}}{B_{n+1}}$. Нам осталось получить рекуррентную формулу для B_{n+1}.

Из (7.21), с учетом изменения индексов в равенстве (7.22), получаем

$$\begin{aligned} B_{n+1} = \frac{A_{n+1}^2 - D}{-B_n} &= \frac{(a_n B_n - A_n)^2 - D}{-B_n} = \\ &= \frac{-B_n(2a_n A_n - a_n^2 B_n) + A_n^2 - D}{-B_n} = \\ &= a_n \left(2A_n - a_n B_n\right) + B_{n-1} = a_n(A_n - A_{n+1}) + B_{n-1}. \end{aligned}$$

□

Доказанная лемма определяет соотношения (7.20), которые используются для эффективного разложения квадратичной иррациональности в непрерывную дробь.

В рассмотренном нами ранее на стр. 123 примере разложение квадратичной иррациональности в непрерывную дробь оказалось периодично. Покажем, что это свойство верно для любой квадратичной иррациональности.

Для этого нам потребуется ввести еще одно определение и доказать две вспомогательные леммы.

Определение 7.6. *Пусть α – квадратичная иррациональность и $\hat{\alpha}$, сопряженная с α. Тогда α называется приведенной квадратичной иррациональностью, если*

$$\alpha > 1 \quad и \quad -1 < \hat{\alpha} < 0. \tag{7.23}$$

Лемма 7.7. *Пусть $\alpha = \dfrac{A + \sqrt{D}}{B}$ приведенная квадратичная иррациональность. Тогда*

$$\begin{aligned} &0 < A < \sqrt{D}, \\ &0 < B < 2\sqrt{D}. \end{aligned}$$

Доказательство. Пусть α удовлетворяет условию леммы, тогда из неравенств (7.23) вытекают следующие утверждения.

1. Так как $\alpha - \hat{\alpha} = \dfrac{2\sqrt{D}}{B} > 0$ и $\sqrt{D} > 0$, то выполнено $B > 0$.
2. Так как $\alpha - \hat{\alpha} = \dfrac{2\sqrt{D}}{B} > 1$, то выполнено $2\sqrt{D} > B$.
3. Так как $\alpha + \hat{\alpha} = \dfrac{2A}{B} > 0$ и $B > 0$, то выполнено $A > 0$.
4. Так как $\hat{\alpha} = \dfrac{A - \sqrt{D}}{B} < 0$ и $B > 0$, то выполнено неравенство $A < \sqrt{D}$ и лемма доказана.

□

Лемма 7.8. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *квадратичная иррациональность и* $\hat{\alpha}_1, \hat{\alpha}_2, \ldots$ *сопряженные полных частных ее разложения в непрерывную дробь. Тогда выполнены следующие утверждения.*

1. *Для всех* $n \geqslant 0$ *верно равенство*
$$\hat{\alpha}_{n+1} = \frac{1}{\hat{\alpha}_n - a_n}. \tag{7.24}$$
2. *Значение* $\hat{\alpha}_{n+1}$ *удовлетворяет равенству*
$$\hat{\alpha}_{n+1} = -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n}. \tag{7.25}$$

Доказательство. Учитывая (7.22), первое утверждение леммы получаем из равенства

$$\frac{1}{\hat{\alpha}_n - a_n} = \frac{B_n}{(A_n - a_n B_n) - \sqrt{D}} = \\ = \frac{B_n\left(-A_{n+1} + \sqrt{D}\right)}{A_{n+1}^2 - D} = \frac{-A_{n+1} + \sqrt{D}}{-B_{n+1}} = \hat{\alpha}_{n+1}.$$

Докажем второе утверждение леммы. Используя первое утверждение леммы, разложим $\hat{\alpha}_0$ в непрерывную дробь

$$\hat{\alpha}_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{\hat{\alpha}_{n+1}}}}}.$$

Таким образом, последовательность подходящих дробей для $\hat{\alpha}_0$ совпадает с последовательностью подходящих дробей $\frac{P_n}{Q_n}$ для α_0 и, согласно (7.7), выполнено равенство

$$\hat{\alpha}_0 = \frac{\hat{\alpha}_{n+1}P_n + P_{n-1}}{\hat{\alpha}_{n+1}Q_n + Q_{n-1}}.$$

Выражая из него $\hat{\alpha}_{n+1}$, получим соотношение (7.25). □

Теорема 7.2. *Пусть* $\alpha = \dfrac{A + \sqrt{D}}{B}$ *квадратичная иррациональность. Тогда ее непрерывная дробь периодична.*

Доказательство. Вначале предположим, что α_0 приведенная квадратичная иррациональность, то есть

$$\alpha_0 > 1, \quad a_0 \geqslant 1, \quad -1 < \hat{\alpha}_0 < 0.$$

Тогда из (7.3) следует, что $\alpha_1 > 1$. Далее, следуя равенству (7.24), получим

$$\frac{1}{\hat{\alpha}_1} = \hat{\alpha}_0 - a_0 < 0 - a_0 \leqslant -1,$$

следовательно, $-1 < \hat{\alpha}_1 < 0$ и α_1 является приведенной квадратичной иррациональностью.

Продолжая далее, мы получим, что α_2 и все остальные полные частные $\alpha_n = \dfrac{A_n + \sqrt{D}}{B_n}$ являются приведенными квадратичными иррациональностями. Из леммы 7.7 следует, что значения A_n, B_n неотрицательны, ограничены сверху и бесконечная последовательность пар A_n, B_n принимает значения на конечном множестве. Следовательно, найдется некоторый индекс n_0 такой, что $A_0 = A_{n_0}$, $B_0 = B_{n_0}$ и последовательность α_n зациклится или, другими словами, периодична.

Для завершения доказательства теоремы нам осталось показать, что для любой квадратичной иррациональности α_0 найдется такой индекс n_0, что α_{n_0} является приведенной квадратичной иррациональностью.

