§7. Целые числа и вычеты.

7.1. Кольцо вычетов $\mathbb{Z}/(n)$. Элементом этого кольца является *класс вычетов* по модулю n, т. е. *подмножество* в $\mathbb{Z}$, образованное всеми числами, дающими один и тот же остаток от деления на n. Мы уже встречались с классами вычетов в примере (n° 5.1.7), где они интерпретировались как смежные классы аддитивной группы $\mathbb{Z}$ по подгруппе $(n) = \{nk \mid k \in \mathbb{Z}\}$, состоящей из чисел, кратных n. Всего имеется n таких классов, взаимно однозначно соответствующих n различным остаткам:

$$[0]_n,\ [1]_n,\ \ldots,\ [(n-1)]_n\ , \quad \text{где} \quad [a]_n = a \,(\mathrm{mod}\, n) = a + (n) = \{a + kn \mid k \in \mathbb{Z}\}\,.$$

Сложение и умножение классов вычетов задаётся правилами:

$$[a] + [b] \stackrel{\text{def}}{=} [a+b]\ , \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\ . \tag{7-1}$$

Упражнение 7.1. Проверьте корректность этого определения (т. е. независимость классов $[a+b]$ и $[ab]$ от выбора представителей $a \in [a]$ и $b \in [b]$), а также выполнение в $\mathbb{Z}/(n)$ всех аксиом коммутативного кольца.

Независимость результатов сложения и умножения от выбора представителей в классе иногда позволяет значительно упростить вычисления. Например, для того чтобы вычислить сотую степень класса $2007 \,(\mathrm{mod}\, 2008)$ нет нужды возводить в 100-ю степень число 2007, поскольку $[2007]_{2008} = [-1]_{2008}$ и согласно упр. 7.1 мы имеем $2007^{100} \equiv (-1)^{100} \equiv 1 \,(\mathrm{mod}\, 2008)$.

7.2. Делители нуля и нильпотенты. В кольцах $\mathbb{Z}/(n)$ мы сталкиваемся с рядом явлений, которые не наблюдаются ни в полях, ни в кольце целых (или гауссовых целых) чисел. Так, в кольце $\mathbb{Z}/(10)$ произведение классов $[2]$ и $[5]$ равно нулю, хотя *каждый* из них отличен от нуля, а в кольце $\mathbb{Z}/(27)$ ненулевой класс $[3]$ имеет нулевой куб $[3]^3 = [27] = [0]$.

Ненулевой элемент a кольца K называется *делителем нуля*, если $ab = 0$ для некоторого ненулевого $b \in K$. Ненулевой элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Отметим, что всякий нильпотент автоматически является делителем нуля.

Кольцо с единицей без делителей нуля называется *целостным*. Кольцо с единицей без нильпотентов называется *приведённым*. Всякое целостное кольцо автоматически приведено.

Упражнение 7.2. Составьте таблицы сложения и умножения в кольцах $\mathbb{Z}/(n)$ для $n = 3,\ 4,\ 5,\ 6,\ 7,\ 8$. Найдите в этих кольцах все делители нуля, все нильпотенты, и все обратимые элементы. Для обратимых элементов составьте таблицу обратных. Какие из этих колец являются полями?

Наличие делителей нуля является простейшим препятствием к тому, чтобы кольцо было полем. В самом деле, никакой делитель нуля a не может быть обратим, поскольку система условий

$$\begin{cases} b \neq 0 \\ ab = 0 \\ aa^{-1} = 1 \end{cases}$$

несовместна: умножая обе части второго равенства на a^{-1} мы получаем $b = 0$, что противоречит первому равенству. Отметим, что написанным выше условиям удовлетворяет, в частности, нулевой элемент $a = 0$. Именно поэтому «на ноль делить нельзя», и в аксиоме существования обратного элемента в поле накладывается требование $a \neq 0$ (см. аксиому (2г) на стр. 37).

7.3. Обратимые элементы кольца $\mathbb{Z}/(n)$. Класс $[m]_n$ обратим в кольце $\mathbb{Z}/(n)$ тогда и только тогда, когда в кольце целых чисел $\mathbb{Z}$ разрешимо относительно x и y уравнение

$$mx + ny = 1\,. \tag{7-2}$$

В самом деле, обратимость класса $[m]_n$ означает существование такого класса $[x]_n$, что

$$[m]_n[x]_n = [mx]_n = [1]_n\ ,$$

а это, в свою очередь, равносильно соотношению (7-2). Чтобы понять, для каких $m, n \in \mathbb{Z}$ уравнение (7-2) обладает целочисленными решениями, зафиксируем какие-нибудь m и n и рассмотрим всю совокупность целых чисел, представимых в виде $mx+ny$ с целыми x, y. Обозначим её через

$$(m,n) \stackrel{\text{def}}{=} \{mx+by \mid x,y \in \mathbb{Z}\}\,. \tag{7-3}$$

