Д. И. МОЛДАВАНСКИЙ

ЦЕЛЫЕ ЧИСЛА
ОСНОВЫ ТЕОРИИ ДЕЛИМОСТИ

Факультативный курс

ИВАНОВО 2001

Ивановский государственный университет
Ивановский областной институт повышения
квалификации и переподготовки педагогических
кадров

Д. И. Молдаванский

Целые числа

Основы теории делимости

Факультативный курс

ИВАНОВО 2001

Учебное издание

Давид Ионович Молдаванский

Целые числа. Основы теории делимости

Учебное пособие

Компьютерный набор и верстка: Д. И. Молдаванский

Лицензия ЛР N 040290 от 02.02.98

Издательство Ивановского областного института
повышения квалификации и переподготовки педагогических кадров.
153000 г. Иваново, ул. Б. Воробьевская, 80

ББК 22.1
М75

Печатается по решению редакционно-издательского совета Ивановского областного института повышения квалификации и переподготовки педагогических кадров

Рецензенты: М. А. Артамонов
А. С. Пряникова

Ответственный за издание В. М. Силин

Корректор Л. С. Кутьина

М75

Д. И. Молдаванский
Целые числа. Основы теории делимости.
Иваново, 2001. – 166 с.

Книга адресована преподавателям математики и учащимся старших классов средней школы. Является элементарным введением в теорию чисел и может служить основой факультативного курса по теории делимости целых чисел.

ББК 22.1

Введение

Предлагаемое пособие является элементарным введением в теорию чисел — раздел математики, в котором изучаются свойства основных числовых систем. Оно предназначено преподавателям математики и учащимся старших классов средней школы и может служить основой факультативного курса по теории делимости целых чисел.

Задачи, связанные с делимостью целых чисел, представляют собой великолепный материал для воспитания математической культуры учащихся, в частности, — логической культуры, интереса к математическому творчеству. К сожалению, школьная программа не предусматривает достаточно основательного знакомства с теорией целого числа; введения в младших классах понятий делимости, наибольшего общего делителя и простого числа и знакомства с некоторыми алгоритмами явно недостаточно для решения даже простых задач в этой области. Свидетельством этого может служить и то обстоятельство, что на математических олимпиадах задачи, связанные с целыми числами, редко получают исчерпывающе обоснованное решение. Следует, впрочем, заметить, что в последнее время программы по математике для классов с углубленной математической подготовкой предусматривают довольно серьезное введение в теорию целых чисел.

Основной причиной затруднений при решении задач, связанных с делимостью целых чисел, является, на наш взгляд, то обстоятельство, что учащиеся не располагают достаточно отчетливым представлением о свойствах целых чисел, о том, чем, собственно, отличаются целые числа от других чисел, рациональных или действительных. Без четкого понимания того, что можно и чего нельзя делать при решении задач, связанных с целыми числами, невозможно и получить удовлетворительное решение таких задач.

Поэтому введение в теорию делимости целых чисел следует начать с обсуждения вопроса о том, что такое целое число. Ответ на этот вопрос можно дать на различных уровнях строгости.

Интуитивная точка зрения на природу целых чисел состоит в том, что в множество целых чисел включают, прежде всего, натуральные числа $1, 2, 3, \ldots$, возникающие при подсчете числа элементов конечных множеств. Далее вводится число 0, как число элементов пустого множества, а затем — отрицательные числа $-1, -2, -3, \ldots$, как противоположные соответствующим натуральным числам. Этот подход к понятию целого числа можно сделать более наглядным, изображая целые числа точками числовой прямой, и на этом пути объяснить смысл операций сложения, умножения и вычитания целых чисел и отношения неравенства. Однако, при изучении более тонких свойств целых чисел, связанных, например, с отношением делимости, мы обнаруживаем, что этих интуитивных представлений недостаточно для того, чтобы судить об истинности или ложности формулируемых предположений. Отсюда — необходимость более точного представления о целых числах, более надежного способа отличать истинные утверждения от ложных.

Такую возможность дает аксиоматический метод, хорошо известный нам по школьному курсу геометрии. Он заключается в том, что некоторый фиксированный перечень (интуитивно ясных) свойств рассматриваемых объектов, в нашем случае — чисел, принимается без доказательства (и эти свойства объявляются ак-

сиомами), а затем постулируется, что все остальные свойства этих объектов считаются истинными тогда и только тогда, когда их можно вывести из аксиом чисто логическим путем. Определенная (и в некоторой степени оправданная) специфика изложения школьного курса математики создает у учащихся неверное представление о том, что аксиоматический метод может быть использован только при изложении геометрии. В действительности, это не так, в чем может убедиться читатель данного пособия.

В первом параграфе будут изложены те свойства целых чисел, которые мы принимаем в качестве аксиом системы целых чисел. Здесь же приведены и некоторые следствия из этих аксиом. При этом, система целых (а также рациональных и действительных) чисел рассматривается как некоторое множество с определенными на нем операциями сложения и умножения и отношением порядка (неравенства).

Для начала перечисляется ряд известных учащимся свойств операций сложения и умножения, присущих всем числовым системам и являющихся, по существу, определением одного из основных понятий современной математики — понятия кольца (точнее, ассоциативно–коммутативного кольца с единицей). Отмечается и демонстрируется на ряде примеров, что многие привычные свойства чисел, такие, например, как правила обращения со знаками при умножении или тождества сокращенного умножения, могут быть совершенно формально выведены из перечисленных свойств и потому являются справедливыми для любого кольца.

Наличие многих примеров колец, свойства которых могут быть весьма различными, говорит о том, что перечисленных к этому моменту аксиом явно недостаточно для однозначного определения системы целых чисел, и потому к ним следует добавить дополнительные свойства, которыми с интуитивной точки зрения обладают целые числа. В формулировках этих свойств наряду с операциями сложения и умножения участвуют и числовые неравенства. Точнее говоря, напоминается, что на множестве чисел (целых, рациональных и действительных) определено отношение "меньше", и перечисляются основные свойства этого отношения. Вместе с фиксированными ранее свойствами сложения и умножения они составляют определение новой алгебраической структуры — упорядоченного кольца. Доказывается ряд свойств упорядоченных колец (в школьной терминологии — свойства числовых неравенств).

Каждая из трех указанных выше числовых систем является упорядоченным кольцом, и потому для выделения среди них системы целых чисел все еще необходимы дополнительные аксиомы. Оказывается, что достаточно всего двух таких аксиом: первая из них утверждает свойство дискретности отношения порядка (из $a < b$ следует, что $a+1 \leqslant b$), а вторая требует, чтобы в каждом непустом подмножестве множества всех положительных чисел существовал наименьший элемент. Эта последняя аксиома фактически равносильна так называемому принципу полной математической индукции, и здесь же подробно обсуждается как эта равносильность, так и метод доказательства по индукции.

Таким образом, в первом параграфе сформулированы достаточно привычные свойства целых чисел, которые могут быть приняты в качестве аксиом, определяющих систему целых чисел (вопросы полноты и непротиворечивости здесь, есте-

ственно, не обсуждаются). На этой основе во втором и третьем параграфах излагаются с подробными доказательствами основные свойства отношения делимости целых чисел и связанных с ним понятий, включая теорему о разложении на простые множители. В четвертом и пятом параграфах развивается аппарат теории сравнений и доказываются классические теоремы Эйлера и Ферма. Демонстрируется эффективность применения этого аппарата к решению задач о делимости целых чисел. Шестой параграф посвящен обоснованию введения позиционных систем счисления и изложению некоторых признаков делимости.

Определение делимости целых чисел может быть дословно перенесено на произвольные кольца, и простейшие свойства этого отношения остаются справедливыми в самом общем случае. Естественно возникает вопрос о том, все ли теоремы о делимости целых чисел можно распространить на любые кольца. В седьмом параграфе показано, что это не так. Приводится пример кольца, теория делимости в котором весьма отлична от теории делимости целых чисел: не выполняется утверждение об однозначности разложения на простые множители и наибольший общий делитель двух элементов не обязательно существует. Вместе с тем, показано, что в кольце так называемых целых гауссовых чисел имеет место практически такая же теория делимости, как и в кольце целых чисел. Этот последний параграф носит более абстрактный характер, и для его понимания необходимо знакомство с комплексными числами.

В пособии используется общепринятая нумерация выделенных утверждений; например, ссылка на теорему 2.1 отсылает читателя к соответствующей теореме из параграфа 2. Значок $\square$ обозначает конец доказательства или решения примера; появление его (в редких случаях) сразу после формулировки некоторого утверждения означает, что это утверждение очевидно, в чем читатель должен убедиться самостоятельно. Изложение теоретических сведений сопровождается достаточным (на взгляд автора) количеством примеров. После каждого параграфа приводится список задач и упражнений для самостоятельного решения. Все задачи снабжены ответами и почти все достаточно подробными указаниями (переходящими в ряде случаев в исчерпывающие решения). Приведен также ряд изданий, в которых заинтересованный читатель найдет дополнительные сведения по теории чисел и алгебре. В этот (далеко не полный) список включены как популярные книги, предназначенные для учащихся средней школы, так и учебники для студентов математических факультетов университетов.

§ 1. Определение системы целых чисел

Этот параграф мы начнем с перечисления ряда известных (или, вернее, привычных) нам свойств, которыми обладает каждое из основных числовых множеств: множество $\mathbb{Z}$ всех целых чисел, множество $\mathbb{Q}$ всех рациональных чисел и множество $\mathbb{R}$ всех действительных чисел. Затем будут указаны те свойства, которые справедливы лишь для целых чисел и которые (вместе со свойствами, общими для всех числовых систем) могут быть приняты в качестве аксиом, определяющих целые числа.

На любом из упомянутых множеств чисел имеются две операции — сложение $+$ и умножение $\cdot$, и в формулировках первой группы общих свойств чисел участвуют только эти операции. Перечислим эти свойства:

1) *Переместительный (коммутативный) закон сложения и умножения: для любых чисел a и b выполнены равенства*

$$a + b = b + a \qquad \text{и} \qquad ab = ba.$$

2) *Сочетательный (ассоциативный) закон сложения и умножения: для любых чисел a, b и c выполнены равенства*

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

3) *Распределительный (дистрибутивный) закон сложения и умножения: для любых чисел a, b и c выполнено равенство*

$$(a + b)c = ac + bc.$$

4) *Существует такое число (называемое нулем и обозначаемое символом 0), что для любого числа a выполнено равенство $a+0 = a$. Существует такое число (называемое единицей и обозначаемое символом 1), что для любого числа a выполнено равенство $a1 = a$.*

5) *Для любого числа a существует такое число x, что выполнено равенство $a + x = 0$.*

Перечень тех исходных свойств чисел, в которых речь идет только об операциях сложения и умножения закончен. Подчеркнем еще раз, что этими свойствами обладают сложение и умножение и целых, и рациональных, и действительных чисел.

В математике встречаются и другие множества объектов, на которых определены операции сложения и умножения, обладающие перечисленными выше свойствами. Типичным примером могут служить всевозможные многочлены от одной переменной x, т. е. выражения вида $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, где $n \geqslant 0$ и a_0, a_1, $\ldots$ a_n — некоторые числа. Сумма и произведение двух таких выражений, вычисляемые по известным правилам (раскрытие скобок и приведение подобных членов), снова являются многочленами, причем эти операции удовлетворяют вышеперечисленным свойствам 1) – 5). Мы принимаем следующее определение:

Произвольное непустое множество K, на котором определены операции сложения и умножения, удовлетворяющие свойствам 1) – 5), *называется кольцом.*

Таким образом, каждое из числовых множеств $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ является кольцом. Кольцом является и множество многочленов от переменной x, коэффициенты которых принадлежат любому из этих числовых колец. Другие примеры колец нам встретятся ниже в параграфах 4 и 7.

Мы сейчас увидим, что ряд известных нам правил обращения со сложением и умножением чисел могут быть выведены из вышеперечисленных пяти свойств чисто логическим путем. Это означает, что все такие правила справедливы в любом кольце, и потому мы будем и формулировать, и доказывать их сразу для произвольного кольца.

Предложение 1.1. а) *В любом кольце элементы нуль и единица, существование которых постулируется свойством 4), являются единственными. При этом, если в кольце имеется более одного элемента, то* $1 \neq 0$.

б) *В любом кольце для произвольного элемента a элемент x, существование которого постулируется свойством 5), является единственным. (Такой элемент мы называем противоположным к элементу a и обозначаем через $-a$.)*

в) *В любом кольце для произвольных элементов a и b выполнены равенства* $a \cdot 0 = 0$, $-(-a) = a$ *и* $a(-b) = -ab$.

Докажем эти утверждения, заодно объяснив более подробно их смысл. Пусть нам дано некоторое кольцо K. Предположим, что в этом кольце нашлись два элемента x и y, каждый из которых удовлетворяет определению нуля, т. е. для любого элемента $a \in K$ имеют место равенства $a + x = a$ и $a + y = a$. Подставляя в первое из них вместо a элемент y, а во второе вместо a элемент x, получаем $y + x = y$ и $x + y = x$, а так как ввиду свойства 1) $x + y = y + x$, мы действительно имеем $x = y$. Аналогично доказывается единственность единицы.

Для доказательства пункта б) опять предположим, что для некоторого элемента a кольца K в этом кольце оказалось два элемента x и y таких, что $a + x = 0$ и $a + y = 0$. Тогда имеем

$$x = x + 0 = x + (a + y) = (x + a) + y = (a + x) + y = 0 + y = y + 0 = y$$

(читателю рекомендуется самостоятельно определить, на каком из перечисленных выше свойств основан переход через каждый знак равенства). Таким образом, для любого элемента a в кольце действительно существует лишь один элемент, который в сумме с элементом a дает нуль. Как указано в формулировке предложения 1.1, этот элемент, однозначно определяемый элементом a, мы будем называть противоположным к элементу a и обозначать $-a$. Еще раз подчеркнем, что именно равенство $a + (-a) = 0$ является для нас определением элемента $-a$, противоположного к элементу a. Так как из этого равенства в силу коммутативности сложения следует равенство $(-a) + a = 0$, то элемент a является противоположным к элементу $-a$, т. е. $a = -(-a)$, и этим доказано второе из равенств пункта в).

Для доказательства первого из них предварительно заметим, что если некоторый элемент b кольца удовлетворяет равенству $b + b = b$, то он равен нулю:

действительно,

$$b = b + 0 = b + (b + (-b)) = (b + b) + (-b) = b + (-b) = 0.$$

Поскольку для любого элемента a имеет место равенство $a \cdot 0 + a \cdot 0 = a \cdot 0$ (так как $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$), отсюда и следует, что $a \cdot 0 = 0$. Наконец, для произвольных элементов a и b кольца имеем $ab + a(-b) = a(b + (-b)) = a0 = 0$, а это и означает, что элемент $a(-b)$ является противоположным к элементу ab, т. е. $a(-b) = -ab$.

Вернемся теперь к оставшемуся недоказанным последнему утверждению пункта а). Если предположить, что некоторый элемент c кольца K обладает одновременно свойствами, определяющими и нуль, и единицу, то для произвольного элемента a из K мы будем иметь $a = a \cdot c$ (по определению единицы) и $a \cdot c = c$ (по доказазанному в пункте в) свойству нуля). Отсюда $a = c$, и наше кольцо должно в этом случае состоять лишь из одного этого элемента c.

(Следует добавить для полноты картины, что такая возможность действительно реализуема. В самом деле, мы можем взять множество, состоящее из единственного элемента c, и определить на этом множестве операции сложения и умножения следующим (единственно возможным) способом: $c + c = c$ и $c \cdot c = c$. Непосредственно проверяется, что эти операции обладают всеми вышеперечисленными свойствами 1) – 5), и потому наше множество является кольцом. Единственный элемент c этого кольца является одновременно и нулем и единицей. Такое кольцо называют *нулевым кольцом*.)

Предложение 1.1 полностью доказано. □

В произвольном кольце K можно ввести операцию вычитания, полагая по определению $a - b = a + (-b)$. Легко проверить, что элемент $x = a - b$, называемый разностью элементов a и b, удовлетворяет равенству $x + b = a$, и поэтому мы говорим, что операция вычитания является обратной к операции сложения. Возможность введения операции, обратной к умножению, будет обсуждаться ниже.

Операции сложения и умножения, по определению, могут быть применены к двум элементам кольца. Чтобы сложить три элемента a, b и c, следует, например, сначала найти сумму $a + b$ первых двух, а затем эту сумму сложить с третьим, получив $(a + b) + c$. Но можно сначала сложить второй и третий элементы, а затем — первый с полученной суммой, получив $a + (b + c)$. Свойство ассоциативности говорит о том, что оба способа вычисления дают один и тот же результат. Для вычисления суммы четырех элементов a, b, c и d имеется уже пять различных способов:

$$(a + b) + (c + d), \quad ((a + b) + c) + d, \quad (a + (b + c)) + d,$$
$$a + ((b + c) + d), \quad a + (b + (c + d))$$

(и их число очень быстро растет с ростом числа слагаемых). С помощью свойства ассоциативности можно доказать, что все они приводят к одному и тому же результату. Например,

$$((a + b) + c) + d = (a + (b + c)) + d = a + ((b + c) + d) = a + (b + (c + d)).$$

Здесь первый знак равенства основан на применении свойства ассоциативности к элементам a, b и c; второй знак равенства основан на применении свойства ассоциативности к элементам a, $b+c$ и d; третий знак равенства основан на применении свойства ассоциативности к элементам b, c и d.

Аналогично, для вычисления суммы пяти, шести и т. д. элементов кольца следует указать (с помощью скобок) порядок выполнения действий так, чтобы в каждом из этих действий складывалось два элемента. Основываясь на свойстве ассоциативности, можно доказать, что любые две расстановки скобок приводят к одному и тому же результату. Разумеется, все это справедливо и для умножения.

Таким образом, в произвольном кольце можно говорить о сумме и произведении произвольного числа элементов a_1, a_2, ... , a_n. В частности, при $n > 1$ (однозначно определенное) произведение элементов a_1, a_2, ... , a_n, каждый из которых равен одному и тому же элементу a нашего кольца, мы обозначаем a^n и называем *степенью элемента a с показателем n*. Полагая также $a^1 = a$ и $a^0 = 1$, мы определяем, таким образом, для любого кольца понятие степени элемента с произвольным неотрицательным целым показателем. При этом непосредственно из нашего определения следует, что для любых неотрицательных целых чисел m и n и любого элемента $a \in K$ выполнены равенства

$$a^{m+n} = a^m \cdot a^n \quad \text{и} \quad (a^m)^n = a^{mn}.$$

Используя свойство коммутативности умножения, можно доказать также, что для любого неотрицательного целого числа m и любых элементов $a, b \in K$ имеет место равенство

$$(ab)^m = a^m \cdot b^m.$$

Возможность введения понятия степени с отрицательным целым показателем будет обсуждаться ниже.

Аналогичным образом для произвольного неотрицательного целого числа n и произвольного элемента a кольца K можно ввести понятие n-кратного na элемента a, полагая

$$na = a + a + \cdots + a$$

(n слагаемых) при $n > 1$, $na = a$ при $n = 1$ и $na = 0$ при $n = 0$.

Разумеется, все вышесказанное можно применить, в частности, и к основным числовым системам $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ (получив привычные нам определения). Целый ряд других известных свойств чисел таких, например, как формулы сокращенного умножения, также могут быть выведены из свойств 1) – 5); именно это имеют в виду математики, когда говорят, что то или иное свойство справедливо для данной числовой системы просто потому, что эта система является кольцом.

Докажем, например, что в произвольном кольце K имеет место знакомое нам тождество $(a+b)^2 = a^2 + 2ab + b^2$. Действительно,

$$(a+b)^2 = (a+b)\cdot(a+b) = (a+b)a + (a+b)b = \\ (a^2 + ba) + (ab + b^2) = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2.$$

Здесь мы применяем последовательно свойство дистрибутивности, ассоциативности (когда опускаем скобки) и коммутативности.

Вернемся, однако, к задаче перечисления тех свойств, которые смогут составить определение системы целых чисел. Отмеченных выше пяти свойств для этого явно недостаточно, так как существуют примеры различных колец, свойства которых весьма разнообразны, и в частности, существует кольцо, состоящее в точности из одного элемента. Чтобы исключить этот вырожденный случай, мы вводим в наш перечень свойств требование

6) *Числа* 0 *и* 1 *различны.*

Разумеется, включение в перечень свойств, определяющих целые числа, этого "тривиального" условия может показаться излишним. В связи с этим, укажем на то, что (как легко проверить) все другие свойства, которые будут нами приняты в качестве аксиом системы целых чисел, выполняются и в нулевом кольце. Поэтому исключение этого свойства приведет к очевидной потере однозначности определяемой системы. Заметим еще, что ввиду предложения 1.1 условие 6) можно заменить равносильным требованием существования хотя бы двух различных чисел.

В формулировках дальнейших необходимых нам свойств чисел наряду с операциями сложения и умножения будет участвовать и отношение неравенства. Как нам хорошо известно, на множестве чисел определено отношение "меньше", обозначаемое символом $<$ и обладающее следующими свойствами:

7) *Для любого числа* a *утверждение о том, что* $a < a$*, неверно (антирефлексивность).*

8) *Для любых чисел* a*,* b *и* c *из того, что* $a < b$ *и* $b < c$*, следует, что* $a < c$ *(транзитивность).*

9) *Для любых неравных чисел* a *и* b *должно иметь место или* $a < b$*, или* $b < a$ *(всюду определенность).*

Отношение $<$, определенное на произвольном множестве A и удовлетворяющее этим трем свойствам, называется *отношением порядка.* Множество A, рассматриваемое вместе с определенным на нем отношением порядка, называется *упорядоченным множеством.*

Иногда определенное только что отношение порядка называют отношением строгого порядка, чтобы отличить его от отношения нестрогого порядка "меньше или равно", обозначаемого $\leqslant$ и определяемого следующими свойствами:

а) *Для любого элемента имеет место* $a \leqslant a$ *(рефлексивность).*

б) *Для любых элементов* a*,* b *и* c *из того, что* $a \leqslant b$ *и* $b \leqslant c$*, следует, что* $a \leqslant c$ *(транзитивность).*

в) *Для любых элементов* a *и* b *из того, что* $a \leqslant b$ *и* $b \leqslant a$*, следует, что* $a = b$ *(антисимметричность).*

г) *Для любых элементов* a *и* b *должно иметь место или* $a \leqslant b$*, или* $b \leqslant a$ *(всюду определенность).*

Эти отношения являются взаимоопределимыми: если на некотором множестве задано отношение $<$, удовлетворяющее свойствам 7), 8) и 9), то полагая по определению, что $a \leqslant b$ тогда и только тогда, когда или $a = b$, или $a < b$, получим отношение, обладающее свойствами а), б), в) и г). Наоборот, имея отношение $\leqslant$,

удовлетворяющее свойствам а), б), в) и г), и полагая, что $a < b$ тогда и только тогда, когда $a \leqslant b$ и $a \neq b$, придем к отношению, обладающему свойствами 7), 8) и 9). Таким образом, считая заданным отношение $<$, мы можем пользоваться, когда нам удобно, и отношением $\leqslant$.

Если A — упорядоченное множество с отношением порядка $<$ ("меньше"), то мы можем для удобства формулировок ввести на этом множестве также и отношение "больше" (и "больше или равно"), полагая по определению, что $a > b$ (или $a \geqslant b$), если $b < a$ (соответственно, $b \leqslant a$).

Напомним, что число a называется положительным (неотрицательным), если $a > 0$ (соответственно, $a \geqslant 0$), и отрицательным (неположительным), если $a < 0$ (соответственно, $a \leqslant 0$).

В следующих двух свойствах говорится о связи отношения "меньше" с операциями сложения и умножения.

10) *Для любых трех чисел a, b и c из того, что $a < b$, следует, что $a + c < b + c$.*

11) *Для любых трех чисел a, b и c из того, что $a < b$ и $c > 0$, следует, что $ac < bc$.*

Произвольное кольцо, на котором определено отношение порядка, удовлетворяющее свойствам 10) и 11) (в формулировках которых следует вместо чисел говорить об элементах кольца), называют *упорядоченным кольцом*. Таким образом, наши основные числовые системы являются упорядоченными кольцами. Все известные нам правила обращения с числовыми неравенствами являются следствиями свойств 7) – 11) (и потому справедливы для произвольного упорядоченного кольца).

Предложение 1.2. а) *Неравенства одинакового знака можно почленно складывать, т. е. для любых чисел a, b, c и d из того, что $a < b$ и $c < d$, следует, что $a + c < b + d$.*

б) *Неравенства одинакового знака с положительными членами можно почленно перемножать, т. е. для любых положительных чисел a, b, c и d из того, что $a < b$ и $c < d$, следует, что $ac < bd$.*

в) *Для любых чисел a и b неравенство $a < b$ имеет место тогда и только тогда, когда выполняется неравенство $-b < -a$. В частности, число a является положительным тогда и только тогда, когда число $-a$ является отрицательным.*

г) *Для любых чисел a, b и c из того, что $a < b$ и $c < 0$, следует, что $ac > bc$.*

Докажем утверждение а). Пусть даны неравенства $a < b$ и $c < d$. Прибавив к обеим частям первого из них число c, а к обеим частям второго число b, в соответствии со свойством 10) получаем $a + c < b + c$ и $b + c < b + d$. В силу свойства транзитивности отношения порядка (свойство 8)) отсюда следует, что $a + c < b + d$. Утверждение б) доказывается аналогично (с использованием свойства 11) вместо свойства 10)).

Для доказательства утверждений пункта в) прибавим к обеим частям неравенства $a < b$ число $-a$. Получаем неравенство $0 < b + (-a)$, которое после прибавления к обеим частям числа $-b$ принимает вид $-b < -a$. Таким образом, мы видим, что из неравенства $a < b$ следует неравенство $-b < -a$. Аналогично доказывается,

что из неравенства $-b < -a$ следует неравенство $a < b$, и первое утверждение пункта в) доказано. Применяя его к неравенству $0 < a$, получаем и второе утверждение.

Докажем, наконец, утверждение г). Пусть $a < b$ и $c < 0$. Тогда в силу уже доказанного пункта в) имеем $-c > 0$, и потому ввиду свойства 11) выполняется неравенство $a(-c) < b(-c)$. Так как $a(-c) = -ac$ и $b(-c) = -bc$ (см. предложение 1.1), это неравенство можно переписать в виде $-ac < -bc$, откуда ввиду пункта в) получаем $ac > bc$, что и требовалось. Предложение 1.2 доказано. □

Покажем теперь, что еще одно важное свойство чисел, постоянно используемое, в частности, при решении уравнений, является следствием перечисленных выше свойств 1) – 11).

Предложение 1.3. *Произведение двух чисел равно нулю тогда и только тогда, когда хотя бы один из сомножителей равен нулю.*

В самом деле, если для двух чисел a и b имеет место равенство $ab = 0$ и, тем не менее, $a \neq 0$ и $b \neq 0$ то ввиду свойства 9) должна выполняться одна из следующих четырех возможностей:

$$\text{а)} \begin{cases} a > 0 \\ b > 0 \end{cases}; \qquad \text{б)} \begin{cases} a > 0 \\ b < 0 \end{cases}; \qquad \text{в)} \begin{cases} a < 0 \\ b > 0 \end{cases}; \qquad \text{г)} \begin{cases} a < 0 \\ b < 0 \end{cases}.$$

Из свойства 11) и пункта г) предложения 2 следует, что в случае а) выполняется неравенство $ab > 0$, в случае б) — неравенство $ab < 0$, в случае в) — неравенство $ab < 0$ и в случае г) — неравенство $ab > 0$. Таким образом, из равенства $ab = 0$ следует (в силу антирефлексивности отношения порядка), что или $a = 0$, или $b = 0$. Обратное утверждение содержится в предложении 1.1, и предложение 1.3 доказано. □

Предложение 1.3 может служить обоснованием известного и часто используемого *правила сокращения*:

Следствие. *Для любых чисел a, b и c из того, что $ac = bc$ и $c \neq 0$, следует, что $a = b$.*

Для доказательства этого достаточно равенство $ac = bc$ переписать в виде $(a - b)c = 0$, а затем воспользоваться предложением 3. □

Следует отметить, что существуют примеры колец, для которых утверждение предложения 1.3 не выполняется, т. е. произведение ненулевых элементов может оказаться равным нулю (см. § 4). Те кольца, для которых утверждение предложения 1.3 справедливо, имеют специальное название. А именно, кольцо K называется *целостным кольцом*, если для любых его элементов a и b из равенства $ab = 0$ следует, что или $a = 0$, или $b = 0$. Следствие из предложения 1.3 фактически говорит о том, что для любого целостного кольца справедливо правило сокращения. Легко понять, что имеет место и обратное: кольцо с правилом сокращения является целостным.

Так как доказательство предложения 1.3 без изменений проходит, разумеется, для произвольного упорядоченного кольца, мы видим, что все упорядоченные

кольца являются целостными. В параграфе 7 будут указаны примеры целостных колец, не являющихся упорядоченными.

Заметим еще, что с помощью тех же рассуждений, что и в доказательстве предложения 1.3, можно доказать еще одно известное свойство: для любого элемента a упорядоченного кольца выполнено неравенство $a^2 \geqslant 0$, а если $a \neq 0$, то $a^2 > 0$. Так как $1 = 1^2$, отсюда следует, что в любом упорядоченном кольце $1 > 0$ и потому для любого элемента a имеет место неравенство $a < a + 1$.

Свойство неотрицательности квадрата любого действительного числа широко используется в доказательствах числовых неравенств. Рассмотрим, например,

Пример 1.1. *Доказать, что для любых двух действительных чисел a и b выполнено неравенство $a^2 + b^2 \geqslant 2ab$. При этом, равенство имеет место тогда и только тогда, когда $a = b$.*

Для доказательства достаточно записать очевидное (в силу отмеченного только что свойства) неравенство $(a - b)^2 \geqslant 0$ в виде $a^2 - 2ab + b^2 \geqslant 0$. Требуемое неравенство $a^2 + b^2 \geqslant 2ab$ получается из последнего прибавлением к обеим частям числа $2ab$. Остается заметить, что равенство во всех трех неравенствах имеет место одновременно. $\square$

С отношением порядка на множестве чисел связано важное понятие абсолютной величины или модуля числа. Для полноты изложения приведем соответствующее определение и покажем, как основные свойства этого понятия можно вывести из сформулированных выше свойств 1) – 11).

Абсолютной величиной или *модулем* числа a называется число, обозначаемое $|a|$ и определяемое по правилу

$$|a| = \begin{cases} a, & \text{если } a \geqslant 0 \\ -a, & \text{если } a < 0. \end{cases}$$

Легко видеть, что для любых чисел a и b выполнено равенство $|ab| = |a| \cdot |b|$. В самом деле, это равенство очевидно, если хотя бы одно из этих чисел равно нулю. Если же $a \neq 0$ и $b \neq 0$, то следует, рассуждая так же, как в доказательстве предложения 1.3, рассмотреть четыре случая в зависимости от знаков чисел a и b. Например, если $a > 0$ и $b < 0$, то $|a| = a$, $|b| = -b$, и так как в этом случае $ab < 0$, имеем

$$|ab| = -ab = a(-b) = |a| \cdot |b|.$$

Поведение модуля суммы и разности двух чисел описывается в следующем предложении.

Предложение 1.4. а) *Для любых двух чисел a и b, где число b неотрицательно, неравенство $|a| \leqslant b$ равносильно двойному неравенству $-b \leqslant a \leqslant b$.*

б) *Для любых двух чисел a и b, где число b неотрицательно, неравенство $|a| \geqslant b$ имеет место тогда и только тогда, когда или $a \leqslant -b$ или $a \geqslant b$.*

в) *Для любых двух чисел a и b выполняются неравенства $|a + b| \leqslant |a| + |b|$ и $|a - b| \geqslant |a| - |b|$.*

Доказательство. Начнем с пункта а). Пусть a и b — произвольные числа, причем $b \geqslant 0$. Предположим сначала, что имеет место неравенство $|a| \leqslant b$. Тогда если $a \geqslant 0$, то $|a| = a$ и потому данное нам неравенство принимает вид $a \leqslant b$. Кроме того, поскольку $-b \leqslant 0$, то выполнено и неравенство $-b \leqslant a$. Если же $a < 0$, то $|a| = -a$. Тогда неравенство $|a| \leqslant b$ совпадает с неравенством $-a \leqslant b$, которое ввиду пункта в) предложения 2 равносильно неравенству $-b \leqslant a$. Неравенство $a \leqslant b$ в этом случае очевидно, так как $a < 0$ и $b \geqslant 0$. Таким образом, в любом случае из неравенства $|a| \leqslant b$ следует двойное неравенство $-b \leqslant a \leqslant b$.

Обратно, предположим, что имеет место неравенство $-b \leqslant a \leqslant b$. Тогда при $a \geqslant 0$ имеем $|a| = a \leqslant b$, а при $a < 0$ поскольку $a = -|a|$, получаем $-b \leqslant -|a|$ и снова $|a| \leqslant b$. Утверждение пункта а) доказано. Утверждение пункта б) доказывается аналогично.

Для доказательства пункта в) заметим сначала, что для любого числа a выполнено неравенство $-|a| \leqslant a \leqslant |a|$. Действительно, так как по определению модуля для любого числа a имеет место неравенство $|a| \geqslant 0$, то при $a \geqslant 0$ имеем $-|a| \leqslant a$ и $a = |a|$, а при $a < 0$ $-|a| = a$ и $a \leqslant |a|$.

Складывая теперь почленно неравенства $-|a| \leqslant a \leqslant |a|$ и $-|b| \leqslant b \leqslant |b|$, получаем $-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|$, откуда ввиду уже доказанного утверждения пункта а) и следует требуемое неравенство $|a + b| \leqslant |a| + |b|$. Второе неравенство из пункта в) получается из первого следующим образом. Имеем

$$|a| = |(a - b) + b| \leqslant |a - b| + |b|,$$

так что $|a| \leqslant |a-b|+|b|$, откуда и следует неравенство $|a-b| \geqslant |a|-|b|$. Предложение полностью доказано. $\square$

Используя предложение 1.4, многие неравенства, содержащие знак абсолютной величины, можно доказать совершенно формально. Покажем, например, что для любых действительных чисел a, b и c имеет место неравенство $|a + b + c| \leqslant |a| + |b| + |c|$. В силу первого неравенства из пункта в) предложения 1.4 имеем

$$|a + b + c| = |(a + b) + c| \leqslant |a + b| + |c| \leqslant (|a| + |b|) + |c| = |a| + |b| + |c|.$$

Рассмотрим еще один

Пример 1.2. *Доказать, что для любых действительных чисел a и b имеет место неравенство $||a| - |b|| \leqslant |a + b|$.*

Из второго неравенства из пункта в) предложения 1.4 получаем

$$|a + b| = |a - (-b)| \geqslant |a| - |-b| = |a| - |b|.$$

Таким образом, имеет место неравенство $|a| - |b| \leqslant |a + b|$, а так как $|a + b| = |b + a|$, то справедливо и неравенство $|b| - |a| \leqslant |a + b|$, т. е. неравенство $-|a + b| \leqslant |a| - |b|$. Требуемое неравенство следует из полученного двойного неравенства

$$-|a + b| \leqslant |a| - |b| \leqslant |a + b|$$

ввиду пункта а) предложения 1.4. $\square$

Вышеперечисленные свойства 1) – 11) по-прежнему справедливы и для целых, и для рациональных, и для действительных чисел. Дополнив их следующими двумя свойствами, мы получаем, наконец, искомую характеризацию целых чисел.

12) *Для любых двух целых чисел a и b из того, что $a < b$, следует, что $a+1 \leqslant b$.*

13) *В любом непустом множестве положительных целых чисел существует наименьшее число.*

Можно показать, что упорядоченное кольцо, обладающее двумя этими свойствами является (в определенном смысле, уточнению которого здесь не место) единственным. Его мы и будем называть *кольцом целых чисел*, а перечисленные свойства 1) — 13) можно рассматривать как систему аксиом, определяющую целые числа. Это означает, что все свойства целых чисел можно вывести из этих тринадцати свойств. Положительные целые числа будем называть *натуральными числами*.

Обсудим теперь некоторые следствия из системы аксиом кольца целых чисел.

Свойство 12) называют свойством *дискретности* упорядочения целых чисел: выражаясь содержательно, в нем говорится о том, что между любыми двумя целыми числами вида a и $a + 1$ нет ни одного целого числа. (Для рациональных и действительных чисел это утверждение уже не выполняется; например, для любых чисел a и b, где $a < b$, имеет место неравенство $a < (a + b)/2 < b$.) Отметим, что из этого свойства следует также, что 1 является наименьшим из положительных целых чисел: если $a > 0$, то $a \geqslant 1$. Целое число $1 + 1$, непосредственно следующее за 1, мы обозначаем символом 2, число, непосредственно следующее за 2, — символом 3 и т. д. Способы обозначения положительных целых чисел будут подробно рассмотрены ниже в § 6.

Упорядоченное множество, любое непустое подмножество которого обладает наименьшим элементом, в математике называют *вполне упорядоченным*. Таким образом, в свойстве 13) утверждается, что множество всех положительных целых чисел, является вполне упорядоченным. Говоря более подробно, это означает, что любое непустое множество A натуральных чисел содержит такой элемент a, что для любого элемента x множества A выполняется неравенство $x \geqslant a$.

Следует заметить, что множество всех целых чисел вполне упорядоченным не является, т. к., например, множество всех отрицательных целых чисел не имеет наименьшего элемента: для любого целого числа a имеет место неравенство $a - 1 < a$, причем если $a < 0$, то и $a - 1 < 0$.

Из свойства вполне упорядоченности множества натуральных чисел вытекает так называемый *принцип полной математической индукции*. Он может быть сформулирован следующим образом.

Предложение 1.5. *Пусть некоторое математическое утверждение зависит от параметра n, принимающего все натуральные значения (будем записывать это утверждение в виде $P(n)$). Предположим, что*

(i) *Утверждение $P(1)$ является истинным.*

(ii) *Для любого натурального числа m из того, что утверждение $P(m)$ является истинным, следует, что и утверждение $P(m+1)$ является истинным.*

Тогда утверждение $P(n)$ является истинным для любого значения параметра n.

В самом деле, предположим, что для утверждения $P(n)$ выполнены условия (i) и (ii), но, тем не менее, существует натуральное число a такое, что $P(a)$ является ложным. Иначе говоря, это означает, что множество A всех натуральных чисел x, для которых $P(x)$ ложно, не является пустым. Поэтому в соответствии со свойством 13) в множестве A есть наименьший элемент; обозначим его символом x_0. Таким образом, говоря более подробно, из свойства 13) следует существование натурального числа x_0 такого, что $P(x_0)$ ложно, но для любого натурального числа m, меньшего, чем x_0, $P(m)$ истинно. Из предположения (i) следует, что $x_0 > 1$ и потому число $m = x_0 - 1$ положительно, т. е. является натуральным числом. Так как $m < x_0$, утверждение $P(m)$ должно быть истинным. Но тогда в силу предположения (ii) истинным должно быть и утверждение $P(m+1)$, т. е. утверждение $P(x_0)$, что противоречит выбору числа x_0. Таким образом, предположение о непустоте множества A приводит к противоречию, и справедливость принципа полной математической индукции доказана. $\square$

(Мы получили принцип полной математической индукции как следствие свойства вполне упорядоченности множества натуральных чисел. В действительности, как будут показано ниже, можно доказать и обратное, т. е. эти два основополагающих свойства положительных целых чисел являются равносильными.)