Вначале рассмотрим частный случай. Пусть

$$\alpha_0 = A_0 + \sqrt{D}$$

и α_0 не является приведенной. Тогда $a_0 = A_0 + \lfloor\sqrt{D}\rfloor$ и равенство (7.24) позволяет записать неравенства

$$-1 < \hat{\alpha}_1 = \frac{1}{\hat{\alpha}_0 - a_0} = \frac{-1}{\sqrt{D} + \lfloor\sqrt{D}\rfloor} < 0.$$

Следовательно, α_1 приведенная квадратичная иррациональность.

Теперь перейдем к общему случаю. Рассмотрим равенство (7.25) и, учитывая равенство (7.12), полученное в ходе доказательства теоремы 7.1, при $n \geqslant 1$, получим

$$\hat{\alpha}_{n+1} = -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n} = \\ = -\frac{Q_{n-1}}{Q_n}\left(\frac{\hat{\alpha}_0 - \frac{P_{n-1}}{Q_{n-1}}}{\hat{\alpha}_0 - \frac{P_n}{Q_n}}\right) = -\frac{Q_{n-1}(1+\omega_{n+1})}{Q_n}, \quad (7.26)$$

где точное значение ω_{n+1} определено равенством

$$\omega_{n+1} = \frac{\left(\frac{(-1)^{n-1}}{Q_{n-1}(\alpha_n Q_{n-1}+Q_{n-2})} - \frac{(-1)^n}{Q_n(\alpha_{n+1}Q_n+Q_{n-1})}\right)}{\hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1}Q_n+Q_{n-1})}}. \quad (7.27)$$

Равенство (7.26) позволяет сделать следующее заключение. Если величина ω_{n+1} удовлетворяет неравенствам

$$-1 < \omega_{n+1} < \frac{Q_n}{Q_{n-1}} - 1, \quad (7.28)$$

то, при $n \geqslant 1$, из (7.26) вытекают неравенства $-1 < \hat{\alpha}_{n+1} < 0$. Следовательно, α_{n+1} приведенная квадратичная иррациональность и, как мы доказали ранее, ее разложение в непрерывную дробь периодично. Следовательно, периодично разложение для α_0.

Нам осталось показать, что найдется индекс $n \geqslant 1$, для которого выполнены неравенства (7.28). Рассмотрим равенство (7.27) более подробно и обозначим символом δ_{n+1} числитель дроби, то есть

$$\delta_{n+1} = \\ (-1)^{n-1}\left(\frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})}\right).$$

Поскольку α_n и Q_n положительные целые числа, то выполнено $|\delta_{n+1}| < 1$. Более того

$$|\delta_{n+1}| = \frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})} \leqslant \\ \leqslant \frac{1}{Q_{n-1}(a_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(a_{n+1}Q_n + Q_{n-1})} = \\ \frac{1}{Q_n Q_{n-1}} + \frac{1}{Q_{n+1}Q_n} = \frac{1}{Q_n}\left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}}\right). \quad (7.29)$$

Обозначим $\gamma = \hat{\alpha}_0 - \alpha_0$ и рассмотрим знаменатель дроби (7.27), тогда

$$\left|\hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})}\right| \geqslant$$
$$|\gamma| - \frac{1}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})} \geqslant |\gamma| - \frac{1}{Q_{n+1}Q_n}.$$

С учетом (7.29), мы получили следующее неравенство

$$|\omega_{n+1}| \leqslant \frac{|\delta_{n+1}|}{|\gamma| - \frac{1}{Q_{n+1}Q_n}} \leqslant$$
$$\left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}}\right)\frac{Q_{n+1}}{Q_{n+1}Q_n|\gamma| - 1} =$$
$$= \frac{Q_{n+1} + Q_{n-1}}{Q_{n+1}Q_nQ_{n-1}|\gamma| - Q_{n-1}}.$$

Полученное неравенство позволяет нам сделать вывод о том, что всегда найдется индекс n, при котором будут выполнены ограничения на ω_{n+1}, то есть неравенства (7.28). Если $|\gamma|$ принимает большие значения, например $|\gamma| > 1$, то выполнение неравенств (7.28) очевидно. Более тонким является случай, когда значения $|\gamma|$ близки к нулю.

Предположим, что $|\gamma|$ ограничен снизу величиной

$$|\gamma| > \frac{3}{Q_nQ_{n-1}} = \frac{3Q_{n+1}}{Q_{n+1}Q_nQ_{n-1}} > \frac{Q_{n+1} + 2Q_{n-1}}{Q_{n+1}Q_nQ_{n-1}},$$

тогда выполнено $|\omega_{n+1}| < 1$.

В силу того, что Q_n образуют монотонно возрастающую последовательность, замечаем, что для сколь угодно малого значения $\gamma = \hat{\alpha}_0 - \alpha_0$ найдется такой индекс n, что будет выполнено неравенство $|\gamma| > \frac{3}{Q_nQ_{n-1}}$ и, следовательно, $|\omega_{n+1}| < 1$. □

Доказанная нами теорема позволяет получить оценку на величину индекса n, начиная с которого полные частные α_n станут приведенными квадратичными иррациональностями.

Следствие 7.2.А. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *квадратичная иррациональность, являющаяся корнем многочлена* $f(x) = ux^2 + vx + w$, $u, v, w \in \mathbb{Z}$, *где* $u > 0$ *и* $D = v^2 - 4uw$. *Тогда* α_n *приведенная квадратичная иррациональность, если*

$$n > \log_2\left(\frac{6u}{\sqrt{D}}\right).$$

Доказательство. Вспомним, что

$$\gamma = \hat{\alpha}_0 - \alpha_0 = \pm\frac{2\sqrt{D}}{B_0} = \pm\frac{\sqrt{D}}{u},$$

тогда из условия леммы следуют неравенства

$$n > \log_2\left(\frac{6u}{\sqrt{D}}\right) = \log_2\left(\frac{6}{|\gamma|}\right) \quad \text{и} \quad 2^{n-1} > \frac{3}{|\gamma|}.$$

Из утверждения леммы 7.5 получаем

$$Q_n Q_{n-1} \geqslant 2^{n-1} > \frac{3}{|\gamma|} \quad \text{или} \quad |\gamma| > \frac{3}{Q_n Q_{n-1}}.$$

Таким образом, $|\omega_{n+1}| < 1$ и следствие доказано. □

Теорема 7.2 позволяет говорить, что разложение любой квадратичной иррациональности периодично. Верно и обратное утверждение.