Упражнение 7.3. Покажите, что подмножество $(m,n) \subset \mathbb{Z}$ обладает следующими свойствами:

а) любое число $z \in (m,n)$ делится на каждый общий делитель чисел m и n

б) $m, n \in (m,n)$ в) $z \in (m,n) \Rightarrow kz \in (m,n)\ \forall\, k \in \mathbb{Z}$ г) $z_1, z_2 \in (m,n) \Rightarrow z_1 \pm z_2 \in (m,n)$

Обозначим через d наименьшее положительное число в (m,n). Отметим, что d, как и все числа в (m,n), представляется в виде $d = mx+ny$ и делится на каждый общий делитель чисел m и n. С другой стороны, любое $z \in (m,n)$ (в частности, $z = m, n$) делится на d. В самом деле, деля $z \in (m,n)$ на d с остатком, мы получаем равенство $z = kd+r$, в котором остаток $r = z-kd$ лежит в (m,n) по упр. 7.3 и находится в пределах $0 \leqslant r \leqslant (d-1)$. В силу выбора d мы должны иметь $r = 0$. Таким образом, $(m,n) = (d)$ совпадает с множеством чисел, кратных d, и $d = \text{НОД}(m,n)$ является *наибольшим общим делителем*[1] m и n.

Итак, уравнение (7-2) разрешимо тогда и только тогда, когда $d = \text{НОД}(a,n) = 1$, а значит, обратимыми элементами кольца $\mathbb{Z}/(n)$ являются классы $[m]_n$ с $\text{НОД}(m,n) = 1$.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют группу относительно умножения. Эта группа называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^*$. Порядок этой группы обозначается через $\varphi(n)$ и называется *функцией Эйлера* числа $n \in \mathbb{N}$. Иначе можно сказать, что $\varphi(n)$ равно количеству натуральных чисел, меньших n и взаимно простых с n. Из следствия (n° 3.3.1) теоремы Лагранжа мы заключаем, что для любого обратимого вычета $[a] \in \mathbb{Z}/(n)^*$ выполняется равенство $[a^{\varphi(n)}] = [a]^{\varphi(n)} = [1]$. Иными словами, справедливо

7.3.1. ПРЕДЛОЖЕНИЕ (ТЕОРЕМА ЭЙЛЕРА). *Если* $\text{НОД}(a,n) = 1$, *то* $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

7.3.2. СЛЕДСТВИЕ (МАЛАЯ ТЕОРЕМА ФЕРМА). *Если p простое, то* $a^p \equiv a \pmod{p}\ \ \forall\, a \in \mathbb{Z}$.

Доказательство. Если a делится на p, то обе части сравнения $a^p \equiv a \pmod{p}$ нулевые. Если a не делится на p, мы можем применить предыдущее предложение. Так как $\varphi(p) = p-1$ для простого p, мы получим $a^{p-1} \equiv 1 \pmod{p}$, а значит, $a^p \equiv a \pmod{p}$. □

Упражнение 7.4. Вычислите остаток от деления $2007^{2008^{2009}}$ на 11.

7.4. Алгоритм Евклида. Практическое отыскание решений уравнения (7-2) производится следующим образом. Пусть $n \geqslant m$. Положим

$$E_0 = n\,, \quad E_1 = m\,, \quad E_k = \text{остатку от деления } E_{k-2} \text{ на } E_{k-1} \text{ (при } k \geqslant 1). \tag{7-4}$$

Числа E_k строго убывают до тех пор, пока какое-то E_r не разделит нацело предыдущее E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой элемент E_r последовательности E_k и будет наибольшим общим общим делителем чисел (m,n), причём он автоматически получится представленным в виде $E_r = x \cdot E_0 + y \cdot E_1$, если при вычислении каждого E_k мы будем представлять его в виде $E_k = x \cdot E_0 + y \cdot E_1$.

Упражнение 7.5. Индукцией по k убедитесь, что все числа E_k представляются в виде $E_k = x \cdot E_0 + y \cdot E_1$ (и стало быть, делятся на любой общий делитель чисел m и n), а затем, убывающей индукцией по k, начинающейся с $k = r+1$ убедитесь, что все числа E_k (включая $E_0 = n$ и $E_1 = m$) делятся на E_r (и стало быть, $E_r = \text{НОД}(m,n)$).