Ряд математических утверждений, зависящих от натурального параметра n, могут либо не иметь смысла при нескольких начальных значениях параметра (например, теорема о сумме внутренних углов выпуклого n-угольника), либо быть ложными при нескольких начальных значениях параметра (например, неравенство $2^n > 2n + 1$). В таких случаях удобнее пользоваться более общей формулировкой принципа полной математической индукции:

Предложение 1.6. *Пусть утверждение $P(n)$ зависит от параметра n, принимающего все натуральные значения, большие некоторого натурального числа k или равные числу k. Предположим, что*

(i) *Утверждение $P(k)$ является истинным.*

(ii) *Для любого натурального числа $m \geqslant k$ из того, что утверждение $P(m)$ является истинным, следует, что и утверждение $P(m+1)$ является истинным.*

Тогда утверждение $P(n)$ является истинным для любого значения параметра $n \geqslant k$.

Для доказательства предложения 1.6 достаточно применить предложение 1.5 к утверждению $P'(n) = P(n + k - 1)$. $\square$

На принципе полной математической индукции основан весьма мощный метод доказательства математических утверждений — *метод доказательства по индукции*. Он состоит в том, что для того, чтобы считать доказанной истинность некоторого утверждения $P(n)$ при всех значениях натурального параметра n, больших

или равных некоторому фиксированному натуральному числу k (возможно, $k = 1$), достаточно выполнить следующие шаги:

Шаг 1. Проверить истинность утверждения $P(n)$ при $n = k$. (Этот шаг называется *основанием* или *базисом индукции*.)

Шаг 2. Предположить, что для некоторого числа $m \geqslant k$ утверждение $P(m)$ является истинным. (Этот шаг называется формулировкой *индуктивного предположения*.)

Шаг 3. Доказать, что из индуктивного предположения, сделанного на втором шаге, следует истинность утверждения $P(m+1)$. (Этот шаг называется *индуктивным переходом*.)

Рассмотрим конкретный пример такого доказательства.

Пример 1.3. *Доказать, что для любого целого числа $n \geqslant 1$ сумма всех целых чисел от 1 до n равна* $\dfrac{n(n+1)}{2}$.

Шаг 1. При $n = 1$ указанная сумма равна 1. С другой стороны, и значение выражения $n(n+1)/2$ при $n = 1$ равно 1. Следовательно, мы располагаем основанием индукции.

Шаг 2. Предположим, что для некоторого целого числа $m \geqslant 1$ доказываемое утверждение истинно, т. е.

$$1 + 2 + \cdots + m = \frac{m(m+1)}{2}$$

.

Шаг 3. Покажем, что тогда наше утверждение истинно и для числа $m + 1$. Имеем

$$1 + 2 + \cdots + (m+1) = (1 + 2 + \cdots + m) + (m+1) =$$
$$\frac{m(m+1)}{2} + (m+1) = \frac{m(m+1) + 2(m+1)}{2} =$$
$$\frac{(m+1)(m+2)}{2} = \frac{(m+1)((m+1)+1)}{2}.$$

Таким образом, сумма всех целых чисел от 1 до $m + 1$ действительно совпадает со значением выражения $\dfrac{n(n+1)}{2}$ при $n = m + 1$, и индуктивный переход выполнен.

В силу принципа полной математической индукции сформулированное утверждение можно считать доказанным. $\square$

Разумеется, совсем не обязательно при проведении индуктивного доказательства настолько подробно расписывать каждый шаг. Рассмотрим еще один

Пример 1.4. *Доказать, что для всех натуральных чисел $n \geqslant 3$ выполнено неравенство $2^n > 2n + 1$.*

Так как $2^3 = 8$ и $2 \cdot 3 + 1 = 7$, при $n = 3$ наше утверждение истинно.

Предположим, что для некоторого натурального $m \geqslant 3$ неравенство $2^m > 2m + 1$ является истинным. Так как $2^{m+1} = 2 \cdot 2^m$, умножив на 2 обе части

неравенства $2^m > 2m + 1$, данного нам индуктивным предположением, получаем $2^{m+1} > 2(2m + 1)$.

Имеем далее $2(2m + 1) = (2(m + 1) + 1) + (2m - 1)$, и поскольку при $m \geqslant 3$ выполнено неравенство $2m - 1 > 0$, отсюда получаем $2(2m + 1) > 2(m + 1) + 1$. Таким образом, имеем $2^{m+1} > 2(m + 1) + 1$, и индуктивный переход выполнен. В силу принципа полной математической индукции наше утверждение доказано. □

Иногда бывает удобно индуктивное доказательство проводить в несколько иной форме. Эта форма индукции основана на утверждении, которое можно назвать *ослабленным принципом полной математической индукции* и которое формулируется следующим образом:

Предложение 1.7. *Пусть утверждение $P(n)$ зависит от параметра n, принимающего все натуральные значения, большие или равные некоторому натуральному числу k. Предположим, что*

(i) *Утверждение $P(k)$ является истинным.*

(ii) *Для любого натурального числа $m \geqslant k$ из того, что утверждение $P(x)$ является истинным для каждого числа x, удовлетворяющего неравенствам $k \leqslant x \leqslant m$, следует, что и утверждение $P(m + 1)$ является истинным.*

Тогда утверждение $P(n)$ является истинным для любого значения параметра $n \geqslant k$.

Предложение 1.7 можно вывести из предложения 1.6, доказав основанным на нем методом математической индукции утверждение $P'(n)$, означающее истинность $P(x)$ для всех целых чисел x таких, что $k \leqslant x \leqslant n$. □

Это предложение выглядит более слабым, чем предложение 1.6, так в формулировке пункта (ii) для заключения об истинности утверждения $P(m+1)$ разрешается использовать более сильное предположение. Тем не менее, обе формулировки принципа индукции равносильны, и мы сейчас же убедимся в этом, доказав, что из утверждения предложения 1.7 следует свойство 13), из которого, напомним, мы вывели исходный принцип индукции. Тем самым будет доказана также равносильность принципа индукции и свойства 13) равносильны.

(Последняя фраза предыдущего абзаца требует уточнения. А именно, при выводе свойства вполне упорядоченности множества положительных целых чисел из утверждения предложения 1.7 мы будем пользоваться (явно или неявно) и теми свойствами целых чисел, которые основаны на принятых нами аксиомах 1) – 12). Поэтому точная формулировка утверждения, выражаемого этой фразой, должна иметь следующий вид: система аксиом 1) – 13) равносильна системе, состоящей из аксиом 1) – 12) и принципа индукции, сформулированного в предложении 1.7.)

Итак, предположим, что некоторое подмножество A множества всех положительных целых чисел не имеет наименьшего элемента. Используя предложение 1.7, мы покажем, что тогда это множество должно быть пустым, доказав тем самым, что свойство 13) имеет место. Для этого договоримся, что $P(n)$ будет обозначать следующее утверждение: "натуральное число n не принадлежит множеству A".

Легко видеть, что $P(1)$ является истинным. Действительно, если бы число 1 входило бы в множество A, то оно явилось бы наименьшим элементом этого множе-

ства, так как в силу свойства 12) является наименьшим среди всех положительных целых чисел.

Предположим теперь, что для некоторого положительного числа m утверждение $P(x)$ является истинным для всех натуральных чисел x, не превосходящих числа m. Это означает, что из неравенства $x \leqslant m$ следует, что число x не входит в множество A. Покажем, что тогда и число $m+1$ не входит в множество A.

Пусть, напротив $m+1$ входит в A. Так как в множестве A нет наименьшего элемента, должно найтись натуральное число x, принадлежащее множеству A и удовлетворяющее неравенству $x < m+1$. Но тогда из свойства 12) следует, что $x \leqslant m$, и мы получаем противоречие с индуктивным предположением. Таким образом, доказана истинность утверждения $P(m+1)$, и индуктивный переход выполнен. Выводимость свойства 13) из ослабленного принципа индукции доказана. Отметим, что при этом мы продемонстрировали еще один способ индуктивного доказательства (основанный на предложении 1.7). $\square$

В ряде случаев для доказательства того, что некоторое утверждение $P(n)$ справедливо для всех натуральных чисел n, можно вместо индуктивного рассуждения воспользоваться *методом бесконечного спуска*, который придумал Пьер Ферма. Этот метод заключается в том, что истинность утверждения $P(n)$ считается установленной, если из предположения о том, что это утверждение ложно для некоторого натурального числа a, можно доказать, что существует натуральное число b, меньшее, чем a, для которого утверждение $P(n)$ также является ложным.

Для обоснования метода бесконечного спуска напомним, что *числовой последовательностью* называется функция $f(n)$, принимающая числовые значения и определенная либо на множестве всех натуральных чисел, либо на множестве всех тех натуральных чисел n, которые удовлетворяют неравенству $n \leqslant m$ (где m — некоторое фиксированное натуральное число). В первом случае последовательность $f(n)$ называется бесконечной, а во втором случае — конечной. Значения этой функции называются элементами последовательности, и для их обозначения вместо $f(n)$ используется символ a_n, а последовательность записывается либо в виде $a_1,\ a_2,\ a_3, \ldots$ (если она бесконечна), либо в виде $a_1,\ a_2,\ a_3, \ldots,\ a_m$ (если она конечна; число m называют числом элементов такой последовательности).

Бесконечная последовательность $a_1,\ a_2,\ a_3, \ldots$ называется *убывающей*, если для любого n выполняется неравенство $a_n > a_{n+1}$; конечная последовательность $a_1,\ a_2,\ a_3, \ldots,\ a_m$ называется убывающей, если это неравенство справедливо для всех $n = 1, 2, \ldots, m-1$. Метод бесконечного спуска основан на том факте, что бесконечных убывающих последовательностей натуральных чисел не существует. А именно, имеет место следующее

Предложение 1.8. *Если последовательность*

$$a_1,\ a_2,\ a_3, \ldots,\ a_m$$

натуральных чисел является убывающей, то $m \leqslant a_1$.

Доказательство проведем индукцией по числу $n = a_1$. Пусть $n = 1$. Так как 1 является наименьшим натуральным числом, натурального числа a_2 такого, что

$a_2 < a_1$, не существует. Следовательно, в этом случае $m = 1$, и наше утверждение справедливо. Предположим теперь, что $n > 1$ и что для любого натурального числа $k < n$ доказываемое утверждение является верным: количество элементов любой убывающей последовательности натуральных чисел, первый член которой равен k, не превосходит k. Покажем, что тогда для убывающей последовательности $a_1,\ a_2,\ a_3, \ldots,\ a_m$, у которой $a_1 = n$ справедливо неравенство $m \leqslant n$. Рассмотрим для этого последовательность $a_2,\ a_3, \ldots,\ a_m$, число элементов которой равно $m-1$. Так как число $k = a_2$ удовлетворяет неравенству $k < n$, по индуктивному предположению имеем $m-1 \leqslant k$, а так как $k+1 \leqslant n$, отсюда получаем $m \leqslant n$. Индуктивный переход выполнен, и предложение 1.8 доказано. $\square$

В заключение этого параграфа обсудим вопрос об обратимости операции умножения в кольце целых чисел, т. е. вопрос о существовании решения уравнения вида $ax = b$.

Известно, что если a и b — произвольные рациональные или действительные числа, причем $a \neq 0$, то указанное уравнение имеет единственное решение. Поэтому каждое из колец $\mathbb{Q}$ рациональных чисел и $\mathbb{R}$ действительных чисел является полем в смысле следующего общего определения: ненулевое кольцо K называется *полем*, если для любых элементов a и b этого кольца, где $a \neq 0$, уравнение $ax = b$ имеет в K хотя бы одно (и можно показать, что в точности одно) решение.

К определению поля можно подойти несколько иначе. Если кольцо K является полем, то для любого его ненулевого элемента a уравнение $ax = 1$ должно иметь решение в K, и потому существует такой элемент c, что $ac = 1$. Этот (однозначно определенный) элемент называют обратным к элементу a и обозначают через a^{-1}. Элемент a кольца K называют *обратимым*, если для него существует обратный элемент. Мы только что показали, что если кольцо K является полем, то каждый ненулевой элемент из K обратим. Легко видеть, что справедливо и обратное: если каждый ненулевой элемент кольца K обратим, то произвольное уравнение $ax = b$, где $a \neq 0$ имеет решение $x = ba^{-1}$, и потому кольцо K является полем. Таким образом, поле можно определить, как ненулевое кольцо, любой ненулевой элемент которого обратим.

Выше для произвольного элемента кольца было введено понятие степени с произвольным неотрицательным целым показателем. Для обратимых элементов можно ввести понятие степени и с отрицательным целым показателем. А именно, если a — обратимый элемент кольца K и n — отрицательное целое число, полагаем по определению $a^n = (a^{-1})^{-n}$ (значение выражения в правой части этого равенства имеет вполне определенный смысл, так как число $-n$ положительно). Таким образом, для обратимых элементов кольца можно говорить о степени с произвольным целым показателем. Из наших определений легко следует, что для произвольного обратимого элемента a кольца K и произвольных целых чисел m и n обычные свойства степени $a^{m+n} = a^m \cdot a^n$ и $(a^m)^n = a^{mn}$ остаются справедливыми. Кроме того, для любых обратимых элементов a и b кольца K и для любого целого числа m имеет место равенство $(ab)^m = a^m \cdot b^m$. Отметим еще, что определить разумным образом (т. е. так, чтобы выполнялись указанные свойства) степень с отрицательным целым показателем необратимого элемента кольца невозможно.

Из предыдущего следует, что если кольцо K является полем, мы можем го-

ворить о степени с произвольным целым показателем любого ненулевого элемента из K. Заметим также, что произвольное поле является целостным кольцом. Действительно, если для элементов a и b данного поля имеет место равенство $ab = 0$ и элемент a отличен от нуля, то после умножения обеих частей на a^{-1} наше равенство принимает вид $b = 0$.

Нам хорошо известно, что кольцо $\mathbb{Z}$ целых чисел полем не является, так как далеко не для любых целых чисел a и b решение уравнения $ax = b$ является целым числом. Теперь, когда у нас есть точное определение целых чисел, мы можем дать этому строгое обоснование.

Покажем, например, что уравнение $2x = 1$ не имеет целых решений. Пусть, напротив, существует такое целое число c, что $2c = 1$. Тогда $c \neq 0$, и потому (в силу условия 12)) $|c| \geqslant 1$. Умножив обе части этого неравенства на положительное число 2, получаем $2|c| \geqslant 2$, откуда ввиду того, что $2 > 1$, имеем $2|c| > 1$. С другой стороны, из равенства $2c = 1$ следует, что $2|c| = 1$. Таким образом, предположение о существовании целого решения рассматриваемого уравнения приводит к неравенству $1 > 1$, противоречащему антирефлексивности отношения порядка (аксиома 7)).

С помощью аналогичных рассуждений можно доказывать неразрешимость в кольце целых чисел и других уравнений рассматриваемого вида. Разумеется, речь здесь идет лишь о том, что мы располагаем принципиальной возможностью обосновать любое утверждение подобного типа, которое кажется нам интуитивно верным. При этом, как и в геометрии, совсем необязательно доводить рассуждение до ссылок на аксиомы, а можно использовать уже доказанные утверждения. Например, неразрешимость уравнения $2x = 3$ следует из предыдущего абзаца, стоит лишь заменить его равносильным уравнением $2(x - 1) = 1$.

Итак, как мы только что видели, операция умножения в кольце целых чисел необратима. Зато взамен мы получаем весьма содержательную и интересную теорию делимости, к изложению которой мы приступаем в следующем параграфе.

ЗАДАЧИ К ПАРАГРАФУ 1

1.1. Показать, что для любых элементов a и b произвольного кольца имеют место равенства $a^2 - b^2 = (a - b)(a + b)$, $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$ и $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$.

1.2. Показать, что для любых элементов a, b и c произвольного кольца имеет место равенство $(a + b + c)^2 = a^2 + b^2 + c^2 + 2ab + 2ac + 2bc$.

1.3. Показать, что для любых элементов a, b и c произвольного кольца имеет место равенство

$$a^3 + b^3 + c^3 = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc) + 3abc.$$

1.4. Показать, что для любых элементов a и b произвольного кольца и произвольного целого числа $n \geqslant 2$ имеет место равенство

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

1.5. Показать, что для любых элементов a и b произвольного кольца и произвольного целого числа $n \geqslant 1$ имеет место равенство

$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - a^{2n-3}b^3 + \cdots + a^2b^{2n-2} - ab^{2n-1} + b^{2n}).$$

1.6. Для произвольных целых чисел n и k, где $n \geqslant 1$ и $0 \leqslant k \leqslant n$ определим по индукции целые числа C_n^k следующим образом:

(i) при $n = 1$ полагаем $C_1^0 = C_1^1 = 1$;

(ii) если для некоторого $n \geqslant 1$ и всех k, $0 \leqslant k \leqslant n$, числа C_n^k уже определены, полагаем для $k = 0$ и $k = n+1$ $C_{n+1}^0 = C_{n+1}^{n+1} = 1$, а для $1 \leqslant k \leqslant n$ полагаем $C_{n+1}^k = C_n^{k-1} + C_n^k$.

а) Доказать, что для любых целых чисел n и k, где $n \geqslant 1$ и $1 \leqslant k \leqslant n$ выполнено равенство $C_n^k = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$. (Здесь $k!$ (читается k-факториал) обозначает произведение всех натуральных чисел от 1 до k.)

б) Доказать, что для любых элементов a и b произвольного кольца и произвольного целого числа $n \geqslant 1$ имеет место равенство

$$(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \cdots + C_n^{n-1}ab^{n-1} + C_n^n b^n.$$

(Это равенство называется формулой *бинома Ньютона*, а числа C_n^k называются биномиальными коэффициентами.)

1.7. Доказать, что для любых действительных чисел a и b выполнено неравенство $a^2 + ab + b^2 \geqslant 0$. При этом равенство имеет место тогда и только тогда, когда $a = b = 0$.

1.8. Доказать, что для любых действительных чисел a, b и c выполнено неравенство $a^2 + b^2 + c^2 \geqslant ab + ac + bc$. При этом равенство имеет место тогда и только тогда, когда $a = b = c$.

1.9. Доказать, что для любых действительных чисел a, b и c выполнено неравенство $a^2 + b^2 + c^2 + 3 \geqslant 2(a + b + c)$. При этом равенство имеет место тогда и только тогда, когда $a = b = c = 1$.

1.10. Доказать, что сумма квадратов первых n натуральных чисел совпадает с числом $\dfrac{n(n+1)(2n+1)}{6}$.

1.11. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \dfrac{n(2n-1)(2n+1)}{3}$.

1.12. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}\frac{n(n+1)}{2}.$$

1.13. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$.

1.14. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство $1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \dfrac{n(n+1)(n+2)}{3}$.

1.15. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство $1 \cdot 4 + 2 \cdot 7 + \cdots + n \cdot (3n+1) = n(n+1)^2$.

1.16. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n \cdot (n+1) \cdot (n+2) = \frac{n(n+1)(n+2)(n+3)}{4}.$$

1.17. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1) \cdot (2n+1)} = \frac{n}{(2n+1)}.$$

1.18. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство

$$\frac{1^2}{1 \cdot 3} + \frac{2^2}{3 \cdot 5} + \cdots + \frac{n^2}{(2n-1) \cdot (2n+1)} = \frac{n(n+1)}{2(2n+1)}.$$

1.19. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство

$$\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \cdots + \frac{1}{(3n-2) \cdot (3n+1)} = \frac{n}{(3n+1)}.$$

1.20. Доказать, что для любого натурального числа $n \geqslant 1$ выполняется равенство

$$\frac{1}{1 \cdot 5} + \frac{1}{5 \cdot 9} + \cdots + \frac{1}{(4n-3) \cdot (4n+1)} = \frac{n}{(4n+1)}.$$

1.21. Доказать, что для любого натурального числа $n > 1$ выполняется неравенство

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} > \frac{13}{24}.$$

1.22. Доказать, что для любого натурального числа $n > 1$ выполняется неравенство

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{3n+1} > 1.$$

1.23. Доказать, что для любого натурального числа $n > 1$ выполняется неравенство

$$\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}.$$

1.24. Доказать, что для любого натурального числа $n > 4$ выполняется неравенство $2^n > n^2$.

1.25. Доказать, что для любого натурального числа $n \geqslant 10$ выполняется неравенство $2^n > n^3$.

1.26. Доказать, что для любого натурального числа $n > 1$ выполняется неравенство $\left(2 - \dfrac{1}{n}\right)^n > n$.

1.27. Доказать, что для любого натурального числа $n > 1$ выполняется неравенство $\dfrac{1}{2^2} + \dfrac{1}{3^2} + \cdots + \dfrac{1}{n^2} < 1$.

1.28. Доказать, что для любого натурального числа $n > 1$ выполняется неравенство $\dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \cdots + \dfrac{1}{\sqrt{n}} > \sqrt{n}$.

1.29. Доказать, что для любого натурального числа $n > 2$ выполняется неравенство $(n!)^2 > n^n$.

1.30. Доказать, что произведение двух чисел, каждое из которых является суммой квадратов двух целых чисел, также является суммой квадратов двух целых чисел.

1.31. Доказать, что квадрат суммы квадратов двух ненулевых различных целых чисел также является суммой квадратов двух ненулевых целых чисел.

1.32. Пусть целые числа a и b таковы, что $ab = 1$. Доказать, что либо $a = b = 1$, либо $a = b = -1$.

1.33. Найти все целые числа a, для которых существует целое число x, удовлетворяющее равенству $(a + 1)x = a$.

1.34. Найти все пары последовательных чисел, каждое из которых является квадратом целого числа.

1.35. Доказать, что произведение четырех последовательных целых чисел, сложенное с единицей, является квадратом некоторого целого числа.

§ 2. Определение и основные свойства отношения делимости целых чисел

Начнем сразу с определения отношения делимости целых чисел. Будем говорить, что *целое число a делит целое число b* и символически записывать это в виде $a \mid b$, если существует такое целое число c, что выполнено равенство $b = ac$. В этом случае мы будем говорить также, что *число a является делителем числа b*, или что *число b делится на a*, или что *число b кратно числу a*.

Например, $2 \mid 6$, так как $6 = 2 \cdot 3$. С другой стороны, в конце предыдущего параграфа фактически показано, что число 2 не является делителем числа 1, т. е. $2 \nmid 1$.

Простейшие свойства отношения делимости, вытекающие непосредственно из определения, собраны в следующем предложении.

Предложение 2.1. *Отношение делимости целых чисел обладает следующими свойствами:*

1) *Каждое целое число a является делителем самого себя, т. е. $a \mid a$.*

2) *Если $a \mid b$ и $b \mid c$, то $a \mid c$.*

3) *Если $a \mid b$ и $a \mid c$, то $a \mid (b + c)$.*

4) *Если $a \mid b$, то $a \mid (bc)$ для любого целого числа c.*

5) *Если $ac \mid bc$ и $c \neq 0$, то $a \mid b$.*

6) *Число 0 делится на любое целое число.*

7) *Произвольное целое число a делится на 0 тогда и только тогда, когда $a = 0$.*

8) *Любое целое число делится на 1.*

9) *Если $a \mid b$ и $b \neq 0$, то $|a| \leqslant |b|$.*

10) *Целые числа a и b одновременно делятся друг на друга тогда и только тогда, когда $|a| = |b|$.*

11) *Произвольное целое число a является делителем 1 тогда и только тогда, когда $|a| = 1$.*

Справедливость некоторых из перечисленных свойств почти очевидна. В самом деле, свойство 1) (равно, как и свойство 8)) вытекает из равенства $a = a \cdot 1$. Если $a \mid b$ и $b \mid c$, то, в соответствии с определением, для некоторых целых чисел x и y должны выполняться равенства $b = ax$ и $c = by$. Так как тогда имеет место равенство $c = a(xy)$ (и число xy целое), имеем $a \mid c$, и свойство 2) доказано. Свойства 3) и 4) доказываются аналогично.

Докажем свойство 5). Если $ac \mid bc$, то для некоторого целого числа x имеем $bc = (ac)x$, откуда после сокращения на c ($\neq 0$) получаем $b = ax$, т. е. $a \mid b$.

Свойство 6) следует непосредственно из равенства $0 = a \cdot 0$. Если целое число a делится на 0, то для некоторого целого числа x мы должны иметь $a = 0 \cdot x$, откуда следует, что $a = 0$. Обратное утверждение содержится в свойстве 6), и, таким образом, доказано и свойство 7).

(Формулировка свойства 7) часто воспринимается с недоумением, аргументированным тем хорошо усвоенным правилом, что "на нуль делить нельзя". Но в этом правиле речь идет об операции деления числа a на число b, результатом которой должно быть такое однозначно определяемое число c, что $a = bc$. Если

$b = 0$, то при $a \neq 0$ такого числа не существует, а при $a = 0$ в качестве c может быть взято произвольное число, т. е. потеряна однозначность результата операции. Отсюда — вышеприведенное правило. Мы же рассматриваем отношение между двумя числами; оно может быть либо истинным, либо ложным, и в свойствах 6) и 7) сформулированы условия его истинности в случае, когда одно из этих чисел равно 0.)

Докажем теперь свойство 9). Пусть $a \mid b$, т. е. $b = ax$ для некоторого целого числа x. Если $b \neq 0$, то и $x \neq 0$, и потому $|x| \geqslant 1$. Следовательно, $|b| = |a| \cdot |x| \geqslant |a|$, что и требовалось доказать.

Из равенства $|a| = |b|$ в свойстве 10) следует, что $a = \pm b$, и потому числа a и b делятся друг на друга. Обратно, если каждое из этих чисел делится на другое и одно из них равно 0, то в силу свойства 7) и другое должно быть равным 0, так что равенство $|a| = |b|$ в этом случае имеет место. Если же оба они отличны от 0, то из свойства 9) следуют неравенства $|a| \leqslant |b|$ и $|b| \leqslant |a|$, откуда снова имеем $|a| = |b|$, и свойство 10) доказано. Наконец, свойство 11) следует из свойств 8) и 10). $\square$

Опираясь лишь на перечисленные в предложении 2.1 свойства, можно уже решать многие задачи о делимости целых чисел. Решим, например, следующую задачу:

Пример 2.1. *Найти все такие целые числа a, для которых число $a^2 + 1$ делится на число $a + 1$.*

Так как $a^2 + 1 = (a^2 - 1) + 2 = (a + 1)(a - 1) + 2$, из свойства 3) предложения 2.1 следует, что $(a + 1) \mid (a^2 + 1)$ тогда и только тогда, когда $(a + 1) \mid 2$. В свою очередь, из свойства 9) следует, что если $(a + 1) \mid 2$, то $|a + 1| \leqslant 2$, и так как $a + 1 \neq 0$, то либо $|a + 1| = 1$, либо $|a + 1| = 2$. Значит, если $(a + 1) \mid (a^2 + 1)$, то либо $a + 1 = \pm 1$, либо $a + 1 = \pm 2$, и потому a совпадает с одним из четырех чисел $-3, -2, 0, 1$. Непосредственная проверка показывает, что при каждом из этих значений a требуемая делимость действительно имеет место. $\square$

Отметим также, что из предложения 2.1 выводится и следующее часто применяемое свойство:

Если сумма двух чисел b и c делится на число a и одно из слагаемых делится на это число, то и другое слагаемое делится на число a.

В самом деле, если $a \mid (b + c)$ и $a \mid b$, то ввиду свойства 4) число a является делителем числа $-b = b \cdot (-1)$, и потому в силу свойства 3) a является делителем числа $c = (-b) + (b + c)$. $\square$

Более глубокие свойства делимости целых чисел основаны на следующем важном утверждении, которое называется *теоремой о делении с остатком.*

Теорема 2.1. *Для любых целых чисел a и b, где $b > 0$, существует единственная пара целых чисел q и r, для которых выполнено равенство*

$$a = bq + r \tag{1}$$

и двойное неравенство $0 \leqslant r < b$.

Прежде, чем перейти к доказательству этой теоремы, проясним ее утверждения и договоримся о терминологии.

Нетрудно видеть, что для данных фиксированных чисел a и b существует много различных пар чисел q и r, для которых выполняется равенство вида (1). Например, если $a = 7$ и $b = 3$, то можно записать, что $7 = 3{\cdot}1{+}4$, или $7 = 3{\cdot}(-2){+}13$, или $7 = 3 \cdot 2 + 1$, или $7 = 3 \cdot 5 + (-8)$ и т. д. Но лишь в одной из этих пар (а именно, 2 и 1) число r удовлетворяет и неравенству из формулировки теоремы 2.1. Смысл теоремы 2.1 и состоит в том, что среди бесконечного множества представлений данного числа a в виде (1) (при фиксированном числе b) обязательно найдется представление, в котором число r удовлетворяет указанным неравенствам, и что такое представление является единственным. В этом представлении число r называется *остатком при делении a на b*, а q — *неполным частным при делении a на b*.

Доказательство теоремы 2.1 начнем с доказательства ее утверждения о единственности пары чисел q и r, удовлетворяющих ее формулировке.

Предположим, что существуют две пары целых чисел q_1, r_1 и q_2, r_2, удовлетворяющих условиям теоремы, т. е. выполнены равенства

$$a = bq_1 + r_1 \qquad \text{и} \qquad a = bq_2 + r_2$$

и неравенства

$$0 \leqslant r_1 < b \qquad \text{и} \qquad 0 \leqslant r_2 < b.$$

Вычитая почленно из первого равенства второе, после очевидных преобразований получим $b(q_1 - q_2) = r_2 - r_1$. Это означает, что число b является делителем числа $r_2 - r_1$, и потому если предположить, что $r_2 - r_1 \neq 0$, из пункта 8) предложения 2.1 будет следовать, что $b \leqslant |r_2 - r_1|$. Но этого не может быть, поскольку складывая почленно неравенства $0 \leqslant r_2 < b$ и $-b < -r_1 \leqslant 0$, получим неравенство $-b < r_2 - r_1 < b$, которое в силу предложения 1.4 равносильно неравенству $|r_2 - r_1| < b$. Таким образом, предположение о том, что $r_2 - r_1 \neq 0$, приводит к противоречию, и потому имеет место равенство $r_1 = r_2$. Теперь равенство $b(q_1 - q_2) = r_2 - r_1$ принимает вид $b(q_1 - q_2) = 0$, и так как $b > 0$, мы заключаем, что $q_1 - q_2 = 0$, т. е. $q_1 = q_2$.

Итак, мы доказали, что может существовать не более одной пары целых чисел q и r, удовлетворяющих условиям теоремы. Покажем теперь, что хотя бы одна такая пара существует.

Обозначим через A множество всех неотрицательных целых чисел, имеющих вид $a - bx$, где x — целое число. Заметим, что это множество непусто. В самом деле, если число a неотрицательно, то оно входит в множество A, поскольку может быть записано в виде $a - bx$ при $x = 0$. Если же $a < 0$, то в силу того, что $b \geqslant 1$, число $a(1 - b)$ неотрицательно. Так как $a(1 - b) = a - ba$, оно имеет требуемый вид (при $x = a$) и потому входит в A. Заметим теперь, что в множестве A есть наименьший элемент. Действительно, если число 0 принадлежит этому множеству, то оно и будет, очевидно, его наименьшим элементом. В противном случае A состоит лишь из положительных целых чисел, и существование в нем наименьшего элемента следует из аксиомы 13).

Обозначим наименьшее число, входящее в множество A, через r. Тогда, по определению множества A, $r \geqslant 0$ и $r = a - bq$ для некоторого целого числа q. Утверждается, что числа r и q искомые. Так как они удовлетворяют равенству (1), то для этого нам остается доказать лишь, что $r < b$. Рассуждая от противного, предположим, что $r \geqslant b$. Тогда $r - b \geqslant 0$, и так как $r - b = (a - bq) - b = a - b(q + 1)$, число $r - b$ следует считать элементом множества A. Но поскольку из условия $b > 0$ следует, что $r - b < r$, это противоречит выбору числа r. Таким образом, $r < b$, и теорема доказана. $\square$

Отметим важное следствие этой теоремы, которое, на первый взгляд, звучит как тавтология, но в действительности является нетривиальным утверждением, основанным на свойстве единственности неполного частного и остатка.

Следствие. *Целое число $b > 0$ является делителем целого числа a тогда и только тогда, когда остаток от деления a на b равен нулю.*

В самом деле, если в равенстве (1) число r равно 0, то это равенство принимает вид $a = bq$, а это и означает, что $b \mid a$. Обратно, если $b \mid a$, то для некоторого целого числа c выполняется равенство $a = bc$. Тогда числа $q = c$ и $r = 0$ удовлетворяют требованиям теоремы, и потому остаток от деления a на b равен нулю. $\square$

Из теоремы о делении с остатком (при $b = 2$) следует, что произвольное целое число a может быть однозначно записано в виде $a = 2n + r$, где n — некоторое целое число, а r равно либо 0, либо 1. Напомним, что целое число называется *четным*, если оно делится на 2, и *нечетным* в противном случае. В силу вышеприведенного следствия из теоремы о делении с остатком целое число a является четным тогда и только тогда, когда оно представимо в виде $a = 2n$, и нечетным — тогда и только тогда, когда оно представимо в виде $a = 2n + 1$ (где число n целое). Таким образом, справедливость этих хорошо известных утверждений основана на теореме о делении с остатком (впрочем, первое из них следует уже непосредственно из определения отношения делимости).

Аналогично, для произвольного целого числа a существует единственное представление одного из трех видов $a = 3n$, $a = 3n + 1$ или $a = 3n + 2$, где n — некоторое целое число. При делении целого числа на 4 может получиться уже четыре остатка и потому имеются четыре вида записи произвольного целого числа и т. д. Разделение на случаи в зависимости от значения остатка от деления целого числа на данное число $b > 0$ является распространенным методом решения задач на делимость. Решим, например, следующую задачу:

Пример 2.2. *Доказать, что для любых целых чисел a и b число $a^2 + b^2$ делится на 3 тогда и только тогда, когда оба числа a и b делятся на 3.*

В одну сторону это утверждение очевидно: если $3 \mid a$ и $3 \mid b$, то $3 \mid a^2$ и $3 \mid b^2$, и потому $3 \mid (a^2 + b^2)$.

С другой стороны, если число a не делится на 3, то либо $a = 3n + 1$, либо $a = 3n + 2$ для некоторого целого числа n. В первом случае

$$a^2 = 3(3n^2 + 2n) + 1,$$

а во втором

$$a^2 = 3(3n^2 + 4n + 1) + 1.$$

Таким образом, квадрат целого числа, не делящегося на 3, при делении на три дает в остатке 1. Следовательно, если одно из чисел a или b не делится на 3, а другое делится, то число $a^2 + b^2$ записывается в виде $3q + 1$ для некоторого целого числа q и потому при делении на 3 дает в остатке 1, а если оба числа a и b не делятся на 3, то число $a^2 + b^2$ записывается в виде $3q + 2$ и потому при делении на 3 дает в остатке 2. Значит, если $3 \mid (a^2 + b^2)$, то $3 \mid a$ и $3 \mid b$. $\square$

Перейдем теперь к введению следующего важного понятия. Интуитивно ясно (и можно строго доказать), что множество всех делителей целого числа $a \neq 0$ является конечным. Поэтому конечным является и множество всех общих делителей двух ненулевых целых чисел a и b, и так как в каждом конечном множестве целых чисел есть наибольший элемент, среди общих делителей чисел a и b, есть наибольшее число. Это число мы и будем называть *наибольшим общим делителем чисел a и b*. Таким образом, мы принимаем следующее определение:

Наибольшим общим делителем двух ненулевых целых чисел называется наибольшее число из всех общих делителей этих чисел.

(Здесь следует заметить, что если $a = 0$ и $b = 0$, то каждое целое число является общим делителем чисел a и b, и потому наибольшего общего делителя этих чисел не существует. С другой стороны, если, скажем, $a \neq 0$ и $b = 0$, то $a \mid b$ и потому наибольшим среди общих делителей чисел a и b является число $|a|$. Тем не менее, чтобы избежать в дальнейшем дополнительных оговорок, мы будем считать, что понятие наибольшего общего делителя имеет смысл лишь для ненулевых целых чисел a и b.)

Тот факт, что число d является наибольшим общим делителем чисел a и b, мы будем записывать в виде $d = (a, b)$. Если $d = 1$, числа a и b называются *взаимно простыми*. Заметим еще, что в силу принятого нами определения наибольший общий делитель двух целых чисел всегда является числом положительным.

В следующей теореме устанавливается одно из основных свойств наибольшего общего делителя двух целых чисел. Следует отметить, что из ее доказательства можно извлечь еще одно обоснование существования наибольшего общего делителя двух любых ненулевых целых чисел.

Теорема 2.2. *Пусть a и b — отличные от нуля целые числа и $d = (a, b)$ — наибольший общий делитель чисел a и b. Тогда существуют целые числа u и v такие, что*

$$d = au + bv. \tag{2}$$

Доказательство. Обозначим через M множество всевозможных чисел вида $ax + by$, где x и y — целые числа. Заметим, что поскольку числа a и b могут быть записаны в виде $a = a \cdot 1 + b \cdot 0$ и $b = a \cdot 0 + b \cdot 1$, то они входят в множество M, и потому, в частности, это множество содержит ненулевые числа. Если целое число c входит в множество M и потому $c = ax + by$ для подходящих x и y, то и число $-c = a(-x) + b(-y)$ также входит в M. Следовательно, множество положительных целых чисел, принадлежащих множеству M, непусто и потому обладает наименьшим элементом.

Пусть $c = au + bv$ — наименьшее из положительных целых чисел, принадлежащих множеству M. Мы покажем, что $c = d$ (и утверждение теоремы, тем самым, будет доказано). Для этого докажем сначала, что c является общим делителем чисел a и b.

Разделим a на c с остатком, т. е. в соответствии с теоремой 2.1 найдем целые числа q и r такие, что $a = cq + r$ и $0 \leqslant r < c$. Тогда число r может быть записано в виде

$$r = a - cq = a - (au + bv)q = a(1 - uq) + b(-vq)$$

и потому принадлежит множеству M. Так как $r < c$ и число c является наименьшим из положительных чисел, принадлежащих множеству M, отсюда следует, что число r не может быть положительным, т. е. $r \leqslant 0$. Вместе с неравенством $0 \leqslant r$ это дает $r = 0$. Следовательно, $c \,|\, a$, и аналогично доказывается, что $c \,|\, b$.