Теорема 7.3. *Пусть последовательность полных частных $\alpha_0 = \alpha$, α_1, α_2, ... периодична. Тогда α является квадратичной иррациональностью.*

Доказательство. Воспользуемся (7.7) и запишем равенство

$$\alpha_n = \frac{P_{n-2} - \alpha_0 Q_{n-2}}{\alpha_0 Q_{n-1} - P_{n-1}},$$

выполненное для любого индекса $n = 1,\ 2,\ \ldots$.

Из определения периодичности следует, что найдутся два индекса n и m, для которых будет выполнено равенство $\alpha_n = \alpha_m$. Тогда

$$\frac{P_{n-2} - \alpha_0 Q_{n-2}}{\alpha_0 Q_{n-1} - P_{n-1}} = \frac{P_{m-2} - \alpha_0 Q_{m-2}}{\alpha_0 Q_{m-1} - P_{m-1}},$$

откуда следует, что

$$\alpha_0^2 \left(Q_{m-1}Q_{n-2} + Q_{m-2}Q_{n-1}\right) + \alpha_0 \left(Q_{m-1}P_{n-2} + P_{m-1}Q_{n-2} - P_{m-2}Q_{n-1} - Q_{m-2}P_{n-1}\right) + P_{m-2}P_{n-1} - P_{m-1}P_{n-2} = 0.$$

Таким образом, величина α_0 является корнем квадратного трехчлена с целыми коэффициентами. Поскольку величины Q_n больше нуля, то старший коэффициент построенного трехчлена отличен от нуля, следовательно, величина α_0 является квадратичной иррациональностью. □

Нам осталось доказать последнюю теорему, которая позволяет связать между собой числители и знаменатели подходящих дробей и коэффициенты A_n, B_n разложения квадратичной иррациональности в непрерывную дробь.

Теорема 7.4. *Пусть* $\alpha_0 = \dfrac{A_0 + \sqrt{D}}{B_0}$ *действительная квадратичная иррациональность и* $\alpha_1, \alpha_2, \ldots$ *последовательность полных частных, удовлетворяющих равенству*

$$\alpha_n = \frac{A_n + \sqrt{D}}{B_n}.$$

Тогда для всех индексов $n = 1, 2, \ldots$ *числители* P_n *и знаменатели* Q_n *подходящих дробей для* α_0 *удовлетворяют равенству*

$$\bigl(P_n B_0 - Q_n A_0\bigr)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}. \tag{7.30}$$

Доказательство. Согласно (7.7), для любого индекса $n = 0, 1, \ldots$, мы можем записать равенство

$$\alpha_0 = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}.$$

Вспоминая, что $\alpha_{n+1} = \dfrac{A_{n+1} + \sqrt{D}}{B_{n+1}}$, получим равенство

$$\frac{A_0 + \sqrt{D}}{B_0} = \frac{P_n(A_{n+1} + \sqrt{D}) + B_{n+1} P_{n-1}}{Q_n(A_{n+1} + \sqrt{D}) + B_{n+1} Q_{n-1}},$$

которое равносильно

$$B_0\bigl(P_n(A_{n+1} + \sqrt{D}) + B_{n+1} P_{n-1}\bigr) = \\ = \bigl(A_0 + \sqrt{D}\bigr)\bigl(Q_n(A_{n+1} + \sqrt{D}) + B_{n+1} Q_{n-1}\bigr).$$

Раскрывая в последнем равенстве скобки и приводя слогаемые со множителем $\sqrt{D}$, получим равенство

$$B_0 B_{n+1} P_{n-1} - A_0 A_{n+1} Q_n - A_0 B_{n+1} Q_{n-1} + B_0 P_n A_{n+1} - Q_n D = \\ = \bigl(A_0 Q_n + A_{n+1} Q_n + B_{n+1} Q_{n-1} - B_0 P_n\bigr)\sqrt{D}.$$

Применяя к последнему равенству рассуждения, аналогичные тем, что были применены к равенству (7.17), получим, что правая и левая части равенства равны нулю. Это позволяет из правой части равенства получить выражение для знаменателя Q_{n-1}

$$Q_{n-1} = \frac{B_0 P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}}, \tag{7.31}$$

а также из левой части равенства, для числителя P_{n-1}

$$P_{n-1} = \frac{A_0A_{n+1}Q_n + A_0B_{n+1}Q_{n-1} + Q_nD - B_0P_nA_{n+1}}{B_0B_{n+1}} = \\ = \frac{Q_n(D - A_0^2) - B_0P_n(A_{n+1} - A_0)}{B_0B_{n+1}}. \quad (7.32)$$

Теперь рассмотрим утверждение леммы 7.3 и равенство (7.8), в правой части которого индекс n заменен на индекс $n-1$, а в левой $(-1)^{n-1}$ на $(-1)^{n+1}$

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}.$$

Подставляя в него полученные выше выражения (7.31), (7.32), запишем

$$P_n\frac{B_0P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}} - \\ - Q_n\frac{Q_n(D - A_0^2) - B_0P_n(A_{n+1} - A_0)}{B_0B_{n+1}} = (-1)^{n+1}.$$

Домножая наше равенство на B_0B_{n+1}, раскрывая скобки и сокращая подобные члены, получим окончательный результат

$$\big(P_nB_0 - Q_nA_0\big)^2 - Q_n^2D = (-1)^{n+1}B_0B_{n+1}.$$

□

В частном случае, когда $\alpha_0 = \sqrt{N}$, выражение (7.30) принимает вид

$$P_n^2 - Q_n^2D = (-1)^{n+1}B_{n+1}, \quad (7.33)$$

поскольку $A_0 = 0$ и $B_0 = 1$.