[1] заметим, что по ходу дела мы доказали, что наибольший общий делитель нацело делится на любой другой общий делитель

Например, для чисел $n = 10\,203$ и $m = 4\,687$ вычисление состоит из восьми шагов:

$$\begin{aligned}
E_0 &= 10\,203 \\
E_1 &= 4\,687 \\
E_2 &= 829 = E_0 - 2\,E_1 = +1\,E_0 - 2E_1 \\
E_3 &= 542 = E_1 - 5\,E_2 = -5\,E_0 + 11E_1 \\
E_4 &= 287 = E_2 - E_3 = +6\,E_0 - 13E_1 \\
E_5 &= 255 = E_3 - E_4 = -11\,E_0 + 24E_1 \\
E_6 &= 32 = E_4 - E_5 = +17\,E_0 - 37E_1 \\
E_7 &= 31 = E_5 - 7\,E_6 = -130\,E_0 + 283E_1 \\
E_8 &= 1 = E_6 - E_7 = +147\,E_0 - 320E_1 \\
(E_9 &= 0 = E_7 - 31\,E_8 = -4\,687\,E_0 + 10\,203E_1)
\end{aligned}$$

(взятая в скобки последняя строка служит для проверки), и мы заключаем из него, что

$$\text{НОД}(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687\,,$$

откуда вытекает, в частности, что класс $[10\,203]$ обратим в $\mathbb{Z}/(4\,687)$ и

$$[10\,203]^{-1} = [147] \,(\mathrm{mod}\, 4\,687)\,,$$

а класс $[4\,687]$ обратим в $\mathbb{Z}/(10\,203)$ и $[4\,687]^{-1} = -[320] \,(\mathrm{mod}\, 10\,203)$.

Упражнение 7.6. Докажите, что представление первого нулевого числа $E_{r+1} = q_0 E_0 + q_1 E_1 = 0$, получающееся согласно алгоритму Евклида, содержит в себе *наименьшее общее кратное* чисел $E_0 = m$ и $E_1 = n$, а именно $\text{НОК}(m, n) = |q_0 E_0| = |q_1 E_1|$ (т. е. «дополнительные множители» q_0, q_1 таковы, что $\text{НОД}(q_0, q_1) = 1$).

Отметим, что с вычислительной точки зрения нахождение наибольшего общего делителя пары чисел при помощи алгоритма Евклида является *несопоставимо* менее трудоёмкой задачей, чем разложение этих чисел на простые множители[1], в чём читатель может убедиться, попробовав разложить на простые множители предыдущие числа $n = 10\,203$ и $m = 4\,687$.

7.5. Прямые произведения групп и колец. Из любого набора групп $G_1, G_2, \ldots, G_m$ можно изготовить новую группу

$$\prod_\nu G_\nu = G_1 \times G_2 \times \cdots \times G_\nu = \{(g_1, g_2, \ldots, g_m) \mid g_\nu \in G_\nu \ \forall \nu\}\,,$$

которая называется *прямым произведением* групп G_ν и состоит из упорядоченных наборов $(g_1, g_2, \ldots, g_m)$ операция на которых определяется покомпонентно:

$$(g_1, g_2, \ldots, g_m) \cdot (h_1, h_2, \ldots, h_m) = (g_1 \cdot h_1,\ g_2 \cdot h_2,\ \cdots,\ g_m \cdot h_m)\,. \tag{7-5}$$

Упражнение 7.7. Проверьте, что так определённая операция ассоциативна и обладает единицей $e = (e_1, e_2, \ldots, e_m)$ (где каждое e_ν — это единица группы G_ν), а также что у каждого элемента $g = (g_1, g_2, \ldots, g_m)$ имеется обратный $g^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_m^{-1})$. Кроме того, убедитесь, что если все группы G_ν коммутативны, то группа $\prod G_\nu$ тоже получится коммутативная.

Отметим, что эта конструкция работает не только для конечных наборов групп, но и для любых семейств групп G_ν, занумерованных элементами $\nu \in X$ произвольного множества X. Соответствующее произведение обозначается тогда $\prod\limits_{\nu \in X} G_\nu$. Отметим также, что если все группы $G_1, G_2, \ldots, G_m$ конечны, то произведение тоже конечно и имеет порядок $|\prod G_\nu| = \prod |G_\nu|$.

[1] найти два больших простых числа, если известно их произведение, за разумное время невозможно даже на мощном компьютере; это обстоятельство лежит в основе большинства используемых в настоящее время систем шифрования данных

Аналогичным образом, для любого множества колец $\{K_\nu\}_{\nu\in X}$ можно образовать прямое произведение $\prod K_\nu$, представляющее собою множество упорядоченных наборов элементов

$$(\dots, a_\nu, \dots)\,, \quad \text{где } a_\nu \in K_\nu$$

и покомпонентными операциями, заданными формулой (7-5):

$$(\dots, a_\nu, \dots) + (\dots, b_\nu, \dots) \stackrel{\text{def}}{=} (\dots, a_\nu + b_\nu, \dots)$$
$$(\dots, a_\nu, \dots)(\dots, b_\nu, \dots) \stackrel{\text{def}}{=} (\dots, a_\nu b_\nu, \dots)\,.$$

Упражнение 7.8. Проверьте, что $\prod K_\nu$ является кольцом, причём если все K_ν были кольцами с единицей, то $\prod K_\nu$ также будет кольцом с единицей.