Таким образом, число c действительно является общим делителем чисел a и b, и потому в силу определения наибольшего общего делителя должно выполняться неравенство $c \leqslant d$. С другой стороны, поскольку число d является общим делителем чисел a и b, то оба слагаемых в правой части равенства $c = au + bv$ делятся на d и потому $d \,|\, c$. Поэтому имеет место и неравенство $d \leqslant c$. (Здесь использовались свойства отношения делимости, перечисленные в предложении 2.1.) Следовательно, $c = d$, и теорема доказана. $\square$

Из теоремы 2.2 выводится ряд важных свойств отношения делимости целых чисел и связанных с ним понятий. Без знания этих свойств невозможно получить удовлетворительное решение практически каждой задачи о целых числах. Отметим, прежде всего,

Следствие 1. *Пусть положительное целое число d является общим делителем целых чисел a и b. Число d является наибольшим общим делителем этих чисел тогда и только тогда, когда произвольный общий делитель чисел a и b является делителем числа d.*

В самом деле, если произвольный общий делитель c чисел a и b является делителем числа d, то в силу предложения 2.1 $|c| \leqslant d$ и так как $c \leqslant |c|$, получаем $c \leqslant d$, так что в этом случае число d действительно является наибольшим среди общих делителей чисел a и b.

Обратно, если d — наибольший общий делитель чисел a и b, то по теореме 2.2 для подходящих целых чисел u и v выполняется равенство $d = au + bv$, делающее утверждение о том, что произвольный общий делитель чисел a и b является делителем d, очевидным. $\square$

Еще один критерий того, когда общий делитель двух целых чисел является их наибольшим общим делителем, дает

Следствие 2. *Пусть положительное целое число d является общим делителем целых чисел a и b и пусть $a = da_1$ и $b = db_1$ для подходящих целых чисел a_1 и b_1. Число d является наибольшим общим делителем чисел a и b тогда и только тогда, когда числа a_1 и b_1 взаимно просты.*

Для доказательства этого следствия предположим сначала, что $d = (a, b)$. Тогда в соответствии с теоремой 2.2 для некоторых целых чисел u и v должно

выполняться равенство $d = au + bv$, переписав которое в виде $d = (da_1)u + (db_1)v$ и сократив обе части на d, приходим к равенству $a_1u + b_1v = 1$. Теперь очевидно, что произвольный общий делитель чисел a_1 и b_1 является делителем числа 1, что и означает взаимную простоту этих чисел.

Обратно, если числа a_1 и b_1 являются взаимно простыми, т. е. их наибольший общий делитель равен 1, то для подходящих целых чисел u и v должно выполняться равенство $a_1u + b_1v = 1$. Умножив обе части этого равенства на число d, получаем $au + bv = d$, откуда видно, что произвольный общий делитель чисел a и b является делителем и числа d. Из следствия 1 вытекает теперь, что $d = (a, b)$. □

Свойство 4) из предложения 2.1 утверждает, что произведение двух чисел делится на третье, если хотя бы один из сомножителей делится на это третье число. Как показывают простые примеры (скажем, $6 | 3 \cdot 4$), обратное утверждение, вообще говоря, неверно. Достаточное условие его справедливости дает

Следствие 3. *Если целое число a является делителем произведения двух целых чисел b и c и если числа a и b взаимно просты, то число a является делителем числа c.*

В самом деле, так как числа a и b являются взаимно простыми, то для подходящих целых чисел u и v выполнено равенство $au + bv = 1$. Умножая обе части его на число c, приходим к равенству $a(uc) + (bc)v = c$, оба слагаемых левой части которого делятся на a. Отсюда $a | c$, что и требовалось доказать. □

Простые примеры показывают, что произведение двух делителей некоторого целого числа c не обязательно будет делителем этого числа: число 12 делится и на 6, и на 4, но не делится на их произведение. В следующем утверждении содержится достаточное условие для того, чтобы соответствующее заключение оказалось справедливым.

Следствие 4. *Если каждое из двух целых чисел a и b является делителем целого числа c и числа a и b взаимно просты, то и произведение ab этих чисел является делителем числа c.*

Действительно, поскольку $b \mid c$, то $c = bx$ для некоторого целого числа x. Таким образом, $a | bx$, и поскольку $(a, b) = 1$, то из предыдущего следствия имеем $a | x$, т. е. $x = ay$ для некоторого целого числа y. Поэтому равенство $c = bx$ может быть переписано в виде $c = (ab)y$, что и делает утверждение $(ab) | c$ очевидным. □

Это следствие оказывается весьма полезным при решении многих задач о делимости целых чисел.

Пример 2.3. *Доказать, что число вида $a(a + 1)(2a + 1)$ при любом целом a делится на 6.*

Так как число 6 является произведением двух взаимно простых чисел 2 и 3, то ввиду следствия 4 достаточно показать, что указанное число делится на 2 и делится на 3.

Докажем сначала, что число $a(a+1)(2a+1)$ при любом целом a делится на 2. Это очевидно (ввиду свойства 4) предложения 2.1), если число a является четным.

В противном случае, если $a = 2n + 1$, то второй сомножитель $a + 1 = 2n + 2$ нашего числа является четным, и доказываемое утверждение снова очевидно.

Теперь покажем, что число $a(a + 1)(2a + 1)$ при любом целом a делится на 3. Для этого рассмотрим отдельно три случая в зависимости от величины остатка от деления числа a на 3. Если $a = 3n$, то первый сомножитель данного числа делится на 3; если $a = 3n + 1$, то его третий сомножитель $2a + 1 = 6n + 3$ делится на 3; если $a = 3n + 2$, то второй сомножитель $a + 1 = 3n + 3$ делится на 3. $\square$

Рассмотрим еще несколько задач, решение которых основано на полученных здесь свойствах делимости целых чисел.

Пример 2.4. *Доказать, что если целое число a взаимно просто с каждым из целых чисел b и c, то a взаимно просто и с их произведением bc. Доказать также, что если $(a, b) = 1$, то для любого целого числа $n \geqslant 1$ $(a, b^n) = 1$.*

Так как $(a, b) = 1$ и $(a, c) = 1$, то для некоторых целых чисел u, v, x и y имеют место равенства $au + bv = 1$ и $ax + cy = 1$. Умножив обе части первого из них на c, получаем $c = auc + bvc$. Подставив это выражение числа c во второе равенство, имеем $ax + (auc + bvc)y = 1$, т. е. $a(x + ucy) + (bc)vy = 1$. Теперь очевидно, что единственным положительным общим делителем чисел a и bc является 1, так что $(a, bc) = 1$.

Второе утверждение выводится из первого методом математической индукции. При $n = 1$ оно тривиально. Если для некоторого числа $n \geqslant 1$ утверждение $(a, b^n) = 1$ справедливо, то поскольку $b^{n+1} = b \cdot b^n$, справедливость утверждения $(a, b^{n+1}) = 1$ следует из первой части задачи. $\square$

Пример 2.5. *Доказать, что если целые числа a и b взаимно просты, то их сумма $a + b$ и произведение ab также являются взаимно простыми числами.*

Пусть, напротив, у чисел $a + b$ и ab существует общий делитель $t > 1$. Тогда t будет делителем числа $a(a + b) = a^2 + ab$, а потому — и делителем числа a^2. Аналогично, t является делителем числа $(a + b)b = ab + b^2$, а потому — и делителем числа b^2. Таким образом, t является общим делителем чисел a^2 и b^2. С другой стороны, двукратное применение к взаимно простым числам a и b второго утверждения задачи из примера 2.4 дает $(a^2, b^2) = 1$. Полученное противоречие и доказывает наше утверждение. $\square$

Пример 2.6. *Пусть произведение двух положительных целых чисел a и b является квадратом некоторого целого числа. Доказать, что если $(a, b) = 1$, то каждое из чисел a и b также является квадратом подходящего целого числа.*

Прежде, чем приступить к решению этой задачи, сделаем два замечания. Первое состоит в том, что несмотря на то, что в формулировке утверждаемого ею свойства нет явного упоминания об отношении делимости, ее решение основано на свойствах этого отношения. Во-вторых, следует обратить внимание на то, что без предположения о взаимной простоте чисел a и b утверждение задачи может не иметь места (например, при $a = 3$ и $b = 12$).

Итак, пусть $(a, b) = 1$ и пусть для некоторого целого числа c имеет место равенство $ab = c^2$. Обозначим через d наибольший общий делитель чисел a и c.

Тогда для некоторых целых чисел a_1 и b_1 выполнены равенства $a = a_1 d$ и $c = c_1 d$, причем ввиду следствия 2 к теореме 2.2 имеем $(a_1, c_1) = 1$. Равенство $ab = c^2$ может теперь быть записано в виде $a_1 db = c_1^2 d^2$, откуда после сокращения на d получаем $a_1 b = c_1^2 d$. Это означает, в частности, что $d \,|\, (a_1 b)$. Из того, что числа a и b взаимно просты и $d \,|\, a$, очевидно следует, что $(d, b) = 1$. Поэтому (см. следствие 3) $d \,|\, a_1$. Записывая $a_1 = a_2 d$ для подходящего целого числа a_2, из равенства $a_1 b = c_1^2 d$ получаем $a_2 b = c_1^2$, и потому $a_2 \mid c_1^2$. Следовательно, $(a_2, c_1^2) = a_2$. Но так как числа a_1 и c_1 взаимно просты и $a_2 \mid a_1$, имеем $(a_2, c_1) = 1$, откуда ввиду второго утверждения примера 2.4 заключаем, что $(a_2, c_1^2) = 1$. Следовательно, $a_2 = 1$, и из равенства $a_2 b = c_1^2$ получаем $b = c_1^2$. Кроме того, $a_1 = d$, и потому $a = d^2$. $\square$

Выше было введено понятие наибольшего общего делителя двух целых чисел. Аналогичным образом можно определить наибольший общий делитель трех ненулевых целых чисел a, b и c, как наибольшее число среди всех общих делителей этих чисел. Точно так же вводится наибольший общий делитель четырех, пяти и, вообще, произвольной конечной последовательности ненулевых целых чисел. Для обозначения того факта, что число d является наибольшим общим делителем чисел $a_1, a_2, \ldots, a_n$, мы снова будем использовать запись $d = (a_1, a_2, \ldots, a_n)$.

Покажем, что и в этом, более общем случае справедливо утверждение следствия 1 из теоремы 2.2:

Произвольный общий делитель любых ненулевых целых чисел $a_1, a_2, \ldots, a_n$ $(n \geqslant 2)$ является делителем их наибольшего общего делителя.

Доказательство этого факта проведем индукцией по n. При $n = 2$ это — утверждение только что упомянутого следствия. Предположим, что $n \geqslant 3$, и введем дополнительные обозначения, полагая $d = (a_1, a_2, \ldots, a_n)$, $d' = (a_1, a_2, \ldots, a_{n-1})$ и $d'' = (d', a_n)$. Если t — произвольный общий делитель чисел $a_1, a_2, \ldots, a_n$, то t является общим делителем чисел $a_1, a_2, \ldots, a_{n-1}$, и в силу индуктивного предположения $t \,|\, d'$. Таким образом, t является общим делителем двух чисел d' и a_n, а потому и делителем числа d''.

Итак, мы показали, что каждый общий делитель чисел $a_1, a_2, \ldots, a_n$ является делителем числа d''. Покажем теперь, что $d = d''$. Так как число d является общим делителем чисел $a_1, a_2, \ldots, a_n$, имеем $d \,|\, d''$ и потому $d \leqslant d''$. С другой стороны, число d'' является общим делителем чисел $a_1, a_2, \ldots, a_n$, так как оно является делителем числа a_n и общего делителя d' чисел $a_1, a_2, \ldots, a_{n-1}$. Следовательно, $d'' \leqslant d$, откуда с учетом предыдущего неравенства и следует, что $d = d''$. Этим завершен индуктивный шаг, и наше утверждение доказано. $\square$

Отметим, что попутно мы установили справедливость и следующего полезного утверждения:

Для любого $n \geqslant 3$ и любых ненулевых целых чисел $a_1, a_2, \ldots, a_n$ наибольший общий делитель этих чисел совпадает с наибольшим общим делителем наибольшего общего делителя чисел $a_1, a_2, \ldots, a_{n-1}$ и числа a_n, т. е.

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n). \tag{3}$$

Равенство (3) позволяет проводить индуктивные рассуждения для распространения на общий случай и многих других свойств наибольшего общего делителя двух целых чисел. Докажем, например, соответствующее обобщение теоремы 2.2:

Предложение 2.2. *Пусть* $a_1, a_2, \ldots, a_n$ $(n \geqslant 2)$ *— отличные от нуля целые числа и* $d = (a_1, a_2, \ldots, a_n)$. *Тогда существуют целые числа* $u_1, u_2, \ldots, u_n$ *такие, что*

$$d = a_1u_1 + a_2u_2 + \cdots + a_nu_n. \tag{4}$$

При $n = 2$ доказываемое утверждение совпадает с утверждением теоремы 2.2. Пусть $n > 2$ и пусть $d' = (a_1, a_2, \ldots, a_{n-1})$. Тогда ввиду (3) имеем $d = (d', a_n)$. По теореме 2.2 существуют такие целые числа u и v, что выполнено равенство

$$d = d'u + a_nv.$$

Кроме того, в соответствии с индуктивным предположением для подходящих целых чисел $v_1, v_2, \ldots, v_{n-1}$ имеет место равенство

$$d' = a_1v_1 + a_2v_2 + \cdots + a_{n-1}v_{n-1}.$$

Подставив в первое равенство выражение числа d' из второго, получаем

$$d = (a_1v_1 + a_2v_2 + \cdots + a_{n-1}v_{n-1})u + a_nv = a_1u_1 + a_2u_2 + \cdots + a_nu_n,$$

где $u_i = v_iu$ при $1 \leqslant i \leqslant n-1$ и $u_n = v$. $\square$

Введем теперь еще одно понятие. Если каждое из чисел a и b является делителем числа c, то c будем называть *общим кратным* чисел a и b. Если числа a и b отличны от нуля, то у них есть ненулевое общее кратное (например, ab), а потому — и положительное общее кратное (например, $|ab|$). *Наименьшим общим кратным* чисел a и b называется наименьшее из положительных общих кратных этих чисел.

Предыдущее рассуждение показывает, что у любых двух ненулевых целых чисел существует наименьшее общее кратное. Тот факт, что число c является наименьшим общим кратным чисел a и b символически будем записывать в виде $c = [a, b]$. Таким образом, запись $c = [a, b]$ означает, что $c > 0$, $a \mid c$, $b \mid c$ и для любого целого числа $x > 0$ из того, что $a \mid x$ и $b \mid x$, следует неравенство $x \geqslant c$. Подчеркнем еще раз, что понятие наименьшего общего кратного определено нами лишь для ненулевых чисел a и b.

Докажем два важных свойства наименьшего общего кратного целых чисел.

Предложение 2.3. *Наименьшее общее кратное двух целых чисел является делителем любого другого общего кратного этих чисел.*

Доказательство. Пусть a и b — целые числа и $k = [a, b]$ — их наименьшее общее кратное. Пусть еще c — произвольное общее кратное чисел a и b, т. е. $a \mid c$ и $b \mid c$. Покажем, что $k \mid c$. Воспользуемся для этого уже встречавшимся нам весьма распространенным способом доказательства делимости одного целого числа на другое: разделим c на k с остатком, а затем попытаемся показать, что этот остаток равен нулю.

В соответствии с теоремой 2.1 найдем целые числа q и r такие, что $c = kq + r$ и $0 \leqslant r < k$. Так как оба слагаемых правой части равенства $r = c - kq$ делятся на a, имеем $a \mid r$. Аналогично $b \mid r$, так что число r является общим кратным чисел a и b. Так как $r < k$, то из определения наименьшего общего кратного следует, что r не может быть положительным числом. Вместе с неравенством $0 \leqslant r$ это и означает, что $r = 0$. Таким образом, $k \mid c$, что и требовалось доказать. $\square$

Предложение 2.4. *Для любых положительных целых чисел a и b имеет место равенство $(a,b)\cdot[a,b]=ab$.*

Доказательство. Снова введем обозначение $k=[a,b]$. Так как произведение ab чисел a и b является общим кратным этих чисел, из предложения 2.3 следует, что $ab=kd$ для некоторого (положительного) числа d. Покажем, что d является наибольшим общим делителем чисел a и b.

Так как числа a и b являются делителями числа k, для подходящих целых чисел x и y должны выполняться равенства $k=ax$ и $k=by$. Подставляя эти выражения числа k в равенство $ab=kd$, после сокращений получаем $b=dx$ и $a=dy$, так что число d является общим делителем чисел a и b. Ввиду следствия 2 к теореме 2.2 остается доказать, что числа x и y взаимно просты. Для этого предположим, что положительное число t является общим делителем чисел x и y, т. е. для некоторых целых чисел x_1 и y_1 выполнены равенства $x=tx_1$ и $y=ty_1$. Поскольку тогда $tx_1y_1d=(dx)y_1=by_1$ и $tx_1y_1d=(dy)x_1=ax_1$, число tx_1y_1d является общим кратным чисел a и b и потому должно делиться на наименьшее общее кратное k этих чисел. Следовательно, найдется целое число z такое, что $tx_1y_1d=kz$. Так как $k=ax=dyx=dy_1x_1t^2$, из последнего равества следует, что $tz=1$, а потому и $t=1$. Таким образом, единственным положительным общим делителем чисел x и y является 1, и потому эти числа взаимно просты. Как отмечено выше, отсюда следует, что $d=(a,b)$, и предложение 2.4 доказано. □

Отметим очевидное

Следствие. *Наименьшее общее кратное двух положительных целых чисел совпадает с произведением этих чисел тогда и только тогда, когда они взаимно просты.* □

В заключение этого параграфа укажем процедуру, следуя которой можно вычислить наибольший общий делитель произвольных положительных (а потому и произвольных ненулевых) целых чисел. Эта процедура называется *алгоритмом Евклида.*

Пусть a и b — положительные целые числа. Первый шаг алгоритма состоит в делении с остатком числа a на число b, т. е. в нахождении таких целых чисел q_1 и r_1, что $a=bq_1+r_1$ и $0\leqslant r_1<b$. Если оказалось, что $r_1=0$, то число b является делителем числа a. Поэтому наибольший общий делитель этих чисел равен b, и процедура отыскания наибольшего общего делителя закончена. Если же $r_1\neq 0$, переходим к выполнению второго шага алгоритма.

На втором шаге алгоритма делим с остатком число b на число r_1, т. е. находим такие целые числа q_2 и r_2, что $b=r_1q_2+r_2$ и $0\leqslant r_2<r_1$. Если $r_2\neq 0$, то переходим к третьему шагу алгоритма.

На третьем шаге алгоритма делим с остатком число r_1 на число r_2, т. е. находим такие целые числа q_3 и r_3, что $r_1=r_2q_3+r_3$ и $0\leqslant r_3<r_2$. Если $r_3\neq 0$, то переходим к четвертому шагу алгоритма, состоящему в делении с остатком числа r_2 на число r_3.

Вообще, если после выполнение n-го шага (где $n\geqslant 3$), состоящего в делении с остатком числа r_{n-2} на число r_{n-1}, полученный остаток r_n отличен от нуля, алгоритм предписывает выполнение следующего шага, состоящего в делении с остатком

числа r_{n-1} на число r_n. Так как возникающая при этом последовательность положительных целых чисел $r_1, r_2, \ldots$ удовлетворяет неравенствам $b > r_1 > r_2 > \cdots$, из предложения 1.8 следует, что наша процедура последовательных делений с остатком должна оборваться не более, чем через b шагов. Это означает существование такого номера n, что после выполнения n-го шага мы окажемся не в состоянии выполнить следующий $(n+1)$-ый шаг. Но единственным препятствием к возможности выполнить $(n+1)$-ый шаг является то, что остаток, полученный на n-ом шаге, окажется равным нулю. Таким образом, существует номер k такой, что число $r_k \neq 0$ и является делителем числа r_{k-1}; тогда наша процедура останавливается после выполнения $k+1$-ого шага.

Результатом выполнения этой процедуры (т. е. алгоритма Евклида) является следующая последовательность равенств и двойных неравенств:

$$\begin{aligned}
a &= b\ q_1 + r_1, && 0 \leqslant r_1 < b;\\
b &= r_1 q_2 + r_2, && 0 \leqslant r_2 < r_1;\\
r_1 &= r_2 q_3 + r_3, && 0 \leqslant r_3 < r_2;\\
r_2 &= r_3 q_4 + r_4, && 0 \leqslant r_4 < r_3;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, && 0 \leqslant r_{k-1} < r_{k-2};\\
r_{k-2} &= r_{k-1} q_k \quad + r_k, && 0 \leqslant r_k \quad < r_{k-1};\\
r_{k-1} &= r_k q_{k+1}.
\end{aligned} \tag{5}$$

Теорема 2.3. *Последний отличный от нуля остаток в алгоритме Евклида, примененном к числам a и b, равен наибольшему общему делителю этих чисел.*

Доказательство этой теоремы основано на следующем простом замечании: если целые числа a, b, c и d связаны соотношением $a = bc + d$, то $(a, b) = (b, d)$.

В самом деле, если целое число t является общим делителем чисел a и b, то очевидно, что $t \mid d$, и потому t является общим делителем чисел b и d. Очевидно также, что из $t \mid b$ и $t \mid d$ следует, что $t \mid a$, и потому всякий общий делитель чисел b и d является общим делителем чисел a и b. Таким образом, множество всех общих делителей чисел a и b совпадает с множеством всех общих делителей чисел b и d, откуда и следует равенство $(a, b) = (b, d)$.

Из сделанного замечания и равенств (5) имеем

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-2}, r_{k-1}) = (r_{k-1}, r_k) = r_k,$$

что и требовалось доказать. $\square$

Рассмотрим пример применения алгоритма Евклида:

Пример 2.7. *Найти наибольший общий делитель чисел* 852 *и* 822.

Выполняя последовательные деления с остатком, получаем

$$\begin{aligned}
852 &= 822 \cdot 1 + 30,\\
822 &= 30 \cdot 27 + 12,\\
30 &= 12 \cdot 2 + 6,\\
12 &= 6 \cdot 2.
\end{aligned}$$

Так как последний отличный от нуля остаток оказался равным 6, получаем $(852, 822) = 6$. $\square$

Вычисления, проделанные при реализации алгоритма Евклида, позволяют наряду с наибольшим общим делителем d чисел a и b, найти и такие числа u и v, что $d = au + bv$. (В теореме 2.2 доказано существование таких чисел, но не указано никакого способа для их вычисления.) Продемонстрируем, как это сделать на только что рассмотренном примере. Из предпоследнего шага вычислений выразим наибольший общий делитель 6 наших чисел через предшествующие остатки 12 и 30: $6 = 30 - 12 \cdot 2$. Выразим остаток 12 из предыдущего равенства, $12 = 822 - 30 \cdot 27$, и подставив его в выражение для 6, выразим число 6 через остаток 30 и число 822:

$$6 = 30 - (822 - 30 \cdot 27) \cdot 2 = 30 - 822 \cdot 2 + 30 \cdot 54 = 30 \cdot 55 + 822 \cdot (-2).$$

Наконец, заменим остаток 30 его выражением $30 = 852 - 822$ из первого равенства:

$$6 = 30 \cdot 55 + 822 \cdot (-2) = (852 - 822) \cdot 55 + 822 \cdot (-2) = 852 \cdot 55 + 822 \cdot (-57).$$

Таким образом, $u = 55$, $v = -57$.

ЗАДАЧИ К ПАРАГРАФУ 2

2.1. При делении с остатком числа 1270 на некоторое положительное число неполное частное оказалось равным 74. Найти остаток и то число, на которое делили.

2.2. Доказать, что квадрат нечетного числа, уменьшенный на 1, делится на 8.

2.3. Доказать, что сумма кубов трех последовательных целых чисел делится на 9.

2.4. Доказать, что сумма квадратов двух последовательных целых чисел, уменьшенная на 1, делится на 4.

2.5. Доказать, что для любого целого числа n число $n^3 + 11n$ делится на 6.

2.6. Доказать, что если сумма квадратов двух целых чисел делится на 7, то каждое из этих чисел делится на 7.

2.7. Доказать, что для любого целого числа $n \geqslant 0$ число
$16^n - 15n - 1$ делится на 225.

2.8. Доказать, что для любого целого числа $n \geqslant 0$ число $3^{2n+2} - 8n - 9$ делится на 64.

2.9. Доказать, что для любого целого числа $n \geqslant 0$ число $3^n + 5 \cdot 2^{8n+5}$ делится на 23.

2.10. Доказать, что для любого целого числа $n \geqslant 0$ число

$$5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$$

делится на 19.

2.11. Доказать, что если числа a и b являются взаимно простыми, то каждое из этих чисел взаимно просто и с их суммой, и с их разностью.

2.12. Доказать, что если числа a и b являются взаимно простыми, то наибольший общий делитель их суммы $a+b$ и разности $a-b$ равен либо 1, либо 2. Можно ли утверждать, что всегда $(a+b, a-b) = 1$?

2.13. Доказать, что если числа a и b являются взаимно простыми, то наибольший общий делитель их суммы $a+b$ и неполного квадрата разности $a^2 - ab + b^2$ равен либо 1, либо 3. Можно ли утверждать, что всегда $(a+b, a^2 - ab + b^2) = 1$?

2.14. Доказать, что для любых целых чисел a, b и c наибольший общий делитель чисел $a + bc$ и $a + b(c-1)$ совпадает с наибольшим общим делителем чисел a и b.

2.15. Доказать, что для любых целых чисел a и b наибольший общий делитель чисел $5a + 3b$ и $13a + 8b$ совпадает с наибольшим общим делителем чисел a и b.

2.16. Пусть d — наибольший общий делитель целых чисел a и b. Доказать, что для любого целого числа $c > 0$ наибольший общий делитель чисел ac и bc равен dc.

2.17. Доказать, что если целые числа a и c взаимно просты, то для любого целого числа b наибольший общий делитель чисел a и b совпадает с наибольшим общим делителем чисел a и bc.

2.18. Доказать, что наибольший общий делитель чисел суммы чисел a и b и наименьшего общего кратного этих чисел совпадает с наибольшим общим делителем чисел a и b.

2.19. Доказать, что если число ab^2, где a и b целые числа, является квадратом целого числа, то и число a является квадратом некоторого целого числа.

2.20. Найти все такие натуральные числа a и b, где $a \leqslant b$, что $a + b = 432$ и $(a, b) = 36$.

2.21. Найти все такие натуральные числа a и b, где $a \leqslant b$, что $ab = 864$ и $(a, b) = 6$.

2.22. Найти все такие натуральные числа a и b, где $a \leqslant b$, что $[a, b] = 840$ и $(a, b) = 15$.

2.23. Доказать, что для любого целого числа $a \neq 1$ и произвольного натурального числа m наибольший общий делитель чисел $\dfrac{a^m - 1}{a - 1}$ и $a - 1$ совпадает с наибольшим общим делителем чисел $a - 1$ и m.

§ 3. Простые числа

Из предыдущего параграфа мы знаем, что у каждого натурального числа $a > 1$ есть по крайней мере два различных натуральных делителя: это 1 и само число a. У некоторых натуральных чисел никаких других натуральных делителей нет. Примером такого числа является 2. В самом деле, если натуральное число x является делителем числа 2, то в силу предложения 2.1 должно выполняться неравенство $x \leqslant 2$, у которого, как мы знаем, имеется лишь два натуральных решения $x = 1$ и $x = 2$, так что эти два числа действительно исчерпывают множество натуральных делителей числа 2. Аналогичным свойством обладают числа 3, 5, 7 и многие другие. Такие числа называют *простыми*. Более точно, мы принимаем следующее определение:

Целое число a называется простым, если $a > 1$ и любой натуральный делитель числа a равен либо 1, *либо a.*

Если целое число $a > 1$ не является простым, мы будем называть его *составным*. Легко видеть, что число a является составным тогда и только тогда, когда существуют натуральные числа b и c такие, что $a = bc$, причем $b < a$ и $c < a$ (или, равносильно, $b > 1$ и $c > 1$).

Предложение 3.1. *Каждое натуральное число, большее, чем* 1, *обладает хотя бы одним простым делителем. Более того, каждое натуральное число $a > 1$ либо само является простым, либо является произведением нескольких простых чисел.*

Очевидно, что первое утверждение этого предложения является непосредственным следствием второго. Тем не менее, представляется целесообразным привести здесь и прямое доказательство первого утверждения. Заметим для этого, что если a — натуральное число и $a > 1$, то множество натуральных делителей числа a, больших, чем 1, непусто, так как в это множество входит, в частности, наше число a. Поэтому существует наименьшее число $p > 1$, являющееся делителем числа a. Легко видеть, что p — простое число. В самом деле, если $x > 1$ — делитель числа p, то $x \leqslant p$. С другой стороны, так как $x \,|\, p$ и $p \,|\, a$, то x является делителем числа a, и потому в силу выбора числа p имеем неравенство $x \geqslant p$. Следовательно, $x = p$, и простота числа p доказана.

Справедливость второго утверждения докажем методом бесконечного спуска. Предположим, что существует такое натуральное число $a > 1$, которое не является простым и не раскладывается в произведение простых чисел. Так как число a не является простым, найдутся целые числа b и c такие, что $a = bc$, причем $1 < b < a$ и $1 < c < a$. Очевидно, что если каждое из этих чисел b и c или является простым числом, или раскладывается в произведение простых чисел, то и число a будет являться произведением простых чисел. Следовательно, хотя бы одно из чисел b или c не является простым и не раскладывается в произведение простых чисел. Итак, мы видим, что из предположения о существовании натурального числа, для которого наше утверждение является ложным следует существование меньшего натурального числа, для которого это утверждение также ложно. Так как бесконечных убывающих последовательностей натуральных чисел не существует, наше утверждение доказано. $\square$

Второе утверждение доказанного предложения можно будет сформулировать более однозначно, если договориться наряду с произведениями двух, трех и большего числа сомножителей рассматривать и произведения с одним сомножителем. А именно, будем, когда это удобно, считать произвольное число a равным произведению, единственным сомножителем которого является это число a. С использованием этого соглашения формулировка второго утверждения предложения 3.1 выглядит следующим образом:

Каждое натуральное число $a > 1$ раскладывается в произведение простых чисел.

Еще два важных свойства простых чисел содержатся в следующем предложении.

Предложение 3.2. *Если целое число a не делится на простое число p, то $(a, p) = 1$. Если произведение нескольких чисел делится на простое число p, то хотя бы один из сомножителей должен делиться на p.*

В самом деле, поскольку общие натуральные делители чисел a и p содержатся в множестве всех натуральных делителей числа p, состоящем лишь из двух чисел 1 и p, то из условия $p \nmid a$ сразу следует, что единственным общим натуральным делителем наших чисел является 1 и потому $(a, p) = 1$.

Предположим теперь, что $a = b_1 b_2 \cdots b_n$ и $p \mid a$. Для доказательства того, что хотя бы одно из чисел $b_1, b_2, \ldots, b_n$ делится на p, воспользуемся индукцией по количеству n сомножителей в разложении числа a. Это утверждение очевидно, если $n = 1$. Пусть $n > 1$ и пусть для любого разложения произвольного целого числа в произведение менее чем n сомножителей доказываемое утверждение справедливо. Полагая $a' = b_2 \cdots b_n$, имеем $a = b_1 a'$. Таким образом, произведение двух чисел b_1 и a' делится на p. Если $p \mid b_1$, то утверждение о том, что один из сомножителей числа a делится на p, выполнено. Если же $p \nmid b_1$, то в силу доказанного выше $(p, b_1) = 1$, и из следствия 3 к теореме 2.2 получаем $p \mid a'$. Поэтому из индуктивного предположения следует, что хотя бы один из сомножителей $b_2, \ldots, b_n$ числа a' должен делиться на p. Следовательно, и в этом случае один из сомножителей числа a делится на p. Индуктивный переход закончен, и наше утверждение доказано. $\square$

Уже перечисленные свойства простых чисел позволяют решать многие задачи о делимости целых чисел и находить более простые решения ряда задач, решенных другими способами. В качестве иллюстрации этого приведем еще одно решение задачи из примера 2.4: Доказать, что если числа a и b взаимно просты, то их сумма $a + b$ и произведение ab также являются взаимно простыми числами.

Если, в самом деле, предположить, что числа $a + b$ и ab не являются взаимно простыми, то у них существует общий делитель $t > 1$. В соответствии с предложением 3.1 существует простое число p, являющееся делителем числа t, а потому — и общим делителем чисел $a + b$ и ab. Но из $p \mid ab$ в силу предложения 3.2 следует, что хотя бы одно из чисел a или b должно делиться на p. Так как на p делится сумма этих чисел, то из делимости на p одного из них следует делимость на p и другого. Таким образом, число p оказывается общим делителем чисел a и b, что противоречит их взаимной простоте. $\square$

Заметим, что использованный в приведенном решении прием, оказывается весьма полезным при решении ряда задач. Он заключается в том, что появившееся в том или ином рассуждении предположение о существовании у двух чисел общего делителя, большего чем 1, можно в силу предложения 3.1 заменить (не теряя общности) более сильным предположением о существовании у этих чисел общего простого делителя.

Рассмотрим еще одну задачу, при решении которой также используется предложение 3.2.

Пример 3.1. *Доказать, что если число, являющееся квадратом некоторого целого числа, делится на простое число p, то оно должно делиться и на число p^2.*

В самом деле, если число $a^2 = a \cdot a$ (являющееся произведением двух одинаковых сомножителей) делится на простое число p, то в силу предложения 3.2 хотя бы один из этих сомножителей должен делиться на p, так что $a = px$ для некоторого целого числа x. Отсюда $a^2 = p^2x^2$. $\square$

Доказанное в примере 3.1 утверждение тоже полезно иметь в виду при решении многих задач. Рассмотрим здесь

Пример 3.2. *Доказать, что сумма квадратов двух нечетных чисел не является квадратом целого числа.*

Действительно, если $a = 2m + 1$ и $b = 2n + 1$ — произвольные нечетные числа, то число $a^2 + b^2 = 2(2(m^2 + m + n^2 + n) + 1)$ делится на 2 и не делится на $4 = 2^2$, а потому в силу утверждения примера 3.1 не может быть квадратом целого числа. $\square$

Следующее важнейшее свойство простых чисел было доказано Евклидом более 2000 лет тому назад.

Теорема 3.1. *Множество простых чисел является бесконечным.*

Доказательство. Покажем, что для любого конечного множества простых чисел всегда найдется хотя бы одно простое число, не принадлежащее этому множеству. Очевидно, что это свойство и будет означать бесконечность множества всех простых чисел.

Итак, пусть p_1, p_2, ... , p_n — конечная последовательность простых чисел. Рассмотрим число

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

Так как $a > 1$, из предложения 3.1 следует, что существует хотя бы одно простое число p, делящее число a. С другой стороны, число a не может делиться ни на одно из чисел p_1, p_2, ... , p_n, так как в противном случае на это число делилось бы и число 1. Следовательно, число p не совпадает ни с одним из чисел p_1, p_2, ... , p_n, что и доказывает наше утверждение. $\square$

Как узнать, является ли данное натуральное число простым? Наиболее прямой путь состоит в непосредственной проверке того, делится ли данное число n на какое-либо натуральное число $m < n$. При этом, разумеется, достаточно ограничиться рассмотрением лишь простых чисел m, и здесь оказывается полезным следующее

Предложение 3.3. *Если натуральное число n является составным, то оно обладает простым делителем p таким, что $p \leqslant \sqrt{n}$.*

В самом деле, если число является составным, то найдутся натуральные числа a и b такие, что $n = ab$ и $1 < a, b < n$. Пусть (без потери общности) $a \leqslant b$ и p — какой-либо простой делитель числа a, а потому и числа n. Тогда $p^2 \leqslant a^2 \leqslant ab = n$, откуда $p \leqslant \sqrt{n}$. $\square$

Например, число 101 является простым, так как не делится ни на 2, ни на 3, ни на 5, ни на 7, а других простых чисел, не превосходящих числа $\sqrt{101}$, нет.

Утверждение предложения 3.3 используется при нахождении списка всех простых чисел, не превосходящих данного числа n, следующим способом, который называется *решетом Эратосфена*.

Выписываем все натуральные числа от 2 до n. Из этого списка вычеркиваем все четные числа, кроме 2. После этого первым невычеркнутым числом (не считая 2) является простое число 3. Оставляя число 3 невычеркнутым, вычеркиваем все числа, кратные 3. После этого первым невычеркнутым числом (не считая 2 и 3) является простое число 5. Оставляя снова число 5 невычеркнутым, вычеркиваем все числа, кратные 5. Очевидно, что при повторении этой процедуры первое невычеркнутое после очередного вычеркивания число в нашем списке окажется простым числом. Процедуру вычеркиваний следует остановить, когда это простое число p оказывается больше, чем $\sqrt{n}$: все оставшиеся невычеркнутыми числа являются простыми. Действительно, если число $m \leqslant n$ является составным, то ввиду предложения 3.3 у него должен быть простой делитель $q < p$, и потому m должно было быть вычеркнутым на соответствующем этапе.

Выше было доказано, что произвольное натуральное число, большее чем 1, раскладывается в произведение простых чисел. Естественно возникает вопрос о том, сколько различных способов разложения данного числа в произведение простых существует. Если при этом такие разложения, как, например, $6 = 2 \cdot 3$ и $6 = 3 \cdot 2$, не считать различными, то можно утверждать, что представление натурального числа в виде произведения простых чисел является единственным:

Теорема 3.2. *Произвольное натуральное число $a > 1$ раскладывается в произведение простых чисел единственным способом, если не принимать во внимание порядок следования сомножителей.*

Говоря более подробно, это означает, что если $a = p_1 p_2 \cdots p_m$ и $a = q_1 q_2 \cdots q_n$ — два разложения данного числа a, в которых все сомножители $p_1, p_2, \ldots, p_m$ и $q_1, q_2, \ldots, q_n$ являются простыми числами, то количество сомножителей в этих разложениях одно и то же, т. е. $m = n$, и сомножители $q_1, q_2, \ldots, q_n$ второго разложения можно, меняя местами, расположить и заново пронумеровать так, что в обоих разложениях на одинаковых местах будут стоять одинаковые простые числа, т. е. $p_i = q_i$ для всех $i = 1, 2, \ldots, m$.

Эта теорема также была известна уже во времена Евклида, и к настоящему времени придумано много различных ее доказательств. Приведем здесь одно из них.

Итак, пусть $a = p_1 p_2 \cdots p_m$ и $a = q_1 q_2 \cdots q_n$ — два разложения данного натурального числа $a > 1$ в произведение простых чисел $p_1, p_2, \ldots, p_m$ и $q_1, q_2, \ldots,$

q_n соответственно. Доказательство того, что $m = n$ и после подходящей перенумерации сомножителей q_1, q_2, ... , q_n второго разложения для всех $i = 1, 2, \ldots, m$ имеют место равенства $p_i = q_i$, проведем индукцией по числу a. Но прежде, чем приступить непосредственно к индуктивному рассуждению, сделаем два общих замечания.

Во-первых, мы можем в дальнейшем без потери общности предполагать, что выполнено неравенство $m \leqslant n$. Во-вторых, очевидно, что натуральное число, большее 1, является простым тогда и только тогда, когда в любом его разложении в произведение простых чисел количество сомножителей равно 1. Следовательно, для числа a, два разложения которого в произведение простых чисел указаны выше, требуемый вывод является очевидным, если нам известно, что или число a простое, или $m = 1$.