7.4 Иррациональности старших степеней

Выше, мы описали алгоритм разложения в непрерывную дробь действительного числа α, являющегося корнем многочлена второй степени. Описанный алгоритм может быть обобщен и применен к разложению в непрерывную дробь корней многочленов произвольной степени.

Определение 7.7. *Пусть задан многочлен* $f(x) = u_mx^m + u_{m-1}x^{m-1} + \cdots + u_0$ *с целыми коэффициентами, неприводимый над полем рациональных чисел. Если действительное число* α *является корнем многочлена* $f(x)$*, то мы будем называть* α *иррациональностью степени* m*.*

Кроме того, для числа α *принято название – алгебраическое число.*

Из неприводимости многочлена $f(x)$ сразу следует, что число α не является рациональным и раскладывается в бесконечную непрерывную дробь. Сам алгоритм разложения тесно связан со следующим преобразованием.

Пусть $f_n(x) = u_m x^m + u_{m-1}x^{m-1} + \cdots + u_0$ многочлен с целыми коэффициентами, неприводимый над полем рациональных чисел. Выберем произвольное целое значение a_n и определим многочлен

$$f_{n+1}(x) = x^m f_n\left(a_n + \frac{1}{x}\right). \tag{7.34}$$

Верна следующая лемма.

Лемма 7.9. *Для многочлена $f_{n+1}(x)$, определенного равенством (7.34), выполнены следующие свойства.*

1. *Верно равенство $f_{n+1}(x) = \sum_{k=0}^{m} \frac{f_n^{(k)}(a_n)}{k!} x^{m-k}$.*
2. *Пусть $e_1, \ldots, e_s$ действительные корни многочлена $f_n(x)$, тогда действительные корни многочлена $f_{n+1}(x)$ принимают вид $\frac{1}{e_1 - a_n}, \ldots, \frac{1}{e_s - a_n}$.*

Доказательство. В силу (7.34) для многочлена $f_{n+1}(x)$ выполнено равенство

$$f_{n+1}(x) = x^m f_n\left(a_n + \frac{1}{x}\right) = \sum_{k=0}^{m} u_k x^{m-k}(a_n x + 1)^k, \tag{7.35}$$

в котором каждое слагаемое, согласно биному Ньютона (**??**), удовлетворяет

$$u_k x^{m-k}(a_n x + 1)^k = \sum_{j=0}^{k} u_k C_j^k a_n^j x^{m-k+j},$$

где $C_j^k = \frac{k!}{j!(k-j)!}$. Таким образом, каждое слагаемое в равенстве (7.35) содержит все степени x от $m-k$ до m.

Перегруппировывая слагаемые при одинаковых степенях x, а также учитывая, что $C_{i-k}^i = C_k^i$ получим, что для (7.35) верно равенство

$$\sum_{k=0}^{m} u_k x^{m-k}(a_n x + 1)^k = \sum_{k=0}^{m}\left(\sum_{i=k}^{m} u_i C_k^i a_n^{i-k}\right) x^{m-k}. \tag{7.36}$$

С другой стороны, согласно (**??**), для k-й производной многочлена выполнено равенство

$$f_n^{(k)}(x) = \sum_{i=k}^{m} u_i \cdot i(i-1)\cdots(i-l+1)\cdot x^{i-k} = k!\sum_{i=k}^{m} u_i C_k^i x^{i-k}.$$

Поставляя это равенство в (7.36), получим первое утверждение леммы.

Перейдем ко второму утверждению. Пусть e произвольный корень многочлена $f_n(x)$. Тогда для любого индекса $i = 1, \ldots, s$ верны равенства

$$0 = f_n(e_i) = f_n\left(a_n + \frac{1}{\gamma_i}\right) = \gamma_i^m f_n\left(a_n + \frac{1}{\gamma_i}\right) = f_{n+1}(\gamma_i),$$

где $\gamma_i = \frac{1}{e_i - a_n}$ – корень многочлена $f_{n+1}(x)$. Лемма доказана. □

Теперь рассмотрим произвольную иррациональность α, являющуюся корнем некоторого неприводимого многочлена $f(x)$, и определим последовательность полных частных $\alpha_0 = \alpha, \alpha_1, \ldots$, вычисляемую при помощи равенства (7.1), тогда

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}.$$

Следовательно, если α_n есть корень некоторого многочлена $f_n(x)$, то α_{n+1}, согласно второму утверждению доказанной нами леммы, является корнем многочлена $f_{n+1}(x)$, определяемого равенством (7.34).

Мы получили, что для вычисления последовательности неполных частных $a_0, a_1, \ldots$ нам необходимо находить корни многочленов, преобразуемых из многочлена $f_0(x)$ в соответствии с формулами из первого утверждения доказанной леммы.

Пример 7.3. Приведем пример и разложим в непрерывную дробь величину $\alpha = \sqrt[3]{5} \sim 1.709$, являющуюся корнем многочлена $f_0(x) = x^3 - 5$. Поскольку многочлен $f_0(x)$ имеет только один действительный корень, то, согласно второму утверждению доказанной леммы, все многочлены $f_1(x), f_2(x), \ldots$ также будут иметь один действительный корень.

