

*Н.Н.Воробьев*

**ПРИЗНАКИ ДЕЛИМОСТИ**

Издание второе, исправленное, М.: НАУКА, 1974

**СОДЕРЖАНИЕ**

Предисловие	3
§ 1. Делимость чисел	7
§ 2. Делимость сумм и произведений	24
§ 3. Признаки равноостаточности и признаки делимости	29
§ 4. Делимость степеней	44
Доказательства теорем	44
Решения задач	53

## ПРЕДИСЛОВИЕ,

которое автор советует прочесть особенно внимательно

Современное школьное математическое образование ориентировано главным образом на воспитание у учащихся функционального мышления, на умение обращаться с непрерывными математическими объектами. Намечающиеся изменения в школьных программах по математике идут в том же направлении. Вместе с тем в последнее время стали интенсивно разрабатываться новые области применения математики: составление программ для вычислительных машин, некоторые аспекты кибернетики и исследования операций, математическая экономика, математическая лингвистика и т. д. Освоение этих областей науки наряду с совершенствованием классического аппарата требует развития комбинаторной техники, анализа дискретного и создания новых плодотворных абстракций. Перечисленные стороны математики должны освещаться и в научно-популярной литературе.

\* \* \*

С опушки леса в чащу ведет множество тропинок. Они извилисты, они сходятся, расходятся вновь и пересекаются одна с другой. На прогулке можно только заметить обилие этих тропинок, походить по некоторым из них и проследить их направление в глубь леса. Для серьезного изучения леса нужно идти по тропинкам, пока они вообще различимы среди сухой хвои и кустиков черники. Для того чтобы использовать дары леса,

приходится вовсе покидать хоженные тропки и проди- раться сквозь сплетения колючих сучьев.

Настоящую брошюру можно рассматривать как опи- сание одной из возможных прогулок по опушке совре- менной математики. Изложение основных фактов, отно- сящихся к признакам делимости, является в ней повод- ом затронуть некоторые довольно абстрактные вопросы дискретной математики. К числу таких вопросов отно- сятся, прежде всего, утверждения элементарной теории чисел, группирующиеся вокруг основной теоремы ариф- метики и анализа канонического разложения натураль- ного числа на простые множители. Далее, сама дели- мость чисел рассматривается как отношение на множе- стве целых чисел, т. е. как реализация довольно общего и абстрактного понятия. Наконец, признаки делимости трактуются здесь как алгоритмы, перерабатывающие каждое число в ответ, делится ли оно на данное число или не делится. Автор счел целесообразным среди при- знаков делимости особо выделить «признаки равнооста- точности», перерабатывающие числа в остатки при их делении на данное число.

Для того чтобы оттенить разнообразные взаимосвязи между отдельными математическими фактами и возмож- ности различных подходов к одному и тому же пред- мету, некоторые утверждения устанавливаются двумя различными путями.

\* \* \*

Книжка рассчитана на школьников старших классов, интересующихся математикой и (если не считать не- скольких упоминаний о формуле бинома) не предпола- гает никаких предварительных знаний, кроме умения производить несложные тождественные преобразования. Однако логическая структура материала довольно сложна, так что усвоение его во всех деталях может потребовать немало внимания и терпения.

Читателю можно порекомендовать следующий план изучения книжки.

При первом чтении можно ограничиться лишь основным текстом §§ 1—3 и не решать задач (за исключением задач №№ 31, 33, 35, 41, 43, 45, 46). Это даст общее, описательное знакомство с предметом. Так как большинство неискушенных в математике людей убеждены в изначальной справедливости теоремы об однозначном разложении натурального числа на простые множители (считая, по-видимому, ее своего рода аксиомой), они могут понимать теоремы 9—13 как ее следствия.

При втором чтении нужно попытаться самостоятельно доказать все теоремы в том порядке, в каком они приведены. Чтобы читатель не поддавался слишком часто соблазну пользоваться готовыми доказательствами теорем, все эти доказательства отнесены в особый раздел. Исключение составляет доказательство теоремы 7, которое призвано служить камертоном, настраивающим читателя уже при первом чтении на должный уровень строгости.

При втором же чтении следует изучить § 4, а также решать задачи основного текста.

Наконец, при третьем чтении изучается мелкий шрифт и относящиеся к нему задачи.

Читателю, желающему углубить свои познания в области теории чисел, следует обратиться к классическому курсу акад. И. М. Виноградова «Основы теории чисел» («Наука», 1972).

Изучение абстрактной теории отношений на множестве и дальнейших связанных с этим вопросов можно рекомендовать по книге А. Г. Куроша «Лекции по общей алгебре» («Наука», 1973) или Г. Биркгофа «Теория структур» (ИЛ, 1951).

Наконец, более подробное и систематическое разъяснение понятия алгорифма содержится в брошюре Б. А. Трахтенброта «Алгоритмы и машинное

решение задач» (Физматгиз, 1960), а строгое изложение теории алгорифмов можно найти в монографии одного из создателей этой теории, А. А. Маркова «Теория алгорифмов» (Труды матем. ин-та АН СССР им. Стеклова, т. 42, 1954).

Второе издание отличается от первого лишь отдельными редакционными улучшениями. За некоторые из них автор благодарен проф. Греллю (ГДР).

*Н. Н. Воробьев*

## § 1. ДЕЛИМОСТЬ ЧИСЕЛ

1. Сумма, разность и произведение двух целых чисел всегда целые числа. Этот факт иногда принято называть *замкнутостью* множества целых чисел по отношению к действиям сложения, вычитания и умножения.

По отношению же к действию деления множество всех целых чисел замкнутым не является: частное от деления одного целого числа на другое может, вообще говоря, и не быть целым.

Поэтому при изучении обстоятельств, связанных с делением целых чисел, одним из первых встает вопрос о выполнимости этого действия для данных двух чисел, т. е. о *делимости* этих чисел. При рассмотрении остальных арифметических действий над целыми числами подобный вопрос, очевидно, не возникает.

В дальнейшем мы будем считать известными основные свойства арифметических действий над целыми числами, а также простейшие свойства равенств и неравенств. Под «числом» всегда, если не оговорено противное, будет пониматься целое число.

Как обычно, целые неотрицательные числа: 0, 1, 2, ... будут называться *натуральными*. Говоря о всех натуральных числах, мы будем пользоваться термином *множество всех натуральных чисел*.

**О п р е д е л е н и е.** Число  $a$  делится на число  $b$  (или, что то же самое, число  $b$  делит число  $a$ ), если существует такое число  $c$ , что  $a = bc$ .

Этот факт называется *делимостью* числа  $a$  на число  $b$  и обозначается как  $a : b$ .

Подчеркнем, что запись  $a : b$  означает не какое-то действие, которое надлежит произвести над числами  $a$  и  $b$ , а некоторое утверждение, касающееся этих чисел.

В зависимости от того, каковы числа  $a$  и  $b$ , утверждение  $a : b$  может быть верным или неверным. Так, например,  $4 : 2$  верно, а  $4 : 3$  — нет.

Для выяснения того, является ли утверждение  $a : b$  верным или нет, т. е. для выяснения делимости числа  $a$  на число  $b$ , имеется довольно много разнообразных способов. Один из них состоит в непосредственном делении числа  $a$  на число  $b$ . Однако такое деление часто оказывается слишком долгим и утомительным занятием, и естественно появляется желание установить истинность интересующей нас делимости, не производя фактического деления. Не лишним представляется и такое соображение: нас интересует только факт делимости числа  $a$  на число  $b$ ; если же мы выполним деление, то мы попутно узнаем еще и частное от этого деления и остаток от него (если деление нацело «не получилось»); все эти числа, однако, для нас никакой ценности не представляют, так как мы в данный момент интересуемся только тем, будет ли остаток от деления равен нулю или нет. Значит, есть основания предполагать, что, выполняя деление, мы какую-то (и по-видимому, немалую) часть работы потратили на получение «отходов производства». Можно надеяться, что более прямые способы выяснения делимости, чем «грубое» деление, которые не дадут нам столь обильных отходов, будут экономнее и позволят установить факт делимости более коротким путем. Эти надежды в действительности оправдываются, и такие способы выяснения делимости существуют. Они называются *признаками делимости*.

Некоторые признаки делимости, несомненно, известны читателю. Целью этой книжки является рассмотрение различных признаков делимости, главным образом с принципиальной стороны.

Сущность всякого признака делимости на данное число  $b$  состоит в том, что при его помощи вопрос о делимости любого числа  $a$  на  $b$  сводится к вопросу о делимости на  $b$  некоторого числа, меньшего, чем  $a$ . (Нетрудно видеть, что проверка делимости обычным делением также основана на этой идее.)

Таким образом, признак делимости является математическим объектом весьма распространенной, хотя и не бросающейся в глаза природы. Это не формула, не теорема, не определение, а некоторый процесс, совершенно такого же типа, что и процесс умножения чисел

«столбиком» или, скажем, процесс вычисления одного за другим членов арифметической прогрессии.

Понятие признака делимости будет уточнено в следующем параграфе.

2. В определении делимости чисел ничего не говорится о том, сколько различных значений может иметь частное от деления  $a$  на  $b$ . Выясним здесь этот вопрос до конца, чтобы в дальнейшем к нему больше не возвращаться.

Пусть

$$a = bc, \quad (1)$$

и вместе с тем

$$a = bc_1.$$

Из этих равенств мы получаем

$$bc = bc_1,$$

или

$$b(c - c_1) = 0.$$

Если при этом  $b \neq 0$ , то  $c - c_1 = 0$ , т. е.  $c = c_1$ . Если же  $b = 0$ , то, очевидно, и  $a = 0$ , а равенство (1) выполняется при любом  $c$ .

Таким образом, на нуль делится только нуль, а частное от такого деления неопределенно. Именно это и имеется в виду, когда говорят о невозможности деления на нуль. Если же делитель отличен от нуля и делимость имеет место, то частное имеет одно, вполне определенное значение.

Говоря о делении, мы всегда будем предполагать делитель отличным от нуля.

Установим несколько простейших свойств делимости.

Теорема 1.  $a : a$ .

Это свойство делимости называется ее *рефлексивностью* (или *возвратностью*).

Теорема 2. Если  $a : b$  и  $b : c$ , то  $a : c$ .

Это свойство делимости называется ее *транзитивностью* (или *переходностью*).

Теорема 3. Если  $a : b$  и  $b : a$ , то либо  $a = b$ , либо  $a = -b$  (*антисимметричность* делимости).

Теорема 4. Если  $a : b$  и  $|b| > |a|$ , то  $a = 0$ .

Следствие. Если  $a : b$  и  $a \neq 0$ , то  $|a| \geq |b|$ .

Теорема 5. Для того чтобы  $a : b$ , необходимо и достаточно, чтобы  $|a| : |b|$ .



На основании этой теоремы в дальнейшем достаточно ограничиваться рассмотрением случая, когда делитель есть положительное число

**Теорема 6.** Если  $a_1 : b, a_2 : b, \dots, a_n : b$ , то

$$a_1 + a_2 + \dots + a_n : b.$$

**С л е д с т в и е.** Если сумма двух чисел и одно из слагаемых делится на некоторое число  $b$ , то другое слагаемое также делится на  $b$ .

Не следует считать все эти теоремы очевидными и не нуждающимися в каком-либо особом доказательстве. Дело здесь даже не в том, что в математике доказательству подлежит всякое утверждение, кроме аксиом и определений. Доказательства этих фактов (например того, что всякое число делится на себя) принципиально необходимы, так как они не могут быть получены только из определения делимости, а нуждаются в использовании свойств самих чисел.

Подробнее в этом разобратся нам поможет следующий пример.

Очевидно, сумма, разность и произведение четных чисел всегда четны. Вместе с тем деление одного четного числа на другое не всегда выполнимо, а если и выполнимо, то частное не обязательно четно. Поэтому можно ввести понятие четной делимости четных чисел.

**О п р е д е л е н и е.** Четное число  $a$  *четно делится* на четное число  $b$ , если существует такое четное число  $c$ , что  $a = bc$ .

Очевидно, для четной делимости теорема 1 неверна, так как, например, не существует такого четного числа  $c$ , для которого  $a = ac$ .

К вопросам, связанным с четной делимостью четных чисел, мы еще будем несколько раз возвращаться. Пример четной делимости показывает, что можно строить различные теории делимости с различными свойствами, и теоремы, верные для одних таких теорий, могут оказаться неверными для других.

**Задачи.** Доказать следующие утверждения:

1.  $0 : a$ .

2.  $a : 1$ .

3. Если  $1 : a$ , то  $a = 1$ .

4. Каково бы ни было  $a \neq 0$ , существует такое отличное от  $a$  число  $b$ , что  $b : a$ .

5. Каково бы ни было число  $a$ , существует такое число  $b$ , что из  $b : c$  и  $c : a$  следует либо  $c = b$ , либо  $c = a$ .

6. Доказать теоремы, аналогичные теоремам 2, 3, 4 и 5, для четной делимости.

7. Построить такую теорию делимости, в которой теоремы 1, 3 и 4 были бы верными, а теоремы 2 и 6 — нет.

3. Уже при самом беглом знакомстве с конкретными фактами делимости бросается в глаза следующее обстоятельство: делимость чисел практически не связана с их величиной. С одной стороны, существуют маленькие числа, которые делятся на сравнительно большое количество чисел. Например, 12 делится на 1, 2, 3, 4, 6 и 12; число 60 имеет 12 делителей. Таким богатым делителями числам можно противопоставить весьма большие числа, которые имеют минимальное число делителей — 2 (согласно теореме 1 и задаче 2, каждое отличное от единицы число делится хотя бы на два различных числа). Хотя в действительности и известны некоторые закономерности, связывающие свойства делимости чисел с их величиной, но эти закономерности носят столь сложный и запутанный характер, что мы не будем их здесь касаться.

4. Тем более интересным оказывается тот факт, что сама делимость позволяет установить среди чисел некоторый порядок, отличающийся от их обычного порядка по величине, но имеющий с ним много общего.

В самом деле, задумаемся, какой точный смысл вкладывается в слова о возможности упорядочить натуральные числа по их величине. Под этой возможностью, как нетрудно видеть, понимается то, что для некоторых пар чисел  $a$  и  $b$  имеет место отношение «больше или равно»:

$$a \geq b,$$

которое означает, что разность  $a - b$  неотрицательна (т. е. должно существовать такое натуральное число  $c$ , что  $a = b + c$ ). Но ведь и явление делимости состоит в том, что некоторые пары чисел  $a$  и  $b$  подчиняются некоторому, вполне определенному условию (именно, существует такое целое  $c$ , что  $a = bc$ )! Таким образом, отношение делимости и отношение «больше или равно» представляют собой понятия одной природы, и потому можно говорить об их общих свойствах или, наоборот, противопоставлять их друг другу.

В частности, подобно отношению делимости, отношение «больше или равно» между двумя натуральными числами является некоторым высказыванием об этих

числах и может быть верным (например,  $5 \geq 3$ ) или неверным (например,  $3 \geq 5$ ).

Заметим сразу же, что отношение «больше или равно» имеет больше общих свойств с отношением делимости, чем отношение «больше». Это связано с тем, что отношение «больше или равно», подобно отношению делимости, рефлексивно (действительно, соотношение  $a \geq a$  справедливо для любого  $a$ ), а отношение «больше» рефлексивным не является (неравенство  $a > a$  не имеет места никогда). Именно поэтому здесь в качестве отношения порядка между натуральными числами рассматривается отношение «больше или равно», а не, казалось бы, более простое и естественное отношение «больше».

5. Отношение  $\geq$  обладает следующими легко проверяемыми свойствами:

1°  $a \geq a$  (рефлексивность).

2° Если  $a \geq b$  и  $b \geq a$ , то  $a = b$  (антисимметричность).

3° Если  $a \geq b$  и  $b \geq c$ , то  $a \geq c$  (транзитивность).

4° Во всякой последовательности натуральных чисел

$$a_1 \geq a_2 \geq a_3 \geq \dots \geq a_n \geq \dots,$$

все члены которой отличны друг от друга, найдется последнее число. Это свойство отношения иногда называется свойством *полной упорядоченности* множества натуральных чисел.

Свойство полной упорядоченности довольно сложно по формулировке и выглядит несколько искусственно. Однако оно вскрывает чрезвычайно важные черты в строении множества натуральных чисел, упорядоченных отношением  $\geq$ . Из него выводятся многие другие свойства этого отношения. Кроме того, мы увидим, что именно на нем основаны столь употребительные в разных вопросах математики рассуждения «по индукции».

В качестве полезного применения этого свойства отметим следующее: существует такое число  $a$ , что из  $a \geq b$  следует  $a = b$  (здесь  $a$  и  $b$  — натуральные числа).

В самом деле, если бы такого числа не было, то мы могли бы по каждому  $a_n$  находить такое  $a_{n+1}$ , что  $a_n \geq a_{n+1}$  и  $a_n \neq a_{n+1}$ . Начав с произвольного  $a_1$ , мы получили бы последовательность

$$a_1 \geq a_2 \geq a_3 \geq \dots \geq a_n \geq a_{n+1} \geq \dots,$$

которая никогда не кончается. Но существование такой последовательности противоречит свойству полной упорядоченности множества натуральных чисел.

Таким образом, указанное число  $a$  действительно существует. Оно называется *первым*, или *минимальным*, числом (очевидно, это нуль). Заметим здесь же, что мы сейчас не установили единственности минимального числа. Эта единственность будет зафиксирована далее косвенным путем.

5° Каково бы ни было число  $a$ , существует отличное от  $a$  число  $b$ , для которого  $b \geq a$ .

Это свойство множества натуральных чисел называется его *неограниченностью* в смысле отношения  $\geq$ .

6° Каково бы ни было число  $a$ , не являющееся минимальным, существует такое  $b$ , что  $a \geq b$ ,  $a \neq b$ , и для любого числа  $c$  из  $a \geq c \geq b$  следует либо  $c = a$ , либо  $c = b$ . Это формальное утверждение в переводе на содержательный язык означает, что каждое натуральное число, кроме нуля, имеет непосредственно предшествующее натуральное число. (Иначе это можно сформулировать так: среди всех чисел, меньших данного, есть наибольшее.)

7° Либо  $a \geq b$ , либо  $b \geq a$ . Это свойство отношения называется его *дихотомичностью*. В математике термин дихотомичность обычно выражает обязательную реализацию одной из двух возможностей. Само это слово греческого происхождения и означает разделение на две части.

Подчеркнем, что 1°—7° являются свойствами *самого отношения* на множестве всех натуральных чисел, а не свойствами тех или иных чисел, связываемых этим отношением. Поэтому может оказаться, что для какого-нибудь другого отношения, связывающего числа в пары, но не по величине, а каким-либо иным способом, некоторые из утверждений 1°—7° могут оказаться и неверными.

**Задача 8.** Опираясь только на свойства 1°—7° отношения  $\geq$  и не пользуясь никакими свойствами самих чисел и действий над ними

а) доказать единственность минимального числа,

б) доказать единственность непосредственно предшествующего числа,

в) сформулировать определение числа, непосредственно следующего за данным числом  $a$  (т. е. числа  $a + 1$ ), и доказать его существование и единственность.