Перейдем теперь к индуктивному доказательству. Так как наименьшим из чисел, для которых формулируется доказываемое утверждение, является число 2, и так как это число простое, основание индукции (при $a = 2$) следует из предыдущего замечания.

Предположим теперь, что $a > 2$, и предполагая доказываемое утверждение справедливым для всех натуральных чисел, меньших a (и больших 1), докажем его справедливость и для числа a. Так как при $m = 1$ это следует из замечания, сделанного выше, нам достаточно рассмотреть случай, когда $m \geqslant 2$ (а потому и $n \geqslant 2$).

Из равенства $a = p_1 p_2 \cdots p_m$ следует, что $p_1 \mid a$, и потому произведение $q_1 q_2 \cdots q_n$ делится на p_1. Так как p_1 — простое число, из предложения 3.2 следует, что один из сомножителей q_1, q_2, ... , q_n должен делиться на p_1. Изменив, если это необходимо, их нумерацию, мы можем без потери общности предполагать, что $p_1 \mid q_1$. Но поскольку и число q_1 является простым, это означает, что $p_1 = q_1$. Полагая теперь $b = p_2 p_3 \cdots p_m$, имеем $p_1 b = a = q_1 q_2 \cdots q_n = p_1 (q_2 q_3 \cdots q_n)$, откуда следует, что $b = q_2 q_3 \cdots q_n$. Поскольку $b < a$, из индуктивного предположения следует, что количество сомножителей в каждом из двух разложений $b = p_2 p_3 \cdots p_m$ и $b = q_2 q_3 \cdots q_n$ числа b в произведение простых чисел должно быть одинаковым, т. е. $m - 1 = n - 1$, а значит и $m = n$. Кроме того, индуктивное предположение говорит о том, что после подходящей перенумерации чисел q_2, q_3, ... , q_n должны выполняться равенства $p_2 = q_2$, $p_3 = q_3$, ... , $p_m = q_m$. Так как равенство $p_1 = q_1$ было отмечено выше, справедливость нашего утверждения для числа a полностью доказана, и индуктивный шаг завершен. Тем самым закончено и доказательство теоремы 3.2. $\square$

Если в разложении натурального числа a в произведение простых чисел сгруппировать одинаковые сомножители и вместо их произведения записать подходящие степени соответствующих простых чисел, то получим запись числа a, имеющую вид

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \tag{1}$$

где p_1, p_2, ... , p_r — попарно различные простые числа, расположенные в порядке возрастания, т. е. $p_1 < p_2 < \cdots < p_r$, и k_1, k_2, ... , k_r — положительные целые числа. Такая запись называется *каноническим представлением (или канонической записью)* числа a. Из теоремы 3.2 получаем очевидное

Следствие. *Произвольное натуральное число $a > 1$ обладает единственным каноническим представлением.* $\square$

Каноническая запись натурального числа позволяет успешно решать ряд задач, связанных с отношением делимости. Одну такую задачу, а именно, задачу описания всех натуральных делителей данного числа мы сейчас решим.

Предложение 3.4. *Пусть a — натуральное число с канонической записью (1). Натуральное число b тогда и только тогда является делителем числа a, когда оно может быть записано в виде*

$$b = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}, \tag{2}$$

где показатели $l_1, l_2, \ldots, l_r$ удовлетворяют двойным неравенствам $0 \leqslant l_i \leqslant k_i$ $(i = 1, 2, \ldots, r)$.

Заметим, что запись (2), вообще говоря, не является каноническим представлением числа b, поскольку, в отличие от канонического представления, показатели степеней $l_1, l_2, \ldots, l_r$ не обязаны быть положительными числами; некоторые из них могут обращаться в нуль, и если, например, все они равны нулю, мы получаем число 1, которое, разумеется, входит в множество делителей числа a. В остальных случаях для получения канонической записи числа b следует в правой части (2) вычеркнуть те простые числа, показатели степеней у которых равны 0.

Доказательство предложения 3.4 начнем с достаточности условий: покажем, что произвольное число b вида (2) действительно является делителем числа a. Для этого полагаем $c = p_1^{k_1 - l_1} p_2^{k_2 - l_2} \cdots p_r^{k_r - l_r}$. Так как ввиду неотрицательности показателей степеней число c является целым и удовлетворяет равенству $a = bc$, имеем $b \mid a$, что и требовалось.

Для доказательства обратного заметим сначала, что если p и q — различные простые числа, то $(p, q) = 1$, откуда следует (см. пример 2.3), что для любых натуральных чисел m и n $(p^m, q^n) = 1$. В частности, сомножители $p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}$ канонической записи (1) числа a являются попарно взаимно простыми числами. Отсюда с учетом предложения 3.2 и следствия 3 к теореме 2.2 следует, что если число вида p^m, где p простое и m натуральное, является делителем числа a, то p совпадает с одним из чисел $p_1, p_2, \ldots, p_r$, и если $p = p_i$, то $m \leqslant k_i$.

Пусть теперь b — произвольный натуральный делитель числа a. Так как возможность записи числа 1 в виде (2) очевидна, мы можем считать, что $b > 1$. Произвольный делитель числа b, имеющий вид p^m, где p простое и m натуральное, должен быть, разумеется, делителем и числа a, и потому из предыдущего замечания следует, что для некоторого i имеют место равенство $p = p_i$ и неравенство $m \leqslant k_i$. Это означает, что в каноническую запись числа b входят лишь степени некоторых (возможно, всех) простых чисел $p_1, p_2, \ldots, p_r$ с показателями, не превосходящими соответствующих чисел $k_1, k_2, \ldots, k_r$. Добавив к канонической записи числа b оставшиеся числа из списка $p_1, p_2, \ldots, p_r$ с нулевыми показателями, получим представление этого числа в виде (2). $\square$

Описание всех натуральных делителей натурального числа a, полученное в предложении 3.4, позволяет узнать, сколько различных натуральных делителей

имеет число a. Иначе говоря, каноническое представление натурального числа a позволяет вычислить значение функции $\tau(x)$, определенной на множестве всех натуральных чисел, значение которой при $x = a$, равно числу всех натуральных делителей числа a. Например, $\tau(1) = 1$; если p — простое число, то $\tau(p) = 2$. В общем случае имеет место следующее

Предложение 3.5. *Пусть $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ — каноническое представление натурального числа $a > 1$. Тогда*

$$\tau(a) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1). \tag{3}$$

В самом деле, ввиду предложения 3.4 множество всех делителей числа a совпадает с множеством чисел, записываемых в виде $b = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$, где для каждого $i = 1, 2, \ldots, r$ число l_i удовлетворяет неравенствам $0 \leqslant l_i \leqslant k_i$ и потому может принимать в точности $k_i + 1$ значений. Так как каждое из $k_1 + 1$ значений числа l_1 может комбинироваться с каждым из $k_2 + 1$ значений числа l_2 и т. д., всего имеется $(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$ различных наборов показателей. Остается заметить, что разным наборам показателей соответствуют разные делители числа a. $\square$

В теории чисел рассматривается еще одна функция от натурального аргумента; это функция $\sigma(x)$, значение которой при $x = a$ равно сумме всех натуральных делителей числа a. Имея каноническое представление числа a, легко вычислить и значение при $x = a$ функции $\sigma(x)$:

Предложение 3.6. *Пусть $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ — каноническое представление натурального числа $a > 1$. Тогда*

$$\sigma(a) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}. \tag{4}$$

Действительно, после раскрытия скобок произведение

$$(1 + p_1 + \cdots + p_1^{k_1})(1 + p_2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + \cdots + p_r^{k_r})$$

явится суммой попарно различных всевозможных выражений вида $p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$, где $0 \leqslant l_i \leqslant k_i$ $(i = 1, 2, \ldots, r)$, т. е. в соответствии с предложением 3.4 — суммой всех делителей числа a. Так как по формуле суммы геометрической прогрессии для каждого $i = 1, 2, \ldots, r$ имеем

$$1 + p_i + \cdots + p_i^{k_1} = \frac{p_i^{k_i+1} - 1}{p_i - 1},$$

равенство (4) доказано. $\square$

Пример 3.3. *Найти число вида* $2^l 3^m$*, если известно, что сумма всех его натуральных делителей равна* 403*.*

Очевидно, что показатели l и m не могут быть одновременно равными 0. Если $l = 0$, то каноническая запись нашего числа имеет вид 3^m, и применяя формулу предложения 3.6, имеем $3^{m+1} - 1 = 2 \cdot 403$. Отсюда получаем равенство $3^{m+1} = 807 = 3 \cdot 269$, невыполнимое при целых m, так как число 269 простое. Если $m = 0$, то каноническая запись нашего числа имеет вид 2^l, и потому $2^{l+1} - 1 = 403$, что также невозможно.

Таким образом, $l > 0$, $m > 0$ и $2^l 3^m$ — каноническая запись нашего числа. По формуле предложения 3.6 имеем

$$(2^{l+1} - 1)(3^{m+1} - 1) = 2 \cdot 403 = 2 \cdot 13 \cdot 31$$

(где, отметим, 2, 13 и 31— простые числа). Так как $2^{l+1} - 1 > 1$ и $3^{m+1} - 1 > 1$, то разложение на простые множители $2{\cdot}13{\cdot}31$ произведения этих чисел должно составляться из соответствующих разложений сомножителей. Поскольку число $2^{l+1} - 1$ нечетно и равенства $2^{l+1} - 1 = 13$ и $2^{l+1} - 1 = 13 \cdot 31$ также невозможны при целых значениях l, имеем $2^{l+1} - 1 = 31$ и $3^{m+1} - 1 = 26$. Отсюда $l = 4$ и $m = 2$, так что искомое число есть $2^4 3^2 = 144$. $\square$

Из предложений 3.5 и 3.6 очевидным образом вытекает

Предложение 3.7. *Если натуральные числа* a *и* b *взаимно просты, то* $\tau(ab) = \tau(a)\tau(b)$ *и* $\sigma(ab) = \sigma(a)\sigma(b)$. $\square$

Свойство функций $\tau(x)$ и $\sigma(x)$, сформулированное в предложении 3.7, называют *мультипликативностью* этих функций. В следующем параграфе будет доказано, что этим свойством обладает еще одна важная теоретико-числовая функция.

С суммой делителей натурального числа связано одно интересное понятие. Натуральное число a называется *совершенным*, если оно совпадает с суммой всех своих натуральных делителей, отличных от самого числа a; иначе говоря, число a является совершенным тогда и только тогда, когда $\sigma(a) = 2a$. Понятие совершенного числа появилось в математике Древней Греции; древние греки знали четыре совершенных числа: 6, 28, 496 и 8128. В действительности, четные совершенные числа можно описать следующим образом:

Предложение 3.8. *Натуральное четное число* a *является совершенным тогда и только тогда, когда оно имеет вид* $a = 2^{k-1}(2^k - 1)$ *для некоторого натурального числа* $k \geqslant 2$*, такого, что число* $2^k - 1$ *является простым.*

Доказательство начнем с достаточности. Пусть число a имеет вид $a = 2^{k-1}(2^k - 1)$, где $k \geqslant 2$ и $2^k - 1$ — простое число. Так как числа 2^{k-1} и $2^k - 1$ взаимно просты, ввиду предложения 3.7 имеем $\sigma(a) = \sigma(2^{k-1})\sigma(2^k - 1)$. По формуле (4) $\sigma(2^{k-1}) = 2^k - 1$, а так как число $2^k - 1$ простое, то $\sigma(2^k - 1) = 1 + (2^k - 1) = 2^k$. Таким образом, $\sigma(a) = (2^k - 1) \cdot 2^k = 2a$, так что число a является совершенным.

Обратно, предположим, что натуральное четное число a является совершенным, т. е. $\sigma(a) = 2a$. Пусть n — наибольшее целое число такое, что $2^n \mid a$. Тогда

$a = 2^n b$ для некоторого нечетного числа b. Заметим, что поскольку число a является четным, $n \geqslant 1$, и потому, полагая $k = n + 1$, получаем представление числа a в виде $a = 2^{k-1}b$, где $k \geqslant 2$. Поскольку число b нечетно, имеем $(2^{k-1}, b) = 1$, откуда ввиду мультипликативности функции $\sigma(x)$ получаем $\sigma(a) = \sigma(2^{k-1})\sigma(b)$. Так как $\sigma(a) = 2a = 2^k b$ и $\sigma(2^{k-1}) = 2^k - 1$, это равенство принимает вид $2^k b = (2^k - 1)\sigma(b)$. Отсюда, в частности, следует, что $2^k b$ делится на $2^k - 1$, и так как числа $2^k b$ и $2^k - 1$ взаимно просты, число b делится на $2^k - 1$, и потому для некоторого натурального числа c имеет место равенство $b = (2^k - 1)c$. Подставляя вместо b это его выражение в равенство $2^k b = (2^k - 1)\sigma(b)$, после очевидного сокращения получаем $\sigma(b) = 2^k c$, откуда $\sigma(b) = (2^k - 1)c + c = b + c$.

Покажем, что $c = 1$. В самом деле, если бы выполнялось неравенство $c > 1$, то ввиду очевидного неравенства $c < b$, числа b, c и 1 были бы попарно различными делителями числа b, и потому должно было бы иметь место неравенство $\sigma(b) \geqslant b + c + 1$, противоречащее равенству $\sigma(b) = b + c$.

Итак, мы показали, что $b = 2^k - 1$ и $\sigma(b) = 2^k$. Отсюда следует, что число b является простым. Действительно, в противном случае должно существовать такое натуральное число d, что числа b, d и 1 являются попарно различными делителями числа b, откуда $\sigma(b) \geqslant b + d + 1 = 2^k + d > 2^k = \sigma(b)$, что невозможно.

Таким образом, $a = 2^{k-1}(2^k - 1)$, где $k \geqslant 2$ и $2^k - 1$ — простое число. Предложение 3.8 доказано. $\square$

Утверждение предложения 3.8 называют теоремой Евклида – Эйлера. Евклид в своих "Началах" доказал, что любое число указанного в формулировке вида является совершенным, а Эйлер спустя 2000 лет показал, что других четных совершенных чисел нет. Следует отметить, что до сих пор неизвестно, существуют ли нечетные совершенные числа. Неизвестно также, является ли множество всех четных совершенных чисел конечным или бесконечным. Ответ на этот вопрос явился бы, разумеется, и ответом на вопрос, является ли конечным или бесконечным множество простых чисел вида $2^k - 1$, и наоборот.

Нетрудно видеть, что если число $2^k - 1$ является простым, то простым должно быть и число k. Действительно, если число k составное и $k = mn$, где $m > 1$ и $n > 1$ — некоторые целые числа, то равенство

$$2^k - 1 = (2^m)^n - 1 = (2^m - 1)(2^{m(n-1)} + 2^{m(n-2)} + \cdots + 2^m + 1)$$

(вытекающее из тождества задачи 1.4) показывает, что и число $2^k - 1$ будет составным.

Тем не менее, обратное не имеет места. Хотя при $k = 2$, 3, 5 и 7 число $2^k - 1$ является простым (и дает четные совершенные числа, перечисленные выше), уже при $k = 11$ число $2^k - 1$ является составным. Простые числа вида $2^k - 1$ называют *простыми числами Мерсенна* по имени французского математика Мерсенна, жившего в одно время с Ферма и интересовавшегося этими числами. Долгое время наибольшим известным простым числом Мерсенна являлось число $2^{31} - 1$; простота его была установлена Эйлером. В настоящее время список известных простых чисел Мерсенна значительно расширен, благодаря возросшим возможностям вычислительной техники. Вопрос о конечности или бесконечности множества таких чисел остается открытым.

В заключение, следует упомянуть и о *простых числах Ферма*; это числа вида $2^k + 1$. Легко заметить, что если такое число является простым, то k должно быть степенью числа 2. В самом деле, если у числа k есть нечетный делитель, больший, чем 1, т. е. для некоторых натуральных чисел m и t имеет место равенство $k = (2m + 1)t$, то ввиду равенства

$$2^k + 1 = (2^t)^{2m+1} + 1 = (2^t + 1)(2^{t(2m)} - 2^{t(2m-1)} + 2^{t(2m-2)} - \cdots + 2^{2t} - 2^t + 1)$$

(см. задачу 1.5) число $2^t + 1$ является делителем числа $2^k + 1$. Так как, к тому же, из очевидных неравенств $1 \leqslant t < k$ следуют неравенства $1 < 2^t + 1 < 2^k + 1$, число $2^k + 1$ не является простым. Ферма предполагал, что это почти очевидное необходимое условие является и достаточным, т. е. что все числа вида $2^{2^n} + 1$ (где $n \geqslant 0$) являются простыми. Тем не менее, хотя при $n = 0$, 1, 2, 3 и 4 действительно получаются простые числа 3, 5, 17, 257 и 65537 соотвественно, как показал Эйлер, при $n = 5$ получается составное число. Таким образом, предположение Ферма оказалось ошибочным.

ЗАДАЧИ К ПАРАГРАФУ 3

3.1. Доказать, что сумма квадратов четырех последовательных целых чисел не может быть квадратом целого числа.

3.2. Доказать, что если для некоторых натуральных чисел $a > 1$ и $n > 1$ число $a^n - 1$ является простым, то $a = 2$ и число n простое.

3.3. Доказать, что для любого целого числа $n > 1$ число $n^4 + 4$ является составным.

3.4. Доказать, что для любого целого числа $n > 1$ число $n^8 + n^4 + 1$ является составным.

3.5. Найти все простые числа p такие, что числа $p+10$ и $p+14$ тоже являются простыми.

3.6. Найти все простые числа p такие, что числа $p+4$ и $p+14$ тоже являются простыми.

3.7. Найти все простые числа p такие, что числа $p+10$ и $p+20$ тоже являются простыми.

3.8. Найти все простые числа p такие, что числа $4p^2+1$ и $6p^2+1$ тоже являются простыми.

3.9. Найти все простые числа p такие, что число $8p^2+1$ тоже является простым.

3.10. Найти все простые числа p, для которых число $4p+1$ является квадратом некоторого целого числа.

3.11. Найти все простые числа p, для которых число $4p + 1$ является кубом некоторого целого числа.

3.12. Найти все простые числа p, для которых число $5p + 1$ является кубом некоторого целого числа.

3.13. Найти все простые числа p, для которых число $13p + 1$ является кубом некоторого целого числа.

3.14. Найти все простые числа p, для которых число $7p + 1$ является кубом некоторого целого числа.

3.15. Доказать, что если числа p и $2p + 1$ являются простыми, причем $p \geqslant 5$, то число $4p + 1$ составное.

3.16. Доказать, что если p — простое число, то для любых целых чисел a и b из того, что числа $a + b$ и ab делятся на p, следует, что числа a и b делятся на p.

3.17. Доказать, что если p — простое число, то для любых целых чисел a и b из того, что числа $a^2 + b^2$ и ab делятся на p, следует, что числа a и b делятся на p.

3.18. Три различных простых числа, каждое из которых больше 3, образуют арифметическую прогрессию. Доказать, что разность этой прогрессии делится на 6. (Заметим, что простые числа 3, 5 и 7 образуют арифметическую прогрессию с разностью 2.)

3.19. Доказать, что произвольное простое число, большее 2, можно однозначно представить в виде разности квадратов двух натуральных чисел.

3.20. Найти число вида $3p^2$, где $p \neq 3$ — простое число, если сумма всех его натуральных делителей равна 124.

3.21. Найти натуральное число, сумма всех натуральных делителей которого равна 465 и число всех натуральных делителей равно 12, если известно, что у него ровно 2 различных простых делителя.

3.22. Найти натуральное число, сумма всех натуральных делителей которого равна 1240 и число всех натуральных делителей равно 12, если известно, что у него ровно 2 различных простых делителя.

3.23. Доказать, что при $n > 2$ числа $2^n - 1$ и $2^n + 1$ не могут одновременно быть простыми.

§ 4. Сравнения целых чисел по данному модулю

При изучении делимости целых чисел весьма полезным является отношение сравнения двух целых чисел по данному модулю. Этот параграф посвящен изложению основных свойств этого понятия. Начнем с определения.

Пусть m — фиксированное натуральное число. Будем говорить, что целое число a сравнимо с целым числом b по модулю m, если разность $a-b$ чисел a и b делится на m.

Тот факт, что число a сравнимо с числом b по модулю m символически мы будем записывать в виде $a \equiv b \pmod m$. Например, так как число $8-2$ делится на 3, мы можем записать $8 \equiv 2 \pmod 3$. С другой стороны, очевидно, что $8 \not\equiv 4 \pmod 3$.

Изучение свойств отношения сравнения целых чисел по модулю m начнем с доказательства следующего утверждения:

Предложение 4.1. 1) *Целое число a сравнимо с целым числом b по модулю m тогда и только тогда, когда остатки от деления на m чисел a и b совпадают.*

2) *Отношение сравнимости целых чисел по модулю m обладает следующими свойствами:*

(2.1) *для любого целого числа a сравнение $a \equiv a \pmod m$ является истинным;*

(2.2) *для любых целых чисел a и b из $a \equiv b \pmod m$ следует, что $b \equiv a \pmod m$;*

(2.3) *для любых целых чисел a, b и c из $a \equiv b \pmod m$ и $b \equiv c \pmod m$ следует, что $a \equiv c \pmod m$.*

Доказательство. Предположим сначала, что остатки от деления на m чисел a и b совпадают. Тогда для подходящих целых чисел q_1, q_2 и r выполнены равенства $a = mq_1+r$ и $b = mq_2+r$, из которых следует, что число $a-b = m(q_1-q_2)$ делится на m. Поэтому в соответствии с определением можно утверждать, что $a \equiv b \pmod m$.

Обратно, пусть $a \equiv b \pmod m$ и пусть $a = mq_1 + r_1$, $b = mq_2 + r_2$, причем $0 \leqslant r_1 < m$ и $0 \leqslant r_2 < m$. Из этих неравенств следует, что $|r_1 - r_2| < m$, а из равенств получаем равенство

$$a - b = m(q_1 - q_2) + (r_1 - r_2).$$

Так как предположение $a \equiv b \pmod m$ означает, что число $a-b$ делится на m, отсюда следует, что и число $r_1 - r_2$ делится на m. Если бы, при этом, это число было бы отличным от нуля, то ввиду свойства 8) из предложения 2.1 мы имели бы неравенство $m \leqslant |r_1 - r_2|$, противоречащее ранее установленному неравенству $|r_1 - r_2| < m$. Поэтому $r_1 - r_2 = 0$, т. е. $r_1 = r_2$, что и требовалось доказать.

Таким образом, первое утверждение предложения доказано. Все свойства, перечисленные во втором утверждении, следуют из него очевидным образом. □

То, что отношение сравнимости целых чисел по модулю m обладает свойствами (2.1) (рефлексивнось), (2.2) (симметричность) и (2.3) (транзитивность), означает, что это отношение является отношением эквивалентности. Поэтому множество $\mathbb{Z}$ всех целых чисел является объединением попарно непересекающихся классов чисел, сравнимых между собой по модулю m. Эти классы называются

классами вычетов по модулю m, а числа, принадлежащие данному классу, называются *вычетами* этого класса. Первое утверждение предложения 4.1 дает более наглядную характеризацию классов вычетов по модулю m: два целых числа являются вычетами одного и того же класса (т. е. принадлежат одному классу) тогда и только тогда, когда при делении на m они дают один и тот же остаток. Поэтому количество различных классов целых чисел, сравнимых между собой по модулю m, равно числу m всевозможных остатков $0, 1, \ldots, m-1$, которые могут получиться при делении на m произвольных целых чисел.

Множество всех классов вычетов по модулю m обозначается через $\mathbb{Z}_m$, а класс вычетов по модулю m, содержащий данное число a, будем записывать в виде $\overline{a}$; таким образом, $\overline{a}$ обозначает множество всех таких целых чисел b, для которых имеет место сравнение $a \equiv b \pmod{m}$. Например, если мы рассматриваем классы вычетов по модулю 6, то число 2 принадлежит классу $\overline{8}$, а число 5 не принадлежит этому классу. Очевидно, что для любых целых чисел a и b равенство $\overline{a} = \overline{b}$ имеет место тогда и только тогда, когда $a \equiv b \pmod{m}$. Поэтому из последнего утверждения предыдущего абзаца следует, что произвольный класс вычетов по модулю m совпадает в точности с одним из классов $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, т. е.

$$\mathbb{Z}_m = \{\overline{0},\ \overline{1},\ \ldots,\ \overline{m-1}\}.$$

Множество чисел, взятых по одному из каждого класса вычетов по модулю m, называется *полной системой вычетов по модулю* m. Таким образом, числа $0, 1, \ldots, m-1$ составляют полную систему вычетов по модулю m. Существует бесконечное множество различных способов выбора полной системы вычетов по данному модулю. Так, полными системами вычетов по модулю m являются и система чисел $1, 2, \ldots, m$, и система чисел $-1, 0, \ldots, m-2$. Еще пример: числа 1, 8, 9, -2, 11, 12 составляют полную систему вычетов по модулю 6, а числа 7, 8, 9, -2, 10, 12 нет, так как два числа этой системы -2 и 10 являются вычетами одного и того же класса, а класс $\overline{5}$ остался без представителя.

Продолжим изучение основных свойств отношения сравнения.

Предложение 4.2. *Если* $a \equiv b \pmod{m}$, *то* $(a, m) = (b, m)$.

Для обоснования этого утверждения достаточно заметить, что если число $a-b$ делится на m, то множество общих делителей чисел a и m совпадает с множеством общих делителей чисел b и m. $\square$

Предложение 4.3. *Для любых целых чисел* a, b *и* c *имеют место следующие утверждения:*

1) *если* $a \equiv b \pmod{m}$, *то* $a + c \equiv b + c \pmod{m}$;

2) *если* $a \equiv b \pmod{m}$, *то* $ac \equiv bc \pmod{m}$;

3) *если* $ac \equiv bc \pmod{m}$ *и число* c *взаимно просто с числом* m, *то* $a \equiv b \pmod{m}$;

4) *если* $c > 0$, *то сравнение* $a \equiv b \pmod{m}$ *имеет место тогда и только тогда, когда справедливо сравнение* $ac \equiv bc \pmod{mc}$.

Все эти утверждения получаются непосредственно из определения сравнения и свойств делимости целых чисел, и их доказательство оставляется читателю. $\square$

В связи с предложением 4.3 выскажем одно предостережение. Сравнение $4 \cdot 2 \equiv 1 \cdot 2 \pmod 6$ справедливо, а сравнение $4 \equiv 1 \pmod 6$ нет. Таким образом, обе части сравнения, вообще говоря, сокращать на общий множитель нельзя. Свойство 3) говорит о том, что такое сокращение возможно, если этот общий множитель взаимно прост с модулем, а свойство 4) разрешает сокращать на общий множитель обе части сравнения и модуль. Так, в нашем примере из сравнения $4 \cdot 2 \equiv 1 \cdot 2 \pmod 6$ следует верное сравнение $4 \equiv 1 \pmod 3$.

Отметим далее вытекающее из свойств 1) и 2) предложения 4.2 простое, но очень важное для нас свойство сравнений.

Следствие. *Два сравнения по одному и тому же модулю можно почленно складывать и перемножать. Говоря более подробно, это означает, что если* $a \equiv b \pmod m$ *и* $c \equiv d \pmod m$, *то* $a + c \equiv b + d \pmod m$ *и* $ac \equiv bd \pmod m$. *В частности, для любого натурального числа* n *из* $a \equiv b \pmod m$ *следует сравнение* $a^n \equiv b^n \pmod m$.

В самом деле, прибавив к обеим частям сравнения $a \equiv b \pmod m$ число c, а к обеим частям сравнения $c \equiv d \pmod m$ число b, получаем сравнения

$$a + c \equiv b + c \pmod m \qquad \text{и} \qquad b + c \equiv b + d \pmod m,$$

из которых в силу транзитивности и следует требуемое сравнение $a + c \equiv b + d \pmod m$. Возможность перемножения сравнений обосновывается аналогично. Последнее утверждение следствия доказывается очевидной индукцией. $\square$

Первые два утверждения этого следствия позволяют определить операции сложения и умножения на множестве $\mathbb{Z}_m$ классов вычетов целых чисел по модулю m следующим образом.

Пусть $\overline{a}$ и $\overline{b}$ — произвольные элементы из $\mathbb{Z}_m$. Мы полагаем

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \text{и} \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$$

Содержательно говоря, мы вводим следующее правило сложения двух классов из $\mathbb{Z}_m$: чтобы сложить два класса $\overline{a}$ и $\overline{b}$, следует взять какие-нибудь вычеты a и b этих классов и сложить их. Класс вычетов, представляемый суммой $a + b$ этих чисел, и будет считаться (по определению) суммой исходных классов. Аналогично, произведением классов $\overline{a}$ и $\overline{b}$ мы считаем класс, представляемый произведением чисел a и b. Например, для элементов $\overline{2}$ и $\overline{5}$ из множества $\mathbb{Z}_6$ в соответствии с этим определением имеем $\overline{2} + \overline{5} = \overline{7}$. А так как $\overline{7} = \overline{1}$, то справедливо равенство $\overline{2} + \overline{5} = \overline{1}$. Аналогично, $\overline{2} \cdot \overline{5} = \overline{4}$.

Здесь возникает одна проблема, связанная с тем, что в сформулированных правилах вычисления суммы и произведения двух классов вычетов мы пользуемся произвольно выбранными из этих классов числами. Если вместо вычета a из класса $\overline{a}$ выбрать другой вычет c, а из класса $\overline{b}$ — вычет d, то в соответствии с нашим правилом суммой классов $\overline{a}$ и $\overline{b}$ придется назвать класс $\overline{c + d}$, который, по меньшей мере, выглядит отличным от класса $\overline{a + b}$, полученного при первом выборе вычетов. Если эти классы действительно могут оказаться различными, то наше определение сложения является плохим, поскольку результат операции сложения должен

зависеть только от складываемых элементов (в данном случае — классов вычетов) и не зависеть ни от каких других обстоятельств (таких, как выбор представителя данного класса).

Таким образом, для того, чтобы утверждать, что мы действительно располагаем операцией сложения элементов множества $\mathbb{Z}_m$, нам следует убедиться в том, что наше определение является хорошим. Это легко сделать, используя следствие к предложению 4.2. Действительно, так как числа a и c принадлежат одному классу вычетов по модулю m, имеет место сравнение $a \equiv c \pmod m$. Аналогично, $b \equiv d \pmod m$. А так как ввиду упомянутого следствия из этих сравнений должно вытекать сравнение $a+b \equiv c+d \pmod m$, то числа $a+b$ и $c+d$ принадлежат одному и тому же классу вычетов, т. е. имеет место равенство $\overline{a+b} = \overline{c+d}$. Аналогично доказывается, что и операция умножения на множестве $\mathbb{Z}_m$ определена хорошо, т. е. и ее результат не зависит от выбора представителей в перемножаемых классах.

Итак, на множестве $\mathbb{Z}_m$ классов вычетов целых чисел по модулю m определены операции сложения и умножения. Непосредственно проверяется, что для этих операций выполнены свойства 1) – 5) из § 1. Проверим, например, справедливость ассоциативности сложения: для произвольных классов вычетов $\overline{a}$, $\overline{b}$ и $\overline{c}$ имеем

$$(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a}+\overline{b+c} = \overline{a}+(\overline{b}+\overline{c}).$$

Отметим еще, что нулем и единицей здесь являются классы $\overline{0}$ и $\overline{1}$ соответственно. Таким образом, $\mathbb{Z}_m$ является кольцом; его называют кольцом вычетов целых чисел по модулю m. Как отмечено в § 1, все правила обращения со сложением и умножением, справедливые в любом кольце, могут применяться и в $\mathbb{Z}_m$. Вместе с тем, кольца вычетов могут обладать свойствами, отличными от свойств числовых колец $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$. Например, в кольце $\mathbb{Z}_6$ элементы $\overline{2}$ и $\overline{3}$ отличны от нуля, но их произведение равно нулю: $\overline{2}\cdot\overline{3} = \overline{6} = \overline{0}$; таким образом, $\mathbb{Z}_6$ не является целостным кольцом.

Замена действий с числами соответствующими действиями с классами вычетов позволяет в ряде случаев избежать громоздких вычислений. При этом удобно вместо равенств в $\mathbb{Z}_m$ писать сравнения по модулю m.

Пример 4.1. *Найти остаток от деления на* 11 *числа* 60^{20}.

Искомым остатком является число r, удовлетворяющее условиям $60^{20} \equiv r \pmod{11}$ и $0 \leqslant r < 11$. Так как $60 = 5\cdot 12$ и $12 \equiv 1 \pmod{11}$, имеем (после умножения обеих частей последнего сравнения на 5) $60 \equiv 5 \pmod{11}$, откуда следует сравнение $60^{20} \equiv 5^{20} \pmod{11}$. Поскольку $5^2 \equiv 3 \pmod{11}$ и $3^2 \equiv -2 \pmod{11}$, имеем

$$5^{20} = (5^2)^{10} \equiv 3^{10} = (3^2)^5 \equiv (-2)^5 = -32 \equiv 1 \pmod{11}.$$

Таким образом, искомый остаток равен 1. □

Рассмотрим еще один пример применения полученных нами свойств сравнений.

Пример 4.2. *Доказать, что число* $8^{30} - 34$ *делится на* 55.

Так как число 55 является произведением двух взаимно простых чисел 5 и 11, достаточно показать, что $8^{30} - 34$ делится на каждое из этих чисел. Для этого, в

свою очередь, достаточно установить справедливость сравнений $8^{30} \equiv 34 \pmod 5$ и $8^{30} \equiv 34 \pmod{11}$.

Возведя обе части очевидного сравнения $8 \equiv 3 \pmod 5$ в 30-ую степень, получаем $8^{30} \equiv 3^{30} \pmod 5$. Используя сравнение $9 \equiv -1 \pmod 5$, имеем

$$3^{30} = 9^{15} \equiv (-1)^{15} = -1 \equiv 4 \pmod 5.$$

Мы видим, таким образом, что $8^{30} \equiv 4 \pmod 5$, откуда ввиду сравнения $4 \equiv 34 \pmod 5$ и получаем $8^{30} \equiv 34 \pmod 5$.

Аналогично доказывается и второе сравнение; приведем без подробных пояснений соответствующую последовательность равенств и сравнений:

$$8^{30} \equiv (-3)^{30} = 9^{15} \equiv (-2)^{15} = (-8)^5 \equiv 3^5 = 3^2 \cdot 3^3 \equiv (-2) \cdot 5 = -10 \equiv 1 \equiv 34 \pmod{11}. \quad \square$$

Обсудим теперь вопрос об обратимости операции умножения в кольце $\mathbb{Z}_m$: для каких классов $\overline{a}$ и $\overline{b}$ вычетов по модулю m найдется такой класс $\overline{c}$, что в $\mathbb{Z}_m$ выполнено равенство $\overline{a} \cdot \overline{c} = \overline{b}$? Из наших определений классов вычетов и их умножения очевидным образом следует, что этот вопрос равносилен следующему: для каких целых чисел a и b существует целое число c такое, что $ac \equiv b \pmod m$?

Таким образом, речь идет о разрешимости *сравнений первой степени с одной неизвестной*; так по аналогии с уравнениями называют сравнения вида $ax \equiv b \pmod m$ (которые в определенном смысле равносильны линейным уравнениям вида $\overline{a} \cdot \overline{x} = \overline{b}$ в кольце $\mathbb{Z}_m$). Вопрос о разрешимости таких сравнений сейчас будет разрешен исчерпывающим образом.

Теорема 4.1. *Пусть a и b — произвольные целые числа и m — некоторое натуральное число. Пусть $d = (a, m)$ — наибольший общий делитель чисел a и m. Сравнение*

$$ax \equiv b \pmod m \tag{1}$$

имеет решение в $\mathbb{Z}$ тогда и только тогда, когда число b делится на d. Кроме того, если $d \mid b$, то множество всех целых чисел, удовлетворяющих сравнению (1), является объединением в точности d различных классов вычетов по модулю m.

Доказательство. Докажем сначала, что сформулированное условие является необходимым для разрешимости сравнения (1). Предположим, что для некоторого целого числа c выполнено сравнение $ac \equiv b \pmod m$. Это означает, что $m \mid (ac - b)$, и так как $d \mid m$, отсюда следует, что число $ac - b$ делится на d. Поскольку $d \mid a$, получаем, что и b делится на d. Итак, мы показали, что если сравнение (1) имеет хотя бы одно целочисленное решение, то $d \mid b$.

Докажем теперь обратное, т. е. покажем, что если $d \mid b$, то сравнение (1) имеет целочисленное решение. Для этого рассмотрим сначала частный случай, когда $d = 1$, т. е. числа a и m взаимно просты. Пусть целые числа u и v таковы, что $au + mv = 1$ (их существование следует из теоремы 2.2). Умножив обе части этого равенства на b, получаем $b = a(ub) + m(vb)$. Отсюда следует, что при $c = ub$ число $ac - b = m(-vb)$ делится на m, и потому указанное число c удовлетворяет сравнению

$ac \equiv b \pmod{m}$. Таким образом, в этом случае существование решения сравнения (1) доказано.

Переходя к общему случаю, запишем числа a, b и m в виде $a = da_1$, $b = db_1$ и $m = dm_1$, где a_1, b_1 и m_1 — подходящие целые числа, причем $(a_1, m_1) = 1$, поскольку $d = (a, m)$. Поэтому ввиду рассмотренного случая найдется целое число c, удовлетворяющее сравнению $a_1 c \equiv b_1 \pmod{m_1}$. Умножив обе части этого сравнения и модуль на число d, получаем сравнение $ac \equiv b \pmod{m}$. Таким образом, число c является решением сравнения (1), и первое утверждение предложения полностью доказано.

Докажем второе утверждение. Если $d \mid b$, то (как только что доказано) сравнение (1) имеет целочисленные решения, и мы покажем, что все эти решения целиком распределены по нескольким классам вычетов по модулю m, причем число этих классов равно d. Мы сохраняем обозначения, введенные в предыдущем абзаце.

Пусть c — произвольное целое число, являющееся решением сравнения (1). Для каждого номера $i = 0, 1, \ldots d-1$ полагаем $c_i = c + im_1$ (заметим, что $c_0 = c$). Покажем, что каждое из чисел c_0, c_1, $\ldots$, c_{d-1} является решением сравнения (1). В самом деле, поскольку

$$ac_i = a(c + im_1) = ac + iam_1 = ac + ia_1 dm_1 = ac + m(ia_1),$$

имеем $ac_i \equiv ac \equiv b \pmod{m}$.

Теперь убедимся в том, что числа c_0, c_1, $\ldots$, c_{d-1} принадлежат попарно различным классам вычетов по модулю m. В самом деле, предположим, напротив, что для некоторых номеров i и j, где $0 \leqslant i < j \leqslant d-1$, числа c_i и c_j сравнимы по модулю m. Это означает, что число $c_j - c_i$ делится на m, и так как $c_j - c_i = (j-i)m_1$ и $m = dm_1$, отсюда следует, что число $j - i$ делится на d. Последнее невозможно, так как из неравенства $0 \leqslant i < j \leqslant d-1$ следует неравенство $0 < j - i < d$.