Поскольку $\lfloor \alpha \rfloor = 1$, то определим $a_0 = 1$ и вычислим многочлен $f_1(x)$, корнем которого является величина α_1

$$f_1(x) = \sum_{k=0}^{3} \frac{f_0^{(k)}(1)}{k!} x^{3-k} = -4x^3 + 3x^2 + 3x + 1.$$

Приближенное значение действительного корня многочлена $f_1(x)$ равно 1.408, следовательно, мы можем определить $a_1 = 1$ и многочлен

$$f_2(x) = 3x^3 - 3x^2 - 9x - 4,$$

корень которого близок к величине 2.448. Аналогично, определим $a_2 = 2$ и многочлен

$$f_3(x) = -10x^3 + 15x^2 + 15x + 3,$$

корень которого близок к величине 2.232. Определим $a_3 = 2$ и запишем равенство

$$\alpha = [1, 1, 2, 2, \alpha_4],$$

где неизвестная величина α_4 является корнем следующего многочлена $f_4(x) = 13x^3 - 45x^2 - 45x - 10$. Мы остановили наши вычисления, поскольку, в силу теоремы 7.3, полученное нами разложение величины α не периодично.

Покажем, что для квадратичных иррациональностей описанный способ разложения в непрерывную дробь аналогичен доказанным ранее соотношениям (7.20). Пусть α_n бóльший корень многочлена второй степени $f_n(x) = u_n x^2 + v_n x + w_n$, тогда верны равенства

$$\alpha_n = \frac{-v_n + \sqrt{v_n^2 - 4u_n w_n}}{2u_n} = \frac{A_n + \sqrt{D}}{B_n},$$

откуда вытекает $A_n = -v_n$, $B_n = 2u_n$.

Заметим, что при преобразовании (7.1) бóльший корень многочлена $f_n(x)$ переходит в меньший корень многочлена $f_{n+1}(x)$ и наоборот. Следовательно, α_{n+1} есть меньший корень многочлена

$$f_{n+1}(x) = \left(u_n a_n^2 + v_n a_n + w_n\right) x^2 + (2u_n a_n + v_n)x + u_n,$$

имеющий вид

$$\alpha_{n+1} = \frac{-2u_n a_n - v_n - \sqrt{D}}{2\left(u_n a_n^2 + v_n a_n + w_n\right)}, \tag{7.37}$$

поскольку дискриминант многочлена $f_{n+1}(x)$ удовлетворяет равенству

$$(2u_n a_n + v_n)^2 - 4u_n\left(u_n a_n^2 + v_n a_n + w_n\right) = v_n^2 - 4u_n w_n = D.$$

Подставляя в (7.37) величины A_n, B_n, домножая числитель и знаменатель дроби на -1, а также замечая, что $2w_n = 2u_{n-1} = -B_{n-1}$, получим равенство

$$\alpha_{n+1} = \frac{A_n - a_n B_n - \sqrt{D}}{a_n(2a_n B_n - 2A_n) - B_{n-1}} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}}$$

в котором величины A_{n+1}, B_{n+1} удовлетворяют соотношениям из утверждения леммы 7.6.

7.5 Эквивалентность действительных чисел

Напомним следующее определение.

Определение 7.8. *Два действительных числа α и γ называются эквивалентными, если найдутся такие целые числа a, b, c, d, что*

$$\gamma = \frac{a\alpha + b}{c\alpha + d}, \quad ad - bc = \pm 1. \tag{7.38}$$

Для обозначения эквивалентности действительных чисел α и γ мы будем использовать запись $\alpha \sim \gamma$.

Если в равенстве (7.38) величина c принимает отрицательные значения, то, домножая числитель и знаменатель на -1, мы получим равенство, в котором $c \geqslant 0$. В этом разделе мы покажем, что аппарат непрерывных дробей позволяет решать задачу об эквивалентности двух произвольных действительных чисел.

Вначале отметим, что введённое нами отношение эквивалентности разбивает всё множество действительных чисел на классы эквивалентности. Действительно, верна следующая лемма.

Лемма 7.10. *Выполнены следующие утверждения.*

1. *Число α эквивалентно самому себе.*
2. *Если $\gamma \sim \alpha$, то выполнено и обратное свойство $\alpha \sim \gamma$.*
3. *Выполнено свойство транзитивности, то есть если выполнено $\gamma \sim \alpha$ и $\theta \sim \gamma$, то выполнено и $\theta \sim \alpha$.*
4. *Выполнены частные случаи $\alpha \sim -\alpha$, $\alpha \sim \frac{1}{\alpha}$ и $\alpha \sim \alpha + q$ для любого целого числа q.*

Доказательство. Первое утверждение леммы, очевидно, выполнено при $a = d = 1$ и $b = c = 0$. Далее, выражая из (7.38) величину α, получим

$$\alpha = \frac{-d\gamma + b}{c\gamma - a} \quad \text{и} \quad (-d)(-a) - bc = \pm 1,$$

следовательно, $\alpha \sim \gamma$.

Для доказательства третьего утверждения будем считать, что

$$\gamma = \frac{a\alpha + b}{c\alpha + d}, \quad \theta = \frac{p\gamma + q}{s\gamma + t}, \quad ad - bc = \pm 1, \quad pt - sq = \pm 1.$$

Подставляя первое равенство во второе, получим

$$\theta = \frac{p(a\alpha + b) + q(c\alpha + d)}{s(a\alpha + b) + t(c\alpha + d)} = \frac{(ap + cq)\alpha + (bp + dq)}{(as + ct)\alpha + (bs + dt)}.$$

Поскольку

$$(ap + cq)(bs + dt) - (bp + dq)(as + ct) = (pt - sq)(ad - bc) = \pm 1,$$

то выполнено $\theta \sim \alpha$. Более того, из второго утверждения леммы следует, что $\alpha \sim \theta$.

Последнее утверждение следует из равенств

$$\begin{aligned} -\alpha &= \frac{-1\cdot\alpha+0}{0\cdot\alpha+1}, & -1\cdot 1-0\cdot 0=-1,\\ \frac{1}{\alpha} &= \frac{0\cdot\alpha+1}{1\cdot\alpha+0}, & 0\cdot 0-1\cdot 1=-1,\\ \alpha+q &= \frac{1\cdot\alpha+q}{0\cdot\alpha+1}, & 1\cdot 1-q\cdot 0=1. \end{aligned}$$

Лемма доказана. □

Теперь мы можем доказать следующую теорему.