**Задача 9.** Проверить, какие из утверждений 1°—7° остаются в силе для отношения «больше» ( $>$ ).

6. Справедливость свойств отношения  $\geq$  (как, впрочем, и любого другого отношения) может быть установлена двояко. Во-первых, мы можем воспользоваться свойствами тех или иных чисел или известными особенностями строения множества всех натуральных чисел. Именно так проверялись нами свойства 1°—7°. Во-вторых, мы можем, уже убедившись в справедливости свойств 1°—7°, отвлечься от того, что отношение  $\geq$  связывает числа в пары, и выводить дальнейшие свойства этого отношения только из его свойств 1°—7°. Так были нами доказаны существование минимального числа и утверждения задачи 8.

Второй подход к вопросу весьма употребителен в современной математике и носит название *аксиоматического*. При таком подходе устанавливаются некоторые *аксиомы* (в нашем случае ими являются утверждения 1°—7°), которые отражают основные свойства изучаемых предметов и не подлежат доказательству, а из них чисто логическим путем, без повторного обращения к свойствам исследуемых предметов, выводятся все остальные утверждения, которые называются *теоремами*.

Быть может, некоторым из читателей рассмотрение свойств отношений в отрыве от связываемых этими отношениями объектов (например, чисел) покажется тем верхом математической абстракции, который в практической жизни совершенно не нужен. По этому поводу следует сделать два замечания.

Во-первых, с точки зрения современной математики все проводимые здесь рассуждения вовсе не являются «особенно абстрактными». Более того, в наши дни математикам приходится рассматривать одновременно много отношений и даже (!) связывать пары различных отношений новыми отношениями (так сказать, отношениями «второго порядка»).

Изложенный до сих пор материал позволяет проиллюстрировать понятие отношения между отношениями примером.

Пусть  $\alpha, \beta, \dots$  — некоторый набор отношений, связывающих натуральные числа. Это значит, что для любой пары чисел  $a$  и  $b$  и любого отношения  $\gamma$  из нашего набора мы знаем, связывается ли пара  $a, b$  отношением  $\gamma$  или нет. Если  $a$  и  $b$  отношением  $\gamma$  связаны, будем писать  $\alpha\gamma b$ .

Будем говорить, что отношение  $\alpha$  сильнее отношения  $\beta$  и записывать это как  $\alpha \supset \beta$ , если любая пара чисел, связанная отношением  $\beta$ , оказывается также связанной и отношением  $\alpha$ , т. е. если из  $\alpha\beta b$  следует  $\alpha a b$ .

Так, например, обозначая отношение четной делимости через  $\underset{4}{:}$ , мы можем написать  $\underset{4}{:} \supset \underset{4}{:}$ . Далее, очевидно, что  $\geq \supset \underset{4}{:}$ . Наоборот, ни  $\underset{4}{:} \supset \geq$ , ни  $\geq \supset \underset{4}{:}$  не имеет места: отношение делимости и отношение «больше или равно» между собой отношением  $\supset$  не связаны. Именно это обстоятельство и было словесно описано в п. 3.

Конечно, для свободного оперирования столь сложными понятиями как отношения между отношениями необходима специальная тренировка.

Во-вторых, такие и даже еще более отвлеченные рассуждения все чаще и чаще начинают встречаться в приложениях математики к экономике, биологии, лингвистике, военному делу. К сожалению, более подробные пояснения на этот счет увели бы нас слишком далеко от основного предмета.

7. С упорядоченностью множества натуральных чисел отношением  $\geq$  тесно связана возможность применять метод *полной индукции* (называемый также методом *совершенной индукции* или методом *математической индукции*). Обычно этот метод применяется в следующей форме. Пусть  $A(n)$  — некоторое утверждение, касающееся произвольного натурального числа  $n$ . Это, по существу, означает, что мы имеем дело с бесконечной последовательностью утверждений

$$A(0), A(1), \dots, A(n), \dots$$

о каждом из натуральных чисел. Предположим, что

а) справедливо утверждение  $A(0)$  («основание индукции» \*);

\*) Часто за основание индукции принимают утверждение  $A(1)$ . Очевидно, это различие не является существенным. Важно лишь, что основание индукции касается первого из рассматриваемых нами чисел.

б) из справедливости утверждения  $A(n)$  следует справедливость утверждения  $A(n+1)$  («индуктивный переход»).

Принцип математической индукции утверждает, что в предположениях а) и б)  $A(n)$  справедливо для любого натурального  $n$ .

Принцип математической индукции не является каким-то самостоятельным утверждением, а может быть выведен из свойств 1°—7° упорядочения множества натуральных чисел отношением  $\geq$ .

Действительно, предположим, что условия а) и б) принципа индукции для утверждений  $A(n)$  выполнены, но заключение этого принципа не имеет места. Последнее означает, что должны существовать такие числа  $m$ , для которых утверждение  $A(m)$  неверно. Пусть  $m_1$  — одно из таких чисел. Если для всех  $n < m_1$  утверждение  $A(n)$  верно, то  $m_1$  — наименьшее из чисел, для которых  $A(n)$  не имеет места. Если же  $A(n)$  верно не для всех  $n < m_1$ , то должно существовать такое  $m_2 < m_1$ , что  $A(m_2)$  неверно.

В итоге мы приходим к некоторой последовательности различных чисел,

$$m_1 \geq m_2 \geq \dots \geq m_r \geq \dots, \quad (2)$$

для каждого из которых  $A(m)$  не имеет места. По свойству полной упорядоченности 4° в последовательности (2) должен быть последний член  $m_r$ . Очевидно, число  $m_r$  является наименьшим из всех чисел, для которых  $A(n)$  неверно.

Поскольку  $A(0)$  верно по условию,  $m_r \neq 0$ , так что существует число  $m_r^*$ , непосредственно предшествующее  $m_r$  (в действительности этим числом является  $m_r - 1$ ). Так как  $m_r^* < m_r$ , утверждение  $A(m_r^*)$  должно быть верным. Но тогда по условию б) принципа математической индукции должно быть верным также и утверждение  $A(m_r^* + 1)$ , т. е.  $A(m_r)$ , и мы получили противоречие. Это противоречие показывает, что нет чисел  $m$ , для которых  $A(m)$  не имело бы места (т. е. не было бы справедливо).

Сделаем следующее замечание. Проведенные только что рассуждения не следует считать ни доказательством принципа индукции, ни его обоснованием. Они означают лишь возможность вывода одного математического утверждения (метода индукции) из других (из свойств отношения  $\geq$ ). Сами же эти свойства принимались нами в качестве аксиом, и потому не доказывались, а лишь проверялись. Всякая попытка их математического доказательства неизбежно натолкнулась бы на необходимость введения в качестве аксиом каких-то новых условий.

В частности, доказательства свойства полной упорядоченности должны использовать те же индуктивные рассуждения (читатель может в этом убедиться сам).

Методу математической индукции в его различных вариантах посвящены брошюры И. С. Соминского «Метод математической индукции» («Наука», 1974) и

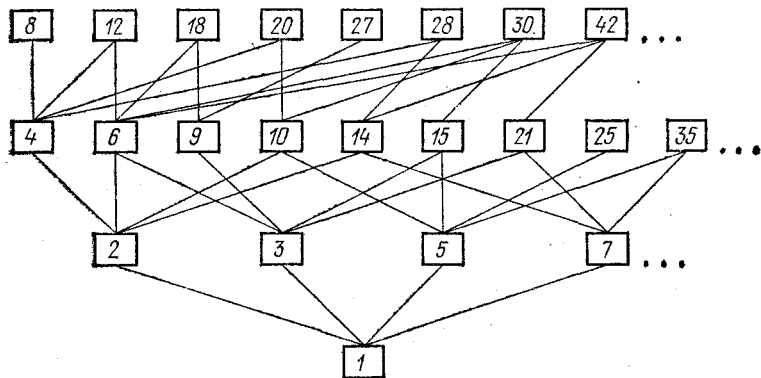
Л. И. Головиной и И. М. Яглома «Индукция в геометрии» («Наука», 1956), содержащие большое количество примеров применения этого метода. На протяжении данной книги этот метод также будет часто применяться.

*Задача 10.* Пусть пары объектов произвольной природы (ими могут быть числа, точки, функции, теоремы и т. д.) связываются некоторым отношением  $\xi$ , обладающим свойствами, аналогичными свойствам  $1^\circ-7^\circ$ . Доказать, что тогда эти объекты (элементы) можно перенумеровать (т. е. выписать их в некотором порядке):  $A_1, A_2, A_3, \dots$  так, что  $A_i \xi A_j$  тогда и только тогда, когда  $i \geq j$ .

Сказанное, по существу, означает, что отношение, обладающее свойствами  $1^\circ-7^\circ$ , упорядочивает множество в линейную цепочку элементов:

$$A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow \dots$$

8. Вернемся, однако, к отношению делимости. В случае положительных чисел теоремы 1, 2, 3 и задачи 3, 4 и 5 показывают, что в утверждениях  $1^\circ-6^\circ$  мы можем заменить отношение  $\geq$  отношением  $\vdots$ . Что же касается утверждения  $7^\circ$ , то в применении к делимости оно гласит: «из двух чисел хотя бы одно делится на другое».



Но это неверно. Таким образом, отношение делимости обладает всеми свойствами отношения порядка за исключением одного. В связи с этим отношение делимости упорядочивает натуральные числа не в виде линейной цепочки, а иным, более сложным образом (см. рисунок). Заметим, что числа, близкие по величине, могут оказаться довольно «далекими» друг от друга в смысле делимости. Наглядно демонстрируют это числа 4 и 5 или 7 и 8.

Попробуем от делимости целых положительных чисел перейти к делимости чисел натуральных, т. е. включим в рассмотрение нуль. Тогда схема на рисунке пополнится клеткой, лежащей выше всех остальных клеток схемы, ибо нуль делится на любое число, и ни одно из чисел, отличных от нуля, на нуль не делится.

Читателю предоставляется самостоятельно переформулировать и проверить утверждения 1°—7° для этого случая.

9. Определение. Любое отношение  $\xi$ , подчиненное условиям:

1° рефлексивности ( $a \xi a$ );

2° антисимметричности (из  $a \xi b$  и  $b \xi a$  следует  $a = b$ );

3° транзитивности (из  $a \xi b$  и  $b \xi c$  следует  $a \xi c$ ),

называется *частично упорядочивающим отношением*. Частично упорядочивающие отношения играют большую роль там, где «настоящее», линейное упорядочение не имеет места, например там, где каждый объект описывается или оценивается по нескольким различным, качественно несравнимым между собой показателям.

В качестве примера можно привести оценку результатов спортивных соревнований по нескольким различным видам спорта. Если одна из команд заняла по всем видам программы соревнований более высокие места, чем другая, то естественно считать, что первая команда добилась больших успехов. Если же эти более высокие места были заняты по всем видам программы, за исключением, скажем, игры в крокет (которая почему-то на этот раз оказалась включенной в программу соревнований), где вторая команда оказалась сильнее, то вопрос об окончательном распределении мест между нашими командами оказывается уже не столь очевидным. Энтузиасты игры в крокет могут даже настаивать на более высоком месте для второй команды. Во всяком случае любое суммарное распределение мест должно быть связано с некоторыми условными пересчетами (например, с приписыванием очков).

10. Условия 1°—3°, соблюдение которых делает отношение  $\xi$  отношением частичного упорядочения, являются довольно свободными. Поэтому частично упорядоченными могут быть самые разнообразные объекты и притом упорядоченными весьма различными способами. В связи с этим о произвольном частично упорядочивающем отношении мало что можно сказать сверх того, что оно частично упорядочивающее. В частности, к объектам, для которых определено частично упорядочивающее отношение, нельзя, вообще говоря, применить метод математической индукции.

Дополним, однако, условия 1°—3° следующими:

4° полная упорядоченность;

5° неограниченность;

6° каждый объект, отличный от минимального, имеет непосредственно предшествующего;

8° каждый объект имеет не более конечного числа предшествующих;

9° каковы бы ни были  $a$  и  $b \xi a$  ( $b \neq a$ ), существует такое  $c$ , непосредственно предшествующее  $b$ , что  $c \xi a$ .

Оказывается, что на основе частичной упорядоченности множества натуральных чисел отношением, которое удовлетворяет условиям 1°—6°, 8° и 9°, можно построить некоторое видоизменение метода индукции, состоящее в следующем.



Пусть снова  $A(n)$  — утверждение, касающееся произвольного числа  $n$ . Предположим, что

а) справедливо утверждение  $A(a)$ , где  $a$  есть минимальное число в смысле упорядочения  $\xi$ ;

б) если  $n$  — некоторое число, и справедливость всех утверждений вида  $A(m)$  для всех таких  $m$ , что  $n \xi m$  и  $n \neq m$ , установлена, то верно и утверждение  $A(n)$ .

Новая форма принципа индукции утверждает, что при соблюдении условий а) и б) утверждение  $A(n)$  справедливо при любом  $n$ .

**Задача 11.** Вывести «новую форму» принципа индукции из ее «старой формы».

Так как отношение делимости условиям  $1^\circ$ — $6^\circ$ ,  $8^\circ$  и  $9^\circ$  удовлетворяет (сформулируйте и проверьте для отношения делимости условия  $8^\circ$  и  $9^\circ$ ), этот принцип индукции к отношению делимости применим.

В применении к делимости новый принцип индукции может быть сформулирован так: если некоторое утверждение  $A(n)$  справедливо при  $n = 1$  и из справедливости его для всех делителей числа  $n$ , отличных от  $n$ , следует его справедливость для  $n$ , то оно имеет место для любого числа.

11. Деление целых чисел, как мы видели, выполнимо не всегда. Поэтому целесообразно наряду с действием деления рассматривать и другое, более общее действие, которое всегда выполнимо, а в случае выполнимости действия деления, по существу, совпадает с ним. Таким действием является *деление с остатком*.

**Определение.** Разделить число  $a$  на число  $b$  ( $b > 0$ ) с остатком — значит представить число  $a$  в виде

$$a = bq + r,$$

где  $0 \leq r < b$ .

Число  $q$  при этом называется *неполным частным*, а число  $r$  — *остатком* от деления  $a$  на  $b$ . Очевидно,  $r = 0$  тогда и только тогда, когда  $a \vdots b$ . В этом случае  $q$  равно частному от деления  $a$  на  $b$ .

Покажем, что деление с остатком всегда выполнимо, а неполное частное и остаток вполне определяются делимым и делителем, т. е. единственны.

Пусть сначала  $a \geq 0$ . Будем выписывать одно за другим числа

$$a, a - b, a - 2b, \dots \quad (3)$$

до тех пор, пока не появится отрицательное число (очевидно, рано или поздно такое число должно появиться \*). Пусть последним из неотрицательных чле-

\*) Точнее говоря, это следует из полной упорядоченности множества натуральных чисел отношением  $\geq$ .

нов последовательности (3), т. е. самым маленьким из них, окажется число  $a - bq$ . Обозначая его через  $r$ , мы имеем

$$a = bq + r. \quad (4)$$

Очевидно,  $r < b$  (иначе бы число  $r - b$ , т. е.  $a - (q + 1)b$ , было бы неотрицательным, а этого не может быть, так как  $r$  — наименьшее из неотрицательных чисел среди (3)). Таким образом, (4) и является искомым представлением числа  $a$ .

Пусть теперь  $a < 0$ . Рассуждая аналогично предыдущему, будем выписывать последовательность чисел

$$a, a + b, a + 2b, \dots$$

до тех пор, пока не появится первое неотрицательное число  $r$  (легко проверить, что  $r < b$ ). Пусть

$$r = a + bq'.$$

Тогда, обозначая  $-q'$  через  $q$ , мы получаем

$$a = bq + r,$$

а это и требовалось.

Возможность деления с остатком доказана во всех случаях.

Докажем теперь однозначность этого деления, т. е. если

$$a = bq + r \quad (5)$$

и вместе с тем

$$a = bq_1 + r_1, \quad (6)$$

то

$$q = q_1 \text{ и } r = r_1.$$

От такого доказательства единственности нельзя отмахнуться попросту, заявив, что так как, дескать, действие вычитания однозначно, последовательность (3) может быть построена единственным способом; последний ее неотрицательный член также вполне определен; пусть это будет наше  $r \dots$  и т. д. Такое рассуждение еще не избавляет нас от возможности

получить другие значения  $q$  и  $r$  каким-нибудь совершенно иным путем.

Сопоставляя отношения (5) и (6), мы видим, что

$$bq + r = bq_1 + r_1,$$

откуда

$$r - r_1 = b(q_1 - q),$$

т. е.  $r - r_1$  делится на  $b$ . Но  $|r - r_1| < b$ , а по теореме 4 это возможно лишь при

$$r - r_1 = 0,$$

т. е. при  $r = r_1$ . Но тогда

$$b(q_1 - q) = 0$$

и ввиду неравенства нулю числа  $b$ ,

$$q_1 - q = 0,$$

т. е.  $q_1 = q$ . Однозначность деления с остатком доказана. Таким образом, нами доказана следующая теорема.

**Теорема 7** (о делении с остатком). Для произвольных чисел  $a$  и  $b$  ( $b > 0$ ) существуют и единственны такие числа  $r$  и  $q$ , что

$$a = bq + r,$$

причем  $0 \leq r < b$ .

**Задача 12.** Сформулировать и доказать теорему о делении с остатком для четной делимости.

**12. Определение.** Число  $p$ , не равное единице, называется *простым*, если оно делится только на себя и на единицу.

Простыми числами являются, например, числа 2, 3, 5, 7, 11, 13 и т. д.

Число, отличное от единицы и не являющееся простым, называется *составным*.

**Теорема 8.** Простых чисел бесконечно много.

Всякое число, делящее одновременно числа  $a$  и  $b$ , называется *общим делителем* этих чисел. Наибольший из общих делителей чисел  $a$  и  $b$  называется их *наибольшим общим делителем* и обозначается обычно через  $(a, b)$ .

Если наибольший общий делитель чисел  $a$  и  $b$  равен единице, то эти числа называются *взаимно простыми*.

Иначе говоря, числа  $a$  и  $b$  называются взаимно простыми, если они одновременно не делятся ни на какое число, кроме единицы.

**Теорема 9.** Если  $a$  и  $p$  — натуральные числа, причем число  $p$  простое, то либо  $a : p$ , либо числа  $a$  и  $p$  взаимно просты.

Всякое число, делящееся одновременно на числа  $a$  и  $b$ , называется *общим кратным* этих чисел. Наименьшее положительное общее кратное  $a$  и  $b$  называется *наименьшим общим кратным* этих чисел.

**Теорема 10.** Если  $M$  — общее кратное  $a$  и  $b$ , а  $m$  — их наименьшее общее кратное, то  $M : m$ .

**Теорема 11.** Наименьшее общее кратное двух взаимно простых чисел равно их произведению.

**Следствие.** Для того чтобы число  $a$  делилось на взаимно простые числа  $b$  и  $c$ , необходимо и достаточно, чтобы оно делилось на их произведение.