Наконец, покажем, что произвольное целое число k, являющееся решением сравнения (1), сравнимо по модулю m с одним из чисел c_0, c_1, $\ldots$, c_{d-1}. Из сравнений $ak \equiv b \pmod{m}$ и $ac \equiv b \pmod{m}$ следует сравнение $ak \equiv ac \pmod{m}$. После сокращения обеих частей и модуля этого сравнения на общий множитель d получаем сравнение $a_1 k \equiv a_1 c \pmod{m_1}$, откуда ввиду взаимной простоты чисел a_1 и m_1, в свою очередь, получаем $k \equiv c \pmod{m_1}$. Это означает, что число $k - c$ делится на m_1, т. е. для некоторого целого числа n имеет место равенство $k = c + nm_1$. Разделим число n на d с остатком: найдем такие целые числа q и r, что $n = dq + r$ и $0 \leqslant< d$. Отсюда

$$k = c + nm_1 = c + (dq + r)m_1 = (c + rm_1) + (dm_1)q = c_r + mq,$$

и потому $k \equiv c_r \pmod{m}$. Все утверждения теоремы доказаны. $\square$

На языке кольца $\mathbb{Z}_m$ доказанная теорема может быть, очевидно, сформулирована следующим образом:

Следствие 1. *Уравнение $\overline{a} \cdot \overline{x} = \overline{b}$ имеет решение в кольце $\mathbb{Z}_m$ тогда и только тогда, когда наибольший общий делитель d чисел a и m является делителем числа b. Кроме того, если $d \mid b$, то это уравнение имеет в точности d решений.* $\square$

Заметим, что и решениями сравнения (1) обычно считают не отдельные целые числа, а классы вычетов по модулю m. Приведем еще

Следствие 2. *Кольцо $\mathbb{Z}_m$ вычетов целых чисел по модулю m является полем тогда и только тогда, когда m является простым числом.*

В самом деле, если m является составным числом, то $m = ab$ для некоторых целых чисел a и b, не делящихся на m. Тогда $\overline{a}$ и $\overline{b}$ являются ненулевыми элементами кольца $\mathbb{Z}_m$, а их произведение равно нулю: $\overline{a}\cdot\overline{b} = \overline{ab} = \overline{m} = \overline{0}$. Таким образом, в этом случае $\mathbb{Z}_m$ не является целостным кольцом, а потому не является полем (напомним, что произвольное поле является целостным кольцом).

Обратно, если число m простое и элемент $\overline{a}$ кольца $\mathbb{Z}_m$ отличен от нуля, то число a не делится на m и потому взаимно просто с m. Тогда ввиду следствия 1 уравнение $\overline{a}\cdot\overline{x} = \overline{b}$ имеет решение в кольце $\mathbb{Z}_m$ при любом элементе $\overline{b}$ этого кольца. Следовательно, кольцо $\mathbb{Z}_m$ является полем. $\square$

Из доказательства теоремы 4.1 можно извлечь и способ решения произвольного сравнения вида $ax \equiv b \pmod m$. Действительно, достаточно уметь найти решение такого сравнения, у которого числа a и m взаимно просты. А для этого, в свою очередь, достаточно найти такие целые числа u и v, что $au + mv = 1$ (тогда, напомним, число $c = ub$ и будет удовлетворять нашему сравнению); это можно сделать при помощи алгоритма Евклида (см. пример 2.7).

Тем не менее, существуют и другие, более удобные способы решения таких сравнений. Одним из наиболее простых является способ преобразования коэффициентов, но применим он лишь к сравнениям, коэффициенты и модуль которых являются не очень большими числами. Рассмотрим несколько примеров.

Пример 4.3. *Решить сравнение* $5x \equiv 8 \pmod{14}$.

Так как числа 5 и 14 взаимно просты, это сравнение имеет решения, причем все целые числа, удовлетворяющие ему, составляют один класс вычетов по модулю 14. Для того, чтобы найти этот класс, достаточно данное сравнение заменить равносильным ему сравнением вида $x \equiv c \pmod{14}$, где c — некоторое целое число (и тогда решением нашего сравнения будет класс вычетов $\overline{c}$).

Если бы в правой части сравнения $5x \equiv 8 \pmod{14}$ стояло не 8, а число, кратное 5, то сократив обе части сравнения на число 5 (взаимно простое с 14), мы и получили бы требуемое сравнение. В связи с этим, возникает простая идея попробовать заменить наше сравнение равносильным ему, но с правой частью, кратной 5. А для этого достаточно заменить 8 числом, сравнимым с 8 по модулю 14 и кратным 5. Выписывая ряд сравнимых с 8 чисел $8 + 14 = 22$, $8 + 14\cdot 2 = 36$, $8 + 14\cdot 3 = 50$, мы обнаруживаем требуемое число. Таким образом, имеем $8 \equiv 50 \pmod{14}$ и потому наше сравнение равносильно сравнению $5x \equiv 50 \pmod{14}$. Сократив обе части его на 5, получаем $x \equiv 10 \pmod{14}$, и исходное сравнение решено. Это означает, что исходному сравнению удовлетворяют целое число 10, все целые числа, сравнимые с 10 по модулю 14, и только они. Последнее сравнение можно считать и записью ответа; ответ можно записать и в виде "класс вычетов $\overline{10}$ по модулю 14". $\square$

Пример 4.4. *Решить сравнение* $15x \equiv 25 \pmod{35}$.

Наибольший общий делитель 5 чисел 15 и 35 является делителем числа 25, и потому это сравнение разрешимо; более того, оно имеет 5 решений по модулю 35. Для нахождения этих решений рассмотрим сравнение $3x \equiv 5 \pmod 7$, полученное сокращением на 5 обеих частей и модуля исходного сравнения. Так как $5 \equiv 12 \pmod 7$, сравнение $3x \equiv 5 \pmod 7$ равносильно сравнению $3x \equiv 12 \pmod 7$, откуда получаем $x \equiv 4 \pmod 7$. Таким образом, все целые числа, удовлетворяющие исходному сравнению, — это числа из класса вычетов $\overline{4}$ по модулю 7. Для получения пяти различных решений этого сравнения по модулю 35 полагаем $c_0 = 4$, $c_1 = 4 + 7 = 11$, $c_2 = 4 + 2 \cdot 7 = 18$, $c_3 = 4 + 3 \cdot 7 = 25$ и $c_4 = 4 + 4 \cdot 7 = 32$. *Ответ*: решениями исходного сравнения являются классы вычетов $\overline{4}$, $\overline{11}$, $\overline{18}$, $\overline{25}$ и $\overline{32}$ по модулю 35. $\square$

Покажем теперь, как с помощью сравнений вида (1) можно решать *диофантовы уравнения первой степени от двух неизвестных*. Так называются уравнения вида

$$ax + by = c, \tag{2}$$

где a, b и c — целые числа. При этом требуется решить такое уравнение в целых числах, т. е. найти все пары (u, v) целых чисел, для которых справедливо равенство $au + bv = c$. Очевидно, что интересен лишь случай, когда оба числа a и b отличны от нуля.

Пусть $d = (a, b)$ — наибольший общий делитель чисел a и b. Если уравнение (2) имеет целочисленное решение (u, v), то поскольку число d является делителем левой части равенства $au + bv = c$, число c должно делиться на d. Значит, если c не делится на d, уравнение (2) не имеет решений в целых числах. Если c делится на d и если записать

$$a = da_1, \quad b = db_1 \quad \text{и} \quad c = dc_1$$

для подходящих целых чисел a_1, b_1 и c_1, то уравнение (2) будет, очевидно, равносильным уравнению $a_1x + b_1y = c_1$, коэффициенты которого a_1 и b_1 взаимно просты. Таким образом, уравнение (2) либо не имеет решений, либо равносильно уравнению, коэффициенты которого при неизвестных взаимно просты.

Докажем теперь, что если $(a, b) = 1$, то уравнение (2) имеет бесконечное множество решений, и покажем, как найти эти решения.

Рассмотрим сравнение $ax \equiv c \pmod{|b|}$. Так как $(a, |b|) = 1$, из теоремы 4.1 следует, что оно имеет решение. Пусть u_0 — произвольное целое число, удовлетворяющее этому сравнению. Тогда число $c - au_0$ делится на b, и потому уравнение $by = c - au_0$ имеет целое решение v_0. Очевидно, что пара (u_0, v_0) является решением уравнения (2).

Таким образом, мы доказали, что (в случае $(a, b) = 1$) уравнение (2) имеет решение, указав заодно конкретный способ отыскания такого решения. Покажем теперь, что множество всех решений уравнения (2) совпадает с множеством пар (u, v), компоненты u и v которых вычисляются по правилу

$$\begin{cases} u = u_0 - bt \\ v = v_0 + at, \end{cases} \tag{3}$$

где t — произвольное целое число.

В самом деле, так как

$$a(u_0 - bt) + b(v_0 + at) = au_0 + bv_0 = c,$$

любая пара чисел, полученных по формулам (3), является решением уравнения (2). С другой стороны, если пара (u, v) является решением уравнения (2), то имеет место равенство $au + bv = c$. Вычитая из него равенство $au_0 + bv_0 = c$, получаем

$$a(u - u_0) + b(v - v_0) = 0,$$

откуда следует, что число $b(v - v_0)$ должно делиться на a. Так как числа a и b взаимно просты, на a делится число $v - v_0$ и потому для некоторого целого числа t имеем $v = v_0 + at$. Подставив это значение v в равенство $a(u - u_0) + b(v - v_0) = 0$, после сокращения на a получим $u = u_0 - bt$.

Пример 4.5. *Найти все целочисленные решения уравнения* $17x - 16y = 31$.

Найдем решение сравнения $17x \equiv 31 \pmod{16}$. Так как оно равносильно сравнению $x \equiv 31 \pmod{16}$, одним из целых чисел, удовлетворяющих ему, является 15. Таким образом, числа $u_0 = 15$ и $v_0 = 14$ (найденное из уравнения $17 \cdot 15 - 16y = 31$) составляют решение заданного уравнения. Произвольное решение имеет вид $u = 15 + 16t$, $v = 14 + 17t$, где t — любое целое число. $\square$

В заключение этого параграфа докажем утверждение, которое принято теперь называть *Китайской теоремой об остатках*. Речь идет о задаче, которая часто встречается в том или ином виде в различных сборниках занимательных задач и которая в общем виде может быть сформулирована следующим образом:

Если некоторое конечное множество попытаться разделить на m_1 равночисленных частей, то образуется остаток, состоящий из a_1 элементов, если это множество разделить на m_2 равночисленных частей, то образуется остаток, состоящий из a_2 элементов, ... Спрашивается, сколько элементов может содержать данное множество? Около ста лет тому назад была найдена рукопись из Китая, относящаяся примерно к первому веку, в которой приводится в определенном смысле решение этой задачи. Отсюда и название.

Очевидно, что указанная формулировка равносильна задаче нахождения целочисленных решений следующей системы сравнений:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{4}$$

Разумеется, такая система сравнений далеко не всегда имеет решение. Например, целое число, удовлетворяющее первому сравнению системы

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{4}, \end{cases}$$

должно быть нечетным, а любое число, удовлетворяющее второму ее сравнению, обязательно четно. Таким образом, у этой системы сравнений решений нет. Китайская теорема об остатках и дает достаточное условие разрешимости системы сравнений указанного вида:

Теорема 4.2. *Пусть натуральные числа m_1, m_2, ... , m_n попарно взаимно просты (т. е. для любых $i \neq j$ $(m_i, m_j) = 1$). Тогда система сравнений*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{5}$$

имеет решение. Кроме того, произвольные целые числа, являющиеся решениями этой системы, сравнимы между собой по модулю $m = m_1 m_2 \cdots m_n$.

Доказательство. Существование у системы (5) целочисленного решения будем доказывать индукцией по числу n ее сравнений. При $n = 1$ наше утверждение очевидно. Рассмотрим еще случай $n = 2$, так как он будет использоваться при индуктивном переходе. В этом случае наша система имеет вид

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2}. \end{cases}$$

Так как числа m_1 и m_2 взаимно просты, то для подходящих целых чисел u и v выполняется равенство $m_1 u + m_2 v = 1$. Полагая $c = a_2 m_1 u + a_1 m_2 v$, имеем

$$c - a_1 = (a_2 m_1 u + a_1 m_2 v) - a_1 = a_2 m_1 u + a_1(-m_1 u) = m_1 u(a_2 - a_1),$$
$$c - a_2 = (a_2 m_1 u + a_1 m_2 v) - a_2 = a_2(-m_2 v) + a_1 m_2 v = m_2 v(a_1 - a_2).$$

Таким образом, число c сравнимо с a_1 по модулю m_1 и сравнимо с a_2 по модулю m_2 и потому является решением нашей системы.

Предположим теперь, что $n > 1$ и что любая система вида (5), состоящая из $n - 1$ сравнений и удовлетворяющая условиям теоремы, имеет целочисленное решение. Покажем, что тогда и система (5) имеет решение.

По индуктивному предположению подсистема

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots\dots \\ x \equiv a_{n-1} \pmod{m_{n-1}} \end{cases}$$

системы (5) (очевидно, удовлетворяющая условиям теоремы) имеет целочисленное решение; обозначим какое-нибудь ее решение через c'. Полагаем также $m' = m_1 m_2 \cdots m_{n-1}$. Так как число m_n взаимно просто с каждым из чисел m_1, m_2, ... , m_{n-1}, то из утверждения примера 2.3 следует (с помощью очевидного индуктивного рассуждения), что $(m', m_n) = 1$. Поэтому ввиду доказанного выше система из двух сравнений

$$\begin{cases} x \equiv c' \pmod{m'} \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{6}$$

имеет целочисленное решение, скажем, c. Покажем, что число c является искомым решением системы (5), т. е. удовлетворяет каждому сравнению этой системы. Для последнего сравнения из (5) это очевидно, так как оно входит в систему (6). С другой стороны, для любого номера $i = 1, 2, \ldots, n-1$ целое число m_i является делителем числа m', и потому сравнение $c \equiv c' \pmod{m'}$ влечет сравнение $c \equiv c' \pmod{m_i}$. Так как $c' \equiv a_i \pmod{m_i}$ имеем $c \equiv a_i \pmod{m_i}$, так что число c удовлетворяет и остальным сравнениям системы (5). Первое утверждение теоремы доказано.

Для доказательства второго утверждения достаточно заметить, что если числа c и c' являются решениями системы (5), то для любого $i = 1, 2, \ldots, n$ выполнено сравнение $c \equiv c' \pmod{m_i}$. Так как числа m_1, m_2, ... , m_n попарно взаимно просты, из следствия 4 к теореме 2.2 вытекает, что $c \equiv c' \pmod{m}$, что и требовалось доказать. $\square$

Из доказательства теоремы 4.2 можно извлечь и алгоритм нахождения решений систем сравнений вида (5). Тем не менее, в следующем примере будет продемонстрирован другой способ решения таких систем.

Пример 4.6. *Найти наименьшее натуральное число, которое при делении на числа* 5, 9 *и* 8 *дает остатки* 1, 2 *и* 5 *соответственно.*

Искомое число должно удовлетворять системе сравнений

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 2 \pmod{9} \\ x \equiv 5 \pmod{8}. \end{cases}$$

Произвольное целое число x, удовлетворяющее первому сравнению этой системы, имеет вид $x = 1 + 5y$ для некоторого целого числа y. Подставив это выражение вместо x во второе сравнение системы, получаем сравнение относительно y: $1 + 5y \equiv 2 \pmod{9}$. После простых преобразований приходим к сравнению $y \equiv 2 \pmod{9}$, все целочисленные решения которого имеют вид $y = 2 + 9z$. Поэтому числа вида $x = 1 + 5(2 + 9z) = 11 + 45z$ исчерпывают множество целочисленных решений системы первых двух сравнений. Подставив это выражение вместо x в третье сравнение системы, получаем сравнение относительно z: $11 + 45z \equiv 5 \pmod{8}$. Решив его, найдем $z \equiv 2 \pmod{8}$. Таким образом, $z = 2 + 8t$ и $x = 101 + 360t$ для некоторого целого числа t. Следовательно, множество целочисленных решений исходной системы сравнений совпадает с классом вычетов $\overline{101}$ по модулю 360, и 101 является наименьшим натуральным числом в этом классе. $\square$

ЗАДАЧИ К ПАРАГРАФУ 4

4.1. Доказать, что число $5^{21} - 27$ делится на 77.

4.2. Найти остаток от деления числа $9^{45} + 17$ на 56.

4.3. Найти остаток от деления числа $7^{50} + 3$ на 43.

4.4. Найти остаток от деления числа $8^{100} + 11^{100}$ на 19.

4.5. Доказать, что число $6^{50} + 7^{25}$ делится на 11.

4.6. Доказать, что число $8^{16} + 8$ делится на 19.

4.7. Доказать, что число $4^{20} + 4^2$ делится на 17.

4.8. Найти, при каких значениях a число $5^{24} + 7a$ делится на 23.

4.9. Известно, что целое число a удовлетворяет сравнениям $a^{25} \equiv 3 \pmod{79}$ и $a^{26} \equiv 29 \pmod{79}$. Найти остаток от деления числа a на 79.

4.10. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ — многочлен с целыми коэффициентами. Доказать, что если числа $f(2)$ и $f(3)$ делятся на 6, то и число $f(5)$ делится на 6.

4.11. Доказать, что если p — простое число, то для любого числа k , удовлетворяющего неравенствам $1 \leqslant k < p$, биномиальный коэффициент C_p^k делится на p.

4.12. Доказать, что если p — простое число, то для любых целых чисел a и b имеет место сравнение $(a + b)^p \equiv a^p + b^p \pmod{p}$.

4.13. Доказать, что если p — простое число, то для любых целых чисел a и b, удовлетворяющих сравнению $a \equiv b \pmod{p}$, выполнено сравнение $a^p \equiv b^p \pmod{p^2}$.

4.14. Доказать, что если для целых чисел a, b и c имеет место сравнение $50a + 8b + c \equiv 0 \pmod{21}$, то выполнено и сравнение $a + b + 8c \equiv 0 \pmod{21}$.

4.15. Решить сравнение $12x \equiv 15 \pmod{35}$.

4.16. Решить сравнение $21x \equiv 10 \pmod{25}$.

4.17. Решить сравнение $15x \equiv 21 \pmod{18}$.

4.18. Решить сравнение $18x \equiv 12 \pmod{30}$.

4.19. Решить в целых числах уравнение $23x + 15y = 19$.

4.20. Решить в целых числах уравнение $10x - 13y = 25$.

4.21. Найти наименьшие целые положительные значения a и b, при которых уравнение $ax - by = 31$ имеет решение $(5, 9)$.

4.22. Найти наибольшие целые отрицательные значения a и b, при которых уравнение $ax + by = 17$ имеет решение $(5, -7)$.

4.23. На прямой, заданной уравнением $8x - 13y + 6 = 0$, найти количество всех точек с целочисленными координатами, абсциссы которых расположены между -42 и 50.

4.24. Решить систему сравнений

$$\begin{cases} x \equiv 19 \pmod{24} \\ x \equiv 10 \pmod{25}. \end{cases}$$

4.25. Решить систему сравнений

$$\begin{cases} 3x \equiv 5 \pmod{14} \\ 5x \equiv 1 \pmod{9} \\ 7x \equiv 2 \pmod{25}. \end{cases}$$

4.26. Найти уравнения всех прямых, параллельных оси ординат, которые пересекают каждую из прямых $x-5y-2=0$, $x-8y-1=0$ и $x-11y-3=0$ в точках с целочисленными координатами.

4.27. Найти все натуральные числа, не превосходящие числа 300, остатки которых от деления на числа 3, 5 и 8 равны числам 2, 4 и 1 соответственно.

§ 5. Функция Эйлера. Теоремы Эйлера и Ферма

Из предложения 4.2, доказанного в предыдущем параграфе, следует, в частности, что если одно из двух целых чисел, сравнимых между собой по модулю m, является взаимно простым с m, то и другое взаимно просто с m. Поэтому несколько классов вычетов по модулю m состоят только из чисел, взаимно простых с m. Количество таких классов совпадает, очевидно, с количеством взаимно простых с m чисел в произвольной полной системе вычетов по модулю m. Если из полной системы вычетов по модулю m вычеркнуть те числа, которые с m не взаимно просты, то оставшиеся числа будут составлять так называемую *приведенную систему вычетов*. Иначе говоря, мы принимаем следующее определение:

Приведенной системой вычетов по модулю m называется множество чисел, взятых по одному из каждого класса вычетов по модулю m, состоящего из чисел, взаимно простых с m.

Например, числа 1, 2, 3, 4, 5, 6 составляют полную систему вычетов по модулю 6. Взаимно простыми с числом 6 в этой системе являются лишь числа 1 и 5. Они и составляют приведенную систему вычетов по модулю 6. Поэтому произвольное целое число, взаимно простое с числом 6, принадлежит одному из двух классов вычетов $\overline{1}$ и $\overline{5}$ по модулю 6.

Аналогичным образом, одну из приведенных систем вычетов по данному (произвольному) модулю m можно получить из полной системы вычетов (по модулю m) вида 1, 2, ... , m. Поэтому количество чисел в приведенной системе вычетов по модулю m совпадает с количеством чисел, лежащих между 1 и m и взаимно простых с m, т. е. — со значением в точке m функции, играющей важную роль в теории чисел и называемой *функцией Эйлера*. Точное определение этой функции звучит следующим образом:

Функцией Эйлера называется функция $\varphi(x)$, определенная на множестве всех натуральных чисел, значение которой при $x = m$ равно количеству натуральных чисел, не превосходящих m и взаимно простых с m.

Так, непосредственно из определения следует, что $\varphi(1) = 1$, $\varphi(2) = 1$ и, как показано выше, $\varphi(6) = 2$. Заметим еще, что если p — простое число, то всякое натуральное число, меньшее чем p, взаимно просто с p и потому $\varphi(p) = p-1$. Ниже будет получена формула, позволяющая вычислять значение функции Эйлера от произвольного натурального числа m по его каноническому представлению. Для этого необходимо доказать сначала одно из основных свойств функции Эйлера — ее мультипликативность (напомним, что в § 3 была отмечена мультипликативность функций числа делителей $\tau(x)$ и суммы делителей $\sigma(x)$ натурального числа x).

Теорема 5.1. *Если натуральные числа m и n взаимно просты, то $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.*

Доказательство. В соответствии с определением для вычисления $\varphi(mn)$ следует подсчитать количество чисел от 1 до mn, взаимно простых с mn. Расположим

все числа от 1 до mn в таблицу следующим образом:

$$\begin{array}{rrcr}
1 & 2 & \dots & m \\
m+1 & m+2 & \dots & 2m \\
2m+1 & 2m+2 & \dots & 3m \\
\multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\
(n-2)m+1 & (n-2)m+2 & \dots & (n-1)m \\
(n-1)m+1 & (n-1)m+2 & \dots & nm
\end{array}$$

Нам надлежит в этой таблице, состоящей из n строк и m столбцов, выбрать все числа, взаимно простые с числом mn.

Легко видеть, что произвольное целое число будет взаимно простым с числом mn тогда и только тогда, когда оно одновременно является взаимно простым и с числом m, и с числом n (необходимость почти очевидна, а достаточность доказана в примере 2.4). Поэтому нам достаточно сначала выбрать из этой таблицы те числа, которые взаимно просты с m, а затем среди этих чисел найти те, которые взаимно просты с n.

Для любого номера $k = 1, 2, \dots, m$ числа, расположенные в k-ом столбце, имеют вид k, $m+k$, $2m+k$, $\dots$, $(n-2)m+k$, $(n-1)m+k$ и потому все они лежат в одном и том же классе вычетов по модулю m, представляемом числом k. Поэтому, если хотя бы одно из чисел этого столбца взаимно просто с m, то и все расположенные в нем числа взаимно просты с m. Следовательно, все числа из таблицы, взаимно простые с m, заполняют целиком несколько ее столбцов, причем, поскольку k-ый столбец состоит из взаимно простых с m чисел тогда и только тогда, когда $(k, m) = 1$, количество таких столбцов совпадает с количеством чисел, лежащих между 1 и m и взаимно простых с m, т. е. равно $\varphi(m)$.

Покажем теперь, что для любого $k = 1, 2, \dots, m$ числа k-ого столбца таблицы, т. е. числа вида $im+k$, где $i = 0, 1, \dots, n-1$, составляют полную систему вычетов по модулю n. Поскольку их количество равно n, для этого достаточно показать, что никакие два из них не принадлежат одному и тому же классу вычетов по модулю n. Пусть, напротив, для некоторых номеров i и j, где $0 \leqslant i < j \leqslant n-1$, имеет место сравнение

$$im + k \equiv jm + k \pmod{n}.$$

Прибавив к обеим его частям число $-k$ и сократив обе части полученного сравнения на общий множитель m (напомним, взаимно простой с модулем n), придем к сравнению $i \equiv j \pmod{n}$, которое несовместимо с неравенствами $0 \leqslant i < j \leqslant n-1$.

Итак, мы доказали, что числа каждого столбца нашей таблицы составляют полную систему вычетов по модулю n. Поэтому числа, расположенные в этом столбце и взаимно простые с n, составляют приведенную систему вычетов по этому модулю. Так как любая приведенная система вычетов по модулю n состоит из $\varphi(n)$ чисел, отсюда следует, что каждый столбец таблицы содержит в точности $\varphi(n)$ чисел, взаимно простых с n. Следовательно, числа, взаимно простые с числом m, занимают целиком $\varphi(m)$ столбцов, в каждом из которых расположено $\varphi(n)$ чисел, взаимно простых с n, и потому количество чисел в таблице, взаимно простых и

с m, и с n, равно $\varphi(m)\cdot\varphi(n)$. Равенство $\varphi(mn)=\varphi(m)\cdot\varphi(n)$, таким образом, доказано. $\square$

Прежде, чем приступить к выводу формулы для вычисления функции Эйлера от произвольного натурального аргумента, рассмотрим сначала следующий частный случай:

Предложение 5.1. *Пусть p — простое число. Для любого целого числа $n\geqslant 1$ выполнено равенство $\varphi(p^n)=p^n-p^{n-1}$.*

Очевидно (ввиду утверждений, доказанных в § 2), что произвольное натуральное число взаимно просто с числом p^n (где $n\geqslant 1$) тогда и только тогда, когда оно взаимно просто с числом p. Поэтому для доказательства предложения 5.1 можно сосчитать количество чисел от 1 до p^n, взаимно простых с числом p. Мы подсчитаем количество тех чисел от 1 до p^n, которые не взаимно просты с числом p. Поскольку произвольное целое число не является взаимно простым с простым числом p тогда и только тогда, когда оно делится на p, все такие числа имеют вид pa для некоторого целого числа a и удовлетворяют неравенствам $1\leqslant pa\leqslant p^n$. Из неравенства $pa\leqslant p^n$ следует неравенство $a\leqslant p^{n-1}$, а из неравенства $1\leqslant pa$ следует неравенство $a\geqslant 1$. Обратно, из неравенства $1\leqslant a\leqslant p^{n-1}$ следует неравенство $1\leqslant pa\leqslant p^n$, и потому интересующие нас числа получаются при $a=1,2,\ldots,p^{n-1}$. Следовательно, среди чисел от 1 до p^n количество не взаимно простых с p равно p^{n-1}, так что $\varphi(p^n)=p^n-p^{n-1}$. $\square$

Предложение 5.1 дает формулу для вычисления функции $\varphi(m)$ в том случае, когда m является степенью некоторого простого числа p. Заметим, что если $m=p^n$, то формула $\varphi(m)=p^n-p^{n-1}$, доказанная в предложении 5.1, может быть записана и в каждом из следующих двух видов:

$$\varphi(m)=p^{n-1}(p-1),\qquad \varphi(m)=m\left(1-\frac{1}{p}\right).$$

В общем случае имеет место

Предложение 5.2. *Пусть $m=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ — каноническое представление натурального числа $m>1$. Тогда*

$$\varphi(m)=p_1^{k_1-1}p_2^{k_2-1}\cdots p_r^{k_r-1}(p_1-1)(p_2-1)\cdots(p_r-1),$$

а также

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

Для доказательства предложения 5.2 достаточно заметить, что поскольку числа $p_1^{k_1}$, $p_2^{k_2}$, ... ,$p_r^{k_r}$ попарно взаимно просты, из теоремы 5.1 очевидной индукцией по r получаем

$$\varphi(m)=\varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_r^{k_r}).$$

Теперь остается применить предложение 5.1 и следующие за ним замечания. $\square$

Решим несколько задач, связанных с функцией Эйлера.

Пример 5.1. *Найти количество тех натуральных чисел, не превосходящих числа* 180, *которые не являются взаимно простыми с числом* 60.

Так как $180 = 2^2 \cdot 3^2 \cdot 5$ и $60 = 2^2 \cdot 3 \cdot 5$, произвольное целое число является взаимно простым с числом 60 тогда и только тогда, когда оно взаимно просто с числом 180. Поэтому количество чисел, не превосходящих 180 и взаимно простых с числом 60, совпадает с количеством чисел, не превосходящих 180 и взаимно простых с числом 180, а количество таких чисел равно $\varphi(180) = 2 \cdot 3 \cdot (2-1) \cdot (3-1) \cdot (5-1) = 48$. Таким образом, количество тех натуральных чисел, не превосходящих числа 180, которые не являются взаимно простыми с числом 60, равно $180 - 48 = 132$. $\square$

Пример 5.2. *Найти количество натуральных чисел, не превосходящих числа* 385 *и взаимно простых с числом* 77.

Так как $385 = 5 \cdot 77$, из теоремы о делении с остатком следует, что произвольное натуральное число, меньшее чем 385, однозначно представимо в виде $77q + r$, где $0 \leqslant r < 77$ и $0 \leqslant q < 5$. Легко видеть, далее, что число вида $77q + r$ взаимно просто с 77 тогда и только тогда, когда число r взаимно просто с 77. Поэтому при фиксированном q количество чисел вида $77q + r$, взаимно простых с 77, равно $\varphi(77) = 24$. А так как число q принимает 5 значений, количество натуральных чисел, не превосходящих числа 385 и взаимно простых с числом 77, равно $5 \cdot 24 = 120$. $\square$

Пример 5.3. *Найти натуральное число* x, *если известно, что* $\varphi(10^x) = 4000$.

Так как из равенства $\varphi(10^x) = 4000$ следует, очевидно, что $x > 0$, в силу предложения 5.2 имеем

$$\varphi(10^x) = \varphi(2^x \cdot 5^x) = 2^{x-1} \cdot 5^{x-1} \cdot (2-1) \cdot (5-1) = 4 \cdot 2^{x-1} \cdot 5^{x-1},$$

и потому исходное равенство принимает вид

$$2^{x-1} \cdot 5^{x-1} = 2^3 \cdot 5^3.$$

Ввиду однозначности разложения на простые множители имеем $x = 4$. $\square$

Следующее утверждение, играющее чрезвычайно важную роль в теории чисел, называется *теоремой Эйлера*:

Теорема 5.2. *Если целое число* a *взаимно просто с натуральным числом* m, *то*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{1}$$

Доказательство. Выберем некоторую приведенную систему вычетов по модулю m

$$b_1, b_2, \ldots b_k \tag{2}$$

(где, разумеется, $k = \varphi(m)$). Покажем, что тогда числа

$$ab_1, ab_2, \ldots ab_k \tag{3}$$

также составляют приведенную систему вычетов по модулю m. Так как каждое из чисел ab_1, ab_2, ... ab_k взаимно просто с m (почему?) и их количество совпадает с $\varphi(m)$, то для этого достаточно показать, что никакие два числа из системы (3) не принадлежат одному и тому же классу вычетов по модулю m. Но это почти очевидно: если для некоторых номеров i и j имеет место сравнение $ab_i \equiv ab_j \pmod m$, то после сокращения его частей на общий множитель a, взаимно простой с модулем m, мы получаем сравнение $b_i \equiv b_j \pmod m$, откуда следует равенство $i = j$, так как различные числа из системы (2) должны лежать в разных классах по модулю m.

Итак, мы имеем две приведенные системы вычетов по модулю m. Это означает, что каждое число из системы (3) должно находиться в одном классе вычетов по модулю m с одним и только одним из чисел системы (2). Другими словами, имеет место следующая система сравнений

$$\begin{aligned} ab_1 &\equiv c_1 \pmod m \\ ab_2 &\equiv c_2 \pmod m \\ &\dots\dots\dots\dots\dots \\ ab_k &\equiv c_k \pmod m, \end{aligned} \tag{4}$$

где каждое из чисел c_1, c_2, ... c_k совпадает с одним и только с одним из чисел системы (2). Это означает, в частности, справедливость равенства

$$c_1 c_2 \cdots c_k = b_1 b_2 \cdots b_k,$$

откуда следует, что после почленного перемножения всех сравнений из (4) мы получим сравнение

$$a^k \cdot b_1 b_2 \cdots b_k \equiv b_1 b_2 \cdots b_k \pmod m.$$

Сокращая обе части его на число $b_1 b_2 \cdots b_k$, взаимно простое с модулем m, и вспоминая, что $k = \varphi(m)$, мы получаем сравнение (1). Теорема Эйлера доказана. □

Частный случай теоремы Эйлера, когда m является простым числом, носит название *теоремы Ферма*. Она формулируется следующим образом:

Теорема 5.3. *Пусть p — простое число. Если целое число a не делится на p, то*

$$a^{p-1} \equiv 1 \pmod p. \tag{5}$$

Действительно, так как для простого числа p имеет место равенство $\varphi(p) = p - 1$, то это утверждение является очевидным следствием теоремы Эйлера. □

В ряде случаев удобно пользоваться другой формулировкой теоремы Ферма:

Теорема 5.3′. *Если p — простое число, то для любого целого числа a выполнено сравнение*

$$a^p \equiv a \pmod p. \tag{6}$$

Покажем, в самом деле, что теоремы 5.3 и 5.3′ равносильны. Если сначала предположить справедливым утверждение теоремы 5.3, то в случае, когда число

a не делится на p (и потому выполнено сравнение (5)) сравнение (6) получается из (5) умножением обеих частей на a. Если же a делится на p, то сравнение (6) имеет место просто потому, что каждое из чисел a^p и a сравнимо с 0 по модулю p. Обратно, если для любого целого числа a выполнено сравнение (6) и если взять число a, не делящееся на p, то поскольку тогда $(a,p)=1$, мы можем сократить на a обе части (6) и получить сравнение (5). $\square$

Теоремы Эйлера и Ферма имеют многочисленные применения в теории чисел и других областях математики. Приведем примеры применения этих теорем для решения задач о делимости целых чисел.

Пример 5.4. *Доказать, что для любого целого числа a число $a^{13}-a$ делится на 7.*

Так как $a^{13}-a=a(a^6-1)(a^6+1)=(a^7-a)(a^6+1)$, достаточно доказать, что на 7 делится число a^7-a. Но поскольку число 7 является простым, это следует из теоремы 5.3′. $\square$

Пример 5.5. *Найти остаток от деления числа 2^{30} на 13.*

По теореме Ферма имеем $2^{12}\equiv 1 \pmod{13}$, откуда возведением в квадрат получаем $2^{24}\equiv 1 \pmod{13}$. Следовательно, $2^{30}=2^{24}\cdot 2^6\equiv 2^6=64\equiv -1\equiv 12 \pmod{13}$, и потому искомый остаток равен 12. $\square$

Пример 5.6. *Доказать, что если целое число a не делится на 5, то на 5 делится в точности одно из чисел a^2+1 и a^2-1.*

Заметим, прежде всего, что оба числа a^2+1 и a^2-1 на 5 делиться не могут, так как в противном случае на 5 делилась бы и разность этих чисел, равная 2.

С другой стороны, из теоремы Ферма следует, что число a^4-1 делится на 5, и так как $a^4-1=(a^2+1)(a^2-1)$, из предложения 3.2 следует, что хотя бы одно из чисел a^2+1 и a^2-1 должно делиться на 5. $\square$

Пример 5.7. *Найти все такие натуральные числа n, что число 2^n-9 делится на 7.*

Число 2^n-9 делится на 7 тогда и только тогда, когда имеет место сравнение $2^n\equiv 9 \pmod{7}$, которое равносильно сравнению $2^n\equiv 2 \pmod{7}$. По теореме Ферма имеем сравнение $2^6\equiv 1 \pmod{7}$. Поэтому если число n представить в виде $n=6q+r$, где $0\leqslant r<6$, то выполнено сравнение

$$2^n=(2^6)^q\cdot 2^r\equiv 2^r \pmod{7},$$

откуда следует, что сравнение $2^n\equiv 2 \pmod{7}$ справедливо тогда и только тогда, когда справедливо сравнение $2^r\equiv 2 \pmod{7}$. Непосредственная проверка показывает, что среди чисел, удовлетворяющих неравенствам $0\leqslant r<6$, последнему сравнению удовлетворяют лишь 1 и 4. Таким образом, исходное сравнение имеет место тогда и только тогда, когда число n имеет вид $n=6q+1$ или $6q+4$. Так как в первом случае $n=3(2q)+1$, а во втором $n=3(2q+1)+1$, окончательный ответ можно сформулировать следующим образом: число 2^n-9 делится на 7 тогда и только тогда, когда число n при делении на 3 дает в остатке 1. $\square$

В заключение отметим, что теорема Эйлера предоставляет нам еще один способ решения сравнений вида $ax \equiv b \pmod m$, где числа a и m взаимно просты (напомним, что к этому случаю сводится решение произвольного сравнения указанного вида). Продемонстрируем этот способ на примере решения сравнения из примера 4.3: $5x \equiv 8 \pmod{14}$. Так как $\varphi(14) = 6$, по теореме Эйлера $5^6 \equiv 1 \pmod{14}$. Поэтому, умножив обе части данного нам сравнения на число 5^5, получаем (равносильное исходному) сравнение $5^6 x \equiv 8 \cdot 5^5 \pmod{14}$ или $x \equiv 8 \cdot 5^5 \pmod{14}$. Остается упростить правую часть этого сравнения:

$$x \equiv 8 \cdot 5^5 = 8 \cdot 5 \cdot (5^2)^2 \equiv (-2) \cdot (-3)^2 = -18 \equiv 10 \pmod{14}.$$

ЗАДАЧИ К ПАРАГРАФУ 5

5.1. Найти натуральное число x, если $\varphi(6^x) = 72$.

5.2. Найти натуральное число x, если $\varphi(12^x) = 6912$.

5.3. Найти натуральное число x, если $\varphi(15^x) = 1800$.

5.4. Найти натуральное число a, если $\varphi(a) = 108$ и $a = 3^m \cdot 7^n$ для некоторых натуральных чисел m и n.

5.5. Найти натуральное число a, если $\varphi(a) = 440$ и $a = 2^m \cdot 11^n$ для некоторых натуральных чисел m и n.

5.6. Найти натуральное число a, если $\varphi(a) = 936$ и $a = 3^m \cdot 13^n$ для некоторых натуральных чисел m и n.