Теорема 7.5. *Два действительных числа α и γ эквивалентны тогда и только тогда, когда их разложения в непрерывные дроби, начиная с некоторого места, совпадают.*

Доказательство. В начале рассмотрим случай, когда разложения двух действительных чисел в непрерывную дробь совпадают. Тогда найдутся такие целые индексы n и m, что

$$\alpha=[a_0,a_1,\ldots,\alpha_n],\quad \gamma=[c_0,c_1,\ldots,\gamma_m]\quad\text{и}\quad \alpha_n=\gamma_m.$$

Воспользовавшись равенством (7.7) запишем

$$\alpha=\frac{\alpha_n P_{n-1}+P_{n-2}}{\alpha_n Q_{n-1}+Q_{n-2}},$$

При этом, согласно лемме 7.3, выполнены равенства

$$P_{n-1}Q_{n-2}-P_{n-2}Q_{n-1}=\pm 1.$$

Следовательно, числа α и α_n эквивалентны. Аналогичными рассуждениями мы получаем, что эквиваленты числа γ и γ_m. Тогда

$$\alpha\sim\alpha_n=\gamma_m\sim\gamma.$$

Докажем обратное утверждение теоремы. Пусть для чисел γ и α выполнено равенство (7.38). Покажем, что найдется последовательность действительных чисел $\gamma_0=\gamma,\gamma_1,\ldots,\gamma_m=\alpha$ таких, что для всех $n=0,1,\ldots,m-1$ выполнено условие $\gamma_n\sim\gamma_{n+1}$ и, кроме того, разложения чисел γ_n и γ_{n+1} в непрерывную дробь, начиная с некоторого места, совпадают. При этом, мы будем считать, что оба числа не являются рациональными, поскольку в противном случае их разложения конечны.

Начнем доказательство с рассмотрения простейших случаев эквивалентности, рассмотренных при доказательстве леммы 7.10.

1. Рассмотрим случай $\gamma \sim \alpha + q$. Разложим α в непрерывную дробь $\alpha = a_0 + \frac{1}{\alpha_1}$, где $\alpha_1 > 1$. Следовательно,

$$\gamma = \alpha + q = a_0 + q + \frac{1}{\alpha_1} = [a_0 + q, \alpha_1].$$

Таким образом, разложения чисел α и γ совпадают.

2. Рассмотрим случай $\gamma \sim -\alpha$. Пусть, как и ранее, $\alpha = a_0 + \frac{1}{\alpha_1}$ и $\alpha_1 > 1$. В начале предположим, что $\alpha_1 > 2$. Тогда

$$\gamma = -a_0 - \frac{1}{\alpha_1} = -a_0 - 1 + \frac{1}{1 + \dfrac{1}{\alpha_1 - 1}} = [-a_0 - 1, 1, \alpha_1 - 1], \quad (7.39)$$

где величина $\alpha_1 - 1 > 1$. Согласно первому свойству, разложения чисел α_1 и $\alpha_1 - 1$ совпадают, следовательно, совпадают разложения чисел α и γ.

Обозначим $\rho = \frac{1}{\alpha_1 - 1}$ и будем считать, что $1 < \alpha_1 < 2$, тогда верно неравенство $\rho > 1$. Более того, из (7.39) и равенства

$$\alpha = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{1 + \dfrac{1}{\rho}} = [a_0, 1, \rho]$$

можно сделать вывод, что разложения чисел α и $\gamma = [-a_0 - 1, 1 + \rho]$ совпадают при $1 < \alpha_1 < 2$.

3. Рассмотрим случай $\gamma \sim \frac{1}{\alpha}$. Доказанное нами второе свойство позволяет рассматривать только случай $\alpha > 0$. Тогда, если $\alpha > 1$, то выполнено равенство $\gamma = [0, \alpha]$ и разложения чисел γ и α совпадают.

В случае $1 > \alpha > 0$ мы получаем, что $\alpha = \frac{1}{\gamma}$ и $\gamma > 1$, следовательно, $\alpha = [0, \gamma]$ и разложения двух чисел опять совпадают.

Теперь рассмотрим общий случай. Пусть $\gamma = \frac{a_0\alpha + b_0}{c_0\alpha + d_0}$ и выполнено равенство $a_0 d_0 - b_0 c_0 = \pm 1$. Определим $\gamma_0 = \gamma$ и рассмотрим преобразование

$$\gamma_{n+1} = \frac{1}{\gamma_n - q_n}, \quad n = 0, 1, \ldots$$

для некоторого целого числа q_n. Из рассмотренных нами частных случаев, а также четвертого утверждения леммы 7.10, следует, что $\gamma_{n+1} \sim \gamma_n$ и их разложения в непрерывную дробь, начиная с некоторого места, совпадают.

Мы будем выбирать последовательность величин q_0, q_1, ... следующим образом. Без ограничения общности мы можем считать, что $c_n > 0$, тогда определим величину q_n равенством

$$a_n = q_n c_n + r_n, \quad 0 \leqslant r_n < c_n.$$

Тогда

$$\gamma_{n+1} = \frac{1}{\gamma_n - q_n} = \frac{c_n\alpha + d_n}{(a_n - q_n c_n)\alpha + (b_n - q_n d_n)} = \frac{a_{n+1}\alpha + b_{n+1}}{c_{n+1}\alpha + d_{n+1}},$$

где

$$a_{n+1} = c_n, \quad b_{n+1} = d_n, \quad c_{n+1} = r_n, \quad d_{n+1} = b_n - q_n d_n$$

и выполнено условие

$$a_{n+1}d_{n+1} - c_{n+1}d_{n+1} = c_n(b_n - q_n d_n) - d_n(a_n - q_n c_n) = \pm 1. \tag{7.40}$$