**Теорема 12.** Если  $ab : c$ , причем числа  $b$  и  $c$  взаимно простые, то  $a : c$ .

**Теорема 13.** Если произведение нескольких сомножителей делится на простое число  $p$ , то хотя бы один из сомножителей делится на  $p$ .

**Следствие.** Если  $p$  — простое и  $0 < k < p$ , то число

$$C_p^k = \frac{1 \cdot 2 \dots (p-1) p}{1 \cdot 2 \dots (k-1) k \cdot 1 \cdot 2 \dots (p-k-1) (p-k)}$$

делится на  $p$ .

**Теорема 14** (основная теорема арифметики). *Всякое целое положительное число, кроме единицы, может быть представлено в виде произведения простых сомножителей и притом единственным способом (произведения, отличающиеся только порядком сомножителей, различными не считаются).*

Основная теорема арифметики указывает на принципиальную возможность разложения любого числа на простые сомножители. Однако практическое осуществление такого разложения встречает большие трудности, которые современная математика иногда еще не может преодолеть. Разложение больших чисел на множители или установление их простоты в настоящее время осуществляется на основе применения электронных

вычислительных машин. Так, лишь совсем недавно было обнаружено, что число  $2^{19937} - 1$  является простым.

Пусть некоторое число  $a$  разложено в произведение простых сомножителей. Объединяя равные сомножители, мы получим формулу вида

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \quad (7)$$

где  $p_1, p_2, \dots, p_r$  — различные простые числа, а  $\alpha_1, \alpha_2, \dots, \alpha_r$  — некоторые целые положительные числа. Произведение, стоящее в правой части формулы (7), называется *каноническим разложением* числа  $a$ .

*Теорема 15.* Для того чтобы числа  $a$  и  $b$  были взаимно простыми, необходимо и достаточно, чтобы ни один из простых сомножителей, входящих в каноническое разложение числа  $a$ , не входил в каноническое разложение числа  $b$ .

*Теорема 16.* Пусть (7) — каноническое разложение числа  $a$ . Тогда для делимости  $b : a$  необходимо и достаточно, чтобы

$$b : p_1^{\alpha_1}, \quad b : p_2^{\alpha_2}, \quad \dots, \quad b : p_r^{\alpha_r}.$$

Из теорем 15 и 16 вытекает, что делимость на произведение нескольких взаимно простых чисел равносильна одновременной делимости на каждое из них.

*Задача 13.* Оценить сверху наименьший простой делитель составного числа  $a$ .

*Задача 14.* Пусть

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

— каноническое разложение числа  $a$ . Тогда для делимости  $a : b$  необходимо и достаточно, чтобы каноническое разложение  $b$  имело вид

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},$$

где

$$0 \leq \beta_1 \leq \alpha_1,$$

$$0 \leq \beta_2 \leq \alpha_2,$$

.....

$$0 \leq \beta_r \leq \alpha_r.$$

*Задача 15.* Указать способ построения по каноническим разложениям двух чисел канонических разложений наименьшего общего кратного этих чисел и их наибольшего общего делителя.

*Задача 16.* Обозначим через  $\tau(a)$  число различных делителей числа  $a$  (включая единицу и само число  $a$ ). Показать, что для числа  $a$  с каноническим разложением  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

*Задача 17.* Найти  $a$ , если известно, что  $a : 3$ ,  $a : 4$  и  $\tau(a) = 14$ .

*Задача 18.* Каноническое разложение числа  $a$  имеет вид  $p_1^{\alpha_1} p_2^{\alpha_2}$  и  $\tau(a^2) = 81$ . Чему равно  $\tau(a^3)$ ?

*Задача 19.* Чему равно  $a$ , если  $a = 2\tau(a)$ ?

*Задача 20.* Верны ли для четной делимости аналоги теорем 11—14?

## § 2. ДЕЛИМОСТЬ СУММ И ПРОИЗВЕДЕНИЙ

1. Во многих случаях при делении с остатком интересно найти именно остаток от деления числа  $a$  на число  $b$ , а величина неполного частного от деления не играет роли.

Пусть, например, мы хотим узнать, какой день недели будет 1 января 2000 г. (разумеется, если до того срока сохранится действующий в настоящее время календарь). Легко справиться по календарю, что 1 января 1975 г. — среда. Двадцать пять лет, разделяющие эти даты, состоят из  $25 \cdot 365 + 6$  (последнее слагаемое — число високосных лет за это время), т. е. из 9131 дней. Эти дни составляют 1304 целых недель и еще 3 дня. По прошествии 1304 целых недель снова наступит среда, так что еще через 3 дня, 1 января 2000 г., будет суббота. Очевидно, для решения поставленной нами сейчас перед собой задачи совершенно неважно знать, сколько именно целых недель прошло за 25 лет, а интересно только число дней, прошедших сверх этих недель.

С задачами такого рода приходится иногда сталкиваться историкам, особенно востоковедам, при сопоставлении дат, указанных по разным календарям.

Казалось бы, для нахождения остатка от деления одного числа на другое проще всего произвести деление с остатком непосредственно. Однако практически выполнить такое деление нередко представляется весьма затруднительным, особенно если подлежащее исследованию делимое записано не в привычной для нас десятичной системе счисления, а задано в виде некоторого сложного выражения, вроде, скажем,  $2^{1000} + 3^{1000}$ . Вместе с тем львиная доля этой работы будет потрачена на нахождение неполного частного, которое нам само по

себе не нужно. Необходимо поэтому попытаться найти способ нахождения остатка непосредственно, минуя вычисление неполного частного.

Продемонстрируем один из таких приемов на только что решавшейся нами задаче о дате 1 января 2000 г. Мы можем рассуждать следующим образом. Каждый простой (невисокосный) год состоит из 365 дней, что составляет 52 полные недели и еще один день. Високосный же год составляет столько же недель и два дня. Значит, весь срок от 1 января 1975 г. до 1 января 2000 г. состоит из некоторого (совершенно неважно, какого) числа полных недель плюс число дней, равное числу содержащихся в этом сроке лет, причем каждый високосный год считается за два. Это число дней равно  $25 + 6 = 31$ . Исключив из него 4 полные недели, получаем 3 дня, которые и следует отсчитать от нашей среды. Оказывается, такая «замена года днем» есть проявление весьма общего приема, изучением которого мы сейчас и займемся.

**2. Определенные.** Назовем числа  $a$  и  $b$  *равноостаточными* при делении на  $m$ , если остатки от деления  $a$  и  $b$  на  $m$  равны.

Установим несколько свойств равноостаточных чисел.

**Теорема 17.** *Для того чтобы числа  $a$  и  $b$  были равноостаточными при делении на  $m$ , необходимо и достаточно, чтобы  $a - b : m$ .*

**Теорема 18.** *Если при делении на  $m$  числа  $a_1, a_2, \dots, a_n$  соответственно равноостаточны числам  $b_1, b_2, \dots, b_n$ , то равноостаточными будут суммы  $a_1 + a_2 + \dots + a_n$  и  $b_1 + b_2 + \dots + b_n$ , а также произведения  $a_1 a_2 \dots a_n$  и  $b_1 b_2 \dots b_n$ .*

**Следствие.** Если при делении на  $m$  числа  $a$  и  $b$  равноостаточны, то такими же являются и степени  $a^n$  и  $b^n$  при любом натуральном  $n$ .

Теорема 18 и ее следствия дают уже довольно богатые возможности для нахождения остатков от деления.

Приведем несколько примеров.

**Пример 1.** Найти остаток от деления на 3 числа:

$$A = 13^{16} - 2^{25} \cdot 5^{15}.$$

Очевидно, при делении на 3 число 13 равноостаточно с 1, 2 равноостаточно с  $-1$ , а 5 тоже с  $-1$ . Значит, на основании доказанного, число  $A$  при делении на 3



равноостаточно с числом

$$1^{16} - (-1)^{25} (-1)^{15} = 1 - 1 = 0,$$

т. е. искомый остаток равен нулю, и  $A$  делится на 3.

**Пример 2.** Найти остаток от деления того же числа  $A$  на 37.

Представим для этого  $A$  в следующем виде:

$$A = (13^2)^8 - (2^5)^5 \cdot (5^3)^5.$$

Так как  $13^2 = 169$  при делении на 37 равноостаточно с  $-16$ ,  $2^5 = 32$  равноостаточно с  $-5$ , а  $5^3 = 125$  с  $+14$ , то все число  $A$  равноостаточно с

$$(-16)^8 - (-5)^5 (+14)^5$$

или, что то же самое, с

$$(16^2)^4 + 70^5.$$

Но  $16^2$ , т. е. 256, равноостаточно с  $-3$ , а  $70$  — с  $-4$ . Значит,  $A$  равноостаточно с

$$(-3)^4 + (-4)^5$$

или, что то же самое, с

$$81 - (2^5)^2,$$

а потому с

$$81 - (-5)^2 = 81 - 25 = 56.$$

Наконец, 56 при делении на 37 равноостаточно с 19, которое неотрицательно и меньше 37 и потому является искомым остатком.

**Задача 21.** Найти остаток от деления:

а)  $A = (116 + 17^{17})^{21}$  на 8;

б)  $A = 14^{256}$  на 17.

**Задача 22.** Доказать, что при любом  $n$ :

а)  $n^3 + 11n \div 6$ ,

б)  $4^n + 15n - 1 \div 9$ ,

в)  $10^{3n} - 1 \div 3^{n+2}$ ,

г) при любом  $a$

$$a^{2n+1} + (a-1)^{n+2} \div a^2 - a + 1.$$

3. Равноостаточные при делении на  $m$  числа  $a$  и  $b$  называются также *сравнимыми по модулю  $m$* . Это обозначается так:

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

а сама эта формула называется *сравнением*.

Сравнимость двух чисел по некоторому фиксированному модулю  $m$  или, что то же самое, их равноостаточность при делении на  $m$ , также является некоторым отношением, связывающим между собой целые числа.

Отметим несколько свойств отношения сравнимости по модулю.

1° Рефлексивность:  $a \equiv a \pmod{m}$ .

Действительно,  $a - a = 0 : m$ .

2° Симметричность: если  $a \equiv b \pmod{m}$ , то  $b \equiv a \pmod{m}$ .

В самом деле, если  $a - b : m$ , то (хотя бы по теореме 5) и  $b - a : m$ .

3° Транзитивность: если  $a \equiv b \pmod{m}$  и  $b \equiv c \pmod{m}$ , то  $a \equiv c \pmod{m}$ .

Для доказательства достаточно заметить, что из  $a - b : m$  и  $b - c : m$  по теореме 6 следует, что  $a - c : m$ .

Если некоторое отношение (обозначим его через  $\sim$ ) обладает свойствами рефлексивности, симметричности и транзитивности, то оно называется отношением эквивалентности (или эквивалентным отношением). Простейшим примером отношения эквивалентности на множестве чисел является отношение равенства.

**Задача 23.** Эквивалентное отношение  $\sim$  на множестве чисел разбивает это множество на такие классы (называемые классами эквивалентности), что любые два числа из одного класса связаны отношением эквивалентности, а никакие два числа из разных классов этим отношением не связаны. (Доказать.)

В этой задаче речь идет об отношении эквивалентности, связывающем числа. Однако это несущественно, и утверждение задачи справедливо для эквивалентных отношений, связывающих объекты совершенно произвольной природы.

Так как отношение сравнимости по модулю  $m$  — отношение эквивалентности, оно также разбивает множество целых чисел на классы. Эти классы называют классами вычетов по модулю  $m$ .

4° Число классов вычетов по модулю  $m$  равно  $m$ .

В самом деле, два числа,  $a$  и  $b$ , принадлежат одному классу вычетов по модулю  $m$  тогда и только тогда, когда они при делении на  $m$  дают один и тот же остаток. Но остаток при делении на  $m$  может принимать ровно  $m$  значений:  $0, 1, 2, \dots, m - 1$ . Следовательно, и число классов равно  $m$ .

Отметим одно чрезвычайно интересное обстоятельство.

Для того чтобы каждый класс вычетов по модулю  $m_1$  содержался в некотором классе вычетов по модулю  $m_2$ , необходимо и достаточно, чтобы  $m_1 : m_2$ .

Действительно, рассмотрим класс вычетов  $K_1$  по модулю  $m_1$ , содержащий число 0. Очевидно, класс  $K_1$  состоит из всех чисел, дающих при делении на  $m_1$  в остатке 0, т. е. делящихся на  $m_1$ . В частности, он содержит число  $m_1$ . Класс вычетов по модулю  $m_2$ , содержащий  $K_1$ , также содержит 0 и потому состоит из всех чисел, делящихся на  $m_2$ . Так как в него входит число  $m_1$ , должно быть  $m_1 : m_2$ . Этим доказана необходимость, достаточность же очевидна.

Таким образом, отношение делимости можно определить через соотношения между классами вычетов. Этот прием позволяет определять делимость для объектов гораздо более общей и сложной природы, чем натуральные числа. Последовательное развитие этих идей приводит к теории групп, важной отрасли современной алгебры, имеющей приложения в теоретической физике и кристаллографии.

Продолжим перечисление свойств сравнимости чисел. Из теоремы 18 немедленно следуют:

5° Если  $a \equiv b \pmod{m}$  и  $c \equiv d \pmod{m}$ , то

$$a + c \equiv b + d \pmod{m}.$$

Следствие. Если  $a \equiv b \pmod{m}$ , то

$$a + r \equiv b + r \pmod{m}$$

для любого целого  $r$ .

6° Если  $a \equiv b \pmod{m}$  и  $c \equiv d \pmod{m}$ , то

$$ac \equiv bd \pmod{m}.$$

Свойства 5° и 6° показывают, что сравнения подобно равенствам можно почленно складывать и перемножать.

*Задача 24.* Если на множестве целых чисел задано эквивалентное отношение  $\sim$ , разбивающее это множество на  $m$  классов, и такое, что из  $a \sim b$  и  $c \sim d$  следует,  $a + c \sim b + d$ , то отношение  $\sim$  есть сравнимость по модулю  $m$  (т. е.  $a \sim b$  тогда и только тогда, когда  $a \equiv b \pmod{m}$ ).

*Задача 25.* Сформулировать и доказать правила сокращения сравнений.

*Задача 26.* Если число  $p$  простое, и  $a$  не делится на  $p$ , то никакие два числа из  $a, 2a, 3a, \dots, (p-1)a$  не сравнимы друг с другом по модулю  $p$ . Поэтому при делении на  $p$  чисел  $a, 2a, 3a, \dots, (p-1)a$  мы получим по одному разу все остатки, кроме нуля.

*Задача 27* (теорема Вильсона). Для того чтобы число  $p$  было простым, необходимо и достаточно, чтобы  $(p-1)! + 1 \equiv 0 \pmod{p}$ .

*Задача 28.* Сформулировать и доказать для равноостаточности теорему, аналогичную теореме 16.

### § 3. ПРИЗНАКИ РАВНООСТАТОЧНОСТИ И ПРИЗНАКИ ДЕЛИМОСТИ

1. Весьма общий способ нахождения остатка от деления произвольного, но фиксированного натурального числа  $a$  на данное натуральное число  $m$  заключается в следующем. Будем строить последовательность натуральных чисел

$$a = A_0, A_1, A_2, \dots, \quad (8)$$

равноостаточных при делении на  $m$ . Способ построения последовательности выберем такой, чтобы после всякого ее члена, большего или равного  $m$ , следовал еще хотя бы один ее член. Тогда, очевидно, последний член последовательности (8) (если, конечно, такой существует) будет равен остатку  $r$  от деления  $a$  на  $m$ .

Простейшим примером такой последовательности является последовательность (3) из п. 11 § 1. В сущности, к построению последовательности такого типа сводятся задачи нахождения остатка в примерах 1 и 2 предыдущего параграфа.

Всякий способ построения последовательности (8) назовем *признаком равноостаточности* при делении на  $m$ .

В частности, одним из признаков равноостаточности при делении на  $m$  является процесс последовательного вычитания числа  $m$  до получения первого числа, меньшего  $m$ .

2. Очевидно, для уверенности в безотказности работы признака равноостаточности необходимо, чтобы он удовлетворял следующим трем требованиям:

1. Признак равноостаточности должен быть *точно определенным*, т. е. число  $a$  должно вполне определять все члены последовательности (8), не оставляя места какой-либо произвольности.

2. Признак равноостаточности должен быть применим к любому натуральному числу  $a$ . Это свойство признака называется его *массовостью*.

3. Наконец, мы должны иметь гарантию того, что в последовательности (8) хотя бы один член будет меньше, чем  $m$ . Это требование равносильно тому, что последовательность (8) должна иметь конечное число членов, т. е. что процесс построения последовательности не может продолжаться неопределенно долго, а рано или поздно закончится появлением остатка от деления  $a$  на  $m$ . Сформулированное свойство признака равноостаточности называется его *результативностью*.

Перечисленные требования могут быть удовлетворены весьма разнообразными путями. Наиболее естественный из них состоит в следующем.

Попробуем найти функцию  $f(x)$ , подчиненную следующим условиям:

- а)  $f(x)$  при  $x \geq m$  есть натуральное число;
- б)  $f(x)$  при  $x < m$  не определена (т. е. не имеет смысла);

(Нет ничего удивительного в том, что та или иная функция теряет смысл при некоторых значениях аргумента. Например, не имеет смысла значение функции

$\frac{1}{x(x-1)}$  при  $x = 0$  или при  $x = 1$ .)

- в) если  $f(x)$  имеет смысл, то  $f(x) < x$ ;
- г) если  $f(x)$  имеет смысл, то числа  $x$  и  $f(x)$  равноостаточны при делении на  $m$ .

Такие функции существуют. Примером является функция  $f_0(x)$ :

$$f_0(x) = \begin{cases} x - m, & \text{если } x \geq m, \\ \text{не определена,} & \text{если } x < m. \end{cases}$$

Именно эта функция и осуществляет построение последовательности (3) в § 1.

Каждой функции  $f(x)$ , удовлетворяющей условиям а) — г), отвечает некоторый способ построения последовательности (8), т. е. некоторый признак равноостаточности при делении на  $m$ .

В самом деле, возьмем произвольное натуральное число  $a$  и будем строить последовательность чисел

$$A_0, A_1, A_2, \dots, \tag{9}$$

где

$$A_0 = a \text{ и } A_{k+1} = f(A_k) \text{ при } k = 0, 1, \dots$$

Если  $A_k \geq m$ , то значение функции  $f(A_k)$  определено, и потому за  $A_k$  следует хотя бы один член. Если же  $A_k < m$ , то  $f(A_k)$  не определена, и  $A_k$  является последним членом последовательности (9).

Итак, мы действительно имеем некоторый признак равноостаточности.

3. Покажем, что этот признак удовлетворяет требованиям 1, 2 и 3.

Первое требование выполняется ввиду того, что каждый член последовательности (9) определяет следующий за ним член однозначно (если разумеется, этот следующий член действительно существует).