5.7. Найти количество натуральных чисел, не превосходящих числа 605 и имеющих с этим числом наибольший общий делитель, равный 5.

5.8. Доказать, что для любого целого числа $m \geqslant 2$ сумма всех натуральных чисел, не превосходящих числа m и взаимно простых с m, равна $\dfrac{1}{2} m \cdot \varphi(m)$.

5.9. Найти остаток от деления числа 3^{50} на 17.

5.10. Найти остаток от деления числа 21^{83} на 24.

5.11. Найти остаток от деления числа 35^{150} на 425.

5.12. Найти остаток от деления числа $3^{100} + 4^{100}$ на 7.

5.13. Найти остаток от деления числа $3 \cdot 5^{75} + 4 \cdot 7^{100}$ на 132.

5.14. Доказать, что если целое число a не делится на 5, то число $a^{12} - 1$ делится на 5.

5.15. Доказать, что если p — простое число, то для любых целых чисел a и b число $a^p - b$ делится на p тогда и только тогда, когда число $a - b$ делится на p.

5.16. Доказать, что если число $a^{6m} + a^{6n}$ делится на 7, то и число a делится на 7.

5.17. Доказать, что если число $a^{10m} + a^{10n}$ делится на 11, то и число a делится на 11.

5.18. Доказать, что если каждое из целых чисел a и b взаимно просто с числом 65, то число $a^{12} - b^{12}$ делится на 65.

5.19. Доказать, что если целые числа a и b взаимно просты, то каждое из чисел $2a^5 + b^5$ и $2a^5 - b^5$ не делится на 11.

5.20. Доказать, что если целые числа a и b взаимно просты, то каждое из чисел $2a^3 + b^3$ и $2a^3 - b^3$ не делится на 7.

5.21. Доказать, что если целые числа a и b взаимно просты, то каждое из чисел $2a^3 + b^3$ и $2a^3 - b^3$ не делится на 13.

5.22. Найти все такие натуральные числа n, что число $2^n - 1$ делится на 5.

5.23. Пусть p и q — такие различные простые числа, что число $p-1$ является делителем числа $q-1$. Доказать, что для любого целого числа a, взаимно простого с pq, имеет место сравнение

$$a^{q-1} \equiv 1 \pmod{pq}.$$

5.24. Доказать, что если p и q произвольные простые числа, то для любого целого числа имеет место сравнение

$$qa^p + pa^q \equiv (p+q)a \pmod{pq}.$$

5.25. Доказать, что для любых неравных простых чисел p и q имеет место сравнение $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

5.26. В задаче 4.12 утверждалось, что для произвольных целых чисел a и b и простого числа p имеет место сравнение $(a+b)^p \equiv a^p + b^p \pmod{p}$. С помощью этого утверждения доказать теорему Ферма. (Поскольку утверждение задачи 4.12 можно доказать без использования теоремы Ферма, тем самым получается еще одно доказательство этой теоремы.)

§ 6. Позиционные системы обозначений натуральных чисел. Признаки делимости

Уже в давние времена возникла острая практическая потребность в удобной системе обозначений натуральных чисел. Выше мы ввели значок 1 для обозначения наименьшего натурального числа. Для обозначения числа $1+1$, непосредственно следующего за числом 1, мы пользуемся значком 2, число $2+1$ мы обозначаем значком 3, ... Понятно, что продолжать аналогичным образом, вводя свой значок для обозначения каждого нового встретившегося нам числа, весьма неразумно и неудобно. Поэтому уже в древности были придуманы различные системы обозначений, позволявшие с использованием небольшого набора значков (или цифр) записывать достаточно много чисел. Такие системы бывают позиционными и непозиционными. Та десятичная система обозначений, которой мы пользуемся в настоящее время является позиционной. Это название происходит от того, что значение каждой цифры зависит от того места, которое эта цифра занимает в записи числа. Система записи чисел с помощью римских цифр является примером непозиционной системы.

Позиционная система записи натуральных чисел не обязательно должна быть десятичной. В разные исторические периоды разные народы пользовались двенадцатиричными, шестидесятиричными и другими позиционными системами. В современной вычислительной технике используется двоичная система. Возможность записи произвольного натурального числа в позиционной системе обозначений с произвольным (фиксированным) основанием b (или, как говорят, в системе счисления с основанием b) основана на следующем утверждении:

Предложение 6.1. *Пусть $b>1$ — фиксированное натуральное число. Произвольное натуральное число a может быть представлено и притом единственным способом в виде*

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0, \tag{1}$$

где $n \geqslant 0$, для любого $i = 0, 1, \ldots, n$ целое число c_i удовлетворяет неравенствам $0 \leqslant c_i \leqslant b-1$ и при $n>0$ $c_n \neq 0$.

Доказательство. Начнем с доказательства существования представления числа a в виде (1), для чего воспользуемся индукцией по числу a.

Предварительно заметим, что если $a<b$, возможность такого представления числа a просто очевидна: достаточно взять $n=0$ и $c_0 = a$.

Основание индукции, т. е. справедливость доказываемого утверждения при $a=1$, вытекает непосредственно из этого замечания. Предположим поэтому, что $a>1$ и что произвольное натуральное число, меньшее, чем a, может быть записано в виде (1). Покажем, что тогда и число a можно записать в таком виде. В силу замечания из предыдущего абзаца, это достаточно проделать в предположении, что $a \geqslant b$.

Итак, предполагая выполненным неравенство $a \geqslant b$, разделим число a на b с остатком: найдем такие числа q и r, что $a = bq + r$ и $0 \leqslant r < b$. Переписывая неравенство $a \geqslant b$ в виде $bq + r \geqslant b$ и учитывая, что $b - r > 0$, имеем $bq > 0$ и потому

$q \geqslant 1$. С другой стороны, так как $b > 1$, то $q < bq = a - r \leqslant a$. Таким образом, q — натуральное число, меньшее, чем a, и потому в силу индуктивного предположения его можно записать в виде (1), т. е.

$$q = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0$$

для некоторых целых чисел $m \geqslant 0$ и d_0, d_1, ... , d_m таких, что $0 \leqslant d_i \leqslant b - 1$ для $i = 0, 1, \ldots, m$ и $d_m \neq 0$. Так как тогда

$$\begin{aligned} a = b(d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0) + r \\ = d_m b^{m+1} + d_{m-1} b^m + \cdots + d_1 b^2 + d_0 b + r, \end{aligned}$$

мы получаем представление числа a в виде (1), где $n = m + 1$, $c_0 = r$ и для $i = 1, 2, \ldots, n$ $c_i = d_{i-1}$. Индуктивный переход закончен, и существование представления натуральных чисел в виде (1) доказано.

Докажем теперь единственность такого представления. Индукцией по числу a докажем, что если

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0, \tag{2}$$

где $n \geqslant 0$, $0 \leqslant c_i \leqslant b - 1$ $(i = 0, 1, \ldots, n)$ и $c_n \neq 0$, а также

$$a = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0, \tag{3}$$

где $m \geqslant 0$, $0 \leqslant d_j \leqslant b - 1$ $(j = 0, 1, \ldots, m)$ и $d_m \neq 0$, то $n = m$ и для каждого $i = 0, 1, \ldots, n$ выполнено равенство $c_i = d_i$.

Заметим, что если в равенстве (2) $n \geqslant 1$ (или в равенстве (3) $m \geqslant 1$), то $a \geqslant b$. Действительно, поскольку $c_n \geqslant 1$ и все слагаемые в (2) неотрицательны, имеем $a \geqslant c_n b^n \geqslant b^n \geqslant b$. Разумеется, справедливо и обратное: если $a \geqslant b$, то $n \geqslant 1$ и $m \geqslant 1$.

Отсюда следует, в частности, что если $a = 1$, то $n = 0 = m$ и $c_0 = 1 = d_0$, так что мы располагаем основанием индукции. Тот же вывод справедлив и при $a < b$, и потому в индуктивном шаге можно предполагать, что $a \geqslant b$. Тогда $n \geqslant 1$, $m \geqslant 1$ и потому равенства (2) и (3) можно переписать в виде

$$a = b(c_n b^{n-1} + c_{n-1} b^{n-2} + \cdots + c_1) + c_0 \tag{4}$$

и

$$a = b(d_m b^{m-1} + d_{m-1} b^{m-2} + \cdots + d_1) + d_0, \tag{5}$$

соответственно. Так как $0 \leqslant c_0 < b$, равенство (4) говорит о том, что c_0 является остатком, а $c_n b^{n-1} + c_{n-1} b^{n-2} + \cdots + c_1$ неполным частным от деления числа a на b. Аналогично, из (5) следует, что остатком и неполным частным от деления a на b служат числа d_0 и $d_m b^{m-1} + d_{m-1} b^{m-2} + \cdots + d_1$ соответственно. Из утверждения единственности в теореме о делении с остатком теперь следует, что $c_0 = d_0$ и

$$c_n b^{n-1} + c_{n-1} b^{n-2} + \cdots + c_1 = d_m b^{m-1} + d_{m-1} b^{m-2} + \cdots + d_1.$$

Так как левая и правая части этого равенства являются представлениями в виде (1) натурального числа, меньшего чем a, из индуктивного предположения следует, что $n = m$ и для всех $i = 1, 2, \ldots, n$ $c_i = d_i$. Этим завершен индуктивный шаг, и предложение 6.1 доказано. $\square$

Из предложения 6.1 следует, что при фиксированном числе $b > 1$ произвольное натуральное число однозначно определяется конечной последовательностью, составленной из чисел 0, 1, ... , $b-1$. Если для обозначения каждого из этих чисел фиксировать определенный значок и назвать эти значки цифрами, то произвольному натуральному числу можно будет взаимно однозначно сопоставить некоторую последовательность цифр, называемую записью этого числа в системе счисления с основанием b (или в b-ичной системе счисления). А именно, если натуральное число a представлено в виде (1), т. е.

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0, \tag{6}$$

где $n \geqslant 0$, $0 \leqslant c_i \leqslant b-1$ $(i = 0, 1, \ldots, n)$ и $c_n \neq 0$, то мы запишем (считая уже c_0, c_1, ... , c_n обозначениями цифр)

$$a = \overline{c_n c_{n-1} \ldots c_1 c_0}_b. \tag{7}$$

Правую часть равенства (7) и называют *записью натурального числа a в системе счисления с основанием b*. Индекс b в этой записи можно опускать, если из контекста ясно, какая система счисления рассматривается. Верхняя черта ставится для того, чтобы отличить эту запись от произведения соответствующих чисел; ее также можно опускать, если это не приводит к недоразумениям. Подчеркнем еще раз, что равенство (7) является по существу сокращенной записью равенства (6).

С давних времен подавляющая часть человечества пользуется десятичной записью натуральных чисел с так называемыми арабскими цифрами 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (некоторые историки полагают, впрочем, что эти обозначения пришли к нам из Индии). Этими же цифрами можно пользоваться и в системах счисления с основанием $b < 10$. Если же $b > 10$, то приходится вводить дополнительные обозначения для недостающих цифр. Договоримся, например, в двенадцатиричной системе для обозначения недостающих цифр 10 и 11 (записанных пока в десятичной системе) употреблять здесь значки $\triangle$ и ∇ соответственно.

Рассмотрим несколько примеров перехода от записи числа в десятичной системе к его записи в другой системе счисления. Соответствующий алгоритм вытекает из доказательства предложения 6.1. Условимся, что отсутствие верхней черты и индекса у записи числа означает, что эта запись десятичная.

Пример 6.1. *Записать число* 231 *в пятиричной системе счисления.*

Для решения этой задачи выполняем следующие шаги:
1. Делим с остатком число 231 на 5: $231 = 5 \cdot 46 + 1$.
2. Делим с остатком число 46 на 5: $46 = 5 \cdot 9 + 1$.
3. Делим с остатком число 9 на 5: $9 = 5 \cdot 1 + 4$.
4. Делим с остатком число 1 на 5: $1 = 5 \cdot 0 + 1$.

На этом вычисления останавливаются. Таким образом, процедура вычислений заканчивается, когда очередное неполное частное оказалось равным нулю. (Разумеется, ее можно было бы остановить уже на предыдущем шаге, когда неполное частное оказалось числом, меньшим чем 5; тем не менее, при наличии последнего шага удобнее формулировать правило выписывания ответа.)

Последовательность полученных остатков, выписываемая в обратном порядке, начиная с последнего, и будет искомой последовательностью цифр пятиричной записи числа 231:

$$231 = \overline{1411}_5.$$

Для проверки полученного результата нам достаточно вспомнить, что запись $a = \overline{1411}_5$ означает, что

$$a = 1 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5 + 1.$$

Выполнив эти действия (в десятичной системе), мы убедимся в правильности ответа. □

Пример 6.2. *Записать число* 5015 *в двенадцатиричной системе счисления.*

Выполняем последовательные деления с остатком, как в предыдущей задаче:
1. $5015 = 12 \cdot 417 + 11$.
2. $417 = 12 \cdot 34 + 9$.
3. $34 = 12 \cdot 2 + 10$.
4. $2 = 12 \cdot 0 + 2$.

Таким образом, $5015 = \overline{2\triangle 9\nabla}_{12}$. □

Обычные правила сложения и умножения "столбиком" и деления "уголком" сохраняются и для систем счисления с произвольным основанием; достаточно лишь создать и запомнить соответствующие таблицы сложения и умножения цифр. Не вдаваясь здесь в дальнейшие детали, перейдем к признакам делимости.

Признаком делимости на фиксированное натуральное число $m > 1$ называют условия, которым должны удовлетворять цифры записи данного числа a в некоторой системе счисления, необходимые и достаточные для того, чтобы число a делилось на m. Типичными примерами являются следующие известные признаки (в десятичной системе счисления):

Число делится на 2 *(на* 5*) тогда и только тогда, когда его последняя цифра делится на* 2 *(соответственно, на* 5*).*

Число делится на 3 *(на* 9*) тогда и только тогда, когда сумма его цифр делится на* 3 *(соответственно, на* 9*).*

Эти (и многие другие) признаки делимости обобщаются на системы счисления с произвольным основанием и являются конкретными проявлениями действия следующего общего утверждения, называемого *признаком Паскаля*:

Предложение 6.2. *Пусть $b > 1$ и $m > 1$ некоторые натуральные числа. Для произвольного целого числа $k \geqslant 0$ обозначим через r_k наименьшее по абсолютной величине число, сравнимое с b^k по модулю m. Пусть*

$$a = \overline{c_n c_{n-1} \ldots c_1 c_0}_b$$

— запись числа a в системе счисления с основанием b. Число a делится на m тогда и только тогда, когда на m делится число

$$c_0 r_0 + c_1 r_1 + \cdots + c_n r_n.$$

Доказывается это утверждение совсем просто. Действительно, по определению чисел r_k для каждого k имеет место сравнение $b^k \equiv r_k \pmod{m}$, откуда для любого $k = 0, 1, \ldots, n$ получаем $c_k b^k \equiv c_k r_k \pmod{m}$. Следовательно,

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 \equiv c_n r_n + c_{n-1} r_{n-1} + \cdots + c_1 r_1 + c_0 r_0 \pmod{m},$$

и остается заметить, что если одно из двух чисел, сравнимых по модулю m, делится на m, то и другое тоже делится на m. $\square$

Приведем ряд конкретных признаков делимости, вытекающих из предложения 6.2.

Следствие 1. *Пусть число m является делителем числа b. Натуральное число a делится на m тогда и только тогда, когда на m делится последняя цифра записи числа a в системе счисления с основанием b.*

Действительно, если $m \mid b$, то $r_0 = 1$, а для любого $k > 0$ имеем, очевидно, $r_k = 0$. Поэтому

$$c_0 r_0 + c_1 r_1 + \cdots + c_n r_n = c_0. \quad \square$$

В десятичной системе счисления утверждение следствия 1 превращается в известные признаки делимости на 2 и на 5.

Следствие 2. *Пусть число m является делителем числа $b-1$. Натуральное число a делится на m тогда и только тогда, когда на m делится сумма всех цифр записи числа a в системе счисления с основанием b.*

В этом случае имеем $b \equiv 1 \pmod{m}$, и потому все числа r_k из формулировки предложения 6.2 равны 1. Отсюда

$$c_0 r_0 + c_1 r_1 + \cdots + c_n r_n = c_0 + c_1 + \cdots + c_n. \quad \square$$

В десятичной системе счисления утверждение следствия 2 превращается в известные признаки делимости на 3 и на 9.

Следствие 3. *Пусть число m является делителем числа $b+1$. Натуральное число a делится на m тогда и только тогда, когда на m делится разность суммы всех цифр, стоящих на четных местах в записи числа a в системе счисления с основанием b, и суммы всех цифр, стоящих на нечетных местах.*

В этом случае имеем $b \equiv -1 \pmod{m}$, и потому для любого $k \geqslant 0$ $b^k \equiv (-1)^k \pmod{m}$. Отсюда

$$c_0 r_0 + c_1 r_1 + \cdots + c_n r_n = c_0 - c_1 + c_2 - \cdots + (-1)^n c_n. \quad \square$$

В десятичной системе счисления следствие 3 дает признак делимости на 11.

Тем же способом можно получить и другие признаки делимости, но они уже будут более сложными и потому менее употребительными. Другой подход к признакам делимости целых чисел можно найти в книжке [5].

ЗАДАЧИ К ПАРАГРАФУ 6

6.1. Найти основание системы счисления b, если
а) $\overline{12}_b + \overline{13}_b = \overline{30}_b$;
б) $\overline{12}_b + \overline{13}_b = \overline{30}_b$;
в) $\overline{89}_b + \overline{69}_b = \overline{103}_b$;
г) $\overline{72}_b + \overline{5}_b = \overline{80}_b$.

6.2. Найти основание системы счисления b, если $\overline{1241}_5 = \overline{304}_b$.

6.3. Найти основание системы счисления b, если $\overline{41}_8 = \overline{201}_b$.

6.4. Натуральное число, запись которого в десятичной системе состоит из трех цифр, в системе счисления с основанием 9 записывается теми же цифрами, но в обратном порядке. Найти это число.

6.5. Показать, что в системе счисления с основанием $b \geqslant 3$ квадрат числа $b-1$ записывается теми же цифрами, что и удвоенное число $b-1$, но взятыми в обратном порядке.

6.6. Записать в системе счисления с основанием n число, равное сумме первых n натуральных чисел.

6.7. Доказать, что для любого натурального $b > 4$ число $\overline{144}_b$ является квадратом некоторого натурального числа.

6.8. Доказать, что для любого натурального $b > 3$ число $\overline{1331}_b$ является кубом некоторого натурального числа.

В последующих задачах речь идет о десятичной записи натуральных чисел.

6.9. Найти все натуральные числа вида $\overline{aba}$, делящиеся на 15.

6.10. Найти все натуральные числа вида $\overline{aba}$, делящиеся на 33.

6.11. Сумма двузначного числа m и числа, записанного теми же цифрами, но в обратном порядке, является квадратом некоторого целого числа. Найти все такие числа m.

6.12. Сумма цифр трехзначного числа равна 7. Доказать, что это число делится на 7 тогда и только тогда, когда две последние цифры его совпадают.

6.13. Найти двузначное число, равное сумме куба своей первой цифры и квадрата второй цифры.

6.14. Доказать, что четырехзначное число, у которого одинаковы первая и третья цифры, а также — вторая и четвертая цифры, не может быть квадратом целого числа.

6.15. Два двузначных числа, записанные одно за другим, образуют четырехзначное число, делящееся на их произведение. Найти эти числа.

§ 7. Кольцо целых гауссовых чисел. Пример кольца с неоднозначным разложением

В этом параграфе мы увидим, что определенная часть утверждений о делимости целых чисел может быть перенесена на произвольные кольца. При этом от кольца K мы будем требовать только одно: K должно быть целостным кольцом (и это требование совершенно естественное, если мы хотим получить теорию делимости, хоть сколько-нибудь похожую на теорию делимости целых чисел). Таким образом, мы договариваемся, что всюду в этом параграфе термин "кольцо" будет обозначать целостное кольцо.

Общие определения и утверждения мы будем иллюстрировать на примере двух конкретных колец, элементами которых являются некоторые комплексные числа. Поэтому для понимания материала, содержащегося в этом параграфе, необходимо начальное знакомство с комплексными числами. Впрочем, нам будет достаточно знать, что комплексными числами называют числа вида $a + b\,i$, где a и b — действительные числа и i — такое число, что $i^2 = -1$. Число a называется действительной частью числа $a + b\,i$, $b\,i$ — его мнимой частью, и b — коэффициентом при мнимой части. Запись числа $a + b\,i$ в указанном виде является единственной; иначе говоря, два комплексных числа равны тогда и только тогда, когда равны их действительные части и коэффициенты при мнимых частях. Действительные числа содержатся в множестве $\mathbb{C}$ всех комплексных чисел; комплексное число является действительным тогда и только тогда, когда коэффициент при мнимой части его равен нулю.

Сложение и умножение двух комплексных чисел $u = a + b\,i$ и $v = c + d\,i$ определяются по правилам $u + v = (a + c) + (b + d)\,i$ и $uv = (ac - bd) + (ad + bc)\,i$.

Непосредственная проверка показывает, что эти операции обладают свойствами 1) – 5) из § 1, и потому множество всех комплексных чисел является кольцом. Действительные числа 0 и 1 являются соответственно нулем и единицей кольца $\mathbb{C}$. Покажем, что каждый ненулевой элемент из $\mathbb{C}$ обратим, т. е. кольцо $\mathbb{C}$ является полем. Действительно, если комплексное число $u = a + b\,i$ отлично от нуля, то хотя бы одно из действительных чисел a и b отлично от нуля и потому $a^2 + b^2 \neq 0$. Поэтому можно записать комплексное число

$$\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\,i,$$

и непосредственно проверяется, что оно является обратным к числу z.

Заметим, что поле комплексных чисел, в отличие от кольца целых и полей рациональных и действительных чисел, не является упорядоченным. Действительно, в любом упорядоченном кольце квадрат любого ненулевого элемента положителен. Поэтому $1 = 1^2$ всегда является положительным элементом кольца, а значит в любом упорядоченном кольце -1 является отрицательным элементом. Но поле $\mathbb{C}$ содержит такой элемент i, что $i^2 = -1$, и потому оно не может быть упорядоченным.

Нас будут интересовать два подмножества множества всех комплексных чисел. Первое из них называется множеством целых гауссовых чисел и обозначается символом Γ. Оно состоит из всевозможных комплексных чисел $a + b\,i$, где a и b —

целые числа. Второе множество, обозначаемое символом Δ, состоит из всевозможных комплексных чисел вида $a + b\sqrt{3}\,i$, где a и b — целые числа. Непосредственно проверяется, что каждое из этих множеств вместе с любыми двумя своими элементами содержит их сумму, разность и произведение и потому является кольцом. Очевидно, что каждое из этих колец содержит все целые числа. Из рассуждений предыдущего абзаца следует, что эти кольца не являются упорядоченными: кольцо Γ содержит i, а кольцо Δ содержит элемент $\sqrt{3}\,i$. С другой стороны, они являются целостными кольцами, поскольку содержатся в поле $\mathbb{C}$, являющимся целостным кольцом.

Здесь будет показано, что ряд исходных свойств делимости целых чисел, переформулированных надлежащим образом, справедлив для произвольных колец. Мы увидим, тем не менее, что такие утверждения, как однозначность разложения на простые множители и существование наибольшего общего делителя, для кольца Δ уже не имеют места, хотя остаются верными в кольце Γ.

Начнем с того, что определение отношения делимости элементов произвольного кольца дословно совпадает с соответствующим определением для целых чисел:

Если K — некоторое кольцо, то будем говорить, что элемент a кольца K делит элемент b этого кольца и записывать это в виде $a \mid b$, если в K существует такой элемент c , что выполнено равенство $b = ac$.

Как и в случае целых чисел, мы будем при этом говорить также, что элемент a является делителем элемента b, или что элемент b делится на a, или что элемент b кратен элементу a.

Например, в кольце Γ целых гауссовых чисел $(1+i) \mid 2$, так как $2 = (1+i)(1-i)$. Аналогично, равенство $(1 + \sqrt{3}\,i)(2 - \sqrt{3}\,i) = 5 + \sqrt{3}\,i$ говорит о том, что в кольце Δ $(1 + \sqrt{3}\,i) \mid (5 + \sqrt{3}\,i)$. Рассмотрим здесь же

Пример 7.1. *Выяснить, является ли в кольце Γ элемент $2 + i$ делителем элемента $3 + 2\,i$.*

Нам требуется узнать, существует ли такое целое гауссово число $a + b\,i$, для которого справедливо равенство $3 + 2\,i = (2 + i)(a + b\,i)$. Так как

$$(2 + i)(a + b\,i) = (2a - b) + (a + 2b)\,i,$$

это равенство принимает вид $3 + 2\,i = (2a - b) + (a + 2b)\,i$. Поскольку два комплексных числа равны тогда и только тогда, когда равны их действительные части и коэффициенты при мнимых частях, последнее равенство равносильно системе

$$\begin{cases} 2a - b = 3 \\ a + 2b = 2. \end{cases}$$

Легко видеть, однако, что эта система не имеет целочисленных решений. Поэтому элемент $2 + i$ не является делителем элемента $3 + 2\,i$. $\square$

(Заметим, что задача примера 7.1 может быть решена и другим, более непосредственным способом. А именно, разделив в поле комплексных чисел число $3+2\,i$ на число $2 + i$, получим то единственное комплексное число $z = \dfrac{8}{5} + \dfrac{1}{5}\,i$, которое

удовлетворяет равенству $3 + 2\,i = (2 + i) \cdot z$. Так как число z не является целым гауссовым, элемент $2 + i$ не является делителем элемента $3 + 2\,i$ в кольце Γ.)

Следует отметить, что сформулированное выше определение делимости имеет смысл и для рациональных чисел, и для действительных чисел, и для комплексных чисел. Тем не менее, в этих случаях, как и вообще в любом поле, теория делимости оказывается бессодержательной: каждый элемент поля делится на любой его ненулевой элемент.

Введем еще одно отношение на множестве элементов кольца K. Будем говорить, что элемент a кольца K *ассоциирован* с элементом b этого кольца и записывать это в виде $a \sim b$, если в K существует такой обратимый элемент c, что выполнено равенство $b = ac$.

Напомним, что элемент c кольца K называется обратимым, если в K существует такой элемент d, что $cd = 1$. Элемент d называется обратным к элементу и обозначается через c^{-1}. Очевидно, что элемент c^{-1}, в свою очередь, обратим, и обратным к нему является элемент c. Отсюда $(c^{-1})^{-1} = c$. В каждом кольце есть хотя бы один обратимый элемент; таковым является, очевидно, единица кольца. Легко проверить также, что произведение двух обратимых элементов является обратимым элементом. Следующее утверждение является непосредственным следствием определения ассоциированности и этих замечаний.

Предложение 7.1. *Отношение ассоциированности элементов кольца K является эквивалентностью на множестве элементов K, т. е. отношение ассоциированности обладает следующими свойствами:*

1) для любого элемента a из K $a \sim a$ (рефлексивность);

2) для любых элементов a и b из K из $a \sim b$ следует, что $b \sim a$ (симметричность);

3) для любых элементов a, b и c из K из $a \sim b$ и $b \sim c$, следует, что $a \sim c$ (транзитивность). $\square$

Множество всех обратимых элементов кольца K будем обозначать через K^*. Так как элемент c кольца K является, очевидно, обратимым тогда и только тогда, когда $a \,|\, 1$, из предложения 2.1 следует, что $\mathbb{Z}^* = \{1, -1\}$. Поэтому целые числа a и b являются ассоциированными элементами кольца $\mathbb{Z}$ тогда и только тогда, когда $a = b$ или $a = -b$. Чтобы получить аналогичный критерий ассоциированности элементов колец Γ и Δ, необходимо иметь описание обратимых элементов этих колец.

Для этого, а также для изучения других свойств указанных колец нам будет полезна так называемая норма комплексного числа. А именно, *нормой* комплексного числа $z = a + b\,i$ называется неотрицательное действительное число $N(z) = a^2 + b^2$. (Для читателя, располагающего более основательным знакомством с комплексными числами, отметим, что норма $N(z)$ числа z совпадает, очевидно, с квадратом модуля этого числа.)

Предложение 7.2. 1) *Для любых комплексных чисел u и v имеет место равенство $N(u \cdot v) = N(u) \cdot N(v)$.*

2) *Если комплексное число z принадлежит любому из колец Γ и Δ, то $N(z)$ является целым числом.*

3) *Если u и v — элементы одного из колец Γ и Δ и в этом кольце u является делителем v, то $N(u)$ является делителем $N(v)$ в кольце $\mathbb{Z}$ целых чисел.*

Доказательство. Запишем комплексные числа u и v в виде $u = a + b\,i$ и $v = c + d\,i$. Тогда $u \cdot v = (ac - bd) + (ad + bc)\,i$ и потому

$$N(u \cdot v) = (ac - bd)^2 + (ad + bc)^2 = \\ a^2b^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2) \cdot (c^2 + d^2) = N(u) \cdot N(v).$$

Таким образом, утверждение 1) доказано.

Если $z = a + b\,i$ — целое гауссово число, то числа a и b целые, и потому $N(z) = a^2 + b^2$ также целое число. Аналогично, если $z = a + b\sqrt{-3}\,i$ — элемент кольца Δ, то число $N(z) = a^2 + 3b^2$ целое.

Наконец, если u и v — элементы любого из рассматриваемых колец и для некоторого элемента z того же кольца имеет место равенство $v = uz$, то ввиду утверждения 1) выполнено равенство $N(v) = N(u)N(z)$, и так как число $N(z)$ также является целым, отсюда следует, что в кольце $\mathbb{Z}$ число $N(u)$ является делителем числа $N(v)$ $\square$

Теперь можем получить описание обратимых элементов колец Γ и Δ.

Предложение 7.3. *Множество Γ^* всех обратимых элементов кольца Γ состоит из чисел 1, -1, i и $-i$.*

Множество Δ^* обратимых элементов кольца Δ состоит из чисел 1 и -1.

Кроме того, элемент u любого из колец Γ и Δ обратим в этом кольце тогда и только тогда, когда $N(u) = 1$.

В самом деле, если u — обратимый элемент одного из колец Γ и Δ, то u является делителем 1, и из предложения 7.2 следует, что неотрицательное целое число $N(u)$ является делителем в $\mathbb{Z}$ числа 1. Поэтому $N(u) = 1$.

Если далее $u = a + b\,i$ — целое гауссово число и $N(u) = 1$, то $a^2 + b^2 = 1$. Очевидными целочисленными решениями этого уравнения относительно a и b являются пары $(1, 0)$, $(-1, 0)$, $(0, 1)$ и $(0, -1)$, и легко видеть, что других целочисленных решений у него нет. Если, например, целое число a отлично от нуля и ± 1, то $|a| \geqslant 2$ и потому для любого b имеем $qa^2 + b^2 \geqslant a^2 \geqslant 2$.

Таким образом, если норма целого гауссова числа u равна 1, то u совпадает с одним из чисел 1, -1, i и $-i$, каждое из которых, очевидно, обратимо в Γ.

Наконец, если $u = a + b\sqrt{3}\,i$ — элемент кольца Δ и $N(u) = 1$, то $a^2 + 3b^2 = 1$. Очевидными целочисленными решениями этого уравнения относительно a и b являются пары $(1, 0)$, $(-1, 0)$, и легко видеть, что других целочисленных решений у него нет. Действительно, если целое число b отлично от нуля, то $|b| \geqslant 1$ и потому для любого a имеем $a^2 + 3b^2 \geqslant 3b^2 \geqslant 3$.

Таким образом, если норма элемента u кольца Δ равна 1, то u совпадает с одним из чисел 1, -1, которые, очевидно, обратимы в Δ. Предложение 7.3 доказано. $\square$

Из этого предложения очевидным образом получается

Следствие 1. *Множество элементов кольца* Γ, *ассоциированных в* Γ *с элементом* u *этого кольца, состоит из чисел* u, $-u$, ui *и* $-ui$.

Множество элементов кольца Δ, *ассоциированных в* Δ *с элементом* u *этого кольца, состоит из чисел* u *и* $-u$. $\square$

Отметим еще одно простое, но полезное

Следствие 2. *Если* u *и* v — *ненулевые элементы одного из колец* Γ *и* Δ *и в этом кольце* u *является делителем* v, *причем* $N(u) = N(v)$, *то элементы* u *и* v *ассоциированы.*

Если, в самом деле, для некоторого элемента z соответствующего кольца имеет место равенство $v = uz$, то в силу предложения 7.2 $N(v) = N(u)N(z)$, и так как $N(u) = N(v) \neq 0$, отсюда получаем, что $N(z) = 1$. Следовательно, ввиду предложения 7.3 элемент z обратим, и потому $u \sim v$. $\square$

Следующее предложение, содержащее перечень простейших свойств отношения делимости, проясняет, в частности, роль отношения ассоциированности в теории делимости элементов данного кольца:

Предложение 7.4. *Если* K *произвольное кольцо, то*

1) *для любого элемента* a *из* K $a|a$;

2) *Если* $a|b$ *и* $b|c$, *то* $a|c$;

3) *Если* $a|b$ *и* $a|c$, *то* $a|(b+c)$;

4) *Если* $a|b$, *то для любого элемента* c *из* K $a|(bc)$;

5) *Если* $ac|bc$ *и* $c \neq 0$, *то* $a|b$.

6) *элемент 0 делится на любой элемент из* K;

7) *произвольный элемент* a *делится на 0 тогда и только тогда, когда* $a = 0$;

8) *любой элемент из* K *делится на 1, а потому и на произвольный обратимый элемент кольца* K;

9) *элементы* a *и* b *одновременно делятся друг на друга тогда и только тогда, когда они ассоциированы.*

Свойства 1) – 8) совпадают с соответствующими свойствами из предложения 2.1, где речь идет об отношении делимости целых чисел, и доказательство их в общем случае произвольного кольца точно такое же, как для целых чисел.

Формулировки свойств 9), 10) и 11) предложения 2.1 содержат понятие абсолютной величины целого числа, которое можно ввести лишь благодаря тому, что кольцо целых чисел является упорядоченным кольцом. Поскольку мы хотим здесь построить теорию делимости для произвольного кольца, не предполагая его упорядоченным, формулировки указанных свойств в общем случае становятся бессмысленными, а вместо них появляется свойство 9) настоящего предложения. Докажем его.

Пусть сначала $a \sim b$. По определению отношения ассоциированности это означает, что $b = ac$ для некоторого обратимого элемента c кольца K. Отсюда $a|b$. Так как ввиду предложения 7.1 из $a \sim b$ следует, что $b \sim a$, то можно утверждать также, что и $b|a$. Таким образом, мы доказали, что если элементы a и b ассоциированы, то они делятся друг на друга.

Обратно, предположим, что элементы a и b делятся друг на друга. Тогда для подходящих элементов c и d кольца K выполнены равенства $b = ac$ и $a = bd$, откуда $b = b(cd)$. Если $b = 0$, то из равенства $a = bd$ следует, что и $a = 0$, и потому ввиду рефлексивности отношения ассоциированности получаем, что в этом случае $a \sim b$. Если же $b \neq 0$, то равенство $b = b(cd)$ можно сократить на b; полученное при этом равенство $cd = 1$ означает, что элемент c обратим, откуда ввиду равенства $b = ac$ мы и в этом случае имеем $a \sim b$. $\square$

Отметим, что свойство 9) предложения 2.1 является очевидным следствием свойства 9) предложения 7.4: два целых числа a и b делятся друг на друга тогда и только тогда, когда они ассоциированы в кольце $\mathbb{Z}$, т. е. тогда и только тогда, когда $a = \pm b$. Аналогичное утверждение справедливо и для элементов кольца Δ.

Свойство 9) предложения 7.4 говорит, в частности, о том, что ассоциированные элементы по отношению к делимости ведут себя одинаково. Более точно, имеем

Следствие. *Пусть a, a_1, b, b_1 — элементы некоторого кольца K, причем $a \sim b$ и $a_1 \sim b_1$. Тогда $a \,|\, b$ в том и только в том случае, когда $a_1 \,|\, b_1$.* $\square$

Обсудим теперь, как должно выглядеть в общем случае понятие, аналогичное понятию простого числа. Напомним, что целое число a мы называем простым, если $a > 1$ и любой натуральный делитель числа a равен либо 1, либо a. Прямой перенос этого определения на случай произвольного кольца K невозможен, так как в нем используется отношение порядка, в общем случае, напомним, отсутствующее. Как сформулировать наиболее существенные признаки простого целого числа без упоминания об отношении порядка $<$?

Пусть a — произвольное ненулевое целое число. Если $a \neq \pm 1$, то у него имеется четыре попарно различных делителя 1, -1, a и $-a$. Очевидно, что если a простое, то никаких других делителей в кольце $\mathbb{Z}$ у него нет. Очевидно также, что если целое число a отлично от нуля и ± 1 и если произвольный целый делитель числа a совпадает с одним из чисел ± 1 и $\pm a$, то либо число a, либо число $-a$ является простым в смысле вышеприведенного определения. Это говорит о том, что если мы примем новое определение простого целого числа, договорившись называть целое число a простым в том случае, когда $a \neq 0$, $a \neq \pm 1$ и произвольный целый делитель числа a совпадает с одним из чисел ± 1 и $\pm a$, то мы что-то приобретаем и что-то теряем. Приобретаем мы возможность переноса этого определения на произвольные кольца, поскольку в этом определении нет упоминаний об отношении порядка. Теряем же мы классическое определение простого числа, поскольку, наряду с простыми числами в классическом смысле, простыми числами в новом смысле должны будут считаться и числа, противоположные к ним. Эта потеря, впрочем, не имеет никакого значения, поскольку говоря о целых числах, мы можем по-прежнему пользоваться классическим определением простого числа.

При определении простого элемента произвольного кольца K кроме соображений, изложенных в предыдущем абзаце, следует принять во внимание еще одно: среди делителей произвольного элемента a нашего кольца содержатся все обратимые элементы кольца K и все элементы, ассоциированные с элементом a. Учитывая все это, мы приходим теперь к следующему определению:

Элемент a кольца K будем называть простым, если он обладает следующими двумя свойствами:

а) a отличен от 0 и не является обратимым элементом,

б) произвольный делитель в кольце K элемента a является либо обратимым, либо ассоциированным с a.

Так как два ассоциированных элемента кольца K имеют одни и те же делители, то всякий элемент, ассоциированный с простым элементом, сам является простым. Легко видеть также, что ненулевой и необратимый элемент a кольца K является простым тогда и только тогда, когда в любом его разложении $a = bc$ в произведение двух элементов кольца K один из сомножителей b или c обратим, а другой ассоциирован с a.