Отметим, что элемент кольца-произведения $a = (a_1, a_2, \dots, a_m) \in K_1 \times K_2 \times \cdots \times K_m$ обратим тогда и только тогда, когда каждая его компонента $a_\nu \in K_\nu$ обратима в своём кольце K_ν. Поэтому группа обратимых элементов кольца $\prod K_\nu$ будет прямым произведением групп обратимых элементов колец K_ν:

$$\Big(\prod K_\nu\Big)^* = \prod K_\nu^* \tag{7-6}$$

Отметим также, что в прямом произведении колец всегда имеются делители нуля: любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0,\,1,\,1,\,\dots,\,1)$ является делителем нуля, поскольку

$$(0,\,1,\,1,\,\dots,\,1)(1,\,0,\,0,\,\dots,\,0) = (0,\,0,\,0,\,\dots,\,0) = 0\,.$$

Таким образом, произведение колец никогда не является полем. В частности, полем не является и произведение полей. Скажем, если $\mathbb{F}_p$ и $\mathbb{F}_q$ — конечные поля, состоящие соответственно из p и q элементов, то в их произведении $\mathbb{F}_p \times \mathbb{F}_q$ будет ровно $(p-1)(q-1)$ обратимых элементов (a, b), образующих мультипликативную группу $\mathbb{F}_p^* \times \mathbb{F}_q^*$ и $p + q - 2$ делителя нуля, имеющих вид $(a, 0)$ и $(0, b)$ с $a, b \neq 0$.

7.6. Взаимная простота. Сделаем несколько важных замечаний о делимости, относящихся к произвольному коммутативному кольцу K с единицей. Элементы $a, b \in K$ называются *взаимно простыми*, если

$$ax + by = 1 \quad \text{для некоторых } x, y \in K\,. \tag{7-7}$$

Если элементы a и b взаимно просты, то произведение mb с произвольным $m \in K$ делится на a только тогда, когда m делится на a. В самом деле, умножая равенство (7-7) на m, мы получаем

$$m = amx + bmy\,, \tag{7-8}$$

и если mb делится на a, то и m делится на a. Это же вычисление показывает, что если m делится на a и на b, то m делится и на произведение ab (поскольку оба слагаемых в правой части (7-8) делятся в этом случае на ab).

Далее, если элемент $a \in K$ взаимно прост с каждым из элементов $b_1, b_2, \dots, b_n$, то он взаимно прост и с их произведением. В самом деле, если для каждого i мы можем подобрать такие $x_i, y_i \in K$, что $ax_i + b_i y_i = 1$, то, перемножив все эти равенства, мы получим равенство вида[1]

$$a \cdot x + (b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n) = 1\,,$$

устанавливающее взаимную простоту a и $b_1 b_2 \cdots b_n$.

7.6.1. Пример: китайская теорема об остатках. Пусть число $n \in \mathbb{Z}$ является произведением m попарно взаимно простых сомножителей: $n = n_1 n_2 \cdots n_m$. Покажем, что в этом случае кольцо вычетов $\mathbb{Z}/(n)$

[1] в первом слагаемом собраны все члены, содержащие сомножитель a, во втором — единственный член не содержащий такого сомножителя

изоморфно прямому произведению колец вычетов $\mathbb{Z}/(n_i)$, т. е. построим такое взаимно однозначное отображение

$$\mathbb{Z}/(n) \xrightarrow{\ \varphi\ } (\mathbb{Z}/(n_1)) \times (\mathbb{Z}/(n_2)) \times \cdots \times (\mathbb{Z}/(n_m)) \ ,$$

что $\forall\, a, b \in \mathbb{Z}/(n)$ $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ в $\prod \mathbb{Z}/(n_i)$. Зададим φ правилом

$$\varphi\left([z]_n\right) \stackrel{\text{def}}{=} \left([z]_{n_1},\, [z]_{n_2},\, \ldots\, ,\, [z]_{n_m}\right) \qquad \forall\, z \in \mathbb{Z} \ .$$