Здесь имеется некоторая тонкость, которая хотя и не бросается в глаза, но играет чрезвычайно важную роль. Дело в том, что для определения последовательности (9) прежде, чем вычислять значение  $f(A_k)$ , мы должны определить, будет ли это значение вообще существовать. Иными словами, мы должны уметь устанавливать, будет ли число  $A_k$  больше или меньше  $m$ . Если числа  $A_k$  и  $m$  даны нам в каком-нибудь удобном для сравнения виде, скажем, в виде их записи в десятичной системе счисления, то такое сравнение осуществляется без труда. Однако сравнение по величине чисел  $2^{20} = 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$  и  $3^{10} = 78 \cdot 757$  требует известных усилий, хотя первое из них есть 1, а второе 3.

В связи с этим мы будем далее применять признаки равноостаточности исключительно к положительным числам, записанным в десятичной системе счисления.

По поводу второго требования достаточно заметить следующее. Если  $a \geq m$ , то мы фактически можем начать построение последовательности, вычислив значение  $f(a)$ , которое по условию существует. Если  $a < m$ , то  $f(a)$  не имеет смысла; однако в этом случае уже само  $a$  является своим остатком от деления на  $m$ . При этом число  $a$  составляет всю последовательность (9), которая здесь состоит только из одного члена.

Переходим к третьему требованию. По условию функция  $f(x)$  выбрана так, что все члены последовательности (9) имеют один и тот же знак, а абсолютные величины членов этой последовательности убывают. Так как первый член последовательности положителен,

в ней найдется наименьший неотрицательный член. (Номер этого члена, как нетрудно проверить, не превосходит числа  $a$ .) Если бы этот член (обозначим его через  $\alpha$ ) был больше или хотя бы равен  $m$ , то существовало бы значение  $f(\alpha)$ , по-прежнему неотрицательное, и меньшее  $\alpha$ . Значит, член  $\alpha$  не был бы последним среди неотрицательных членов последовательности (9). Следовательно, последний неотрицательный член (9) должен быть меньше, чем  $m$ . Но тогда значение  $f(\alpha)$  не имеет смысла, и  $\alpha$  оказывается вообще последним членом нашей последовательности. Процесс построения последовательности, таким образом, заканчивается и последний ее член является остатком от деления  $a$  на  $m$ .

В результате мы установили, что описанный нами признак равноостаточности действительно обладает требуемыми свойствами определенности, массовости и результативности. Процессы, обладающие этими тремя свойствами, называются *алгоритмами* и играют в современной математике все большую роль. Некоторые простые примеры алгоритмов были приведены в конце п. 1 § 1. С другими примерами алгоритмов мы познакомимся ниже.

4. Одним из наиболее важных в математике алгоритмов является так называемый *алгоритм Евклида*, который состоит в следующем.

Пусть  $a$  и  $b$  — два натуральных числа, причем  $b > 0$ . Разделим  $a$  на  $b$  с остатком:  $a = bq_0 + r_1$ , где  $0 \leq r_1 < b$ . Если  $r_1 \neq 0$ , то мы имеем возможность разделить с остатком  $b$  на  $r_1$ :  $b = r_1q_1 + r_2$ , причем  $0 \leq r_2 < r_1$ . Продолжая эти последовательные деления с остатком на остаток от предыдущего деления, мы получим дальнейшие равенства:  $r_1 = r_2q_2 + r_3$ ,  $r_2 = r_3q_3 + r_4$  и т. д.

Покажем, что описанный процесс действительно является алгоритмом, т. е. обладает свойствами определенности, массовости и результативности.

Заметим, что рассматриваемый нами процесс состоит в последовательном выполнении действия деления с остатком.

Поэтому определенность и массовость этого процесса являются следствием неограниченной выполнимости и однозначности действия деления с остатком. Результативность нашего процесса устанавливается также довольно просто. Число  $b$  и остатки от делений, составляющих наш процесс, образуют, очевидно, убывающую последовательность неотрицательных чисел:

$$b, r_1, r_2, \dots \quad (10)$$

Но число всех неотрицательных и не превосходящих  $b$  чисел равно  $b + 1$ . Поэтому и последовательность (10) не может насчитывать более чем  $b$  членов, так что наш процесс может состоять не более

чем из  $b$  делений с остатком \*). Таким образом, рассматриваемый процесс действительно является алгоритмом и вполне оправдывает свое название.

Выясним условия окончания процесса. Очевидно, последнее деление должно быть таким, чтобы дальнейшее деление на его остаток было уже невозможно. Но это может быть лишь в том случае, когда этот последний остаток равен нулю, т. е. когда последнее деление совершилось нацело.

*Задача 29.* а) Последний отличный от нуля остаток  $r_n$  в применении алгоритма Евклида к числам  $a$  и  $b$  есть  $(a, b)$ .

б) Каковы бы ни были натуральные  $a$  и  $b$ , существуют такие целые  $A$  и  $B$ , что  $aA + bB = (a, b)$ .

*Задача 30.* Вывести из результата б) задачи 29 теоремы 9, 12, 13 и 14. (Подчеркнем, что наши рассуждения, связанные с алгоритмом Евклида, были основаны только на возможности деления с остатком. Мы не пользовались в них ни теоремами 9—14, ни какими-либо иными соображениями, опирающимися на основную теорему арифметики.)

5. Разумеется, приведенное в п. 3 описание алгоритма не является его точным определением, которое сравнительно сложно и не может быть здесь сформулировано. Однако перечисленные требования довольно полно отражают те условия, которым должны удовлетворять называемые алгоритмами математические процессы. Роль алгоритмов определяется тем, что они являются единообразными способами решения целого ряда однотипных задач. Так, алгоритмы, о которых только что шла речь, позволяют вычислить остаток от деления варьируемого числа  $a$  на некоторое фиксированное  $m$ . Частными случаями алгоритмов являются всевозможные вычисления по формулам, в которые вместо букв можно подставлять те или иные числа.

Говоря несколько вольно, к алгоритмам сводятся все те математические задачи, решение которых можно автоматизировать. Поэтому не случайно развитие теории алгоритмов исторически совпало с появлением и распространением вычислительных машин.

К алгоритмам сводятся не только вычислительные задачи в узком смысле этого слова, т. е. такие задачи, в которых по более или менее сложным правилам можно на основе исходных данных получить численный ответ. Можно ставить вопрос о поисках алгоритма, позволяющего

---

\*) На самом деле число этих делений не может превосходить числа  $5 \log b$ . Это следует из рассмотрения чисел Фибоначчи (см., например, книжку автора «Числа Фибоначчи», «Наука», 1969, стр. 72—73).



доказывать любую задачу из некоторой области математики. Этот алгоритм должен уметь перерабатывать формулировки теорем в их доказательства. Как ни фантастично это может показаться, такие алгоритмы существуют, хотя и не для очень широких областей математики. Вместе с тем для некоторых ее областей (например, для любой области, содержащей всю арифметику) таких алгоритмов принципиально быть не может.

6. Пользуясь изложенным в п. 1 приемом построения признаков равноостаточности, найдем несколько таких признаков. Здесь и далее мы будем считать, что числа, остатки от деления которых требуется найти, записаны в десятичной системе счисления.

Сначала найдем признак равноостаточности при делении на 5.

Пусть  $A$  — натуральное число. Представим  $A$  в виде  $10a + b$  ( $b$  — последняя цифра числа  $A$ ) и положим

$$f_1(A) = \begin{cases} b, & \text{если } A \geq 10, \\ b - 5, & \text{если } 5 \leq A < 10, \\ \text{не определено,} & \text{если } A < 5. \end{cases}$$

Читатель сам может проверить, что так определенная функция удовлетворяет условиям а) — г) п. 2.

Таким образом, для нахождения остатка от деления некоторого числа на 5 достаточно взять последнюю цифру этого числа. Если эта цифра меньше пяти, то она и будет искомым остатком; в противном случае от нее следует отнять 5. Заметим, что применение этого признака равноостаточности к любому числу приводит к построению последовательности типа (9), состоящей не более чем из трех членов.

Разумеется, целью всех проведенных рассуждений является не обнаружение известного всем «признака делимости» на 5, а получение его тем единообразным приемом, который был описан в п. 2.

*Задача 31.* Указать и проанализировать аналогичные признаки равноостаточности при делении на 2, 4, 8, 10, 16, 20 и 25.

*Задача 32.* Представим натуральное число  $A$  в виде

$$10^k a + b \quad (0 \leq b < 10^k)$$

и положим

$$f(A) = \begin{cases} b, & \text{если } A \geq 10^k, \\ \text{остатку от деления } A \text{ на } m, & \text{если } m \leq A < 10^k, \\ \text{не определена,} & \text{если } A < m. \end{cases}$$

Для каких чисел  $m$  такой алгоритм при некотором  $k$  является признаком равноостаточности?

7. В качестве второго примера рассмотрим признак равноостаточности при делении на 3.

Представим для этого натуральное число  $A$  в виде

$$10^n a_n + 10^{n-1} a_{n-1} + \dots + 10a_1 + a_0,$$

где  $0 \leq a_i < 10$  (числа  $a_0, a_1, \dots, a_{n-1}, a_n$  являются цифрами числа  $A$ ). Положим

$$f_2(A) = \begin{cases} a_0 + a_1 + \dots + a_{n-1} + a_n, & \text{если } A \geq 10, \\ \text{остатку от деления } A \text{ на } 3, & \text{если } 3 \leq A < 10, \\ \text{не определена,} & \text{если } A < 3. \end{cases}$$

*Задача 33.* Проверить, что функция  $f_2(x)$  удовлетворяет условиям а) — г) и определяет тем самым некоторый признак равноостаточности при делении на 3.

*Задача 34.* Применить построенный признак равноостаточности при делении на 3:

а) к числам 858 773 и 789 988,

б) к числу, десятичная запись которого состоит из 4444 четверок.

*Задача 35.* Указать и проанализировать аналогичные признаки равноостаточности при делении на 7, 9, 11, 13 и 37.

8. Во многих задачах несущественна не только величина неполного частного от деления одного числа на другое, но также и величина остатка от деления, а интересно только, обращается этот остаток в нуль или нет, т. е. делится или нет первое число на второе. После сказанного в п. 1 ясно, как подходить к задачам такого рода.

Назовем числа  $a$  и  $b$  *равноделимыми* при делении на  $m$ , если либо  $a$  и  $b$  делятся на  $m$ , либо на  $m$  ни  $a$ , ни  $b$  не делятся.

*Задача 36.* Каково бы ни было  $m$ , любые равноостаточные при делении на  $m$  числа являются равноделимыми на  $m$ . Показать на примере, что обратное неверно.

*Задача 37.* Для каких  $m$  из равноделимости двух чисел при делении на  $m$  следует их равноостаточность при этом делении?

**Задача 38.** Доказать, что отношение равноделимости на данное число  $m$  является эквивалентным отношением и разбивает множество целых чисел на два класса.

**Задача 39.** Будет ли справедлива для равноделимых чисел теорема 18? Ее следствие?

9. Пусть нужно выяснить делимость на  $m$  числа  $A$ . Будем строить последовательность убывающих по абсолютной величине целых чисел:

$$A = A_0, A_1, A_2, \dots, \quad (11)$$

равноделимых с  $A$  при делении на  $m$  с остатком. Способ построения последовательности (11) выберем такой, чтобы за всяким членом этой последовательности, бóльшим или равным  $m$  по абсолютной величине, следовал еще хотя бы один член. Если при этом последний член (11) будет равен нулю, то  $A$  делится на  $m$ , а если не равен нулю, то не делится.

Всякий способ построения последовательности (11) назовем *признаком делимости на  $m$* .

**Задача 40.** Доказать, что всякий признак равноостаточности при делении на  $m$  является признаком делимости на  $m$ .

Очевидно, признаки делимости должны удовлетворять таким же условиям определенности, массовости и результативности, что и признаки равноостаточности.

Нетрудно проверить (это предоставляется читателю), что при помощи всякой функции  $f(x)$ , удовлетворяющей условиям а) — в) из п. 2 и условию

г\*) если  $f(x)$  имеет смысл, то числа  $x$  и  $f(x)$  равноделимы на  $m$ ,

можно построить признак делимости на  $m$  точно таким же образом, как строился признак равноостаточности при делении на  $m$  по всякой функции, удовлетворяющей условиям а) — г).

Найдем несколько признаков делимости.

Согласно теореме 16 достаточно уметь определять делимость чисел на числа вида  $p^a$  (степени простого числа).

10. Признак делимости на 7. Пусть  $A$  — натуральное число. Представим  $A$  в виде  $10a + b$ , где  $0 \leq b < 10$ , как это уже делалось раньше. Положим

$$f_3(A) = \begin{cases} a - 2b, & \text{если } A \geq 19, \\ \text{остатку от деления } A \text{ на } 7 & \text{при } 7 \leq A < 19, \\ \text{не определена} & \text{при } A < 7. \end{cases}$$

**Задача 41.** Проверить выполнение для функции  $f_3(A)$  условий а) — в) и г\*).

Функция  $f_3(A)$  дает нам известный признак делимости на 7: число  $10a + b$  ( $0 \leq b < 10$ ) делится на 7 тогда и только тогда, когда на 7 делится число  $a - 2b$ ; полученное число снова проверяется этим же способом на делимость на 7 и т. д.

**Задача 42.** Доказать, что полученный признак делимости на 7 не является признаком равноостаточности при делении на 7 с остатком.

11. Признак делимости на 13. Представим натуральное число  $A$  в виде  $10a + b$  и положим

$$f_4(A) = \begin{cases} a + 4b, & \text{если } A \geq 40, \\ \text{остатку от деления } A \text{ на } 13, & \text{если } 13 \leq A < 40, \\ \text{не определена,} & \text{если } A < 13. \end{cases}$$

**Задача 43.** Проверить выполнение условий а) — в) и г\*) для функции  $f_4(x)$  и сформулировать полученный признак делимости на 13.

**Задача 44.** К каким последствиям приведет замена в определении функции  $f_4$  числа 40 на меньшее?

**Задача 45.** По аналогии с построенными признаками делимости на 7 и 13 построить аналогичные признаки делимости на 17, 19, 23, 29 и 31.

**Задача 46.** Построить два признака делимости на 49.

12. В предыдущих пунктах этого параграфа мы познакомились с большим количеством самых разнообразных признаков равноостаточности и признаков делимости. Практической целью построения всех этих признаков является получение удобно работающих алгоритмов нахождения остатков при делении на некоторые определенные числа (признаки равноостаточности) или алгоритмов, обнаруживающих, равны эти остатки нулю или нет (признаки делимости). Насколько же мы осуществили поставленную цель?

Некоторые признаки равноостаточности, такие, как при делении на 2, 3, 5, 10, действительно оказались весьма практичными и удобными. Применение других признаков связано с более или менее громоздкими вычислениями.

Естественно поэтому искать и применять такие признаки делимости и равноостаточности, использование

которых приводит к цели по возможности более простым путем.

Одна из трудностей, с которой мы сталкиваемся при такого рода попытках, состоит в том, что мы должны уметь простоту (или, наоборот, сложность) применения того или иного признака оценивать некоторым числом. В качестве такой числовой характеристики можно, например, взять число арифметических действий над однозначными числами, которые необходимо произвести в процессе применения данного признака к тому или иному числу.

К сожалению, всякая такая характеристика объема вычислений в сильной мере зависит от индивидуальных свойств того числа, делимость которого мы хотим испытать.

Так, например, очень легко убедиться в том, что остаток от деления числа 31 025 на 8 есть 1. Для этого достаточно найти остаток от деления на 8 числа 25. Но для нахождения остатка от деления 30 525 на 8 следует разделить на 8 с остатком число 525, а это уже требует большего числа выкладок (безразлично, проводимых в уме или на бумаге).

В качестве другого примера рассмотрим признак равноостаточности при делении на 37 (см. задачу 35). Остаток от деления на 37 числа 10 014 023 находится сложением  $10 + 14 + 23$  и делением полученной суммы на 37. Остаток, как легко видеть, равен 10. Однако немногие смогут в уме применить этот признак равноостаточности к числу 782 639 485.

Поэтому, говоря об удобстве использования признаков делимости и равноостаточности, мы должны отвлекаться от сложностей индивидуальных испытаний чисел на делимость, а оценивать возможности каждого признака «в среднем». При таком подходе мы можем надеяться точно сформулировать меру сложности признака делимости или равноостаточности и даже найти наиболее экономный в этом смысле признак. К сожалению, мы лишены здесь возможности развивать эту сторону вопроса более подробно.

13. Все построенные выше признаки равноостаточности, а также признаки делимости выглядят несколько искусственно, и на первый взгляд может показаться, что эти признаки или, во всяком случае, некоторые из них были найдены случайно или же в результате проб

и испытаний. На самом деле это не так. Оказывается, существуют способы построения признаков делимости и равноостаточности на любое наперед заданное число. Они называются *общими признаками делимости* или соответственно *общими признаками равноостаточности*.

Общие признаки делимости являются *способами* получения конкретных признаков делимости. Поэтому конкретные признаки делимости можно считать теми результатами, к которым приводят общие признаки. С этой точки зрения общие признаки делимости относятся к конкретным совершенно так же, как конкретный признак делимости относится к результату своего применения к некоторому числу, т. е. к остатку от деления данного числа  $a$  на данное число  $m$ .

Общие признаки делимости и равноостаточности напоминают алгоритмы, и притом алгоритмы довольно своеобразные: их итогами, результатами должны быть снова алгоритмы, именно, конкретные признаки делимости или равноостаточности.

Однако для того чтобы говорить об общих признаках делимости и равноостаточности как об алгоритмах, мы должны убедиться в том, что они обладают нужными условиями определенности, массовости и результативности.

Говоря подробнее, указывая общий признак делимости (равно как и общий признак равноостаточности), мы должны проверить выполнение следующих условий. Во-первых, по всякому числу  $m$  он должен действительно давать признак делимости (равноостаточности) на это число. Он должен, так сказать, «перерабатывать» каждое натуральное число  $m$  в соответствующий признак. Именно в этом и состоит его результативность. Во-вторых, общий признак должен быть определенным, т. е., примененный к заданному числу  $m$ , он должен приводить вполне определенным способом к вполне определенному конкретному признаку делимости (равноостаточности) на это число. Наконец, в-третьих, признак должен быть массовым, т. е. действительно общим, и давать признаки делимости или равноостаточности на любое наперед заданное натуральное число.

В этом смысле описанный в п. 2 способ задания признака равноостаточности, а также описанный в п. 6 способ нахождения признаков делимости не являются общими признаками. Действительно, указание функций,

удовлетворяющих нужным условиям, является процессом, не удовлетворяющим пока ни одному из требований определенности, массовости и результативности.

В самом деле, эти способы не дают нам никакой гарантии в том, что нужная функция будет найдена; значит, они лишены результативности. Далее, если требуемая функция и существует, к ней можно прийти разными путями, не говоря уже о том, что таких функций может оказаться несколько. Значит, эти способы лишены определенности. Наконец, ему не хватает и массовости, так как, быть может, требуемых функций для некоторых чисел нам найти и не удастся. Сам способ нам, во всяком случае, ничего об этом не говорит. Таким образом, для того чтобы описанный процесс стал алгоритмом, он должен быть еще дополнен точными указаниями, гарантирующими построение вполне определенной функции  $f_m$  для каждого конкретного числа  $m$ .