Как уже отмечалось выше, в кольце $\mathbb{Z}$ целых чисел простыми элементами в смысле этого общего определения являются числа вида $\pm p$, где целое число p простое в классическом смысле. Что можно сказать о простых элементах колец Γ и Δ? Из предложений 7.2 и 7.3 легко получить следующее достаточное условие простоты элементов этих колец:

Предложение 7.5. *Если норма $N(z)$ элемента z одного из колец Γ или Δ является простым целым числом, то z является простым элементом соответствующего кольца.*

В самом деле, если $N(z) = p$ — простое число, то, очевидно, что $z \neq 0$. Кроме того z не является обратимым элементом соответствующего кольца, поскольку в силу предложения 7.3 норма обратимого элемента любого из рассматриваемых колец равна 1. Наконец, если u — произвольный делитель элемента z, то в силу простоты числа p из предложения 7.2 следует, что либо $N(u) = 1$, либо $N(u) = p$, и потому элемент u является, соответственно, либо обратимым, либо ассоциированным с элементом z (см. предложение 7.2 и следствие 2 из предложения 7.3). $\square$

Так как все целые числа входят в каждое из колец Γ и Δ, возникает естественный вопрос, какие простые целые числа являются простыми элементами этих колец. Ответ на этот вопрос дает

Предложение 7.6. *Пусть p — простое целое число. Тогда*

1) число p не является простым элементом кольца Γ в том и только в том случае, когда p является суммой квадратов двух целых чисел;

2) число p не является простым элементом кольца Δ в том и только в том случае, когда $p = a^2 + 3b^2$ для некоторых целых чисел a и b.

В самом деле, если простое целое число p не является простым элементом кольца Γ, то найдутся необратимые элементы u и v из Γ такие, что $p = uv$. Отсюда $N(u)N(v) = p^2$, и так как $N(u)$ и $N(v)$ — целые числа, каждое из которых больше чем 1, мы должны иметь $N(u) = N(v) = p$. Если теперь элемент u записать в виде $u = a + bi$ (где a и b — целые числа), то равенство $N(u) = p$ дает $p = a^2 + b^2$, так что число p является суммой квадратов двух целых чисел. Обратно, если для некоторых целых чисел a и b выполнено равенство $p = a^2 + b^2$, то число p имеет разложение $p = (a+bi)(a-bi)$, сомножители которого $a+bi$ и $a-bi$ являются необратимыми элементами кольца Γ (поскольку норма каждого из них равна p). Таким

образом, p не является простым элементом в Γ, и первое утверждение доказано. Второе доказывается аналогично. $\square$

Из предложения 7.6 следует, например, что число 2 не является простым элементом кольца Γ, а число 3 является простым элементом этого кольца. Наоборот, в кольце Δ 2 является простым элементом, а 3 нет.

Следующее предложение говорит, в частности, о том, что достаточное условие из предложения 7.5 не является необходимым.

Предложение 7.7. *Всякий элемент кольца Δ, норма которого равна 4, является простым. В частности, элементы 2, $1+\sqrt{3}\,i$ и $1-\sqrt{3}\,i$ являются простыми элементами кольца Δ.*

Пусть, в самом деле, u — такой элемент кольца Δ, что $N(u)=4$. Если u не является простым, то в Δ существует делитель z элемента u, который необратим и не ассоциирован с u. Из предложения 7.2 и следствия 2 к предложению 7.3 легко видеть, что $N(z)=2$. Покажем, что в кольце Δ таких элементов нет. Действительно, если записать элемент z в виде $z=a+b\sqrt{3}\,i$, где a и b — целые числа, то равенство $N(z)=2$ принимает вид $a^2+3b^2=2$. Если $b\neq 0$, то $b^2\geqslant 1$, и потому $a^2+3b^2\geqslant 3b^2\geqslant 3$. Следовательно, $b=0$, и наше равенство имеет вид $a^2=2$. Однако, хорошо известно (и легко доказать), что такого целого числа a не существует. $\square$

Рассмотрим теперь возможность представления элементов кольца K в виде произведения простых элементов. Так как простые элементы отличны от нуля (по определению) и так как мы рассматриваем здесь лишь целостные кольца, нулевой элемент кольца K нельзя разложить в произведение простых. Такого разложения не допускают и обратимые элементы нашего кольца, поскольку, как легко видеть, всякий делитель обратимого элемента и сам является обратимым.

Таким образом, возможность разложимости в произведение простых элементов следует обсуждать лишь для ненулевых и необратимых элементов данного кольца. Существуют (довольно сложные) примеры колец, в которых не всякий ненулевой и необратимый элемент можно представить в виде произведения простых элементов. Тем не менее, имеет место

Предложение 7.8. *В каждом из колец Γ и Δ произвольный ненулевой и необратимый элемент может быть представлен в виде произведения простых элементов.*

Доказывать это предложение можно так же, как и соответствующее утверждение предложения 3.1, но здесь мы воспользуемся индукцией по норме элемента любого из данных колец. Наименьшим значением, принимаемым нормой на множестве ненулевых и необратимых элементов, является 2 для кольца Γ и 3 для кольца Δ. Так как каждое из этих натуральных чисел является простым числом, основание индукции обеспечивается предложением 7.5.

Пусть z — такой элемент любого из рассматриваемых колец Γ и Δ, что для каждого элемента того же кольца с нормой, меньшей, чем норма z, существует разложение в произведение простых элементов (соответствующего кольца). Покажем, что тогда и элемент z обладает аналогичным разложением. Это очевидно, если

элемент z простой. В противном случае в том же кольце существует делитель u элемента z, являющийся необратимым и не ассоциированным с z. Отсюда следует (в силу предложений 7.2 и 7.3 и следствия 2 из последнего), что $1 < N(u) < N(z)$. Кроме того, для подходящего элемента v того же кольца выполнено равенство $z = u \cdot v$, и так как $N(z) = N(u) \cdot N(v)$, имеют место и неравенства $1 < N(v) < N(z)$. По индуктивному предположению элементы u и v раскладываются в произведение простых элементов. Очевидно, что тогда аналогичное разложение существует и для элемента z, и индуктивный переход завершен. $\square$

Переходя к вопросу об однозначности разложения элементов кольца K в произведение простых, прежде всего, следует договориться о том, какой должна быть формулировка требования однозначности.

Напомним, что теорема 3.2 утверждает, что произвольное целое число $a > 1$ раскладывается в произведение простых чисел однозначно, если не обращать внимание на порядок следования сомножителей. Это утверждение оказывается неверным даже для целых чисел, если принять определение простого элемента, не использующее отношение порядка. Действительно, от разложения числа 6 вида $6 = (-2) \cdot (-3)$ к разложению $6 = 2 \cdot 3$ нельзя перейти никакой перестановкой сомножителей. Аналогичный пример можно найти в кольце Γ: два разложения $5 = (2 + i) \cdot (2 - i)$ и $5 = (-1 + 2\,i) \cdot (-1 - 2\,i)$ числа 5 также различаются не только порядком следования сомножителей (отметим, что числа $2+i$, $2-i$, $-1+2\,i$ и $-1-2\,i$ являются простыми элементами кольца Γ в силу предложения 7.4). Тем не менее, можно заметить, что сомножители этих двух разложений попарно ассоциированы в Γ, так как $-1 + 2\,i = (2 + i) \cdot i$ и $-1 - 2\,i = (2 - i) \cdot (-i)$.

Рассмотренные примеры подсказывают, что подобная неоднозначность разложения на простые множители имеет место и в произвольном кольце. В самом деле, если $a = p_1 p_2 \cdots p_m$ — разложение элемента a кольца K в произведение простых элементов и если c_1, c_2, ... , c_m — такие обратимые элементы кольца K, что $c_1 c_2 \cdots c_m = 1$, то $a = (c_1 p_1) \cdot (c_2 p_2) \cdots (c_m p_m)$ является еще одним разложением элемента a в произведение простых элементов $c_1 p_1$, $c_2 p_2$ ... ,$c_m p_m$. В этом разложении можно поменять местами некоторые сомножители, получив тем самым еще одно разложение того же элемента.

Будем считать, что в кольце имеет место хорошая теория делимости, если неоднозначность разложения его элементов на простые множители имеет лишь только что указанный характер. Точнее говоря, мы принимаем следующее определение:

Будем говорить, что кольцо K является кольцом с однозначным разложением на множители, если оно удовлетворяет следующим требованиям:

1) *Произвольный ненулевой и необратимый элемент кольца K раскладывается в произведение простых элементов.*

2) *Разложение элемента a из K в произведение простых элементов является единственным с точностью до порядка следования сомножителей и их ассоциированности. Говоря более подробно, это означает, что если $a = p_1 p_2 \cdots p_m$ и $a = q_1 q_2 \cdots q_n$ — два разложения элемента a, где все сомножители p_1, p_2, ... , p_m и q_1, q_2, ... , q_n являются простыми элементами кольца K, то количество сомножителей в этих разложениях одно и то же, т. е. $m = n$, и сомножители q_1, q_2, ... , q_n*

второго разложения можно, меняя местами, расположить и заново пронумеровать так, что в обоих разложениях на одинаковых местах будут стоять ассоциированные элементы, т. е. $p_i \sim q_i$ для всех $i = 1, 2, \ldots, m$.

Из теоремы 3.2 легко следует, что кольцо $\mathbb{Z}$ является кольцом с однозначным разложением на множители. Предложение 7.8 говорит о том, что в каждом из колец Γ и Δ выполнено первое требование определения кольца с однозначным разложением на множители. Тем не менее, в кольце Δ второе требование не имеет места:

Предложение 7.9. *Кольцо Δ не является кольцом с однозначным разложением на множители.*

Для доказательства этого достаточно заметить, что элемент 4 кольца Δ допускает два разложения на множители

$$4 = 2 \cdot 2 \qquad \text{и} \qquad 4 = (1 + \sqrt{3}\,i) \cdot (1 - \sqrt{3}\,i),$$

причем ввиду предложения 7.7 эти множители являются простыми элементами кольца Δ, а ввиду предложения 7.3 они попарно не ассоциированы. Таким образом, здесь ни один множитель одного разложения не ассоциирован с множителем другого. $\square$

Уже утверждение предложения 7.9 говорит о том, что теория делимости в кольце Δ отличается от теории делимости в кольце целых чисел. Можно указать и другие различия в этих теориях. Например, приведенные только что разложения элемента 4 кольца Δ позволяют показать, что в этом кольце не выполняется одно из основных свойств простых целых чисел, выражаемое предложением 3.2: если произведение нескольких чисел делится на простое число p, то хотя бы один из сомножителей должен делиться на p. Наш пример показывает, что в кольце Δ произведение элементов $1 + \sqrt{3}\,i$ и $1 - \sqrt{3}\,i$ делится на простой элемент 2, но ни один из сомножителей на этот элемент не делится. (Следует заметить, впрочем, что существование такого простого элемента в кольце Δ следует уже из формулировки предложения 7.9, так как доказательство теоремы 3.2 об однозначности разложения целых чисел на простые множители фактически использует лишь предложение 3.2.)

Ниже будет показано, что и положение с существованием наибольшего общего делителя элементов кольца Δ отличается от ситуации в кольце целых чисел. Для этого нам необходимо сформулировать определение наибольшего общего делителя, пригодное для произвольного кольца K, поскольку, как и в случае понятия простого элемента, дословный перенос соответствующего определения с кольца целых чисел невозможен. Мы хотим найти такое свойство наибольшего общего делителя двух целых чисел, в формулировке которого не участвует отношение порядка, и которое "почти" равносильно определению.

На самом деле, такое свойство нам уже встречалось в следствии 1 к теореме 2.2: положительный общий делитель d чисел a и b является наибольшим общим делителем этих чисел тогда и только тогда, когда произвольный общий делитель чисел a и b является делителем d. Опуская здесь требование положительности числа d, мы и приходим к искомому определению.

Наибольшим общим делителем элементов a и b кольца K называется такой их общий делитель, который делится на все остальные общие делители этих элементов.

Например, в кольце $\mathbb{Z}$ для чисел $a = 18$ и $b = 24$ существует в точности два числа 6 и -6, удовлетворяющих требованиям этого определения. Вообще, если d — наибольший общий делитель целых чисел a и b (определенный в параграфе 2), то определению из предыдущего абзаца удовлетворяют числа d и $-d$ и только они. Эти числа являются ассоциированными элементами кольца $\mathbb{Z}$, и аналогичное положение имеет место в общем случае:

Предложение 7.10. *Наибольший общий делитель элементов кольца K определен однозначно с точностью до ассоциированности. Говоря более подробно, это означает, что если элемент d является наибольшим общим делителем элементов a и b и $d' \sim d$, то и элемент d' является наибольшим общим делителем элементов a и b, т. е. удовлетворяет требованиям определения, приведенного выше. Кроме того, если каждый из двух элементов d_1 и d_2 удовлетворяют этим требованиям, то $d_1 \sim d_2$.*

Действительно, пусть элемент d является наибольшим общим делителем элементов a и b кольца K. По определению, это означает, во-первых, что d является общим делителем этих элементов. Но тогда и элемент d' такой, что $d' \sim d$, также будет их общим делителем, поскольку $d' \mid d$. Во-вторых, произвольный общий делитель t элементов a и b является делителем элемента d. Но тогда t будет делителем и элемента d', поскольку $d \mid d'$. Таким образом, элемент d' вместе с элементом d вполне заслуживает того, чтобы называться наибольшим общим делителем элементов a и b.

С другой стороны, если элементы d_1 и d_2 удовлетворяют требованиям определения наибольшего общего делителя элементов a и b, то d_1, как и любой другой общий делитель этих элементов, должен быть делителем d_2 и, аналогично, d_2 должен быть делителем d_1. Следовательно, $d_1 \sim d_2$. $\square$

В предложении 7.10 ничего не говорится о существовании наибольшего общего делителя элементов кольца K. В нем утверждается лишь, что если у двух элементов кольца есть наибольший общий делитель, то и любой ассоциированный с ним элемент имеет право называться наибольшим общим делителем этих элементов и других претендентов на это звание нет. Из следующего утверждения видно, что в общем случае элементы кольца могут не иметь наибольшего общего делителя.

Предложение 7.11. *Элементы $u = 4$ и $v = 2 + 2\sqrt{3}\,i$ кольца Δ не имеют наибольшего общего делителя.*

Для доказательства достаточно выписать все общие делители элементов u и v. Так как $N(u) = N(v) = 16$, норма произвольного общего делителя z этих элементов должна быть натуральным делителем числа 16. Случай $N(z) = 16$ невозможен, так как тогда в силу следствия 2 к предложению 7.3 каждый из элементов u и v был бы ассоциирован с z и потому они были бы ассоциированы между собой. При доказательстве предложения 7.7 было показано, что в кольце Δ нет элементов с нормой, равной 2; аналогично доказывается, что в нем нет и элементов с нормой,

равной 8. Если $N(z) = 1$, то (см. предложение 7.3) $z = \pm 1$. Легко видеть, что если $N(z) = 4$, то z совпадает с одним из чисел ± 2, $\pm(1 + \sqrt{3}\,i)$, $\pm(1 - \sqrt{3}\,i)$. Нетрудно показать, что все они являются общими делителями элементов u и v.

Таким образом, общими делителями в кольце Δ элементов u и v являются числа ± 1, ± 2, $\pm(1 + \sqrt{3}\,i)$, $\pm(1 - \sqrt{3}\,i)$ и только они. Из предложения 7.7 следует, что ни одно из них не может делиться на все остальные, так что наибольшего общего делителя у элементов u и v нет. $\square$

Покажем теперь, что кольцо Γ целых гауссовых чисел является кольцом с однозначным разложением на множители. Последовательность рассуждений здесь аналогична тем, которые в параграфах 2 и 3 привели к доказательству теоремы 3.2, и мы, опуская подробности, укажем лишь на основные вехи. Первой из них является теорема о делении с остатком. Для кольца целых гауссовых чисел она формулируется следующим образом:

Предложение 7.12. *Для любых целых гауссовых чисел u и v, где $v \neq 0$, существует пара целых гауссовых чисел q и r такая, что $u = vq + r$ и $N(r) < N(v)$.*

Доказательство. Пусть $q' = uv^{-1}$. Из определения умножения комплексных чисел и вида обратного к комплексному числу следует, что число q' имеет вид $q' = x' + y'i$, где x' и y' — некоторые рациональные числа. Легко видеть, что существуют целые числа x и y ближайшие к числам x' и y', т. е. такие, что $|x' - x| \leqslant 1/2$ и $|y' - y| \leqslant 1/2$. Тогда $q = x + y\,i$ является целым гауссовым числом. Покажем, что числа q и $r = u - qv$ составляют искомую пару элементов кольца Γ. Так как $u = vq + r$, для этого достаточно показать, что $N(r) < N(v)$. Заметим, что так как $u = vq'$, то

$$N(r) = N(vq' - vq) = N(v(q' - q)),$$

и ввиду предложения 7.2 $N(r) = N(v) \cdot N(q' - q)$. Поскольку $q' - q = (x' - x) + (y' - y)i$ и $|x' - x| \leqslant 1/2$ и $|y' - y| \leqslant 1/2$, имеем

$$N(q' - q) = (x' - x)^2 + (y' - y)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1.$$

Так как $N(v) > 0$, отсюда и следует, что $N(r) < N(v)$. Предложение доказано. $\square$

Как и для целых чисел, элементы q и r, удовлетворяющие требованиям предложения 7.12, называют соответственно неполным частным и остатком от деления элемента u на элемент v. Правда, в отличие от целых чисел, утверждение о единственности неполного частного и остатка здесь не имеет места. Например, элемент $2 + i$ можно разделить с остатком на элемент $1 + i$ по меньшей мере двумя различными способами: $2 + i = (1 + i) \cdot 2 + (-i)$ и $2 + i = (1 + i) \cdot (1 - i) + i$. Алгоритм деления с остатком в кольце Γ содержится в доказательстве предложения 7.12.

Пример 7.2. *Найти неполное частное и остаток от деления целого гауссова числа $u = 7 + 5\,i$ на число $v = 2 - i$.*

Пользуясь правилами, указанными в начале параграфа, находим, что число $q' = uv^{-1}$ имеет вид $q' = \dfrac{9}{5} + \dfrac{17}{5}\,i$. Поскольку ближайшими целыми числами к рациональным числам $\dfrac{9}{5}$ и $\dfrac{17}{5}$ являются числа 2 и 3 соответственно, искомое неполное

частное есть $q = 2+3\,i$. Найдем теперь остаток: $r = u-vq = (7+5\,i)-(2-i)(2+3\,i) = i$. $\square$

Используя предложение 7.12 можно доказать, что в кольце Γ у любых элементов существует наибольший общий делитель. Более того, здесь имеет место точный аналог теоремы 2.2:

Предложение 7.13. *Произвольные ненулевые элементы u и v кольца Γ обладают наибольшим общим делителем. Если элемент w из Γ является наибольшим общим делителем элементов u и v, то для подходящих элементов f и g из Γ имеет место равенство $w = uf + vg$.*

Доказательство практически дословно повторяет доказательство теоремы 2.2. А именно, вводится в рассмотрение множество M всевозможных элементов вида $uf + vg$, где f и g — произвольные целые гауссовы числа. Затем из ненулевых элементов множества M выбирается элемент $w = uf + vg$ с наименьшей нормой. Его запись делает очевидным тот факт, что всякий общий делитель элементов u и v является делителем и элемента w. Остается показать, что элемент w является общим делителем элементов u и v. Как и в доказательстве теоремы 2.2, найдем (в соответствии с предложением 7.12) такие элементы q и r, что $u = wq + r$ и $N(r) < N(w)$. Тогда элемент $r = u - wq = u(1 - fq) + v(-gq)$ принадлежит множеству M и в силу выбора элемента w должно выполняться равенство $r = 0$. Таким образом, $w \mid u$ и, аналогично, $w \mid v$. $\square$

Если наибольший общий делитель двух целых гауссовых чисел равен 1, то эти числа мы будем называть взаимно простыми. Следует заметить, что в соответствии с предложением 7.10 наибольшим общим делителем двух взаимно простых целых гауссовых чисел наряду с 1 является и любой элемент из Γ, ассоциированный с 1, т. е. -1, i и $-i$.

Практически не меняя рассуждений, с помощью которых были доказаны следствия 2, 3 и 4 из теоремы 2.2, из предложения 7.13 получаем следующие точные их аналоги для кольца Γ:

Предложение 7.14. *1) Пусть целое гауссово число w является общим делителем целых гауссовых чисел u и v и пусть $u = wu_1$ и $v = wv_1$. Число w является наибольшим общим делителем чисел u и v тогда и только тогда, когда числа u_1 и v_1 взаимно просты.*

2) Если целое гауссово число w является делителем произведения двух целых гауссовых чисел u и v и если числа w и u взаимно просты, то число w является делителем числа v.

3) Если каждое из двух целых гауссовых чисел u и v является делителем целого гауссова числа w и числа u и v взаимно просты, то и произведение uv этих чисел является делителем числа w. $\square$

Используя свойство 2) этого предложения, можно без труда доказать следующий аналог предложения 3.2:

Предложение 7.15. *Если целое гауссово число u не делится на простой элемент p кольца Γ, то элементы a и p взаимно просты. Если произведение*

нескольких целых гауссовых чисел делится на простой элемент p, то хотя бы один из сомножителей должен делиться на p.

Теперь мы в состоянии показать, что в кольце Γ выполнено второе требование из определения кольца с однозначным разложением на множители. Это можно сделать, в точности следуя доказательству теоремы 3.2. Тем не менее, мы приведем здесь другое рассуждение (которое тоже может быть использовано для доказательства теоремы 3.2).

Пусть $u = p_1 p_2 \cdots p_m$ и $u = q_1 q_2 \cdots q_n$ — два разложения элемента u кольца Γ, где $m \geqslant 1$, $n \geqslant 1$ и все сомножители p_1, p_2, $\ldots$, p_m и q_1, q_2, $\ldots$, q_n являются простыми элементами этого кольца. Требуется доказать, что тогда $m = n$ и сомножители q_1, q_2, $\ldots$, q_n второго разложения можно, меняя местами, расположить и заново пронумеровать так, что $p_i \sim q_i$ для всех $i = 1, 2, \ldots, m$.

Не теряя общности, мы можем считать, что $m \geqslant n$. Поскольку простой элемент p_1 очевидно является делителем произведения $q_1 q_2 \cdots q_n$, в силу предложения 7.15 один из его сомножителей должен делиться на p_1. Меняя, если это необходимо, нумерацию сомножителей, можем считать, что $p_1 \mid q_1$. Но так как элемент q_1 также является простым, то элементы p_1 и q_1 оказываются ассоциированными, т. е. $q_1 = e_1 p_1$ для некоторого обратимого элемента e_1 кольца Γ. Сократив равенство $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ на общий множитель p_1, приходим к равенству $p_2 p_3 \cdots p_m = e_1 q_2 q_3 \cdots q_n$, из которого следует, что простой элемент p_2 является делителем произведения $e_1 q_2 \cdots q_n$. Поэтому один из его сомножителей должен делиться на p_2. Этим сомножителем не может быть обратимый элемент e_1, и потому на p_2 должен делиться один из элементов q_2, q_3, $\ldots$, q_n. Опять перенумеровав, если нужно, эти элементы, мы можем считать, что $p_2 \mid q_2$. Как и выше, отсюда следует, что $q_2 = e_2 p_2$ для некоторого обратимого элемента e_2 кольца Γ. Переписав равенство $p_2 p_3 \cdots p_m = e_1 q_2 q_3 \cdots q_n$ в виде $p_2 p_3 \cdots p_m = e_1 e_2 p_2 q_3 \cdots q_n$, после сокращения получаем $p_3 \cdots p_m = e_1 e_2 q_3 \cdots q_n$. Продолжая аналогичным образом, мы видим, что при подходящей перенумерации элементов q_1, q_2, $\ldots$, q_n справедливы равенства $q_i = e_i p_i$ $(i = 1, 2, \ldots, m)$, где e_1, e_2, $\ldots$, e_m — обратимые элементы кольца Γ. Если $n > m$, то имеет место и равенство $1 = e_1 e_2 \cdots e_m q_{m+1} \cdots q_n$. Но это невозможно, так как простые элементы q_{m+1}, $\ldots$, q_n необратимы. Таким образом, $m = n$, и наше утверждение доказано.

Итак, кольцо Γ целых гауссовых чисел является кольцом с однозначным разложением на множители. Многие утверждения о делимости целых чисел (в формулировке которых отсутствует упоминание об отношении порядка) могут быть доказаны для элементов кольца Γ. Таким утверждением является, например, теорема 2.3, являющаяся обоснованием алгоритма Евклида вычисления наибольшего общего делителя двух целых чисел. Аналогичная процедура позволяет вычислить наибольший общий делитель двух целых гауссовых чисел. Рассмотрим

Пример 7.3. *Найти наибольший общий делитель целых гауссовых чисел* $u = -3 + 13\,i$ *и* $v = 9 + 3\,i$.

Выполнив деление u на v с остатком (как в примере 7.2), найдем, что $u = vq_1 + r_1$, где $q_1 = i$ и $r_1 = 4\,i$. Так как остаток r_1 отличен от нуля, делим с остатком v на r_1: $v = r_1 q_2 + r_2$, где $q_2 = 1 - 2\,i$ и $r_2 = 1 - i$. Так

как остаток r_2 отличен от нуля, делим с остатком r_1 на r_2: $r_1 = r_2 q_3 + r_3$, где $q_3 = -2 - 2\,i$ и $r_3 = 0$. Так как остаток r_3 оказался равным нулю, вычисления закончены. Последний отличный от нуля остаток $1 - i$ является наибольшим общим делителем целых гауссовых чисел $u = -3 + 13\,i$ и $v = 9 + 3\,i$. $\square$

ЗАДАЧИ К ПАРАГРАФУ 7

7.1. Доказать, что целое число c является делителем целого гауссова числа $a + b\,i$ в кольце Γ тогда и только тогда, когда в кольце $\mathbb{Z}$ числа a и b делятся на c.

7.2. Доказать, что целое гауссово число $a + b\,i$ делится в кольце Γ на число $1 + i$, если целые числа a и b имеют одинаковую четность.

7.3. Доказать, что если a и b — взаимно простые нечетные целые числа, то целое гауссово число $a + b\,i$ делится в кольце Γ на число $1 + i$ и не делится на число $(1 + i)^2$.

7.4. Доказать, что числа $2 + 3\,i$ и $2 + 5\,i$ являются простыми элементами кольца Γ.

7.5. Найти разложение в произведение простых элементов кольца Γ числа $3 + i$.

7.6. Найти разложение в произведение простых элементов кольца Γ числа $-4 + 7\,i$.

7.7. Найти разложение в произведение простых элементов кольца Γ числа $5 - 5\,i$.

7.8. Найти разложение в произведение простых элементов кольца Γ числа $3 + 7\,i$.

7.9. Найти разложение в произведение простых элементов кольца Γ числа $7 + 9\,i$.

7.10. В кольце Γ разделить с остатком число $6 + 12\,i$ на число $-8 + 4\,i$.

7.11. В кольце Γ разделить с остатком число $5 + 3\,i$ на число $2 - i$.

7.12. В кольце Γ найти наибольший общий делитель элементов $4 + 3\,i$ и $10 + 5\,i$.

7.13. В кольце Γ найти наибольший общий делитель элементов $7 + 9\,i$ и $3 + 5\,i$.

7.14. Доказать, что множество Λ всевозможных комплексных чисел вида $a + b\sqrt{2}\,i$, где a и b — целые числа, является кольцом. Доказать, что это кольцо является кольцом с однозначным разложением на множители.

Ответы, решения и указания к задачам

§ 1

1.3. Разумеется, можно убедиться в справедливости этого равенства, раскрыв скобки и приведя подобные члены в его правой части. Более интересным является следующее решение:

$$a^3+b^3+c^3=(a+b)^3-3a^2b-3ab^2+c^3=$$
$$((a+b)+c)^3-3(a+b)^2c-3(a+b)c^2-3a^2b-3ab^2=$$
$$(a+b+c)^3-(3(a+b)^2c+3(a+b)c^2)-(3a^2b+3ab^2+3abc)+3abc=$$
$$(a+b+c)^3-3(a+b)c(a+b+c)-3ab(a+b+c)+3abc=$$
$$(a+b+c)((a+b+c)^2-3(a+b)c-3ab)+3abc=$$
$$(a+b+c)(a^2+b^2+c^2-ab-ac-bc)+3abc.$$

1.4. Индукция по n. Основание индукции $n=2$ — в задаче 1.1. Для индуктивного перехода воспользоваться преобразованием

$$a^{n+1}-b^{n+1}=a^{n+1}-ab^n+ab^n-b^{n+1}=a(a^n-b^n)+(a-b)b^n.$$

1.5. Индукция по n. Основание индукции $n=1$ — в задаче 1.1. Для индуктивного перехода воспользоваться преобразованием

$$a^{2n+3}+b^{2n+3}=a^{2n+3}+a^2b^{2n+1}-a^2b^{2n+1}+b^{2n+3}$$
$$=a^2(a^{2n+1}+b^{2n+1})-(a^2-b^2)b^{2n+1}.$$

1.7. Воспользоваться равенством $a^2+ab+b^2=(a+\frac{1}{2}b)^2+\frac{3}{4}b^2$.

1.8. Воспользоваться неравенством $x^2+y^2\geqslant 2xy$.

1.9. Воспользоваться неравенством $x^2+1\geqslant 2x$.

1.10. Пусть $s_n=1^2+2^2+\cdots+n^2$ — сумма квадратов первых n натуральных чисел ($n\geqslant 1$). Справедливость равенства $s_n=\dfrac{n(n+1)(2n+1)}{6}$ докажем индукцией по n.

При $n=1$ это проверяется непосредственно. Предполагая, что для некоторого $n\geqslant 1$ оно справедливо, имеем

$$s_{n+1}=s_n+(n+1)^2=\frac{n(n+1)(2n+1)}{6}+(n+1)^2$$
$$=\frac{(n+1)(n(2n+1)+6(n+1))}{6}=\frac{(n+1)(2n^2+7n+6)}{6}$$
$$=\frac{(n+1)((2n^2+4n)+(3n+6))}{6}=\frac{(n+1)(n+2)(2n+3)}{6}$$
$$=\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.$$

1.21. Пусть $s_n = \dfrac{1}{n+1} + \dfrac{1}{n+2} + \cdots + \dfrac{1}{2n}$. При $n = 2$ имеем $s_2 = \dfrac{1}{3} + \dfrac{1}{4} = \dfrac{7}{12} > \dfrac{13}{24}$, так что основание индукции справедливо. Далее,

$$\begin{aligned} s_{n+1} - s_n &= \left(\frac{1}{n+2} + \frac{1}{n+3} + \cdots + \frac{1}{2(n+1)}\right) - \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}\right) \\ &= \frac{1}{2n+1} + \frac{1}{2n+2} - \frac{1}{n+1} = \frac{1}{2(n+1)(2n+1)}. \end{aligned}$$

Так как при $n > 1$ имеем, очевидно, $\dfrac{1}{2(n+1)(2n+1)} > 0$, то $s_{n+1} > s_n$. Поэтому из индуктивного предположения $s_n > \dfrac{13}{24}$ следует, что $s_{n+1} > \dfrac{13}{24}$, и индуктивный переход завершен.

1.23. Пусть $s_n = \dfrac{4^n}{n+1}$ и $t_n = \dfrac{(2n)!}{(n!)^2}$. Справедливость неравенства $s_2 < t_2$ проверяется непосредственно. Так как

$$s_{n+1} = \frac{4(n+1)}{n+2} \cdot s_n \quad \text{и} \quad t_{n+1} = \frac{2(2n+1)}{n+1} \cdot t_n,$$

то для индуктивного перехода достаточно доказать, что при любом $n > 1$ выполнено неравенство $\dfrac{4(n+1)}{n+2} < \dfrac{2(2n+1)}{n+1}$. Действительно, поскольку при рассматриваемых значениях n число t_n положительно, тогда будем иметь

$$\frac{4(n+1)}{n+2} \cdot t_n < \frac{2(2n+1)}{n+1} \cdot t_n,$$

а так как $\dfrac{4(n+1)}{n+2} > 0$, из индуктивного предположения $s_n < t_n$ получаем

$$\frac{4(n+1)}{n+2} \cdot s_n < \frac{4(n+1)}{n+2} \cdot t_n.$$

Таким образом,

$$s_{n+1} = \frac{4(n+1)}{n+2} \cdot s_n < \frac{4(n+1)}{n+2} \cdot t_n < \frac{2(2n+1)}{n+1} \cdot t_n = t_{n+1}.$$

Указанное неравенство получается из следующих вычислений:

$$\frac{4(n+1)}{n+2} - \frac{2(2n+1)}{n+1} = 2 \cdot \frac{2(n+1)^2 - (n+2)(2n+1)}{(n+1)(n+2)} = \frac{-2n}{(n+1)(n+2)} < 0.$$

1.24. Для индуктивного перехода воспользоваться, например, тем, что $2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2 > 0$, если $n \geqslant 3$.

1.25. Для индуктивного перехода воспользоваться, например, тем, что $2n^3 - (n+1)^3 = (n-2)^3 + 3(n-2)^2 + 3(n-7) + 1 > 0$, если $n \geqslant 7$.

1.26. Так как $\left(2 - \frac{1}{2}\right)^2 = \frac{9}{4} > 2$, основанием индукции мы располагаем. Далее, поскольку $\left(2 - \frac{1}{n+1}\right) > \left(2 - \frac{1}{n}\right) > 0$, имеем

$$\left(2 - \frac{1}{n+1}\right)^n > \left(2 - \frac{1}{n}\right)^n,$$

откуда, используя индуктивное предположение, получаем

$$\left(2 - \frac{1}{n+1}\right)^{n+1} = \left(2 - \frac{1}{n+1}\right) \cdot \left(2 - \frac{1}{n+1}\right)^n > \left(2 - \frac{1}{n+1}\right) \cdot n.$$

Но $\left(2 - \frac{1}{n+1}\right) \cdot n > n+1$, так как при $n \geqslant 2$

$$\left(2 - \frac{1}{n+1}\right) \cdot n - (n+1) = \frac{2n(n+1) - n - (n+1)^2}{n+1}$$

$$= \frac{n^2 - n - 1}{n+1} = \frac{(n-1)n - 1}{n+1} > 0.$$

1.27. Пусть $s_n = \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2}$. Тогда $s_{n+1} = s_n + \frac{1}{(n+1)^2}$. При $n = 2$ доказываемое утверждение очевидно, но попытка выполнить индуктивный переход оказывается несостоятельной, так как индуктивное предположение $s_n < 1$ приводит к неравенству $s_{n+1} < 1 + \frac{1}{(n+1)^2}$, вывести из которого неравенство $s_{n+1} < 1$ невозможно.

Один из способов выхода из такого положения состоит в том, чтобы попытаться доказать более сильное утверждение, чем формулируемое в задаче. (Этот часто используемый при доказательствах по индукции прием нередко приводит к успеху. И это понятно, так как доказывая более сильное утверждение, мы располагаем и более сильным индуктивным предположением.)

Итак, попробуем доказать, что для любого натурального числа $n > 1$ выполняется неравенство $s_n < 1 - \frac{1}{n}$. Справедливость его при $n = 2$ снова очевидна, а из индуктивного предположения следует неравенство

$$s_{n+1} < 1 - \frac{1}{n} + \frac{1}{(n+1)^2}.$$

Таким образом, для завершения индуктивного перехода нам достаточно доказать, что $\frac{1}{(n+1)^2} - \frac{1}{n} < -\frac{1}{n+1}$. Поскольку

$$\frac{1}{(n+1)^2} - \frac{1}{n} + \frac{1}{n+1} = \frac{n - (n+1)^2 + n(n+1)}{n(n+1)^2} = -\frac{1}{n(n+1)^2} < 0,$$

это действительно так, и задача решена.

1.28. И основание индукции, и индуктивный переход получаются из неравенства

$$\sqrt{n}+\frac{1}{\sqrt{n+1}}>\sqrt{n+1},$$

справедливого для всех $n \geqslant 1$. Для его доказательства при помощи простых преобразований, сохраняющих равносильность неравенств, следует привести его к неравенству $\sqrt{n(n+1)} > n$, справедливость которого очевидна ввиду того, что $n(n+1) > n^2$.

1.29. Справедливость неравенства при $n = 3$ проверяется непосредственно. Поскольку в силу индуктивного предположения имеем

$$((n+1)!)^2 = (n+1)^2 \cdot (n!)^2 > (n+1)^2 \cdot n^n,$$

для индуктивного перехода достаточно показать, что для всех $n > 2$ выполнено неравенство $(n+1)^2 \cdot n^n > (n+1)^{n+1}$, т. е. равносильное ему неравенство $n^n > (n+1)^{n-1}$. Разделив обе части последнего неравенства на n^{n-1}, получим равносильное ему неравенство

$$\left(1+\frac{1}{n}\right)^{n-1} < n,$$

которое и будем доказывать. По формуле бинома Ньютона имеем

$$\left(1+\frac{1}{n}\right)^{n-1} = 1 + C_{n-1}^1 \frac{1}{n} + C_{n-1}^2 \frac{1}{n^2} + \cdots + C_{n-1}^{n-2} \frac{1}{n^{n-2}} + C_{n-1}^{n-1} \frac{1}{n^{n-1}}.$$

Для $k = 2, 3, \ldots, n-1$ оценим сверху k-ое слагаемое $C_{n-1}^k \frac{1}{n^k}$ правой части этого равенства:

$$C_{n-1}^k \frac{1}{n^k} = \frac{(n-1)(n-2)\cdots(n-k)}{k!} \cdot \frac{1}{n^k} < \frac{n^k}{k!} \cdot \frac{1}{n^k} < \frac{1}{k!} < 1.$$

Таким образом,

$$\left(1+\frac{1}{n}\right)^{n-1} < 1 + (n-1) = n,$$

что и требовалось показать.

Стоит привести еще одно доказательство того же неравенства $(n!)^2 > n^n$, уже не использующее метода математической индукции. Запишем левую часть неравенства в виде

$$(n!)^2 = (1 \cdot n)(2 \cdot (n-1)) \cdots ((n-1) \cdot 2)(n \cdot 1).$$

Так как $k \cdot (n-k+1) - n = k(n-k) - (n-k) = (n-k)(k-1)$, то для любого $k = 1, 2, \ldots, n$ выполнено неравенство $k \cdot (n-k+1) \geqslant n$, причем равенство имеет место тогда и только тогда, когда $k = 1$ или $k = n$. Поэтому при $n > 2$ среди этих

n неравенств хотя бы одно строгое, и почленное их перемножение дает требуемое неравенство.

1.30. Воспользоваться тождеством

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(bc-ad)^2$$

.

1.31. Воспользоваться тождеством

$$(a^2+b^2)^2)=(a^2-b^2)^2+(2ab)^2$$

.

1.33. Переписать равенство $(a+1)x=a$ в виде $(a+1)(1-x)=1$ и воспользоваться предыдущей задачей. *Ответ*: 0 и -2.

1.34. *Ответ*: 0 и 1.

§ 2

2.1. Обозначив число, на которое делили, через b, а остаток через r, имеем $1270=b\cdot 74+r$ и $0\leqslant r<b$. Поэтому b должно принадлежать интервалу $\left(\dfrac{1270}{75},\dfrac{1270}{74}\right]$, единственным целым числом, принадлежащим которому, является 17. *Ответ*: $b=17$, $r=12$.