Мы получили, что каждый элемент последовательности γ_0, γ_1, ... выражается через число α и при этом последовательность неотрицательных величин c_n убывает, так как $c_{n+1} = r_n < c_n$. Следовательно, найдется индекс m такой, что $c_m = 0$, тогда

$$\gamma_m = \frac{a_m\alpha + b_m}{0 \cdot \alpha + d_m}.$$

Учитывая равенство (7.40) мы получаем, что верно равенство $a_m d_m = \pm 1$, тогда $\gamma_m = \pm(\alpha + b_m)$ для некоторого целого числа b_m. Из доказанных выше первого и второго частных случаев следует, что γ_m и α эквивалентны и их разложения в непрерывную дробь, начиная с некоторого места, совпадают. Теорема доказана. □

Из доказательства теоремы явным образом следует метод проверки эквивалентности двух заданных действительных чисел. Приведем пример.

Пример 7.4. Покажем, что бóльшие корни многочленов

$$f(x) = x^2 - 3x - 2 \quad \text{и} \quad h(x) = 2x^2 - 15x + 26$$

эквивалентны. Поскольку мы исследуем квадратичные иррациональности, то их разложения в непрерывную дробь периодичны. Это позволит нам вычислить все элементы последовательности полных частных для каждого их чисел, а потом сравнить найденные значения.

В начале найдем разложение $\alpha = \frac{3+\sqrt{17}}{2}$ – бóльшего корня многочлена $f(x)$, и сведем полученные результаты в следующую таблицу.

n	α_n	a_n	P_n	Q_n
0	$\alpha_0 = \frac{3+\sqrt{17}}{2}$	3	$P_0 = 3$	$Q_0 = 1$
1	$\alpha_1 = \frac{3+\sqrt{17}}{4}$	1	$P_1 = 4$	$Q_0 = 1$
2	$\alpha_2 = \frac{1+\sqrt{17}}{4}$	1	$P_2 = 7$	$Q_0 = 2$
3	$\alpha_3 = \alpha_0$			

Отметим, что вместе с разложением в непрерывную дробь мы вычислили числители и знаменатели подходящих дробей. Эти величины будут использованы нами для определения соотношения между раскладываемыми числами.
Теперь разложим в непрерывную дробь $\gamma = \frac{15+\sqrt{17}}{4}$ – бóльший корень многочлена $h(x)$. Легко видеть, что $\lfloor \gamma \rfloor = 4$ и

$$\gamma_1 = \frac{1}{\gamma - 4} = \frac{1+\sqrt{17}}{4} = \alpha_2.$$

Тогда, используя равенство (7.7) при $n = 1$, запишем равенство

$$\alpha = \frac{4\alpha_2 + 3}{\alpha_2 + 1} = \frac{4\left(\frac{1}{\gamma-4}\right) + 3}{\left(\frac{1}{\gamma-4}\right) + 1} = \frac{3\gamma - 8}{\gamma - 3}.$$

Поскольку верно равенство $3 \cdot (-3) - (-8) \cdot 1 = -1$, то мы доказали, что числа α и γ эквивалентны, а также в явном виде предъявили соотношение, позволяющее выразить одно число через другое.

7.6 Наилучшие приближения

Мы завершим эту главу результатами, иллюстрирующими связь между непрерывными дробями и, так называемыми, наилучшими приближениями.

Рассмотрим задачу приближения действительного числа α рациональной дробью $\frac{P}{Q}$. В теории вычислительных методов, традиционно, наибольший интерес представляет собой величина ϵ, представляющая собой оценку погрешности приближения, то есть $\epsilon > \left|\alpha - \frac{P}{Q}\right|$. Если α не является рациональным числом, то из теоремы 7.1 следует, что для любого значения ϵ найдется бесконечно много подходящих дробей, удовлетворяющих указанному неравенству. Однако, как следует из леммы 7.5, знаменатели этих дробей быстро растут и принимают сколь угодно большие значения.

Если же мы ограничим сверху величину знаменателя некоторой константой, зависящей от ϵ, то приближений к числу α окажется конечное число, среди которых можно будет выделить одно, в некотором смысле, *наилучшее*. Дадим строгое определение.

Определение 7.9. *Пусть α действительное, отличное от нуля число. Рациональная дробь $\frac{P}{Q}$ называется наилучшим приближением к числу α, если любой другой дроби $\frac{A}{B} \neq \frac{P}{Q}$ такой, что $1 \leqslant B \leqslant Q$, выполнено неравенство*

$$|B\alpha - A| > |Q\alpha - P|.$$

Наилучшее приближение есть несократимая дробь. Предположив обратное, получим $P = uA$, $Q = uB$ при $u > 1$, откуда вытекает неравенство $|Q\alpha - P| = u|B\alpha - A| > |B\alpha - A|$, противоречащее определению наилучшего приближения.

Теорема 7.6. *Всякое наилучшее приближение к действительному числу α есть подходящая дробь к нему. И наоборот, каждая подходящая дробь $\frac{P_n}{Q_n}$ к числу α при $n \geqslant 1$ есть наилучшее приближение.*

Прежде чем переходить к доказательству, заметим, что данное нами определение 7.9 эквивалентно тому, что система неравенств

$$\begin{cases} |x - \alpha y| \leqslant |P - \alpha Q|, \\ 0 < y \leqslant Q, \end{cases} \tag{7.41}$$

имеет единственное решение в целых числах $x = P$, $y = Q$. Нам понадобится следующая лемма.

Лемма 7.11. *Пусть $\frac{P_n}{Q_n}$, $\frac{P_{n+1}}{Q_{n+1}}$ две соседние подходящие дроби к числу α, причем $\frac{P_{n+1}}{Q_{n+1}} \neq \alpha$. Тогда система неравенств*

$$\begin{cases} |x - \alpha y| \leqslant |P_n - \alpha Q_n|, \\ 0 < y \leqslant Q_{n+1}, \end{cases} \tag{7.42}$$

имеет лишь два решения в целых числах, а именно $x = P_n$, $y = Q_n$ и $x = P_{n+1}$, $y = Q_{n+1}$.