Это правило корректно (не зависит от выбора числа $z \in \mathbb{Z}$ в классе $[z]_n \subset \mathbb{Z}$), поскольку равенство $[z_1]_n = [z_2]_n$ означает, что разность $z_1 - z_2$ делится на $n = n_1 n_2 \cdots n_m$, а значит, она делится и на каждое n_i, и стало быть, для каждого i мы будем иметь равенство $[z_1]_{n_i} = [z_2]_{n_i}$. Очевидно, также, что φ является гомоморфизмом:

$$\begin{aligned}\varphi\left([z]_n + [w]_n\right) = \varphi\left([z+w]_n\right) &= \left([z+w]_{n_1},\, [z+w]_{n_2},\, \ldots\, ,\, [z+w]_{n_m}\right) = \\ &= \left([z]_{n_1} + [w]_{n_1},\, [z]_{n_2} + [w]_{n_2},\, \ldots\, ,\, [z]_{n_m} + [w]_{n_m}\right) = \\ &= \left([z]_{n_1},\, [z]_{n_2},\, \ldots\, ,\, [z]_{n_m}\right) + \left([w]_{n_1},\, [w]_{n_2},\, \ldots\, ,\, [w]_{n_m}\right) = \varphi\left([z]_n\right) + \varphi\left([w]_n\right)\end{aligned}$$

и ровно то же самое произойдёт с умножением. Покажем, что φ, рассматриваемый как гомоморфизм аддитивных групп, имеет нулевое ядро. В самом деле, рассмотрим класс $[z]_n \in \ker(\varphi)$. Поскольку для любого i класс $[z]_{n_i}$ нулевой, z делится на каждое n_i, а так как все n_i попарно взаимно просты, то z должен делиться и на их произведение (см. n° 7.6), которое равно n. Тем самым $[z]_n = 0$, что и требовалось.

Из следствия (n° 5.1.2) теоремы о строении гомоморфизма групп мы заключаем, что φ является вложением. А так как оба кольца $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ состоят из одинакового числа элементов $n = \prod n_i$, гомоморфизм φ должен быть биекцией. Этот факт известен как *китайская теорема об остатках*, поскольку на классическом языке он утверждает, что для любого набора остатков $r_1, r_2, \ldots, r_m$ от деления на попарно взаимно простые числа $n_1, n_2, \ldots, n_m$ можно подобрать такое целое число z, которое даёт остаток r_i от деления *на каждое* из n_i, причём любые два числа z_1, z_2, решающие эту задачу, различаются на целое кратное числа $n = n_1 n_2 \cdots n_k$.

Для практического отыскания такого числа z полезно установить сюръективность гомоморфизма φ непосредственно, не прибегая к теореме о гомоморфизме групп. Для этого заметим, что из взаимной простоты числа n_i с остальными n_ν вытекает, что n_i взаимно просто и с их произведением $m_i = \prod\limits_{\nu \neq i} n_\nu$ (см. n° 7.6), т. е. для каждого i найдутся такие $x_i, y_i \in \mathbb{Z}$, что $n_i x_i + m_i y_i = 1$. Числа $b_i = m_i y_i$ обладают, таким образом, следующим замечательным свойством:

$$[b_i]_{n_i} = [1]_{n_i} \quad \text{и} \quad \forall\, \nu \neq i \ \ [b_i]_{n_\nu} = [0]_{n_\nu} \ . \tag{7-9}$$

Поэтому в качестве числа z, отображающегося в заданные классы $[r_i]_{n_i}$ при всех i, можно взять

$$z = r_1 b_1 + r_2 b_2 + \cdots + r_m b_m \ .$$

Для демонстрации эффективности этого алгоритма найдём, к примеру, наименьшее натуральное число, имеющее остатки $r_1 = 2$, $r_2 = 7$ и $r_3 = 43$ от деления, соответственно, на $n_1 = 57$, $n_2 = 91$ и $n_3 = 179$. Сначала найдём $y_1 \in \mathbb{Z}$, такое что $91 \cdot 179 \cdot y_1 \equiv 1 \,(\mathrm{mod}\, 57)$. Поскольку $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \,(\mathrm{mod}\, 57)$, достаточно применить алгоритм Евклида к $E_0 = 57$ и $E_1 = 13$. В результате получим $22 \cdot 13 - 5 \cdot 57 = 1$. Таким образом, число

$$b_1 = -22 \cdot 91 \cdot 179 \quad (\equiv 22 \cdot 13 \,(\mathrm{mod}\, 57))$$

даёт при делении на 57, 91 и 179 остатки (1, 0, 0). Аналогичным образом находим числа

$$\begin{aligned} b_2 &= -33 \cdot 57 \cdot 179 \quad (\equiv 33 \cdot 11 \,(\mathrm{mod}\, 91)) \\ b_3 &= -45 \cdot 57 \cdot 91 \quad\ \ (\equiv 45 \cdot 4 \,(\mathrm{mod}\, 179)) \end{aligned}$$

дающие при делении на 57, 91 и 179 остатки (0, 1, 0) и (0, 0, 1) соответственно. Тогда остатки (2, 7, 43) будет иметь число

$$\begin{aligned} z = 2\, b_1 + 7\, b_2 + 43\, b_3 &= -(2 \cdot 22 \cdot 91 \cdot 179 + 7 \cdot 33 \cdot 57 \cdot 179 + 43 \cdot 45 \cdot 57 \cdot 91) = \\ &= -(716\,716 + 2\,356\,893 + 10\,036\,845) = -13\,110\,454 \,, \end{aligned}$$

а все остальные числа с такими остатками будут отличаться от z на целые кратные числа

$$n = 57 \cdot 91 \cdot 179 = 928\,473\,.$$

Наименьшим положительным среди них является $z + 15\,n = 816\,641$.