Эта задача «алгоритмизации» построения признаков делимости может быть решена, и даже без особого труда, а общие признаки делимости известны уже давно.

Один такой общий признак равноостаточности фактически нами уже был построен в п. 11 § 1 при выяснении вопроса о делении с остатком. Мы его можем сформулировать так: каждому целому положительному числу  $m$  сопоставляется процесс последовательного вычитания этого числа  $m$  до получения числа, меньшего, чем  $m$  (см. последнюю фразу п. 1). Ясно, что такое сопоставление обладает необходимыми свойствами определенности (мы точно знаем, что сопоставляется числу  $m$ : процесс последовательного вычитания  $m$ ), массовости (процесс последовательного вычитания можно попытаться сопоставить любому  $m$ ) и результативности (такая попытка обязательно приведет к успеху). Однако практическая ценность описанного общего признака равноостаточности весьма невелика.

Некоторое усовершенствование общего признака равноостаточности, основанного на последовательном вычитании, приводит к известному процессу деления целых чисел «столбиком». Этот процесс деления тоже может рассматриваться как общий признак равноостаточности. Нелишним будет напомнить, что подавляющее большинство людей пользуется при нахождении остатков от деления именно этим признаком. При этом рас-

суждение ведется по следующей схеме, которую мы воспроизведем в двух вариантах: на обычном, житейском языке и на языке алгорифмов.

На житейском языке	На языке алгорифмов
<p>1. Я должен найти остаток от деления данного <math>a</math> на данное <math>m</math>;</p> <p>2. для этого я должен делить на <math>m</math>;</p> <p>3. вот я начинаю делить <math>a</math> на <math>m</math>...</p> <p>4. ... делю и получаю остаток.</p>	<p>Общий признак равноостаточности начинает переработку числа <math>m</math>;</p> <p>общий признак «выдает» результат переработки числа <math>m</math>: конкретный признак равноостаточности при делении на <math>m</math>, заключающийся в непосредственном делении на <math>m</math>;</p> <p>полученный конкретный признак начинает переработку числа <math>a</math>;</p> <p>конкретный признак приводит к цели: к остатку от деления <math>a</math> на <math>m</math>.</p>

В этом рассуждении первые три шага уже очень просты, и поэтому не приходится удивляться, что четвертый шаг, состоящий в фактическом выполнении деления, оказывается таким громоздким. Цель создания общих признаков равноостаточности и делимости и состоит в разгрузке четвертого шага за счет усовершенствования второго. Именно это и имеют обычно в виду, когда говорят об общих признаках делимости и равноостаточности.

14. Исторически первым общим признаком делимости (точнее, даже признаком равноостаточности) является следующий, предложенный знаменитым французским математиком Паскалем еще в середине XVII столетия. Сущность этого признака такова.

Пусть  $m$  — натуральное число. Составим последовательность чисел

$$r_1, r_2, r_3, \dots, \quad (12)$$

полагая

$$\begin{array}{llll}
 r_1 & \text{равным остатку от деления } 10 & \text{на } m, & \\
 r_2 & \gg & \gg & 10r_1 \gg m, \\
 r_3 & \gg & \gg & 10r_2 \gg m
 \end{array}$$

и т. д.



Представим теперь произвольное натуральное число  $A$  в виде

$$10^n a_n + 10^{n-1} a_{n-1} + \dots + 10a_1 + a_0,$$

и определим функцию

$$F_m(a) = \begin{cases} a_0 + r_2 a_1 + r_2^2 a_2 + \dots + r_2^n a_n, & \text{если } 10^n \geq m, \\ \text{остатку от деления } A \text{ на } m, & \text{если } 10^n < m \leq A, \\ \text{не определена,} & \text{если } A < m. \end{cases}$$

*Задача 47.* Проверить, что функция  $F_m$  при любом  $m$  удовлетворяет условиям а) — г).

Итак, нами построен признак равноостаточности при делении на произвольное  $m$ , т. е. некоторый общий признак равноостаточности.

*Задача 48.* Сформулировать получаемые из общего признака равноостаточности Паскаля признаки равноостаточности при делении:

- а) на 2, 5 и 10;
- б) на 4, 20 и 25;
- в) на 3 и 9;
- г) на 11;
- д) на 7.

*Задача 49.* Пусть в последовательности (12)

$$\begin{array}{llll} r_1 & \text{есть остаток от деления } 100 & \text{на } m, & \\ r_2 & \gg & \gg & 100r_1 \text{ на } m, \\ r_3 & \gg & \gg & 100r_2 \text{ на } m \end{array}$$

и т. д.

Вывести отсюда общий признак равноостаточности, аналогичный общему признаку равноостаточности Паскаля.

15. В п. 12 мы говорили о сравнительных качествах признаков делимости (или равноостаточности) на данное число. Так как общий признак делимости должен давать нам признаки делимости на любое натуральное число, то неудивительно, что он может для различных чисел приводить к признакам делимости весьма различного качества.

Так, например, общий признак Паскаля наряду с вполне приемлемыми признаками равноостаточности при делении на 3 и 11 дает весьма громоздкий и неудобный к применению признак равноостаточности при делении на 7 (см. задачу 48, д)).

В связи с этим по поводу общих признаков делимости и равноостаточности можно высказать соображения, подобные тем, которые приводились в п. 12 при обсуждении качества конкретных признаков делимости. В этом смысле наилучшим общим признаком делимости (равноостаточности) должен считаться тот, который в применении к любому наперед заданному целому положительному  $m$  дает наилучший признак делимости (равноостаточности) на это  $m$ . Читатель должен отдавать себе отчет в том, что задача нахождения наилучшего общего признака делимости далека не только от своего решения, но даже от строгой постановки.

## § 4. ДЕЛИМОСТЬ СТЕПЕНЕЙ

1. Вопрос о делимости степени является, по существу, вопросом о делимости некоторого произведения, именно произведения нескольких равных сомножителей. Поэтому решать этот вопрос можно и на основании результатов § 2. Однако в случае больших показателей уменьшение основания степени еще не приводит сразу к нахождению остатка от деления степени, и нам приходится пользоваться несколько искусственными приемами (см. примеры в п. 2 § 2). Кроме того, при построении общих признаков делимости мы вычисляли остатки от деления последовательных степеней числа  $10^k$  на  $m$ . Хотя сам по себе этот процесс и не сложен, но он еще не указывает никаких закономерностей в последовательности (12), а также не дает возможности так распорядиться числом  $k$ , чтобы все эти остатки были достаточно маленькими (вместе с тем такая возможность существует; больше того, оказывается, что число  $k$  можно выбрать так, чтобы все эти остатки были равны единице).

Все сказанное приводит к необходимости заняться изучением делимости степеней более подробно.

2. Расширим несколько наши познания в области теории чисел.

**Теорема 19 (теорема Ферма).** *Если число  $p$  простое, то разность  $a^p - a$  делится на  $p$ .*

Не следует путать эту так называемую «малую теорему Ферма» с «великой теоремой Ферма». Последняя утверждает, что при целом  $n > 2$  не существует таких целых  $a$ ,  $b$  и  $c$ , что  $a^n + b^n = c^n$ . Несмотря на многочисленные попытки, великая теорема Ферма до сих пор не доказана и не опровергнута.

**С л е д с т в и е.** Если  $p$  — простое и  $a$  не делится на  $p$ , то  $a^{p-1} - 1$  делится на  $p$ .

**Задача 50.** Привести пример, показывающий, что как теорема 19, так и ее следствие для составного  $p$ , вообще говоря, неверны.

**Задача 51.** Доказать теорему Ферма, опираясь на результат задачи 26.

Пусть натуральное  $m$  имеет каноническое разложение:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}; \quad (13)$$

положим

$$\varphi(m) = p_1^{\alpha_1-1} (p_1 - 1) p_2^{\alpha_2-1} (p_2 - 1) \dots p_k^{\alpha_k-1} (p_k - 1). \quad (14)$$

Формулы (13) и (14) ставят в соответствие каждому натуральному числу  $m$  некоторое вполне определенное число  $\varphi(m)$ : Это значит, что мы можем говорить о функции  $\varphi$  от натурального аргумента.

**О п р е д е л е н и е.** Определенная выше функция  $\varphi$  называется *функцией Эйлера*.

Функция Эйлера играет исключительно важную роль во многих вопросах теории чисел. Даже в этой книжке будет указано несколько применений этой функции.

**Т е о р е м а 20.** При взаимно простых  $m_1$  и  $m_2$  имеет место равенство

$$\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2).$$

**Задача 52.** Вычислить  $\varphi(12)$ ,  $\varphi(120)$ ,  $\varphi(1000)$ .

**Задача 53.** Определить все числа  $m$ , для которых

а)  $\varphi(m) = 10$ ,

б)  $\varphi(m) = 8$ .

**Задача 54.** Доказать, что не существует такого  $m$ , для которого  $\varphi(m) = 14$ .

**Задача 55.** Показать, что  $\varphi(m)$  равно числу натуральных чисел, взаимно простых с  $m$  и меньших  $m$ . Это свойство функции Эйлера является чрезвычайно важным. Его часто принимают за определение этой функции.

**Т е о р е м а 21 (теорема Эйлера).** Если числа  $a$  и  $m$  взаимно просты, то  $a^{\varphi(m)} - 1$  делится на  $m$ .

3. Применяя доказанные теоремы, построим несколько общих признаков делимости и равноостаточности.

Фиксируем натуральное  $m$  и представим число  $A$  в виде

$$A = a_0 + a_1 10^{\varphi(m)} + a_2 10^{2\varphi(m)} + \dots + a_k 10^{k\varphi(m)},$$

где

$$0 \leq a_0, a_1, a_2, \dots, a_k \leq 10^{\varphi(m)},$$

т. е. все  $a_i$  ( $i = 0, 1, \dots, k$ ) являются  $\varphi(m)$ -значными числами.

Функция  $F$

$$F(A) = \begin{cases} a_0 + a_1 + \dots + a_k, & \text{если } A \geq 10^{\varphi(m)}, \\ \text{остатку от деления } A \text{ на } m, & \text{если } m \leq A < 10^{\varphi(m)}, \\ \text{не определена,} & \text{если } A < m, \end{cases}$$

определяет, как нетрудно проверить, некоторый общий признак равноостаточности.

*Задача 56.* Проверить это обстоятельство.

*Теорема 22.* Если числа  $a$  и  $m$  взаимно просты, а числа  $k_1$  и  $k_2$  равноостаточны при делении на  $\varphi(m)$ , то числа  $a^{k_1}$  и  $a^{k_2}$  равноостаточны при делении на  $m$ .

*Задача 57.* Доказать, что  $n^{13} - n : 2730$ .

4. Построенный общий признак равноостаточности не является во многих случаях, так сказать, «достаточно экономным», так как число  $\varphi(m)$  может, вообще говоря, оказаться довольно большим. Поэтому, с одной стороны, при пользовании этим признаком приходится складывать большие числа, а с другой стороны,  $\varphi(m)$ -значные числа при этом приходится делить на  $m$  непосредственно (или же пользоваться каким-нибудь другим признаком делимости и равноостаточности). Желательно поэтому попытаться взять вместо  $\varphi(m)$  другой, меньший показатель. В ряде случаев это удастся сделать. Например, при  $m = 37$  вместо  $\varphi(m) = 36$  можно взять показатель 3, ибо 1000 при делении на 37 дает в остатке единицу; при  $m = 11$  вместо  $\varphi(m) = 10$  можно взять показатель 2 и т. д.

**О п р е д е л е н и е.** Наименьшее число  $\delta$ , для которого  $a^\delta$  при делении на  $m$  с остатком дает в остатке 1, называется *показателем, которому принадлежит число  $a$  при делении на  $m$  с остатком.*

Чаще это число принято называть *показателем, которому принадлежит число  $a$  по модулю  $m$ .*

Очевидно, каковы бы ни были взаимно простые числа  $a$  и  $m$ , показатель, которому принадлежит  $a$  при делении на  $m$ , не превосходит  $\varphi(m)$ . Этот показатель и можно взять вместо  $\varphi(m)$  в формулировке общего признака делимости из п. 3.

**Задача 58.** Модифицировать построенный общий признак делимости, используя вместо  $\varphi(m)$  показатель, которому принадлежит 10 при делении на  $m$  с остатком.

5. Применения функции Эйлера и теоремы Эйлера не ограничиваются признаками делимости. Например, при их помощи можно решать уравнения в целых числах.

**Теорема 23.** Если числа  $a$  и  $b$  взаимно просты, то уравнение

$$ax + by = c \quad (15)$$

всегда разрешимо в целых числах, и целыми его решениями будут все пары чисел  $(x_t, y_t)$ , где

$$x_t = ca^{\varphi(b)-1} + bt,$$

$$y_t = c \frac{1 - a^{\varphi(b)}}{b} - at$$

( $t$  — любое целое число).

**Задача 59.** Доказать теорему, аналогичную теореме 23, не предполагая взаимной простоты чисел  $a$  и  $b$ .

**Задача 60.** Найти способ решения уравнений вида (15) в целых числах на основе результата задачи 29, б).

**Задача 61.** Решить в целых числах уравнения

а)  $5x + 7y = 9$ ;

б)  $25x + 13y = 8$ .

6. **Теорема 24.** Пусть  $m$  взаимно просто с 10, и  $k$  равноостаточно с  $10^{\varphi(m)-1}$  при делении на  $m$ . Тогда числа

$$10a + b \quad \text{и} \quad a + kb$$

равноделимы на  $m$ .

Опираясь на эту теорему, можно построить следующий общий признак делимости. Обозначим через  $k'$  остаток от деления  $10^{\varphi(m)-1}$  на  $m$  с остатком, представим произвольное число  $A$  в виде

$$10a + b \quad (0 \leq b < 10)$$

и положим:

$$F(A) = \begin{cases} a + k'b & \text{при } A > a + k'b, \\ \text{остатку от деления } A \text{ на } m \text{ при } m \leq A < a + k'b, \\ \text{не определена} & \text{при } A < m. \end{cases}$$

Если  $k'$  велико (близко к  $m$ ), то вместо него в формулировке соответствующего признака целесообразно брать  $k' - m$ .

*Задача 62.* Проверить для функции  $F$  выполнение условий а) — б) и г\*).

*Задача 63.* На основании только что построенного общего признака делимости вывести признаки делимости на числа 17, 19, 27, 29, 31 и 49.

*Задача 64.* Построить аналогичный общий признак делимости, представляя произвольное натуральное число в виде

$$100a + b \quad (0 \leq b < 100)$$

и вывести из него признаки делимости на 17, 43, 49, 67, 101, 199.

## ДОКАЗАТЕЛЬСТВА ТЕОРЕМ

1. Достаточно заметить, что  $a = a \cdot 1$ .

2. По условию, найдутся такие  $d_1$  и  $d_2$ , что  $a = bd_1$  и  $b = cd_2$ . Но тогда  $a = cd_1d_2$ , т. е.  $d_1d_2 = a/c$ .

3. Мы имеем  $a = bc_1$  и  $b = ac_2$ , откуда следует, что  $a = ac_1c_2$ , т. е.  $c_1c_2 = 1$ . Так как числа  $c_1$  и  $c_2$  по условию целые, то либо  $c_1 = c_2 = 1$ , либо  $c_1 = c_2 = -1$ . В первом из этих случаев  $a = b$ , а во втором  $a = -b$ .

4. Пусть  $a = bc$ . Если  $|c| \geq 1$ , то поскольку  $|b| > |a|$ , должно быть и  $|bc| > |a|$ , что, однако, противоречит предположенному. Значит,  $|c| < 1$ , а так как по условию число  $c$  целое, должно быть  $c = 0$ , а потому и  $a = 0$ .

5. Очевидно, из  $a = bc$  следует  $|a| = |b||c|$ , а из  $|a| = |b||c|$  следует  $a = bc$  или  $a = b(-c)$ , причем числа  $c$ ,  $-c$  и  $|c|$  целые или нет одновременно.

6. В самом деле, пусть

$$a_1 = bc_1,$$

$$a_2 = bc_2,$$

$$\dots$$

$$a_n = bc_n,$$

где все числа  $c_1, c_2, \dots, c_n$  — целые. Сложив все эти равенства почленно, мы получим

$$a_1 + a_2 + \dots + a_n = b(c_1 + c_2 + \dots + c_n).$$

В скобках стоит целое число, что и доказывает требуемое.

8. Доказательство ведется от противного. Предположим, что простых чисел конечное число, так что все они могут быть выписаны:

$$p_1, p_2, \dots, p_n.$$

(16)



Произведение всех этих чисел обозначим через  $P$  и рассмотрим разность  $P - 1$ . Эта разность больше каждого из простых чисел, перечисленных в списке (16), и потому не может быть простым числом. Следовательно, она делится хотя бы на одно простое число  $p_k$ . Но  $P$  также делится на  $p_k$ . Следовательно, на основании следствия теоремы 6, должно быть и  $1 : p_k$ , откуда следует, что  $p_k = 1$ , а это противоречит простоте числа  $p_k$  (см. стр. 20).

Приведенное доказательство бесконечности множества простых чисел было найдено Евклидом (IV век до н. э.).

9. Если числа  $a$  и  $p$  взаимно просты, то теорема доказана. Если же эти числа не взаимно просты, то оба они делятся на одно и то же число, отличное от единицы. Ввиду простоты  $p$  таким числом может быть только само  $p$ . Значит, в этом случае  $a : p$ , а это и требовалось.

10. Разделив  $M$  на  $m$  с остатком, получим

$$M = mq + r,$$

где  $0 \leq r < m$ . Так как  $M$  и  $m$  делятся на  $a$  и  $b$ , по следствию теоремы 6, число  $r$  также должно делиться и на  $a$ , и на  $b$  и тем самым быть общим кратным этих чисел. Но  $r < m$ , а  $m$  есть наименьшее положительное общее кратное  $a$  и  $b$ . Значит,  $r$  не может являться положительным числом, так что  $r = 0$ . Поэтому  $M : m$ .

11. Пусть числа  $a$  и  $b$  взаимно просты, и  $m$  — их наименьшее общее кратное. Так как  $ab : a$  и  $ab : b$ , по предыдущей теореме  $ab : m$ . Пусть  $ab = mk$ . Положим  $m = ac$ . Тогда  $ab = ack$ , т. е.  $b = ck$ , так что  $b : k$ . Точно так же убеждаемся в том, что и  $a : k$ . Так как числа  $a$  и  $b$  по условию взаимно простые, должно быть  $k = 1$ , а это и означает, что  $m = ab$ .

12. Обозначим через  $m$  наименьшее общее кратное чисел  $b$  и  $c$ . По предыдущей теореме  $m = bc$ . Далее, по условию  $ab : c$ , кроме того, очевидно,  $ab : b$ . Значит, по теореме 10,  $ab : bc$ , т. е.  $ab = bck$  или, после сокращения на  $b$ ,  $a = ck$ , а это и требовалось.