Доказательство. Пусть x, y целые числа, решения системы неравенств (7.42). Представим их в виде

$$\begin{aligned} x &= uP_n + vP_{n+1}, \\ y &= uQ_n + vQ_{n+1}, \end{aligned}$$

где u, v неизвестные значения. Выражая в явном виде неизвестные u, v и воспользовавшись равенством (7.8), получим

$$u = (-1)^n(yP_{n+1} - xQ_{n+1}), \quad v = (-1)^n(xQ_n - yP_n).$$

Следовательно, неизвестные u, v могут принимать только целые значения, поскольку $P_n, Q_n, P_{n+1}, Q_{n+1}, x, y \in \mathbb{Z}$.

Наборы $u = 0$, $v = 1$ и $u = 1$, $v = 0$ дают нам два решения неравенства (7.42), указанные в формулировке леммы. Покажем, что других решений не существует.

Предположим, что u и v имеют одинаковые знаки. Тогда из условия $y > 0$ следует, что $uQ_n + vQ_{n+1} > 0$ и $u > 0$, $v > 0$. Но тогда $y \geqslant Q_n + Q_{n+1}$, что противоречит второму неравенству в (7.42). Таким образом, нам осталось рассмотреть случай, когда u и v имеют разные знаки.

Из неравенств (7.10) и утверждения теоремы 7.1 получаем, что числа $P_n - \alpha Q_n$ и $P_{n+1} - \alpha Q_{n+1}$ тоже имеют разные знаки, поэтому выполнено неравенство

$$|x - \alpha y| = |u(P_n - \alpha Q_n) + v(P_{n+1} - \alpha Q_{n+1})| = \\ = |u||P_n - \alpha Q_n| + |v||P_{n+1} - \alpha Q_{n+1}| > |P_n - \alpha Q_n|,$$

которое противоречит (7.42). Лемма доказана. □

Перейдем к доказательству теоремы 7.6. Пусть дробь $\frac{P}{Q}$ является наилучшим приближением к числу α и n максимальный индекс такой, что $Q_n \leqslant Q$. Предположим, что

$$|P - \alpha Q| < |P_n - \alpha Q_n|, \tag{7.43}$$

тогда, согласно утверждению леммы 7.11, дробь $\frac{P}{Q}$ совпадает с одной из подходящих дробей $\frac{P_n}{Q_n}$ или $\frac{P_{n+1}}{Q_{n+1}}$. Если (7.43) не выполнено, то $|P - \alpha Q| \geqslant |P_n - \alpha Q_n|$ и, в силу того, что $\frac{P}{Q}$ – наилучшее приближение, выполнено $P = P_n$, $Q = Q_n$. В обоих случаях первое утверждение теоремы выполнено.

Теперь докажем обратное утверждение и покажем, что для всех индексов $n \geqslant 0$ каждая подходящая дробь $\frac{P_{n+1}}{Q_{n+1}}$ является наилучшим приближением. Рассмотрим значения x, y, являющиеся решением системы сравнений

$$\begin{cases} |x - \alpha y| \leqslant |P_{n+1} - \alpha Q_{n+1}|, \\ 0 < y \leqslant Q_{n+1}. \end{cases} \tag{7.44}$$

Из неравенств (7.10) и утверждения теоремы 7.1 получаем, что выполнено $|P_n - \alpha Q_n| > |P_{n+1} - \alpha Q_{n+1}$. Тогда из (7.44) следуют неравенства

$$\begin{cases} |x - \alpha y| \leqslant |P_n - \alpha Q_n|, \\ 0 < y \leqslant Q_{n+1}, \end{cases}$$

которым, согласно лемме 7.11, удовлетворяет не более двух решений, а именно пары P_n, Q_n и P_{n+1} и Q_{n+1}. Поскольку P_n, Q_n не удовлетворяет (7.44), то $\frac{P_{n+1}}{Q_{n+1}}$ наилучшее приближение. Теорема доказана. □

Докажем еще одну теорему, которая будет использована нами позднее при обосновании алгоритмов факторизации целых чисел.

Теорема 7.7. *Если несократимая дробь* $\frac{P}{Q}$, *при* $Q > 0$, *удовлетворяет неравенству*

$$\left|\alpha - \frac{P}{Q}\right| < \frac{1}{2Q^2}, \tag{7.45}$$

то она есть наилучшее приближение к α.

Доказательство. Предположим, что целые числа $x = A$, $y = B$ удовлетворяют неравенствам (7.41), то есть

$$\begin{cases} |A - \alpha B| \leqslant |P - \alpha Q|, \\ 0 < B \leqslant Q. \end{cases}$$

Тогда рассмотрим разность целых чисел $AQ - BP$ и получим неравенство

$$|AQ - BP| = |Q(A - \alpha B) - B(P - \alpha Q)| \leqslant$$
$$\leqslant Q|A - \alpha B| + B|P - \alpha Q| \leqslant 2Q|P - \alpha Q| < qQ^2 \left|\alpha - \frac{P}{Q}\right| < 1,$$

из которого следует, что разность $AQ - BP$ равна нулю или, что равносильно, $AQ = BP$. Поскольку дробь $\frac{P}{Q}$ несократима, то числа P и Q взаимно просты и мы получаем, что $Q|B$. Поскольку $B < Q$, то получаем, что $B = Q$, откуда вытекает равенство $A = P$. Следовательно, система неравенств (7.41) имеет только одно решение. Теорема доказана. □

Заметим, что из утверждения теорем 7.6 и 7.7 следует, что всякая несократимая дробь $\frac{P}{Q}$, удовлетворяющая неравенству (7.45), является подходящей дробью к числу α.

Предметный указатель