7.7. Наибольший общий делитель. Рассмотрим произвольное целостное[1] кольцо K. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b. Из равенств $a = mb$ и $b = na$ вытекает равенство $a - mb = a - mna = a(1 - mn) = 0$, откуда[2] $mn = 1$. Таким образом, ассоциированность элементов a и b равносильна тому, что a и b получаются друг из друга умножением на обратимый элемент кольца. Например, в кольце целых чисел $\mathbb{Z}$ числа a и b ассоциированы тогда и только тогда, когда $a = \pm b$.

Всякое $d \in K$, делящее a и b и делящееся на любой другой элемент, делящий a и b, называется *наибольшим общим делителем* элементов a и b и обозначается $\text{НОД}(a, b)$. Отметим, что применительно к произвольному целостному кольцу K это определение никоим образом не гарантирует ни существования, ни единственности наибольшего общего делителя. Если наибольшие общие делители существуют, то все они ассоциированы друг с другом. Поэтому запись $\text{НОД}(a, b) = d$ не вполне корректна, но ей всё-таки принято пользоваться, имея в виду, что d в правой части определено с точностью до умножения на любой обратимый элемент. Для некоторых специальных колец K наибольший общий делитель можно зафиксировать однозначно, используя особые свойства кольца K. Так, в кольце целых чисел $\mathbb{Z}$ из двух ассоциированных чисел $\text{НОД}(a, b) = \pm d$ наибольшим общим делителем принято называть *положительный* наибольший общий делитель.

Подчеркнём, что в общем случае из условия $\text{НОД}(a, b) = 1$ *не вытекает*, что a и b взаимно просты. Например, в кольце $\mathbb{Q}[t_1, t_2]$ многочленов с рациональными коэффициентами от переменных t_1, t_2 элементы $a = t_1$ и $b = t_2$ таковы, что $\text{НОД}(t_1, t_2) = 1$, однако $t_1 \cdot x + t_2 \cdot y \neq 1$ ни при каких $x, y \in \mathbb{Q}[x, y]$, т. е. одночлены t_1 и t_2 *не взаимно просты*. Этот же пример показывает, что в произвольном кольце $\text{НОД}(a, b)$ (даже если он существует) вовсе не обязан представляться в виде $ax + by$.

Рассуждение из (n° 7.3) и (n° 7.4) *доказывают* следующее предложение:

7.7.1. ПРЕДЛОЖЕНИЕ. *В кольце целых чисел $\mathbb{Z}$ любые два числа a, b обладают наибольшим общим делителем*[3]*, причём он может быть представлен в виде $\text{НОД}(a, b) = ax + by$. Взаимная простота чисел $a, b \in \mathbb{Z}$ равносильна условию $\text{НОД}(a, b) = 1$.* □

7.8. Разложение на неприводимые множители. Элемент q произвольного коммутативного кольца K называется *неприводимым*, если он не обратим, и из равенства $q = mn$ вытекает, что один из множителей m, n обратим. Если элемент $q \in K$ неприводим, то $\text{НОД}(a, q) = 1$ для любого $a \in K$, не делящегося на q. Неприводимые элементы кольца целых чисел $\mathbb{Z}$ — это простые числа. Из предложения (n° 7.7.1) вытекает, что любое простое число p взаимно просто с любым целым числом a, не делящимся на p. В частности, произведение нескольких целых чисел делится на простое число p только при условии, что хотя бы один из множителей делится на p, и если какое-то целое число n делится на каждое из m различных простых чисел $p_1, p_2, \ldots, p_m$, то n делится и на их произведение. Из этих двух свойств вытекает, что разложение произвольного целого числа n в произведение простых множителей *единственно* с точностью до выбора знаков у этих множителей.