13. Доказательство ведется индукцией по числу сомножителей. Если сомножитель один, то теорема тривиальна. Предположим, что теорема доказана для любого произведения  $n$  сомножителей. Пусть  $a_1 a_2 \dots \dots a_n a_{n+1} : p$ . Обозначим  $a_1 a_2 \dots a_n$  через  $A$ . Тогда

$Aa_{n+1} : p$ . Если  $a_{n+1} : p$ , то теорема доказана, а если нет, то по теореме 9 числа  $a_{n+1}$  и  $p$  взаимно просты. Но тогда по предыдущему  $A : p$ . Так как  $A$  есть произведение  $n$  сомножителей, по индуктивному предположению один из них должен делиться на  $p$ . Теорема доказана.

**С л е д с т в и е.** Вся дробь представляет собой целое число, т. е. ее числитель делится на знаменатель. Будем считать, что числитель является произведением двух сомножителей:  $p$  и  $1 \cdot 2 \dots (p - 1) = (p - 1)!$

Ни один из сомножителей знаменателя дроби не делится на  $p$ . Следовательно, по предыдущей теореме, на  $p$  не делится и весь знаменатель. Но тогда на основании теоремы 9 он взаимно прост с  $p$ . Поэтому на знаменатель должен делиться второй сомножитель числителя. Обозначая частное от этого деления через  $q$ , мы имеем  $C_p^k = pq$ , и требуемое доказано.

**14.** Сначала докажем возможность разложения любого числа, отличного от единицы, на простые множители. Предположим, что все числа, меньшие  $N$ , могут быть так разложены. Если число  $N$  простое, то оно автоматически разлагается в произведение простых (именно, в произведение, состоящее только из одного сомножителя — самого числа  $N$ ), и теорема доказана. Пусть теперь  $N$  составное,  $N_1$  — некоторый делитель  $N$ , отличный как от  $N$ , так и от единицы, и  $N_2$  — частное от деления  $N$  на  $N_1$ . Тогда  $N = N_1 N_2$ , причем, как легко проверить,  $1 < N_2 < N$ . Так как  $N_1$  и  $N_2$  меньше  $N$  то, по предположению, они разлагаются в произведения простых множителей. Пусть  $N_1 = p_1 p_2 \dots p_k$  и  $N_2 = q_1 q_2 \dots q_l$  — эти разложения. Тогда  $p_1 p_2 \dots p_k q_1 q_2 \dots q_l$  является искомым разложением числа  $N$ . Возможность разложения, таким образом, доказана.

Переходим к доказательству единственности разложения. Пусть нам даны два разложения числа  $N$  на простые множители:  $p_1 p_2 \dots p_k$  и  $q_1 q_2 \dots q_l$ . Очевидно,

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_l. \quad (17)$$

Так как  $q_1 q_2 \dots q_l$  делится на  $p_1$ , то по предыдущей теореме хотя бы одно из чисел  $q_1, q_2, \dots, q_l$  делится на  $p_1$ . Пусть  $q_1 : p_1$  (то, что мы считаем именно первый сомножитель в (17) справа делящимся на  $p_1$ , никакого дополнительного предположения не означает, так как мы вправе переставлять сомножители местами и обозначить

через  $q_1$  именно тот из них, который делится на  $p_1$ ). Так как число  $q_1$  простое, это возможно лишь при  $p_1 = q_1$ . Сокращая равенство (17) на  $p_1$ , получаем

$$p_2 p_3 \dots p_k = q_2 q_3 \dots q_l. \quad (18)$$

Аналогично предыдущему убеждаемся в том, что некоторое из чисел  $q_2, q_3, \dots, q_l$  (например  $q_2$ ) делится на  $p_2$ , и потому  $p_2 = q_2$ . Сокращая равенство (18) на  $p_2$ , мы уменьшаем число сомножителей в его частях еще на единицу. Такой процесс сокращения, очевидно, можно продолжать до тех пор, пока мы не сократим одно из произведений полностью. Пусть первым сократится произведение, стоящее в (17) слева. Произведение, стоящее в (17) справа, тоже должно при этом сократиться нацело, так как в противном случае мы получили бы равенство вида

$$1 = q_{k+1} \dots q_l,$$

которое невозможно, так как единица не делится ни на какое простое число. При этом мы получаем также, что

$$p_1 = q_1, p_2 = q_2, \dots, p_k = q_k.$$

Теорема полностью доказана.

15. Пусть  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  и  $q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$  — соответственно канонические разложения чисел  $a$  и  $b$ , а  $d$  — некоторый общий делитель этих чисел. Если  $d \neq 1$ , то  $d$  делится на некоторое простое число  $p$ . Тогда по теореме 3  $a : p$  и  $b : p$ , так что  $p$  находится как среди чисел  $p_1, p_2, \dots, p_k$ , так и среди чисел  $q_1, q_2, \dots, q_l$ . Поэтому среди простых чисел, входящих в каноническое разложение  $a$ , существует хотя бы одно, входящее в каноническое разложение  $b$ .

Наоборот, если  $a$  и  $b$  взаимно просты, и  $p$  входит в каноническое разложение  $a$ , то  $b$  не делится на  $p$ , так что  $p$  не может входить в каноническое разложение  $b$ .

16. Необходимость. Так как  $a : p_i^{\alpha_i}$  ( $i = 1, 2, \dots, k$ ), мы из  $b : a$  получаем требуемое простой ссылкой на теорему 2.

Достаточность доказывается по индукции. Делимость  $b : p_1^{\alpha_1}$  мы имеем в числе условий. Предположим, что нами уже установлено, что

$$b : p_1^{\alpha_1} \dots p_l^{\alpha_l} \quad (1 \leq l < k).$$

Кроме того, в нашем распоряжении имеется делимость  $b : p_{l+1}^{\alpha_{l+1}}$ . Так как числа  $p_1^{\alpha_1} \dots p_l^{\alpha_l}$  и  $p_{l+1}^{\alpha_{l+1}}$  по предыдущей теореме взаимно просты, мы можем применить следствие теоремы 11, которое дает нам

$$b : p_1^{\alpha_1} \dots p_l^{\alpha_l} p_{l+1}^{\alpha_{l+1}}.$$

Этим индуктивный переход обоснован.

17. **Необходимость.** Пусть

$$a = mq_1 + r_1 \quad (0 \leq r_1 < m), \quad (19)$$

$$b = mq_2 + r_2 \quad (0 \leq r_2 < m). \quad (20)$$

Ввиду равноостаточности  $a$  и  $b$  должно быть  $r_1 = r_2$ . Значит,

$$a - b = m(q_1 - q_2),$$

т. е.  $a - b : m$ .

**Достаточность.** Пусть  $a - b : m$ . Разделив  $a$  и  $b$  на  $m$  с остатком, мы получим (19) и (20). При этом

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

т. е.

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

По теореме 6  $r_1 - r_2 : m$ . Но  $|r_1 - r_2| < m$ . Значит, по теореме 4  $r_1 - r_2 = 0$  или  $r_1 = r_2$ , а это и требовалось.

18. Из условия на основании теоремы 16 мы имеем

$$\left. \begin{aligned} a_1 &= b_1 + mq_1, \\ a_2 &= b_2 + mq_2, \\ \dots &\dots \dots \dots \\ a_n &= b_n + mq_n. \end{aligned} \right\} \quad (21)$$

Сложив почленно эти равенства, мы после простых преобразований получаем

$$\begin{aligned} (a_1 + a_2 + \dots + a_n) - (b_1 + b_2 + \dots + b_n) &= \\ &= m(q_1 + q_2 + \dots + q_n), \end{aligned}$$

что по теореме 17 и означает равноостаточность сумм.

Для доказательства равноостаточности произведений отметим следующее тождество:

$$(k + bm)(p + qt) = kp + (pq + lp + lqt) m.$$

Из него следует, что произведение двух чисел вида  $a + bm$  снова является числом такого же вида. Поэтому, рассуждая по индукции, мы убеждаемся в том, что

произведение любого количества чисел вида  $a + bt$  есть число этого же вида.

Перемножив теперь почленно все равенства (21) и применив к правой части только что проведенные рассуждения, мы получаем

$$a_1 a_2 \dots a_n = b_1 b_2 \dots b_n + mt,$$

где  $t$  — некоторое целое число. Равноостаточность произведений, таким образом, доказана.

19. Доказательство ведется индукцией по  $a$ . При  $a = 1$  имеем

$$a^p - a = 1 - 1 = 0$$

и  $0 \div p$ .

Предположим, что  $a^p - a$  делится на  $p$ , и докажем, что  $(a + 1)^p - (a + 1)$  также делится на  $p$ . Действительно, разлагая  $(a + 1)^p$  по формуле бинома Ньютона, имеем

$$\begin{aligned} (a + 1)^p - (a + 1) &= \\ &= a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + C_p^{p-1} a + 1 - a - 1 = \\ &= a^p - a + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + C_p^{p-1} a. \end{aligned} \quad (22)$$

$a^p - a$  делится на  $p$  по предположению. По следствию теоремы 13  $C_p^k$  (при  $1 \leq k \leq p - 1$ ) также делится на  $p$ . Следовательно, на  $p$  делится каждое слагаемое суммы (22), а потому (теорема 6) и вся сумма.

Индуктивный переход обоснован, и вся теорема доказана.

С л е д с т в и е. По теореме Ферма

$$a^p - a = a(a^{p-1} - 1) \div p.$$

Если при этом  $a$  не делится на  $p$ , то по теореме 13 на  $p$  должно делиться  $a^{p-1} - 1$ .

20. Пусть

$$m_1 = p_1^{\alpha_1} \dots p_k^{\alpha_k} \text{ и } m_2 = q_1^{\beta_1} \dots q_l^{\beta_l}.$$

По теореме 15 каждое из чисел  $p_1, \dots, p_k$  отлично от каждого из чисел  $q_1, \dots, q_l$ . Значит, каноническим разложением  $m_1 m_2$  будет  $p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_l}$ . Поэтому

$$\begin{aligned} \varphi(m_1 m_2) &= p_1^{\alpha_1 - 1} (p_1 - 1) \dots p_k^{\alpha_k - 1} (p_k - 1) \times \\ &\quad \times q_1^{\beta_1 - 1} (q_1 - 1) \dots q_l^{\beta_l - 1} (q_l - 1), \end{aligned}$$

т. е.

$$\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2).$$

21. Докажем сначала индукцией по  $\alpha$ , что  $a^{p^{\alpha-1}(p-1)} - 1$  делится на  $p^\alpha$ . При  $\alpha = 1$  доказываемое утверждение является, очевидно, следствием теоремы Ферма, справедливость которого уже была установлена. Таким образом, основание индукции доказано.

Предположим теперь, что

$$a^{p^{\alpha-1}(p-1)} - 1 : p^\alpha,$$

и рассмотрим выражение  $a^{p^\alpha(p-1)} - 1$ . Мы должны доказать, что оно делится на  $p^{\alpha+1}$ . Но

$$a^{p^\alpha(p-1)} - 1 = (a^{p^{\alpha-1}(p-1)})^p - 1.$$

Так как  $a^{p^{\alpha-1}(p-1)} - 1$ , по предположению, делится на  $p^\alpha$ , число  $a^{p^{\alpha-1}(p-1)}$  имеет вид  $Np^\alpha + 1$ . Значит,

$$a^{p^\alpha(p-1)} - 1 = (Np^\alpha + 1)^p - 1,$$

т. е., по формуле бинома,

$$a^{p^\alpha(p-1)} - 1 = N^p p^{\alpha p} + C_p^1 N^{p-1} p^\alpha (p-1) + \dots + C_p^{p-1} N p^\alpha + 1 - 1.$$

В последней сумме первое слагаемое делится на  $p^{\alpha+1}$ , так как оно делится на  $p^{\alpha p}$  и  $\alpha p \geq \alpha + 1$ . В каждое из следующих  $p - 1$  слагаемых этой суммы входит  $p$  с показателем, не меньшим  $\alpha$  и, кроме того, биномиальный коэффициент, в силу следствия теоремы 13 делящийся на  $p$ . Значит, каждое из этих слагаемых также делится на  $p^{\alpha+1}$ . Наконец, разность  $1 - 1 = 0$  может быть отброшена. Поэтому по теореме 6

$$a^{p^\alpha(p-1)} - 1 : p^{\alpha+1}.$$

Случай, когда число  $m$  имеет только один простой делитель, таким образом, разобран.

Предположим теперь, что теорема Эйлера доказана для показателей  $m_1$  и  $m_2$ , причем числа  $m_1$  и  $m_2$  взаимно простые. Докажем теорему Эйлера для показателя  $m = m_1 m_2$ . Если потом положить

$$m_1 = p_1^{\alpha_1} \dots p_k^{\alpha_k} \quad \text{и} \quad m_2 = p_{k+1}^{\alpha_{k+1}},$$

то мы, очевидно, и получим индуктивный переход, необходимый нам для завершения доказательства теоремы. Итак, доказываем высказанное утверждение.

Пусть числа  $a$  и  $m$  взаимно просты. Тогда  $a$  также взаимно просто с  $m_1$ . Значит, и  $a^{\varphi(m_2)}$  взаимно просто с  $m_1$ . Поэтому, по предположению,

$$(a^{\varphi(m_2)})^{\varphi(m_1)} - 1 = a^{\varphi(m_1)\varphi(m_2)} - 1 = a^{\varphi(m_1 m_2)} - 1 = a^{\varphi(m)} - 1$$

делится на  $m_1$ . Точно так же убеждаемся в том, что  $a^{\varphi(m)} - 1$  делится и на  $m_2$ . А так как числа  $m_1$  и  $m_2$  взаимно простые,  $a^{\varphi(m)} - 1$  делится и на их произведение, т. е. на  $m$ . Теорема Эйлера доказана.

22. Пусть

$$k_1 = \varphi(m) q_1 + r,$$

$$k_2 = \varphi(m) q_2 + r.$$

Тогда

$$a^{k_1} = a^{\varphi(m) q_1 + r} = (a^{\varphi(m)})^{q_1} a^r.$$

На основании теоремы Эйлера и теоремы 18 число  $a^{\varphi(m) q_1} a^r$  равноостаточно при делении на  $m$  с числом  $a^r$ . Аналогично устанавливается равноостаточность при этом делении чисел  $a^{k_2}$  и  $a^r$ . Значит, и числа  $a^{k_1}$  и  $a^{k_2}$  при делении на  $m$  равноостаточны.

23. Найдем сначала хотя бы одно решение  $(x', y')$  этого уравнения. Очевидно, для этого достаточно найти такое число  $x'$ , что  $ax' - c \equiv b \pmod{m}$ . По теореме Эйлера  $a^{\varphi(m)} - 1 \equiv 0 \pmod{m}$ . Значит,  $ca^{\varphi(m)} - c \equiv b \pmod{m}$ , и в качестве  $x'$  можно взять число  $ca^{\varphi(m)-1}$ .

Пусть теперь  $(x'', y'')$  — какое-то другое решение уравнения  $ax + by = c$ . Покажем, что числа  $x'$  и  $x''$  равноостаточны при делении на  $b$ . В самом деле, пусть

$$ax' + by' = c,$$

$$ax'' + by'' = c.$$

Вычитая почленно второе равенство из первого, получаем

$$a(x' - x'') - b(y' - y'') = 0,$$

откуда  $a(x' - x'') \equiv b(y' - y'') \pmod{m}$ . Так как  $a$  и  $b$  по условию взаимно просты, по теореме 12  $x' - x'' \equiv b(y' - y'') \pmod{m}$ , и нам остается сослаться на теорему 17.

Таким образом, все искомые значения  $x$  находятся среди чисел

$$x_t = ca^{\varphi(m)-1} + bt.$$

Но  $ax_t - cb$ , так что, полагая

$$y_t = \frac{-ax_t + c}{b} = c \frac{1 - a^{\varphi(b)}}{b} - at,$$

мы получаем, что все пары чисел  $x_t$  и  $y_t$  являются решениями нашего уравнения.

24. Ввиду взаимной простоты  $m$  и  $10$ , числа  $10a + b$  и  $(10a + b)10^{\varphi(m)-1}$  по теореме 15 равноделимы на  $m$ . Но

$$(10a + b)10^{\varphi(m)-1} = 10^{\varphi(m)}a + 10^{\varphi(m)-1}b,$$

так что по теореме Эйлера и теореме 18 число  $10a + b$  равноделимо на  $m$  с числом  $a + kb$ .



## РЕШЕНИЯ ЗАДАЧ

1.  $0 = a \cdot 0$  при любом  $a$ .

2.  $a = 1 \cdot a$ , значит,  $a : 1$ .

3. Пусть  $1 : a$ . Это значит, что  $1 = ac$  при некотором целом  $c$ . Отсюда следует, что  $|a| \leq 1$ . А так как  $a \neq 0$ , должно быть  $a = 1$ .

4. Достаточно взять любое  $c > 1$  и положить  $b = ac$ .

5. В качестве такого  $b$  можно взять, например,  $2a$ . Пусть при этом для некоторого  $c$  и  $2a : c$  и  $c : a$ . Это значит, что найдутся такие  $d_1$  и  $d_2$ , что  $2a = d_1 c$  и  $c = d_2 a$ . Отсюда следует, что  $2a = d_1 d_2 a$  или, после сокращения на  $a$ ,

$$2 = d_1 d_2.$$

Но при целых  $d_1$  и  $d_2$  такое равенство возможно лишь в случае, когда одно из этих чисел равно 1, а другое 2. Если  $d_1 = 1$ , то  $c = 2a = b$ ; если же  $d_2 = 1$ , то  $c = a$ .

6. Доказательства ничем не отличаются от доказательств в случае обычной делимости.

7. Пусть  $n$  — некоторое фиксированное число, большее единицы. Положим  $a : b$ , если найдется такое целое  $c$ , что  $a = bc$  и  $c \leq n$ .

Справедливость теорем, аналогичных теоремам 1, 3 и 4, проверяется без труда. Однако если мы возьмем  $a = nb$  и  $b = nc$ , то  $a : b$  и  $b : c$ . В этом случае  $a = n^2 c$ , а так как  $n^2 > n$ , делимость  $a : c$  не имеет места. Точно так же не имеет места делимость  $a + a : b$ .

8. а) Пусть имеются два минимальных числа,  $a_1$  и  $a_2$ . В силу дихотомичности либо  $a_1 \geq a_2$ , либо  $a_2 \geq a_1$ . Если  $a_1 \geq a_2$ , то из минимальности  $a_1$  следует, что  $a_1 = a_2$ . Если же  $a_2 \geq a_1$ , то  $a_1 = a_2$  следует из минимальности  $a_2$ .

б) Пусть  $a$  — некоторое число, а  $b_1$  и  $b_2$  — два непосредственно предшествующих ему числа. По дихотомичности должно быть либо  $b_1 \geq b_2$ , либо  $b_2 \geq b_1$ . Пусть, для определенности,

$b_1 \geq b_2$ . Мы имеем  $a \geq b_1 \geq b_2$ , а так как число  $b_2$  непосредственно предшествует числу  $a$ , должно быть либо  $b_1 = a$ , либо  $b_1 = b_2$ . Но по условию  $b_1 \neq a$ ; значит,  $b_1 = b_2$ , и требуемая единственность доказана.