2.7. Воспользоваться методом математической индукции. Для индуктивного перехода заметить, что $16^{n+1}-15(n+1)-1=16(16^n-15n-1)+225n$.

2.12. Пусть $d=(a+b,a-b)$. Тогда d делит сумму и разность чисел $a+b$ и $a-b$, т. е. $d\mid 2a$ и $d\mid 2b$. Поэтому если d нечетно, т. е. взаимно просто с 2, то $d\mid a$ и $d\mid b$, откуда $d=1$. Пусть $d=2d_1$, тогда $d_1\mid a$ и $d_1\mid b$, откуда $d_1=1$ и потому $d=2$. Если оба числа a и b нечетны, то $(a+b,a-b)=2$.

2.13. Воспользоваться равенством $a^2-ab+b^2=(a+b)^2-3ab$ и тем, что $(a+b,ab)=1$ (см. пример 2.5). При $a=1$ и $b=2$ имеем $a+b=a^2-ab+b^2=3$.

2.16. Так как число d является общим делителем чисел a и b, очевидно, что dc является общим делителем чисел ac и bc. Выберем целые числа x и y так, чтобы $ax+by=d$. Тогда $(ac)x+(dc)y=dc$, откуда следует, что произвольный общий делитель чисел ac и bc является делителем числа dc. Поэтому (см. следствие 1 из теоремы 2.2) число dc является наибольшим общим делителем чисел ac и bc.

2.17. Очевидно, что всякий общий делитель чисел a и b является общим делителем и чисел a и bc. Обратно, пусть t — произвольный общий делитель чисел a и bc. Так как $t\mid a$ и $(a,c)=1$, легко видеть, что $(t,c)=1$. Поэтому из $t\mid bc$ следует, что $t\mid b$, так что t является общим делителем чисел a и b. Итак, множество общих делителей чисел a и b совпадает с множеством общих делителей чисел a и bc, откуда и следует, что $(a,b)=(a,bc)$.

2.18. Записать числа a и b в виде $a=a_1d$ и $b=b_1d$, где $d=(a,b)$. Воспользоваться предложением 2.3, следствием 2 из теоремы 2.2, утверждением задачи примера 2.5 и задачей 2.16.

2.19. Пусть $ab^2 = c^2$ для некоторого целого числа c. Пусть $d = (b, c)$, $b = db_1$ и $c = dc_1$. Тогда равенство $ab^2 = c^2$ может быть переписано в виде $ab_1^2 = c_1^2$, откуда следует, что $b_1^2 \,|\, c_1^2$. Так как $(b_1^2, c_1^2) = 1$ (почему?), имеем $b_1^2 = 1$ и потому $a = c_1^2$.

2.20. Записать $a = 36a_1$ и $b = 36b_1$. Тогда $a_1 + b_1 = 12$, и остается найти все разложения числа 12 в сумму двух взаимно простых слагаемых. *Ответ*: $a = 36$ и$b = 396$ или $a = 180$ и $b = 252$.

2.21. *Ответ*: $a = 6$ и $b = 144$ или $a = 18$ и $b = 48$.

2.22. *Ответ*: $a = 15$ и $b = 840$ или $a = 105$ и $b = 120$.

2.23. При $m = 1$ утверждение очевидно. Так как при $m > 1$ (см. задачу 1.4) $\dfrac{a^m - 1}{a - 1} = a^{m-1} + a^{m-2} + \cdots + a + 1$, имеем

$$\frac{a^m - 1}{a - 1} = (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + m.$$

Учитывая, что при $k \geqslant 1$ число $a - 1$ является делителем числа $a^k - 1$, вывести отсюда, что множество общих делителей чисел $\dfrac{a^m - 1}{a - 1}$ и $a-1$ совпадает с множеством общих делителей чисел $a - 1$ и m.

§ 3

3.2. Так как $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ и при указанных значениях a выполнено неравенство $a^{n-1} + a^{n-2} + \cdots + a + 1 > 1$, из простоты числа $a^n - 1$ следует, что $a - 1 = 1$, т. е. $a = 2$. Простота числа n доказана в конце параграфа 3.

3.3. Заметим, что $n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2n + 2)(n^2 - 2n + 2)$. Неравенство $n^2 + 2n + 2 > 1$ при указанных значениях n очевидно. Кроме того, $n^2 - 2n + 2 = (n - 1)^2 + 1 > 1$.

3.4. Воспользоваться тождеством $n^8 + n^4 + 1 = (n^4 + 1)^2 - n^4 = (n^4 + n^2 + 1)(n^4 - n^2 + 1)$.

3.5. Очевидно, что $p = 2$ не удовлетворяет, а $p = 3$ удовлетворяет условию задачи. Если p простое и $p > 3$, то p не делится на 3 и потому либо $p = 3k + 1$, либо $p = 3k + 2$ для некоторого целого числа k. Но при $p = 3k + 1$ число $p + 14 = 3(k + 5)$ не является простым, а при $p = 3k + 2$ число $p + 10 = 3(k + 4)$ не является простым. *Ответ*: $p = 3$.

3.6. *Ответ*: $p = 3$.

3.7. *Ответ*: $p = 3$.

3.8. Непосредственно проверяется, что при $p = 2$ и $p = 3$ число $6p^2 + 1$ не является простым. При $p = 5$ числа $4p^2 + 1 = 101$ и $6p^2 + 1 = 151$ являются простыми. Если простое число $p > 5$ при делении на 5 дает в остатке 1 или 4, то число $4p^2 + 1$ не является простым, а если остаток равен 2 или 3, то число $6p^2 + 1$ не является простым. *Ответ*: $p = 5$.

3.9. *Ответ*: $p = 2$ или $p = 3$.

3.10. Пусть для некоторого целого числа a имеет место равенство $4p+1=a^2$. Тогда $4p=(a-1)(a+1)$, и потому число a должно быть нечетным, $a=2k+1$. Поскольку число a можно без потери общности считать положительным, $k\geqslant 0$. Отсюда $p=k(k+1)$, и так как число p простое, один из этих сомножителей (а именно, меньший из них) должен быть равен 1. Таким образом, $k=1$ и $p=2$. Непосредственная проверка показывает, что найденное значение p удовлетворяет условию задачи. *Ответ*: $p=2$.

3.11. Пусть для некоторого целого числа a имеет место равенство $4p+1=a^3$. Тогда $4p=(a-1)(a^2+a+1)$. Число $a^2+a+1=a(a+1)+1$ нечетно, поскольку для любого целого a число $a(a+1)$ является четным. Поэтому число $a-1$ должно делиться на 4, $a-1=4k$. Тогда $p=k(a^2+a+1)$, и так как $k<a<a^2+a+1$ (и $k>0$, поскольку $a^2+a+1>0$), в силу простоты числа p мы должны иметь $k=1$. Отсюда $a=5$ и $p=31$. *Ответ*: $p=31$.

3.12. Пусть для некоторого целого числа a имеет место равенство $5p+1=a^3$ и потому $5p=(a-1)(a^2+a+1)$, причем в правой части оба сомножителя положительны (поскольку $a^2+a+1>0$ и $5p>0$) и $a-1<a^2+a+1$. Если $a-1=1$, то $a=2$ и потому $5p=7$, что невозможно. Таким образом, оба сомножителя в правой части равенства $5p=(a-1)(a^2+a+1)$ являются числами, большими единицы, и из однозначности разложения на простые множители легко следует, что один из этих сомножителей должен быть равным 5, а другой p. Уравнение $a^2+a+1=5$ не имеет целочисленных решений. Следовательно, $a=6$ и $p=43$ (простое число). *Ответ*: $p=31$.

3.13. *Ответ*: $p=2$ или $p=211$.

3.14. *Ответ*: $p=73$.

3.15. Поскольку число p простое и $p>3$, то оно не делится на 3. Если $p=3k+1$, то $2p+1=3(2k+1)$, что невозможно, так как $2k+1>1$ и $2p+1$ простое число. Таким образом, $p=3k+2$, откуда $4p+1=3(4k+3)$. Остается заметить, что $4k+3>1$.

3.16. Так как число $a+b$ делится на p, то и число $a(a+b)$ делится на p, а потому и число $a^2=a(a+b)-ab$ делится на p. Поскольку p простое число, отсюда следует, что a делится на p. Теперь из того, что числа a и $a+b$ делятся на p, следует, что и число b делится на p.

3.17. Заметить, что из того, что числа a^2+b^2 и ab делятся на p, следует, что число $(a+b)^2$ делится на p.

3.18. Пусть $p<q<r$ — простые числа, $p>3$ и $q-p=r-q$. Так как все эти числа нечетные, разность прогрессии $q-p$ делится на 2. Остается доказать, что эта разность делится на 3. Для этого достаточно показать, что все числа p, q и r при делении на 3 дают одинаковые остатки. Заметим, что ни одно из них на три не делится. Если остатки от деления на 3 чисел p и r различны и, скажем, $p=3k+1$ и $r=3l+2$, то из равенства $2q=p+r$ имеем $2q=3(k+l+1)$, что невозможно, так как ни одно из чисел 2 и q не делится на 3. Таким образом, остатки от деления на 3 чисел p и r совпадают. Если $p=3k+1$ и $r=3l+1$ и $q=3n+2$, то с одной стороны, $2q=3(k+l)+2$, а с другой, $2q=3(2n+1)+1$. Если $p=3k+2$ и $r=3l+2$ и $q=3n+1$, то с одной стороны, $2q=3(k+l+1)+1$, а с другой, $2q=3(2n)+2$.

3.19. Пусть a и b — такие натуральные числа, что $p = a^2 - b^2$. Тогда $p = (a-b)(a+b)$, откуда, в частности, следует, что $0 < a - b < a + b$, и так как число p простое, должны выполняться равенства $a - b = 1$ и $a + b = p$. Из этих равенств получаем $a = \dfrac{p+1}{2}$ и $b = \dfrac{p-1}{2}$. Таким образом, существует не более одной пары натуральных чисел a и b, удовлетворяющих равенству $p = a^2 - b^2$. С другой стороны, так как p — нечетное простое число, числа $a = \dfrac{p+1}{2}$ и $b = \dfrac{p-1}{2}$ являются натуральными и удовлетворяют нашему равенству.

3.20. *Ответ*: 75.

3.21. Искомое число a имеет вид $a = p^m q^n$, где p и q — различные простые числа, $m \geqslant 1$, $n \geqslant 1$ и без потери общности можно предполагать, что $m \leqslant n$. Ввиду предложения 3.5 и условия задачи имеем $(m+1)(n+1) = 12$. Так как числа $m+1$ и $n+1$ натуральные и $2 \leqslant m+1 \leqslant n+1$, имеются две возможности: $m = 1$, $n = 5$ или $m = 2$, $n = 3$. Рассмотрим их отдельно.

Пусть $a = pq^5$, тогда из предложения 3.6 имеем

$$(p+1)(q^4 + q^3 + q^2 + q + 1) = 465.$$

Отсюда число $p + 1$ является нечетным и потому $p = 2$. Следовательно, $q^4 + q^3 + q^2 + q + 1 = 155$, откуда $q(q^3 + q^2 + q + 1) = 154 = 2 \cdot 7 \cdot 11$. Так как $q \neq p = 2$, для q имеем два возможных значения 7 и 11, ни одно из которых, очевидно, данному равенству не удовлетворяет. Таким образом, в этом случае решений нет.

Пусть теперь $a = p^2 q^3$, тогда

$$(p^2 + p + 1)(q^3 + q^2 + q + 1) = 465 = 3 \cdot 5 \cdot 31.$$

Из нечетности числа $q^3 + q^2 + q + 1$ следует, что $q = 2$. Поэтому $p^2 + p + 1 = 31$, откуда находим (решая квадратное уравнение или сравнивая разложения $p(p+1) = 2 \cdot 3 \cdot 5$ на простые множители), что $p = 5$. *Ответ*: 200.

3.22. Как и в предыдущей задаче, искомое число имеет вид либо $a = pq^5$, либо $a = p^2 q^3$. Если $a = pq^5$, получаем равенство

$$(p+1)(q^4 + q^3 + q^2 + q + 1) = 1240 = 2^3 \cdot 5 \cdot 31,$$

из которого ввиду того, что число $q^4 + q^3 + q^2 + q + 1$ при любом целом q является нечетным, следует, что $p + 1 = 8$, либо $p + 1 = 40$, либо $p + 1 = 248$. Во втором и третьем случаях $p = 39$ и $p = 247 = 13 \cdot 19$ не являются простыми числами. В первом случае $p = 7$ и имеем равенство $q^4 + q^3 + q^2 + q + 1 = 155$, т. е. $q(q^3 + q^2 + q + 1) = 154 = 2 \cdot 7 \cdot 11$. Непосредственные вычисления показывают, что единственно возможные (в силу соображений делимости) значения $q = 2$ и $q = 11$ не годятся.

При $a = p^2 q^3$ имеем равенство

$$(p^2 + p + 1)(q^3 + q^2 + q + 1) = 2^3 \cdot 5 \cdot 31.$$

Так как число $p^2 + p + 1$ всегда нечетно, либо $p^2 + p + 1 = 5$, либо $p^2 + p + 1 = 31$, либо $p^2 + p + 1 = 5 \cdot 31$. В первом случае целочисленных решений вообще нет, во

втором случае $p = 5$, а в третьем случае получаем равенство $q^3 + q^2 + q + 1 = 8$, т. е. $q(q^2 + q + 1) = 7$, не имеющее ввиду простоты числа 7 целочисленных решений $q \geqslant 2$. При $p^2 + p + 1 = 31$ имеем $q^3 + q^2 + q + 1 = 40$, откуда $q = 3$. *Ответ*: 675.

3.23. Если число n четное, то число $2^n - 1$ делится на число $3 = 2^2 - 1$ и не равно ему; если число n нечетное, то число $2^n + 1$ делится на число $3 = 2 + 1$ и не равно ему.

§ 4

4.1. Имеем

$$5^{21} \equiv (-2)^2 1 = (-8)^7 \equiv -1 \equiv 27 \pmod 7 \quad \text{и}$$
$$5^{21} = (5^3)^7 \equiv 4^7 = (4^2)^3 \cdot 4 \equiv 5^3 \cdot 4 \equiv 4 \cdot 4 \equiv 5 \equiv 27 \pmod{11}.$$

4.2. Воспользоваться тем, что $9^3 = 9{\cdot}81 \equiv 9{\cdot}25 = 225 \equiv 1 \pmod{56}$. *Ответ*: 18.

4.3. Заметить, что $7^3 \equiv -1 \pmod{43}$. *Ответ*: 9.

4.4. Заметить, что так как $8^3 = 512$ и $19 \cdot 27 = 513$, имеем сравнение $8^3 \equiv -1 \pmod{19}$. *Ответ*: 3.

4.5. Имеем

$$6^{50} = (36)^{25} \equiv 3^{25} = 9^{12} \cdot 3 \equiv (-2)^{12} \cdot 3 = (2^5)^2 \cdot 4 \cdot 3 \equiv 1 \pmod{11},$$
$$7^{25} = (49)^{12} \cdot 7 \equiv 5^{12} \cdot 7 = (25)^6 \cdot 7 \equiv 3^6 \cdot 7 = 9^3 \cdot 7 \equiv (-8) \cdot 7 \equiv -1 \pmod{11},$$

так что $6^{50} + 7^{25} \equiv 0 \pmod{11}$.

4.8. Показать, что $5^{24} \equiv 2 \pmod{23}$, а затем решить сравнение $7a \equiv -2 \pmod{23}$. *Ответ*: $a \equiv 3 \pmod{23}$.

4.9. Умножив на a обе части первого из данных сравнений $a^{25} \equiv 3 \pmod{79}$ и $a^{26} \equiv 29 \pmod{79}$, получаем $a^{26} \equiv 3a \pmod{79}$. Из него и второго из данных сравнений имеем $3a \equiv 29 \pmod{79}$, т. е. $3a \equiv 108 \pmod{79}$, откуда $a \equiv 36 \pmod{79}$. *Ответ*: 36.

4.10. Заметим предварительно, что для любого многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ с целыми коэффициентами, произвольных целых чисел u и v и натурального числа m из сравнения $u \equiv v \pmod m$ следует сравнение $f(u) \equiv f(v) \pmod m$. Действительно, из того, что $u \equiv v \pmod m$, следует, что для любого целого числа $k \geqslant 0$ $u^k \equiv v^k \pmod m$. Отсюда имеем следующую систему сравнений

$$\begin{aligned}
a_0u^n &\equiv a_0v^n \pmod m\\
a_1u^{n-1} &\equiv a_1v^{n-1} \pmod m\\
&\cdots\cdots\cdots\cdots\cdots\\
a_{n-1}u &\equiv a_{n-1}v \pmod m\\
a_n &\equiv a_n \pmod m,
\end{aligned}$$

складывая почленно которые и получаем $f(u) \equiv f(v) \pmod m$.

Перейдем теперь непосредственно к решению задачи. Так как по доказанному в силу очевидного сравнения $5 \equiv 2 \pmod 3$ имеем $f(5) \equiv f(2) \pmod 3$, а по условию $f(2) \equiv 0 \pmod 3$, то получаем $f(5) \equiv 0 \pmod 3$, т. е. число $f(5)$ делится на 3. Аналогично, из сравнения $5 \equiv 3 \pmod 2$ имеем $f(5) \equiv f(3) \pmod 2$, и так как по условию $f(3) \equiv 0 \pmod 2$, то получаем $f(5) \equiv 0 \pmod 2$, т. е. число $f(5)$ делится на 2. Так как числа 2 и 3 взаимно просты, этим доказано, что $f(5)$ делится на 6.

4.11. Перепишем равенство $C_p^k = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!}$ (см. задачу 1.6) в виде $k! \cdot C_p^k = p(p-1)(p-2)\cdots(p-k+1)$, из которого следует, что число $k! \cdot C_p^k$ делится на p. Так как при $k < p$ числа $k!$ и p взаимно просты, то $p \,|\, C_p^k$.

4.12. По формуле бинома Ньютона имеем

$$(a+b)^p = C_p^0\, a^p + C_p^1\, a^{p-1}b + C_p^2\, a^{p-2}b^2 + \cdots + C_p^{p-1}\, ab^{p-1} + C_p^p\, b^p.$$

Так как $C_p^0 = C_p^p = 1$ и в силу задачи 4.11 для любого числа k, удовлетворяющего неравенствам $1 \leqslant k < p$, выполнено сравнение $C_p^k \equiv 0 \pmod p$, действительно получаем $(a+b)^p \equiv a^p + b^p \pmod p$.

4.13. Так как $a \equiv b \pmod p$, то для некоторого целого числа t имеем равенство $a = b + pt$. Отсюда по формуле бинома Ньютона получаем

$$a^p = b^p + C_p^1\, b^{p-1}(pt) + C_p^2\, b^{p-2}(pt)^2 + \cdots + C_p^{p-1}\, b(pt)^{p-1} + C_p^p\, (pt)^p.$$

Так как все слагаемые, начиная со второго, в правой части этого равенства делятся на p^2, требуемое сравнение из него следует.

4.14. Умножить обе части данного сравнения на 8.

4.15. *Ответ*: $x \equiv 10 \pmod{35}$.

4.16. *Ответ*: $x \equiv 10 \pmod{25}$.

4.17. *Ответ*: $x \equiv 5 \pmod{18}$, $x \equiv 11 \pmod{18}$, $x \equiv 17 \pmod{18}$.

4.18. *Ответ*: $x \equiv 4 \pmod{30}$, $x \equiv 9 \pmod{30}$,
$x \equiv 14 \pmod{30}$, $x \equiv 19 \pmod{30}$,
$x \equiv 24 \pmod{30}$, $x \equiv 29 \pmod{30}$.

4.19. *Ответ*: $x = 8 - 15t, y = -11 + 23t$, где $t \in \mathbb{Z}$.

4.20. *Ответ*: $x = 9 + 13t, y = 5 + 10t$, где $t \in \mathbb{Z}$.

4.21. Если пара чисел $(5, 9)$ является решением уравнения $ax - by = 31$, то должно выполняться равенство $a \cdot 5 - b \cdot 9 = 31$. Значит, искомые значения a и b должны составлять решение уравнения $5a - 9b = 31$ от неизвестных a, b. Решая это уравнение, находим $a = 8 + 9t, b = 1 + 5t$, где $t \in \mathbb{Z}$. Наименьшие положительные значения a и b получаются при $t = 0$. *Ответ*: $a = 8, b = 1$.

4.22. *Ответ*: $a = -5, b = -6$.

4.23. Координаты точек прямой совпадают с решениями уравнения $8x - 13y + 6 = 0$. Все решения этого уравнения описываются формулами $x = 9 + 13t, y = 6 + 8t$ ($t \in \mathbb{Z}$). Искомые точки получаются при тех значениях t, которые удовлетворяют

неравенствам $-42 \leqslant 9 + 13t \leqslant 50$. Остается найти количество его целочисленных решений. *Ответ*: 7.

4.24. *Ответ*: $x \equiv 235 \pmod{600}$.

4.25. *Ответ*: $x \equiv 11 \pmod{3150}$.

4.26. Уравнение такой прямой имеет вид $x = a$, где a — целое число. Ордината y точки пересечения этой прямой с прямой $x - 5y - 2 = 0$ вычисляется из уравнения $a - 5y - 2 = 0$ и потому является целым числом тогда и только тогда, когда $a - 2$ делится на 5, т. е. $a \equiv 2 \pmod{5}$. Аналогично, целочисленность координат точки пересечения нашей прямой с прямыми $x - 8y - 1 = 0$ и $x - 11y - 3 = 0$ равносильна справедливости сравнений $a \equiv 1 \pmod{8}$ и $a \equiv 3 \pmod{11}$ соответственно. Таким образом, множество искомых чисел a совпадает с множеством целых чисел, удовлетворяющих системе сравнений

$$\begin{cases} a \equiv 2 \pmod{5} \\ a \equiv 1 \pmod{8} \\ a \equiv 3 \pmod{11}. \end{cases}$$

Ответ: $x = a$, где $a \equiv 377 \pmod{440}$.

4.27. *Ответ*: 89, 209.

§ 5

5.1. *Ответ*: $x = 3$.

5.2. *Ответ*: $x = 4$.

5.3. *Ответ*: $x = 3$.

5.4. *Ответ*: $a = 189$.

5.5. *Ответ*: $a = 968$.

5.6. *Ответ*: $a = 1521$.

5.7. Так как $605 = 5 \cdot 121$, то произвольное натуральное число, не превосходящее числа 605 и имеющее с этим числом наибольший общий делитель, равный 5, имеет вид $5n$, где n — натуральное число, не превосходящее числа 121 и взаимно простое с этим числом. *Ответ*: 110.

5.8. Если a — натуральное число, не превосходящее числа m и взаимно простое с m, то $m - a$ также является натуральным числом, не превосходящим числа m и взаимно простым с m. Так как из $a_1 \neq a_2$ следует, что $m - a_1 \neq m - a_2$, это означает, что если a принимает без повторений все значения из приведенной системы вычетов по модулю m, выбранной из полной системы вычетов $1, 2, \ldots, m$ по этому модулю, то и $m - a$ будет принимать без повторений все значения из той же приведенной системы вычетов. Поэтому сложив $\varphi(m)$ слагаемых вида $a + (m - a)$ (где a пробегает упомянутую приведенную систему вычетов), мы получим удвоенную сумму всех чисел, не превосходящих числа m и взаимно простых с m. Так как каждое из этих слагаемых равно m, требуемый результат теперь очевиден.

5.9. *Ответ*: 9.

5.10. Пусть r — остаток от деления числа 21^{83} на 24. Тогда должно выполняться сравнение $r \equiv 21^{83} \pmod{24}$, правая часть которого и модуль делятся на 3. Поэтому и число r должно делиться на 3, $r = 3r_1$. После сокращения обеих частей и модуля предыдущего сравнения на 3, получаем $r_1 \equiv 7 \cdot 21^{82} \pmod 8$. Так как числа 21 и 8 взаимно просты и $\varphi(8) = 4$, по теореме Эйлера $21^4 \equiv 1 \pmod 8$, откуда получаем $7 \cdot 21^{82} \equiv (-1) \cdot 21^2 \equiv (-1) \cdot 5^2 \equiv 7 \pmod 8$. *Ответ*: 21.

5.11. *Ответ*: 375.

5.12. *Ответ*: 1.

5.13. Найти остаток от деления на 132 отдельно каждого слагаемого. *Ответ*: 7.

5.14. Возвести в куб обе части сравнения $a^4 \equiv 1 \pmod 5$.

5.15. Воспользоваться равенством $a^p - b = (a^p - a) + (a - b)$ и применить теорему Ферма.

5.16. Если число a не делится на 7, то из теоремы Ферма следуют сравнения $a^{6m} \equiv 1 \pmod 7$ и $a^{6n} \equiv 1 \pmod 7$, складывая почленно которые получаем $a^{6m} + a^{6n} \equiv 2 \pmod 7$, что противоречит условию.

5.17. См. указание к предыдущей задаче.

5.18. С помощью теоремы Ферма доказать делимость данного числа на 5 и на 13.

5.19. Так как числа a и b взаимно просты, оба они на 11 делиться не могут. Если одно из них делится на 11, а другое не делится, наше утверждение очевидно. Если оба числа a и b не делятся на 11, из теоремы Ферма следует, что число $4a^{10} - b^{10}$ на 11 не делится. Остается заметить, что $4a^{10} - b^{10} = (2a^5 + b^5)(2a^5 - b^5)$.

5.20. См. указание к задаче 5.19.

5.21. См. указание к задаче 5.14.

5.22. *Ответ*: $n = 4k$.

5.23. По условию $q - 1 = (p-1)k$ для некоторого натурального числа k. Пусть целое число a взаимно просто с произведением pq. Тогда оно взаимно просто с каждым из чисел p и q, и потому в силу теоремы Ферма выполнены сравнения

$$a^{p-1} \equiv 1 \pmod p \qquad \text{и} \qquad a^{q-1} \equiv 1 \pmod q.$$

После возведения обеих частей первого из них в k-ую степень, получаем $a^{q-1} \equiv 1 \pmod p$. Таким образом, число $a^{q-1} - 1$ делится на два взаимно простых числа p и q, а потому делится и на произведение этих чисел. Это и означает, что $a^{q-1} \equiv 1 \pmod{pq}$.

5.24. По теореме Ферма справедливы сравнения $a^p \equiv a \pmod p$ $a^q \equiv a \pmod q$. Умножив обе части и модуль каждого из них на числа q и p соответственно, получим сравнения $qa^p \equiv qa \pmod{pq}$ и $pa^q \equiv pa \pmod{pq}$, почленно сложив которые, приходим к требуемому.

5.25. Так как числа p и q взаимно просты, по теореме Ферма имеем $p^{q-1} \equiv 1 \pmod q$ и $q^{p-1} \equiv 1 \pmod p$. По определению сравнения это означает, что для подходящих целых чисел m и n имеют место равенства $p^{q-1}-1 = qm$ и $q^{p-1}-1 = pn$. Перемножив их почленно, имеем $(p^{q-1}-1)(q^{p-1}-1) = pqmn$. Так как

$$(p^{q-1}-1)(q^{p-1}-1) = p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1$$

с учетом того, что $p, q \geqslant 2$, получаем равенство

$$p^{q-1} + q^{p-1} - 1 = pq(p^{q-2}q^{p-2} - mn),$$

из которого и следует, что $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

5.26. Методом математической индукции показать, что для любого целого числа $n \geqslant 1$ и произвольных целых чисел a_1, a_2, ... , a_n выполнено сравнение

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \pmod p.$$

Полагая в нем для данного $n \geqslant 1$ $a_1 = a_2 = \cdots = a_n = 1$, получаем $n^p \equiv n \pmod p$. Таким образом, сравнение $a^p \equiv a \pmod p$, утверждаемое теоремой Ферма, доказано для всех целых чисел $a \geqslant 1$. При $a = 0$ оно очевидно. Если $a < 0$, то $-a > 0$, и потому при $p > 2$ имеем $a^p = -(-a)^p \equiv -(-a) = a \pmod p$, а при $p = 2$ — $a^2 = (-a)^2 \equiv -a \equiv a \pmod 2$.

§ 6

6.1. *Ответ*: а) $b = 5$; б) $b = 11$; в) $b = 15$; г) такой системы счисления не существует.

6.2. *Ответ*: $b = 8$.

6.3. *Ответ*: $b = 4$.

6.4. По условию искомое число n имеет записи вида $n = \overline{abc}_{10}$ и $n = \overline{cba}_9$. Это означает, что $n = a \cdot 10^2 + b \cdot 10 + c$ и $n = c \cdot 9^2 + b \cdot 9 + a$, откуда получаем равенство $a \cdot 10^2 + b \cdot 10 + c = c \cdot 9^2 + b \cdot 9 + a$. Переписав его в виде $100a - 80c = a - b$, видим, что число $a - b$ должно делиться на 10. Но из условия задачи следует, что числа a и b являются цифрами в девятиричной системе счисления и потому удовлетворяют неравенствам $0 \leqslant a, b < 9$. Поэтому $a = b$. Равенство $100a - 80c = a - b$ теперь принимает вид $5a = 4c$, откуда следует, что число c делится на 5. Следовательно, либо $c = 0$, либо $c = 5$. Но если $c = 0$, то и $a = 0$, что невозможно, так как число n является по условию трехзначным. Таким образом, $c = 5$ и $a = 4$. *Ответ*: 445.

6.5. Так как $b \geqslant 3$, число $b - 2$ является цифрой в системе счисления с основанием b; будем обозначать эту цифру символом c. Тогда равенство $2(b-1) = b + (b-2) = 1 \cdot b + c$ означает, что $2(b-1) = \overline{1c}_b$, а равенство $(b-1)^2 = (b-2)b + 1 = c \cdot b + 1$ означает (поскольку $c \neq 0$), что $(b-1)^2 = \overline{c1}_b$.

6.6. Пусть s_n обозначает сумму первых n натуральных чисел, тогда (см. пример 1.3) $s_n = \dfrac{n(n+1)}{2}$. Предположим сначала, что число n является четным, тогда $n = 2k$, причем символ k можно считать обозначением соответствующей цифры.

Так как $k \neq 0$ и $s_n = k \cdot n + k$, в этом случае имеем $s_n = \overline{kk}_n$. Если же число n нечетно, $n = 2k + 1$, то $k > 0$ и потому $k + 1 < n$. Тогда $s_n = (k + 1) \cdot n = \overline{l0}_n$, где символ l обозначает цифру, равную числу $k + 1$. *Ответ*: $\overline{kk}_n$, где k обозначает цифру, равную $\frac{n}{2}$, если n — четное число, и $\overline{l0}_n$, где l обозначает цифру, равную $\frac{n+1}{2}$, если n — нечетное число.

6.7. $\overline{144}_b = b^2 + 4b + 4 = (b + 2)^2 = (\overline{12}_b)^2$.

6.9. Число $\overline{aba}$ делится на 15 тогда и только тогда, когда оно делится на 3 и на 5. Данное число делится на 5 тогда и только тогда, когда a равно или 0, или 5. Так как первая цифра десятичной записи числа не может быть равной 0, $a = 5$. Число $\overline{aba}$ делится на 3 тогда и только тогда, когда на 3 делится его сумма цифр $2a + b = 10 + b$, т. е. тогда и только тогда, когда b равно 2, 5 или 8. *Ответ*: 525, 555, 585.

6.10. Число $\overline{aba}$ делится на 33 тогда и только тогда, когда оно делится на 3 и на 11. Признак делимости на 11 (следствие 3 из предложения 6.2) говорит о том, что число $\overline{aba}$ делится на 11 тогда и только тогда, когда на 11 делится число $2a-b$. Так как $a < 10$ и $b \geqslant 0$, то $2a - b < 20$, а так как $b < 10$ и $a \geqslant 0$, то $2a - b > -10$. Таким образом, число $2a - b$ делится на 11 тогда и только тогда, когда либо $2a - b = 0$, либо $2a - b = 11$. Кроме того, число $\overline{aba}$ делится на 3 тогда и только тогда, когда на 3 делится число $2a + b$.

Если $2a-b = 0$, то $b = 2a$, откуда $a < 5$. Кроме того, число $2a+b = 4a$ делится на 3 тогда и только тогда, когда число a делится на 3. Следовательно, $a = 3$ и $b = 6$.

Если $2a - b = 11$, то $2a \geqslant 11$ и потому $a \geqslant 6$. Следовательно, a может быть равным 6, 7, 8 или 9, а b соответственно равно 1, 3, 5 и 7. Лишь одна из этих четырех пар значений a и b удовлетворяет требованию делимости на 3 числа $2a+b$: $a = 8$, $b = 5$. *Ответ*: 363, 858.

6.11. Пусть $m = \overline{ab}$. Тогда число $\overline{ab} + \overline{ba} = (10a + b) + (10b + a) = 11 \cdot (a + b)$ делится на 11, и так как это число является квадратом (и число 11 простое), то оно должно делиться на 11^2. Отсюда $11 \mid a + b$, и так как $1 < a + b < 20$, то $a + b = 11$. Обратно, если $a + b = 11$, то $\overline{ab} + \overline{ba} = 11^2$. *Ответ*: m равно одному из чисел 29, 38, 47, 56, 65, 74, 83, 92.

6.12. Записать данное число $\overline{abc}$ в виде $\overline{abc} = 100a + 10b + c = (98a + 7b) + 2a + 3b + c = 7(14a + b) + 2(a + b + c) + (b - c) = 7(14a + b + 2) + (b - c)$.

6.13. Если данное число имеет вид $\overline{ab}$, то $10a + b = a^3 + b^2$ или $a(10 - a^2) = b(b - 1)$. Число, стоящее в правой части последнего равенства неотрицательно и четно. Поэтому $a^2 \leqslant 10$ и число a является четным. Отсюда $a = 2$ и $b = 4$. *Ответ*: 24.

6.14. Данное число имеет вид $\overline{abab} = a \cdot 10^3 + b \cdot 10^2 + a \cdot 10 + b = m \cdot 101$, где $m = \overline{ab}$, и потому делится на простое число 101. Если бы оно являлось квадратом, то должно было бы делиться на число 101^2, а потому m должно было бы делиться на 101, что невозможно, так как $0 < m < 100$.

6.15. Если a и b — данные двузначные числа, то соответствующее четырехзначное число m имеет вид $m = 100a + b$. Так как $ab \mid m$, то $a \mid m$ и $b \mid m$, откуда следует, что $a \mid b$ и $b \mid 100a$ соответственно. Тогда $b = ak$, причем поскольку $a \geqslant 10$

и $b < 100$, выполнено неравенство $k < 10$. Условие $b \mid 100a$ теперь дает $k \mid 100$, так что k совпадает с одним из чисел 1, 2, 4, 5. Если $k = 1$, то $a = b$ и число $m = 101a$ должно делиться на a^2. Но тогда простое число 101 должно делиться на двузначное число a, что невозможно. Пусть $k = 2$, тогда $b = 2a$ и число $m = 102a$ должно делиться на $2a^2$, откуда $a \mid 51$. Число 51 имеет два двузначных делителя 17 и 51. Но при $a = 51$ число $b = 2a$ не является двузначным. Таким образом, в этом случае $a = 17$ и $b = 34$. Пусть $k = 4$, тогда $b = 4a$ и число $m = 104a$ должно делиться на $4a^2$, откуда $a \mid 26$. Таким образом, в этом случае $a = 13$ и $b = 52$. Пусть, наконец, $k = 5$, тогда $b = 5a$ и число $m = 105a$ должно делиться на $5a^2$, откуда $a \mid 21$. Единственный двузначный делитель числа 21, совпадающий с самим этим числом, не подходит, так как тогда число $b = 5a$ не будет двузначным. *Ответ*: 17 и 34 или 13 и 52.

§ 7

7.1. Ввиду единственности записи комплексного числа равенство $a + b\,i = c(x + y\,i)$ выполнено тогда и только тогда, когда $a = cx$ и $b = cy$.

7.2. Воспользоваться равенством $a + b\,i = a(1 + i) + (b - a)i$, четностью числа $b - a$ и тем, что $2 = (1 + i)(1 - i)$.

7.3. Первое утверждение содержится в задаче 7.2, а второе в силу равенства $(1 + i)^2 = 2\,i$ вытекает из задачи 7.1.

7.4. Воспользоваться предложением 7.5.

7.5. Если число $z = a + b\,i$ делит в кольце Γ число $3 + i$, то целое число $a^2 + b^2$ должно быть делителем числа $N(3 + i) = 10$. Так как нас интересуют лишь необратимые делители числа $3 + i$, имеем $a^2 + b^2 = 2$ или $a^2 + b^2 = 5$. Если $a^2 + b^2 = 2$, то $z = \pm(1 + i)$ или $z = \pm(1 - i)$. Остается понять, является ли одно из этих чисел делителем числа $3 + i$, и непосредственная проверка показывает, что $3 + i = (1 + i)(2 - i)$. Простота сомножителей этого разложения следует из предложения 7.5. *Ответ*: $3 + i = (1 + i)(2 - i)$.

7.6. *Ответ*: $-4 + 7\,i = (1 + 2\,i)(2 + 3\,i)$.

7.7. *Ответ*: $5 - 5\,i = (1 + 2\,i)(1 - 2\,i)(1 - i)$.

7.8. *Ответ*: $3 + 7\,i = (1 + i)(5 + 2\,i)$.

7.9. *Ответ*: $7 + 9\,i = (1 + i)(1 + 2\,i)(-3 - 2\,i)$.

7.10. *Ответ*: $6 + 12\,i = (-8 + 4\,i) \cdot (-i) + (2 + 4\,i)$.

7.11. *Ответ*: $5 + 3\,i = (2 - i) \cdot (1 + 2\,i) + 1$.

7.12. *Ответ*: $1 + 2\,i$.

7.13. *Ответ*: $1 + i$.

7.14. Доказать для кольца Λ аналоги предложений 7.2, 7.3, 7.8, 7.12 7.13, 7.14 и 7.15. Для доказательства единственности разложения в произведение простых элементов провести рассуждение, аналогичное соответствующему рассуждению для кольца Γ.

Литература для дополнительного чтения

1. Соминский И. С. О математической индукции. М., 1967.
2. Фомин С. В. Системы счисления. (Серия "Популярные лекции по математике") М., 1964.
3. Калужнин Л. А. Основная теорема арифметики. (Серия "Популярные лекции по математике") М., 1969.
4. Успенский В. А. Треугольник Паскаля. (Серия "Популярные лекции по математике") М., 1966.
5. Воробьев Н. Н. Признаки делимости. (Серия "Популярные лекции по математике") М., 1988.
6. Оре О. Приглашение в теорию чисел. (Библиотечка журнала "Квант". Вып. 3) М., 1980.
7. Серпинский В. 250 задач по элементарной теории чисел. (Серия "Математическое просвещение") М., 1968.
8. Бухштаб А. А. Теория чисел. М., 1966.
9. Виноградов И. Н. Основы теории чисел. М., 1965.
10. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М., 1987.
11. Феферман С. Числовые системы. Основания алгебры и анализа. М., 1971.
12. Кострикин А. И. Введение в алгебру. М., 1977.

Оглавление