7.8.1. ПРЕДЛОЖЕНИЕ. *Каждое целое число $n \neq \pm 1$ представляется в виде произведения простых чисел, причём любые два таких представления $p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_m$ состоят из одинакового числа сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $p_i = \pm q_i$ для всех i.*

[1] напомним (см. n° 7.2) что кольцо называется *целостным*, если в нём нет делителей нуля

[2] здесь мы пользуемся тем, что в K нет делителей нуля

[3] и единственен с точностью до знака; обычно этот знак выбирают положительным и называют наибольшим общим делителем целых чисел их *натуральный* наибольший общий делитель

Доказательство. Докажем вначале существование разложения. Если n простое, то доказывать нечего. Если нет, представим его в виде $n = m_1 m_2$ с $|m_1|, |m_2| < |n|$. Если среди сомножителей имеются составные, также разложим их в произведение меньших по абсолютной величине сомножителей и т. д. Поскольку абсолютная величина непростых сомножителей всё время уменьшается, этот процесс когда-то должен закончиться и мы получим требуемое разложение. Докажем теперь единственность. Пусть $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, где все сомножители просты. Как мы уже говорили, из простоты p_1 вытекает, что хотя бы один из сомножителей в правой части делится на p_1. Пусть это $q_1 = s p_1$. Поскольку q_1 неприводим, s обратим, т. е. $q_1 = \pm p_1$. Вынося p_1, получим $p_1(p_2 \cdots p_k \pm q_2 \cdots q_m) = 0$, откуда следует более короткое равенство $p_2 p_3 \cdots p_k = (\pm q_2) q_3 \cdots q_m$ и т. д. □

7.9. Поле $\mathbb{F}_p = \mathbb{Z}/(p)$. Из данного в (n° 7.3) описания обратимых элементов кольца $\mathbb{Z}/(n)$ вытекает, что это кольцо является полем тогда и только тогда, когда $n = p$ является *простым числом*. В самом деле, если $n = mk$ составное, ненулевые классы $[m], [k] \in \mathbb{Z}/(n)$ будут делителями нуля, что противоречит их обратимости. Напротив, если p простое число, $\text{НОД}(m, p) = 1$ для всех m не кратных p, а значит, каждый ненулевой класс $[m] \in \mathbb{Z}/(p)$ обратим. Обратный класс $[m]^{-1}$ находится применением алгоритма Евклида к $E_0 = p$ и $E_1 = m$.

Поле $\mathbb{Z}/(p)$, где p простое, принято обозначать $\mathbb{F}_p$. В поле $\mathbb{F}_p$ выполняется замечательное равенство

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ раз}} = 0 .$$

В результате $\forall\, a, b \in \mathbb{F}_p$ имеет место тождество $(a + b)^p = a^p + b^p$. В самом деле, при раскрытии скобок в биноме $(a + b)^p$ одночлены $a^k b^{p-k}$ возникают в виде суммы всевозможных слов, состоящих из k букв a и $(p - k)$ букв b, и приведение всех этих подобных слагаемых означает представление этой суммы в виде

$$a^k b^{p-k} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{\frac{p!}{k!(p-k)!} \text{ раз}} .$$

Поскольку $\frac{p!}{k!(p-k)!}$ делится на p при простом p и $1 \leqslant k \leqslant (p - 1)$ (ибо числитель делится на p, а знаменатель — нет), сумма в скобках обращается в нуль при всех $k \neq 0, p$. Это даёт ещё одно доказательство *малой теоремы Ферма* (см. n° 7.3.2):

$$[a]^p = \underbrace{([1] + [1] + \cdots + [1])^p}_{a \text{ раз}} = \underbrace{[1]^p + [1]^p + \cdots + [1]^p}_{a \text{ раз}} = \underbrace{[1] + [1] + \cdots + [1]}_{a \text{ раз}} = [a] .$$

7.9.1. Пример: конечные геометрии. Многие понятия и конструкции из геометрии вещественной координатной плоскости $\mathbb{R}^2$ или вещественного координатного пространства $\mathbb{R}^3$ сохраняют свой смысл после замены поля вещественных чисел $\mathbb{R}$ *произвольным* полем $\Bbbk$. А именно, будем называть *координатной плоскостью* над полем $\Bbbk$ множество упорядоченных пар элементов поля $\Bbbk$:

$$\Bbbk^2 \stackrel{\text{def}}{=} \Bbbk \times \Bbbk = \{(x, y) \mid x, y \in \Bbbk\} .$$