в) *Непосредственно следующим* за  $a$  числом называется такое  $b$ , что  $b \geq a$ ,  $b \neq a$ , и из  $b \geq c \geq a$  следует либо  $c = b$ , либо  $c = a$ .

Предположим, что некоторое  $a$  не имеет непосредственно следующего за ним числа. Это значит, что для любого  $a_n \geq a$  и отличного от  $a$  найдется такое  $a_{n+1}$ , отличное как от  $a_n$ , так и от  $a$ , что  $a_n \geq a_{n+1} \geq a$ . Возьмем теперь произвольное  $a_1 \geq a$  и отличное от  $a$  (в силу 2° это сделать можно) и, исходя из него, построим бесконечную последовательность различных чисел

$$a_1 \geq a_2 \geq \dots \geq a_n \geq a_{n+1} \geq \dots \geq a.$$

Существование же этой последовательности противоречит 4°. Следовательно, непосредственно следующее число существует. Единственность его устанавливается при помощи дихотомичности подобно тому как это делалось в пп. а) и б).

9. Остается в силе транзитивность (3°), неограниченность множества чисел (5°), свойство 4° и существование непосредственно предшествующего числа (6°). Дихотомичность заменяется *трихотомичностью* (либо  $a > b$ , либо  $b > a$ , либо  $a = b$ ).

Становится неверным свойство рефлексивности (1°), ибо  $a > a$  всегда неверно.

Что же касается, наконец, утверждения 2°, то формально оно остается в силе.

В самом деле, говоря строго, это утверждение в нашем случае формулируется так: для любых натуральных чисел  $a$  и  $b$  из  $a > b$  и  $b > a$  следует  $a = b$ .

Предположим, что это высказывание неверно. Тогда найдутся такие натуральные числа  $a$  и  $b$ , что одновременно будет и  $a > b$ , и  $b > a$ , и  $a \neq b$ , а этого не может быть. Полученное противоречие доказывает истинность нашего утверждения.

10. Пусть множество упорядочено отношением  $\xi$ , обладающим свойствами 1°—7°. Как уже было установлено, оно обладает минимальным элементом. Обозначим этот элемент через  $a_0$ . Из результатов задачи 8 следует, что каждый элемент обладает непосредственно следующим. Обозначим непосредственно следующий за  $a_0$  элемент через  $a_1$ , непосредственно следующий за  $a_1$  — через  $a_2$  и т. д. В итоге мы получаем последовательность

$$a_0, a_1, a_2, \dots, \quad (23)$$

в которой  $a_{n+1} \xi a_n$  при любом  $n$ . По рефлексивности и транзитивности отношения  $\xi$  отсюда следует, что  $a_i \xi a_j$  тогда и только тогда, когда  $i \geq j$ . Нам остается показать, что последовательность (23) охватывает все рассматриваемые нами объекты. Это достигается довольно тонким рассуждением по индукции.

Предположим, что  $b_0$  не принадлежит последовательности (23). Получение этого  $b_0$  будем считать первым шагом нашего индуктивного рассуждения. Пусть  $n$  его шагов уже проведены, в результате чего нами получен некоторый элемент  $b_{n-1}$ .

Если  $b_{n-1} = a_0$ , то наш процесс будем считать законченным; если же  $b_{n-1} \neq a_0$ , то элемент  $b_{n-1}$  имеет непосредственно предшествующий, который мы и возьмем в качестве  $b_n$ . В результате мы

получаем последовательность различных элементов

$$b_0 \succ b_1 \succ b_2 \succ \dots \succ b_n \succ \dots$$

На основании 4° эта последовательность должна иметь последний член. Но по самому принципу построения этой последовательности ее последним членом может быть только  $a_0$ . Пусть для определенности  $b_n = a_0$ .

Нетрудно проверить, что если некоторое  $a$  непосредственно предшествует  $b$ , то  $b$  непосредственно следует за  $a$ . Значит,  $b_{n-1} = a_1$ ,  $b_{n-2} = a_2$ , ...,  $b_0 = a_n$ .

Последнее означает, что  $b_0$  принадлежит последовательности (23), но это противоречит предположенному. Следовательно, последовательность (23) содержит все рассматриваемые нами объекты.

11. Пусть  $a$  — некоторое число. Всякую последовательность различных чисел  $a_0 = a, a_1, a_2, \dots, a_n$ , для которых

$$a_0 \succ a_1 \succ a_2 \succ \dots \succ a_n, \quad (24)$$

где  $a_n$  минимально в смысле упорядочения  $\succ$ , назовем *цепью предшественников*  $a_0$ . Число  $n$  называется *длиной* этой цепи.

Покажем сначала, что при тех условиях, которые мы наложили на упорядочение  $\succ$ , каждое конкретное число не может иметь сколь угодно длинных цепей предшественников.

В самом деле, пусть  $a$  — некоторое число, а  $b_1, b_2, \dots, b_k$  — непосредственно предшествующие ему числа.

Если  $a_1$  не предшествует  $a_0$  непосредственно, мы можем на основании 9° вставить в цепь (24) некоторое непосредственно предшествующее  $a$  число. Поэтому если имеются сколь угодно длинные цепи предшественников  $a$ , должны найтись и такие его сколь угодно длинные цепи предшественников, которые начинаются с чисел, непосредственно предшествующих  $a$ . Будем далее рассматривать только такие цепи.

Каждая цепь предшественников  $a$  ровно на единицу длиннее некоторой цепи предшественников одного из непосредственно предшествующих ему чисел. Если бы каждое из них имело цепи предшественников ограниченной длины, то само  $a$  не могло бы иметь сколь угодно длинных цепей предшественников.

Значит, при нашем предположении хотя бы одно из чисел, непосредственно предшествующих  $a_0$ , имеет сколь угодно длинные цепи предшественников. Обозначим это число через  $a_1$  и повторим в применении к нему все только что проведенные рассуждения. Это даст нам некоторое число  $a_2$ , непосредственно предшествующее  $a_1$  и имеющее сколь угодно длинные цепи предшественников. Повторяя этот процесс, мы приходим к последовательности

$$a_0 \succ a_1 \succ a_2 \succ \dots,$$

которая в силу 4° должна рано или поздно оборваться. Это значит, что последовательность будет иметь такой член, к которому наши рассуждения уже будут неприменимы. Но применимость рассуждений к каждому последующему члену последовательности нами уже была установлена. Полученное противоречие показывает, что ни одно число не имеет сколь угодно длинных цепей предшественников.

Следовательно, для каждого числа  $a$  среди его цепей предшественников можно выбрать самую длинную. Обозначим ее

длину через  $n(a)$ . Если  $b$  непосредственно предшествует  $a$ , то очевидно,  $n(b) = n(a) - 1$ , а для всех минимальных  $a$   $n(a) = 0$ .

Пусть, наконец,  $A(a)$  — высказывание, зависящее от  $a$ . Обозначим через  $B(n)$  высказывание « $A(a)$  верно для всех чисел  $a$ , для которых  $n(a) = n$ ». Тогда, как легко видеть, формулировка принципа индукции в новой форме для утверждений  $A(a)$  совпадает с формулировкой этого принципа в старой форме для утверждений  $B(n)$ .

12. Каковы бы ни были четные числа  $a$  и  $b$ , существуют такие четные числа  $q$  и  $r$ , что

$$a = bq + r \quad (0 \leq r < 2b).$$

Такие числа  $q$  и  $r$  единственны.

Доказательство. Разделим  $a$  на  $2b$  с остатком обычным образом:

$$a = 2bq + r \quad (0 \leq r < 2b). \quad (25)$$

При этом числа  $q$  и  $r$  определяются однозначно. Из четности  $a$  и  $2b$  следует четность их разности, т. е. числа  $r$ . Нам остается, положив  $2q = q'$ , переписать (25) в виде

$$a = q'b + r \quad (0 \leq r < 2b)$$

и заметить, что оба числа  $q'$  и  $r$  четные и определяются единственным образом.

13. Пусть  $p$  — наименьший простой делитель числа  $a$ . Отсюда следует, что  $a = pb$ . Всякий простой делитель  $q$  числа  $b$  является вместе с тем и делителем  $a$ . Поэтому  $q \geq p$ , значит, и  $b \geq p$ , так что  $a \geq p^2$  и, наконец,  $p \leq \sqrt{a}$ .

14. Необходимость. Пусть  $a : b$ . Из теоремы 13 следует, что каждый простой делитель  $b$  является простым делителем  $a$ . Таким образом,  $b$  имеет вид

$$p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \quad (26)$$

где  $0 \leq \beta_1, 0 \leq \beta_2, \dots, 0 \leq \beta_k$ . Предположим, что  $\beta_1 > \alpha_1$ . Так как

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}} = \frac{p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \dots p_k^{\beta_k}}$$

— целое число, числитель последней дроби должен делиться на знаменатель и тем более на число  $p_1^{\beta_1 - \alpha_1}$ . Но тогда по теореме 13 на  $p_1$  должно делиться хотя бы одно из чисел  $p_2, \dots, p_k$ , чего не может быть. Значит,  $\beta_1 \leq \alpha_1$ . Так как нумерация простых делителей  $a$  для нас

безразлична, мы тем самым доказали, что и  $\beta_2 \leq \alpha_2, \dots, \beta_k \leq \alpha_k$ . Необходимость доказана.

Для доказательства достаточности заметим, что если  $b$  имеет указанный вид, то

$$a = bp_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k}.$$

15. Пусть  $p_1, p_2, \dots, p_k$  — полный список всех простых чисел, входящих хотя бы в одно из канонических разложений  $a$  и  $b$ . Положим

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}.$$

(Если  $a$  не делится на  $p_i$ , то  $\alpha_i = 0$ ; если  $b$  не делится на  $p_i$ , то  $\beta_i = 0$ .) Пусть  $\gamma_i$  — наибольшее из чисел  $\alpha_i$  и  $\beta_i$  для  $i = 1, 2, \dots, k$ , а  $\delta_i$  — наименьшее из них.

Тогда на основании установленного при решении задачи 13, наибольший общий делитель  $a$  и  $b$  есть  $p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$ , а их наименьшее кратное —  $p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$ .

16. Как уже выяснилось, каждый делитель числа  $a$  с каноническим разложением  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  должен иметь вид (26), где  $\beta_1$  принимает  $\alpha_1 + 1$  значений:  $0, 1, 2, \dots, \alpha_1$ ;  $\beta_2$  принимает  $\alpha_2 + 1$  значений и т. д. Так как любые комбинации этих значений возможны и дают нам все делители  $a$ , причем каждый по одному разу (если бы какой-нибудь делитель повторился несколько раз, то это означало бы наличие у него нескольких канонических разложений), число делителей  $a$  равно

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

17. Пусть каноническое разложение  $a$  есть  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ . Очевидно, можно положить  $p_1 = 2, \alpha_1 \geq 2$  и  $p_2 = 3, \alpha_2 \geq 1$ . Далее, мы имеем:

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) = 14.$$

Отсюда  $k=2, \alpha_1+1=7$  и  $\alpha_2+1=2$ . Таким образом,  $a=2^6 \cdot 3=192$ .

18. Мы имеем:

$$\tau(a^2) = \tau(p_1^{2\alpha_1} p_2^{2\alpha_2}) = (2\alpha_1 + 1)(2\alpha_2 + 1) = 81,$$

так что  $(2\alpha_1 + 1)(2\alpha_2 + 1)$  есть разложение числа 81 на два множителя. Так как нумерация простых делителей  $a$  зависит от нас, ограничимся рассмотрением следующих возможностей:

$$2\alpha_1 + 1 = 1, \quad 2\alpha_2 + 1 = 81,$$

$$2\alpha_1 + 1 = 3, \quad 2\alpha_2 + 1 = 27,$$

$$2\alpha_1 + 1 = 9, \quad 2\alpha_2 + 1 = 9.$$

В первом из этих случаев  $\alpha_1 = 0$ , что противоречит предположенной положительности числа  $\alpha_1$ . Оставшиеся случаи дают нам

$$\alpha_1 = 1, \quad \alpha_2 = 13;$$

$$\alpha_1 = 4, \quad \alpha_2 = 4.$$

Значит, либо

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_2}) = \tau(p_1^3 p_2^{39}) = (3+1)(39+1) = 160,$$

либо

$$\tau(a^3) = \tau(p_1^{3\alpha_1} p_2^{3\alpha_2}) = \tau(p_1^{12} p_2^{12}) = 13 \cdot 13 = 169.$$

19. Пусть  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  — каноническое разложение числа  $a$ . Условие задачи дает нам

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = 2(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1),$$

или

$$\frac{p_1^{\alpha_1}}{\alpha_1 + 1} \frac{p_2^{\alpha_2}}{\alpha_2 + 1} \dots \frac{p_k^{\alpha_k}}{\alpha_k + 1} = 2. \quad (27)$$

Заметим, что

$$\frac{2^1}{1+1} = 1 < \frac{2^2}{2+1} < \frac{2^3}{3+1} = 2 < \frac{2^\alpha}{\alpha+1} \quad (\alpha \geq 4),$$

$$1 < \frac{3^1}{1+1} < 2 < \frac{3^\alpha}{\alpha+1} \quad (\alpha \geq 2),$$

$$2 < \frac{p^\alpha}{\alpha+1} \quad (p \geq 5, \alpha \geq 1).$$

Поэтому в (27) слева каждая дробь не менее единицы и, следовательно, ни одна из дробей не может быть больше, чем 2. Значит, в левой части (27) могут стоять лишь дроби из следующего набора:

$$\frac{2^1}{1+1}, \frac{2^2}{2+1}, \frac{2^3}{3+1}, \frac{3^1}{1+1},$$

причем их произведение есть 2. Но это может быть лишь в двух случаях: когда в (27) слева стоит только одна дробь  $\frac{2^3}{3+1}$ , или когда там стоят две дроби,  $\frac{2^2}{2+1}$  и  $\frac{3^1}{1+1}$ . Этим двум случаям соответствуют два ответа задачи: 8 и 12.

20. Аналоги теорем 11—14 для четной делимости неверны.

В самом деле, числа 30 и 42 четно простые. Их наименьшее общее четное кратное есть 420, а произведение — 1260.

Далее,  $60 = 6 \cdot 10$  четно делится на четно простое число 30; 6 и 30 четно взаимно просты, а 10 четно на 30 не делится.

Наконец,  $60 = 6 \cdot 10 = 30 \cdot 2$  — два различных разложения числа 60 на четно простые множители.

21. а) 116 при делении на 8 равноостаточно с 4, а 17 — с 1. Значит,  $A$  равноостаточно с  $5^{21} = (5^2)^{10} \cdot 5$ . Но  $5^2 = 25$  при делении на 8 равноостаточно с единицей. Следовательно,  $A$  при делении на 8 дает в остатке 5.

б) 14 при делении на 17 равноостаточно с  $-3$ . Поэтому  $A$  равноостаточно с  $(-3)^{256} = 3^{256} = (3^3)^{85} \cdot 3$ . Но  $3^3$  мы можем заменить на  $10:10^{85} \cdot 3 = (10^2)^{42} \cdot 30$ . Далее,  $10^2$  при делении на 17 равноостаточно с числом  $-2$ , а  $2^4$  с  $-1$ . Значит,  $A$  равноостаточно с  $(-2)^{42} \cdot 30 = 2^{42} \cdot 30 = (2^4)^{10} \cdot 4 \cdot 30 = (-1)^{10} \cdot 4 \cdot 30 = 120$ . Последнее же число при делении на 17 дает в остатке 1.

22. а) Пусть  $n_1$  — остаток от деления  $n$  на 6. Тогда  $n_1$  может принимать значения 0, 1, 2, 3, 4 и 5, а  $n_1^3 + 11n_1$  при делении на 6 равноостаточно с  $n^3 + 11n$ . Значит, нам следует испытать делимость на 6 чисел 0, 12, 30, 60, 108 и 180. Но все эти числа на 6 делятся.

б) При  $n \geq 2$  мы имеем (пользуясь формулой бинома):

$$\begin{aligned} 4^n + 15n - 1 &= (3 + 1)^n + 15n - 1 = \\ &= 3^n + 3^{n-1}C_n^1 + \dots + 3^2C_n^{n-2} + 3C_n^{n-1} + 1 + 15n - 1 = \\ &= 9(3^{n-2} + 3^{n-3}C_n^1 + \dots + C_n^{n-2}) + 18n, \end{aligned}$$

и оба слагаемых, очевидно, делятся на 9.

При  $n = 1$  наше выражение равно  $4^1 + 15 \cdot 1 - 1 = 18$ .

в) Доказательство ведется по индукции.

При  $n = 0$

$$10^{3^0} - 1 = 10^1 - 1 = 9 \quad \text{и} \quad 3^{0+2} = 9.$$

Пусть теперь делимость

$$10^{3^n} - 1 : 3^{n+2}$$

имеет место. Тогда

$$10^{3^{n+1}} - 1 = (10^{3^n})^3 - 1^3 = (10^{3^n} - 1)(10^{2 \cdot 3^n} + 10^{3^n} + 1).$$

Первый сомножитель справа делится на  $3^{n+2}$  по индуктивному предположению. Во втором же сомножителе мы можем заменить десятки на равноостаточные им при делении на 3 единицы; полученное число 3 показывает, что второй сомножитель делится на 3. Следовательно, все произведение делится на  $3^{n+3} = 3^{(n+1)+2}$ , что и требовалось.

г) При делении на  $a^2 - a + 1$ , очевидно,  $a^2$  равноостаточно с  $a - 1$ . Значит,  $a^{2n+1} + (a - 1)^{n+2}$  равноостаточно с

$$\begin{aligned} a^{2n+1} + (a^2)^{n+2} &= a^{2n+1} + a^{2n+4} = a^{2n+1}(1 + a^3) = \\ &= a^{2n+1}(1 + a)(1 - a + a^2), \end{aligned}$$

что и требовалось.

23. Пусть  $\sim$  — эквивалентное отношение на множестве чисел. Возьмем произвольное число  $a$  и рассмотрим все числа, эквивалентные  $a$ . Все они ввиду транзитивности отношения  $\sim$  эквивалентны между собой. Обозначим через  $K$  класс всех этих чисел.

Рассмотрим теперь произвольное число  $b$ , не принадлежащее  $K$ . Если бы было  $b \sim c$ , где  $c$  — некоторое число из  $K$ , то было бы и  $b \sim a$ , чего, однако, не может быть по выбору  $b$ . Значит, ни одно из чисел, лежащих вне  $K$ , не эквивалентно ни одному из чисел  $K$ . Следовательно,  $K$  есть класс эквивалентности, содержащий  $a$ .

Так как число  $a$  было нами взято совершенно произвольно, проведенные рассуждения показывают, что каждое число принадлежит некоторому классу эквивалентности. Это и требовалось.

24. Очевидно, среди чисел  $0, 1, \dots, m$  найдутся два, принадлежащие одному классу. Пусть этими числами будут  $k$  и  $l$ :  $k \sim l$ . Таких пар чисел из одного класса может оказаться, вообще говоря, и несколько. Выберем ту из них, для которой величина  $|k - l|$  будет наибольшей. Поскольку  $-l \sim -l$ , мы, по условию, получаем

$$k - l \sim l - l = 0.$$

Далее, мы находим, что и при любом целом  $n$

$$n(k - l) \sim 0.$$

Наконец, при любом  $r$

$$n(k - l) + r \sim r,$$

т. е. из  $a \equiv b \pmod{k - l}$  следует  $a \sim b$ . Таким образом, классы отношения  $\sim$  содержат целиком классы вычетов по модулю  $m$ .