Элементы (x, y) этой плоскости мы будем называть *точками*. Наряду с точками в геометрии рассматриваются *векторы*, также представляющие собою упорядоченные пары чисел $(a_1, a_2) \in \Bbbk \times \Bbbk$. Пространство векторов удобно рассматривать отдельно от пространства точек. Векторы можно складывать и умножать на числа из поля $\Bbbk$: если $a = (a_1, a_2)$, $b = (b_1, b_2)$ и $\lambda \in \Bbbk$, то по определению $a + b = (a_1 + a_2, b_1 + b_2)$ и $\lambda \cdot a = (\lambda a_1, \lambda a_2)$. В частности, векторы образуют абелеву группу относительно операции сложения. Эта абелева группа действует на точечном пространстве $\Bbbk^2$ преобразованиями сдвига: каждому вектору $v = (v_1, v_2)$ отвечает *сдвиг на вектор* v

$$\tau_v : \Bbbk^2 \xrightarrow{(x,y) \mapsto (x+v_1, y+v_2)} \Bbbk_2$$

(проверьте, что композиции сдвигов отвечает сложение векторов, т. е. $\tau_v \tau_w = \tau_{v+w}$). Прямую на плоскости $\Bbbk^2$ можно определить либо как множество точек (x, y), удовлетворяющих какому-нибудь линейному

уравнению $ax + by = c$, в котором хотя бы один из коэффициентов a, b отличен от нуля, либо как траекторию движения какой-нибудь точки $z_0 = (x_0, y_0)$ с ненулевой постоянной скоростью $v = (v_1, v_2)$, т. е. как множество точек вида $z_t = z_0 + tv = (x_0 + tv_1, y_0 + tv_2)$, где «время» t пробегает поле $\Bbbk$.

Упражнение 7.9. Убедитесь, что эти два определения эквивалентны в том смысле, что прямая, заданная уравнением $ax + by = c$ представляет собой траекторию любой своей точки, выпущенной со скоростью $(-b, a)$, и наоборот, траектория точки (x_0, y_0), выпущенной со скоростью $v = (v_1, v_2)$, задаётся уравнением $v_2x - v_1y = v_2x_0 - v_1y_0$.

Упражнение 7.10. Проверьте, что на плоскости $\Bbbk^2$ над любым полем $\Bbbk$ выполняются евклидовы аксиомы инцидентности:

а) имеются три точки, не лежащие на одной прямой;

б) через любые две точки проходит ровно одна прямая;

в) через точку, не лежащую на данной прямой, проходит ровно одна прямая, не пересекающаяся с данной.

Таким образом, любые конфигурационные задачи[1] школьной планиметрии можно рассматривать над любым полем. Например, над конечным полем $\mathbb{F}_p$ из p элементов.

Плоскость $\mathbb{F}_p^2$ над полем $\mathbb{F}_p$ состоит из p^2 точек. Каждая лежащая на ней прямая содержит в точности p из них, поскольку точки $z + t_1v$ и $z + t_2v$ различны при $t_1 \neq t_2$. Так как через любую пару различных точек проходит единственная прямая, через каждую точку плоскости проходит ровно $(p^2 - 1)/(p-1) = p+1$ прямых[2], а всего на плоскости $\mathbb{F}_p^2$ будет $\binom{p^2}{2}/\binom{p}{2} = p(p+1)$ прямых[3].

На рис. 7◇1 изображены все 25 точек плоскости $\mathbb{F}_5^2$. Начало координат помечено символом +, горизонтальная и вертикальная координатные оси состоят из точек, помеченных символами «0» и «∞» соответственно, точки каждой из проходящих через начало координат прямых $y = kx$, где $k \equiv 0, 1, \ldots, 5$, также помечены соответствующей цифрой k (вертикальная координатная ось $x = 0$ отвечает значению $k = \infty$).

Обратите внимание, что четыре точки «3», также как и четыре точки «2», тоже составляют одну прямую вместе с точкой «+».

④	③	∞	②	①
②	④	∞	①	③
0	0	+	0	0
③	①	∞	④	②
①	②	∞	③	④

Рис. 7◇1. Шесть проходящих через начало координат прямых на плоскости $\mathbb{F}_5^2$.

Упражнение 7.11. Нарисуйте на плоскости $\mathbb{F}_5^2$ коники $y = x^2$, $x^2 + y^2 = 1$ и $x^2 + y^2 = -1$.

Упражнение 7.12. Сколько прямых и плоскостей имеется в трёхмерном пространстве $\mathbb{F}_p^3$ над полем из p элементов, и сколько из них проходит через начало координат?

[1] т. е. относящиеся к взаимному расположению точек и прямых и не использующие понятий из метрической геометрии, таких как расстояния или величины углов

[2] при фиксированном $z \in \mathbb{F}_p^2$ имеется $p^2 - 1$ записей (z, w) с $w \neq z$, $w \in \mathbb{F}_p^2$, и для каждой проходящей через z прямой ℓ имеется ровно $p - 1$ способ записать её в виде (z, w) с $w \neq z$, $w \in \ell$

[3] всего имеется $\binom{p^2}{2}$ записей (z, w) с $z, w \in \mathbb{F}_p^2$ и $w \neq z$, и каждая прямая ℓ ровно $\binom{p}{2}$ способами записывается в виде (z, w) с $z, w \in \ell$ и $w \neq z$