Для того чтобы классов  $\sim$ -эквивалентности было  $m$ , необходимо, чтобы каждый класс  $\sim$ -эквивалентности содержал не более одного класса вычетов и чтобы  $k - l = m$ .

25. а) Обе части сравнения и модуль можно разделить на одно и то же число (разумеется, отличное от нуля).

В самом деле,

$$ad \equiv bd \pmod{md}$$

означает, что

$$ad - bd = (a - b)d : md,$$

т. е.  $a - b : m$ , откуда  $a \equiv b \pmod{m}$ .

б) Обе части сравнения можно разделить на число, взаимно простое с модулем.

Действительно, если  $d$  и  $m$  взаимно просты, то из

$$ad \equiv bd \pmod{m},$$

т. е. из  $(a - b)d : m$ , следует на основании теоремы 12, что  $a - b : m$ , что и требовалось.

26. Предположим, что

$$1 \leq k < l \leq p - 1, \quad ka \equiv la \pmod{p}.$$

Это значит, что  $(l - k)a : p$ . Поскольку  $a$  не делится на  $p$ , должно быть  $l - k : p$ . Но и этого не может быть, так как  $0 < l - k < p$ .



27. Необходимость. Пусть число  $p$  простое. Возьмем  $0 < q < p$ . Среди чисел  $q, 2q, \dots, (p-1)q$  найдется ровно одно, дающее при делении на  $p$  в остатке единицу. Пусть этим числом будет  $\bar{q}q$ :

$$\bar{q}q \equiv 1 \pmod{p}. \quad (28)$$

С другой стороны, среди чисел  $\bar{q}, 2\bar{q}, \dots, (p-1)\bar{q}$  также может быть лишь одно, дающее при делении на  $p$  в остатке единицу. Это, как уже установлено, число  $q\bar{q}$ .

Выясним, в каких случаях  $q = \bar{q}$ . Во всех таких случаях сравнение (28) переписывается так:

$$q^2 \equiv 1 \pmod{p},$$

или, что то же самое,

$$q^2 - 1 \equiv 0 \pmod{p}.$$

Это значит, что

$$q^2 - 1 = (q + 1)(q - 1) : p.$$

Ввиду того, что число  $p$  простое, по теореме 13 должно быть либо  $q + 1 : p$ , либо  $q - 1 : p$ . Так как число  $q$  заключено между нулем и  $p$ , первый из этих случаев возможен лишь при  $q = p - 1$ , а второй — при  $q = 1$ . Таким образом, при  $p = 2$  и  $p = 3$  всегда  $q = \bar{q}$ , при  $p \geq 5$  — лишь в случаях  $q = 1$ , и  $q = p - 1$ .

Следовательно, при  $p \geq 5$  все оставшиеся числа  $2, \dots, p - 2$  можно объединить в такие  $(p - 3)/2$  пары, что произведение чисел, составляющих каждую из пар, при делении на  $p$  дает в остатке 1. Выпишем сравнения вида (28) для всех таких пар, добавим в этот список сравнение

$$p - 1 \equiv p - 1 \pmod{p}$$

и перемножим все  $(p - 1)/2$  полученных сравнений почленно.

В результате такого умножения мы получим слева произведение всех чисел от 2 до  $p - 1$ , а справа  $p - 1$ :

$$2 \cdot 3 \dots (p - 1) \equiv p - 1 \pmod{p},$$

или

$$1 \cdot 2 \cdot 3 \dots (p - 1) + 1 \equiv 0 \pmod{p}.$$

Последнее сравнение означает, что

$$1 \cdot 2 \dots (p - 1) + 1 : p,$$

а это и требовалось.

Остается проверить случаи  $p = 2$  и  $p = 3$ . Но для них, очевидно,  $1 + 1 : 2$  и  $2 + 1 : 3$ .

Достаточность. Если число  $p$  не простое, то оно может быть разложено в произведение двух меньших множителей:  $p = p_1 p_2$ .

Если  $p_1 \neq p_2$ , то и  $p_1$  и  $p_2$  входят сомножителями в произведение  $1 \cdot 2 \dots (p - 1)$ , которое тем самым делится на  $p_1 p_2$ , т. е. на  $p$ . Пусть теперь  $p_1 = p_2 = q$ . Тогда  $p = q^2$  (т. е.  $p$  есть квадрат простого числа). Если  $q > 2$ , то  $p > 2q$ , и в произведение  $1 \cdot 2 \dots (p - 1)$  входят множителями  $q$  и  $2q$ , так что в этом случае оно делится на  $q^2$ , т. е. на  $p$ . В обоих случаях  $1 \cdot 2 \dots (p - 1) + 1$  на  $p$  делиться не может. Наконец, если  $p = 4$ , то  $1 \cdot 2 \cdot 3 - 1 = 5$ , и на 4 не делится.

28. Теорема. Пусть  $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  — каноническое разложение  $m$ . Тогда для того чтобы числа  $A$  и  $B$  были равноостаточными при делении на  $m$ , необходимо и достаточно, чтобы они были равноостаточными при делении на  $p_1^{\alpha_1}$ , на  $p_2^{\alpha_2}$ , ..., на  $p_k^{\alpha_k}$ .

Доказательство. Необходимость. Равноостаточность  $A$  и  $B$  при делении на  $m$  означает  $A - B \div m$ . Тем более  $A - B \div p_i^{\alpha_i}$  ( $i = 1, \dots, k$ ), и числа  $A$  и  $B$  оказываются равноостаточными при делении на все  $p_i^{\alpha_i}$ .

Достаточность. Пусть числа  $A$  и  $B$  при делении на каждое  $p_i^{\alpha_i}$  равноостаточны. Обозначим через  $r_i$  остаток от деления  $A$  и  $B$  на  $p_i^{\alpha_i}$  ( $i = 1, 2, \dots, k$ ). Это значит, что

$$A \equiv r_i \pmod{p_i^{\alpha_i}}. \quad (29)$$

Положим, далее,

$$\frac{m}{p_i^{\alpha_i}} = m_i, \quad i = 1, \dots, k,$$

и умножим в сравнении (29) обе части и модуль на  $m_i$ :

$$Am_i \equiv m_i r_i \pmod{m}.$$

Сложив все такие сравнения почленно, мы получим

$$A(m_1 + m_2 + \dots + m_k) \equiv m_1 r_1 + m_2 r_2 + \dots + m_k r_k \pmod{m}. \quad (30)$$

Ввиду равноостаточности  $A$  и  $B$  при делении на  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ , мы получаем также

$$B(m_1 + m_2 + \dots + m_k) \equiv m_1 r_1 + m_2 r_2 + \dots + m_k r_k \pmod{m}. \quad (31)$$

Вычтя почленно сравнение (31) из (30), мы имеем

$$(A - B)(m_1 + m_2 + \dots + m_k) \equiv 0 \pmod{m},$$

т. е.  $(A - B)(m_1 + m_2 + \dots + m_k) \div m$ .

Но сумма  $m_1 + m_2 + \dots + m_k$  взаимно проста с  $m$ . В самом деле, если бы она имела с  $m$  некоторый общий простой делитель  $p$ , то он входил бы в каноническое разложение  $m$ , т. е. имел бы вид  $p_i$ . Но тогда на него делилась бы как вся сумма, так и каждое слагаемое, кроме одного,  $m_i$ , а этого быть не может.

Теперь мы можем применить теорему 12, которая даст, что  $A - B \div m$ , т. е. числа  $A$  и  $B$  при делении на  $m$  равноостаточны.

29. а) Выпишем систематически все равенства, описывающие деления с остатком, которые составляют применение алгоритма Евклида к числам  $a$  и  $b$ :

$$\left. \begin{aligned} a &= bq_0 + r_1, \\ b &= r_1q_1 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\dots \dots \dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n. \end{aligned} \right\} \quad (32)$$

Мы имеем  $r_{n-1} : r_n$ . Вместе с  $r_{n-2} = r_{n-1}q_{n-1} + r_n$ , это дает нам  $r_{n-2} : r_n$ . Продвигаясь аналогичным образом вверх по системе равенств (32), мы получаем, наконец, что  $a : r_n$  и  $b : r_n$ . Значит,  $r_n$  есть общий делитель  $a$  и  $b$ .

Пусть  $d$  — любой общий делитель  $a$  и  $b$ . Вместе с  $a = bq_0 + r_1$  это дает нам  $r_1 : d$ . Продвигаясь по системе равенств (32) вниз, мы будем последовательно получать, что  $r_2 : d, r_3 : d, \dots, r_n : d$ . Значит,  $r_n$  делится на любой общий делитель  $a$  и  $b$ , являясь тем самым и наибольшим общим делителем этих чисел.

б) Доказательство ведется по индукции. Полагая  $A_0 = 0, B_0 = 1, A_1 = 1, B_1 = -q_0$ , мы имеем  $r_0 = b = aA_0 + bB_0$  и  $r_1 = aA_1 + bB_1$ . Пусть теперь

$$\begin{aligned} r_{k-1} &= A_{k-1}a + B_{k-1}b, \\ r_k &= A_k a + B_k b. \end{aligned}$$

Но тогда

$$r_{k+1} = r_{k-1} - r_k q_{k+1} = (A_{k-1} - q_{k+1}A_k)a + (B_{k-1} - q_{k+1}B_k)b,$$

и нам остается положить

$$\begin{aligned} A_{k-1} - q_{k+1}A_k &= A_{k+1}, \\ B_{k-1} - q_{k+1}B_k &= B_{k+1}. \end{aligned}$$

Числа  $A_n$  и  $B_n$  окажутся искомыми  $A$  и  $B$ .

30. Если  $b$  и  $c$  взаимно просты, то по предыдущему можно найти такие целые  $B$  и  $C$ , что

$$bB + cC = 1,$$

или, после умножения на  $a$ ,

$$abB + acC = a;$$

$ab : c$  по условию;  $ac : c$  очевидным образом; значит, и  $a : c$ .

31. Ограничимся рассмотрением признака равноостаточности при делении на 8.

Пусть произвольное натуральное  $A$  представлено в виде  $1000a + b$ , где  $0 \leq b < 1000$  (т. е.  $b$  — трехзначное число, которым оканчивается  $A$ ), и

$$f(A) = \begin{cases} b, & \text{если } A \geq 1000, \\ \text{остатку от деления } A \text{ на } 8, & \text{если } 8 \leq A < 1000, \\ \text{не определена,} & \text{если } A < 8. \end{cases}$$

32. Для тех, у которых каноническое разложение имеет вид  $2^a \cdot 5^b$ .

33. Условия а) и б) выполняются автоматически. Поскольку при делении на 3 числа 10 и 1 равноостаточны, равноостаточными же должны быть и числа  $A$  и  $f(A)$ . Наконец, то, что  $f(A) < A$  при  $A \geq 3$ , устанавливается простым подсчетом.

34. а)  $f(858\ 773) = 38$ ;  $f(38) = 11$ ;  $f(11) = 2$ .

б)  $f(A) = 4444 \cdot 4 = 17\ 776$ ;  $f(17\ 776) = 28$ ;  $f(28) = 10$ ;  $f(10) = 1$ .

35. Признак равноостаточности при делении на 9 аналогичен рассмотренному признаку равноостаточности при делении на 3.

Для получения признака равноостаточности при делении на 11 представим число  $A$  в виде

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \dots + 10^2a_1 + a_0,$$

где  $0 \leq a_i < 100$ . Очевидно, такое представление соответствует разбиению числа на двузначные «границы» (справа налево). Пусть

$$f(A) = \begin{cases} a_0 + a_1 + \dots + a_n, & \text{если } A \geq 100, \\ \text{остатку от деления } A \text{ на } 11, & \text{если } 11 \leq A < 100, \\ \text{не определена,} & \text{если } A < 11. \end{cases}$$

Нам остается указать, что числа  $A$  и  $f(A)$  действительно равноостаточны при делении на 11 и, кроме того,  $f(A) < A$ .

Другой признак равноостаточности при делении на 11 получается на основе представления числа  $A$  в виде

$$A = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10a_1 + a_0$$

и использования того, что 10 при делении на 11 равноостаточно с  $-1$ , а 100 с 1. Поэтому  $A$  равноостаточно с числом  $a_0 - a_1 + a_2 - a_3 + \dots \pm a_n$ , и формулировка соответствующего признака равноостаточности не составляет труда.

Наконец, можно, разбивая число  $A$  на трехзначные «границы», представить его в виде

$$10^{3n}a_n + 10^{3n-3}a_{n-1} + \dots + 10^3a_1 + a_0$$

( $0 \leq a_i < 1000$ ). Тогда  $A$  при делении на 37 равноостаточно с суммой  $a_0 + a_1 + \dots + a_n$ , а при делении на 7, 11 и 13 — со знакопеременной суммой  $a_0 - a_1 + a_2 - a_3 + \dots \pm a_n$ .

36. Если числа  $a$  и  $b$  равноостаточны, то  $a - b \div m$ . Поэтому в силу теоремы 6 числа  $a$  и  $b$  делятся или не делятся на  $m$  одновременно.

4 и 5 равноделимы, но не равноостаточны при делении на 3.

37. Пусть из равноделимости на  $m$  следует равноостаточность при делении на  $m$ . Это значит, что все не

делящиеся на  $m$  числа имеют при делении на  $m$  один и тот же остаток. Значит, этот остаток должен быть равен единице, так что  $m = 2$ .

38. Отношение равноделимости на  $m$ , очевидно, является рефлексивным (всякое число равноделимо на  $m$  с самим собой), симметричным (если  $a$  равноделимо с  $b$ , то и  $b$  равноделимо с  $a$ ) и транзитивным (если  $a$  равноделимо с  $b$ , а  $b$  равноделимо с  $c$ , то и  $a$  равноделимо с  $c$ ).

Следовательно, это есть отношение эквивалентности. При этом в один класс попадают все числа, делящиеся на  $m$ , а в другой — все не делящиеся на  $m$ .

39. Нетрудно проверить, что при  $m > 2$  равноделимость сумм не следует из равноделимости слагаемых.

Для того чтобы равноделимость произведений вытекала из равноделимости их сомножителей, необходимо и достаточно, чтобы число  $m$  было простым.

В самом деле, если одно из произведений делится на простое  $p$ , то по теореме 13 на это  $p$  должен делиться хотя бы один из сомножителей этого произведения. Но тогда на  $p$  делится равноделимый ему сомножитель другого произведения, а потому и все произведение. Если же одно произведение на  $p$  не делится, то и другое на  $p$  делиться не может (ибо в противном случае, на основании только что установленного, на  $p$  делилось бы и первое произведение).

Наоборот, если число  $p$  составное, то произведения равноделимых сомножителей могут уже равноделимыми не быть. Достаточно положить  $p = p_1 p_2$  ( $p_1 \neq 1$ ,  $p_2 \neq 1$ ). Тогда числа 1 и  $p_1$ , а также числа 1 и  $p_2$ , на  $p$  равноделимы, а их произведение, очевидно, нет.

40. Непосредственное следствие задачи 36.

41. Выполнение условий а) и б) очевидно.

Если, далее,  $a - b \geq 0$ , то, очевидно,  $f(A) < A$ . Если же  $a - 2b < 0$ , то это неравенство может и нарушиться. При этом наибольшее значение модуля  $|a - 2b|$  достигается при  $a = 0$  и  $b = 9$  и равно поэтому 18. Следовательно, при  $A \geq 19$  должно быть  $f(A) < A$ . Справедливость этого неравенства при меньших значениях обеспечивается определением функции  $f$ .

Наконец,  $10a + b$  равноделимо на 7 с  $50a + 5b$  (ибо числа 5 и 7 взаимно простые) и тем самым с  $50a + 5b - 7(7a + b) = a - 2b$ .

42. 15 при делении на 7 дает в остатке 1, а  $1 - 2 \cdot 5 = -9$  дает в остатке 5.

43. Условие в)  $f(A) < A$  означает  $a + 4b < 10a + 1 + b$ , т. е.  $3b < 9a$ . Поэтому при  $a \geq 4$  нужное условие выполняется.

Условие г). Очевидно,  $10a + b$  при делении на 13 равноделимо с  $40a + 4b$ , а последнее число равноостаточно с  $a + 4b$ .

44. Признак делимости утратит результативность; так как  $f(39) = 39$ .

45. Пусть нам нужно построить признак делимости на некоторое  $m$ . Постараемся подобрать такое  $s$ , взаимно простое с  $m$  и по возможности небольшое, что  $10s + 1 \div m$  (так было в случае  $m = 7$ ;  $s$  оказалось равным 3) или же  $10s - 1 \div m$  (например, при  $m = 13$ ,  $s = 4$ ).

В первом из этих случаев  $A = 10a + b$  равноделимо на  $m$  с

$$10as + bs = (10s + 1)a - a + bs,$$

т. е. с  $a - bs$ , а во втором — с

$$(10s - 1)a + a + bs,$$

т. е. с  $a + bs$ .

В связи со сказанным число  $10a + b$

при делении на 17 равноделимо с  $a - 5b$ ,

» 19 »  $a + 2b$ ,

» 23 »  $a + 7b$ ,

» 29 »  $a - 3b$ ,

» 31 »  $a + 3b$ .

Завершение точных формулировок этих признаков делимости предоставляется читателю.

46. а) Так как 100 при делении на 49 равноостаточно с 2, всякое число вида

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \dots + 10^2a_1 + a_0 \quad (0 \leq a_i < 100)$$

при делении на 49 равноостаточно с

$$2^n a_n + 2^{n-1} a_{n-1} + \dots + 2a_1 + a_0.$$

б)  $10a + b$  при делении на 49 равноделимо с  $a + 5b$ .

47. Условия а) и б) выполняются автоматически. Условия в) и г) соблюдаются потому, что переход от  $A$  к  $F(A)$  сводится к замене некоторых чисел на их остатки при делении на  $A$  (которые меньше самих чисел и равноостаточны с ними).



для определенности  $p_1 = 5$ ), либо на 5 делится одна из разностей  $p_1 - 1, p_2 - 1, \dots, p_k - 1$  (пусть в этом случае  $p_1 - 1 \div 5$ ). В первом из этих случаев  $p_1 - 1 = 4$ , чего не может быть, так как 10 на 4 не делится. Второй случай, поскольку  $p_1$  должно быть простым числом, и  $10 \div p_1 - 1$ , возможен лишь при  $p_1 = 11$ . Но тогда  $\alpha_1 = 1$ , и из теоремы 20 следует, что

$$\varphi\left(\frac{m}{11}\right) = 1,$$

т. е. либо  $\frac{m}{11} = 1$ , либо  $\frac{m}{11} = 2$ .

В итоге мы имеем  $m_1 = 11, m_2 = 22$ .

$$б) p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\dots p_k^{\alpha_k-1}(p_k-1) = 8.$$

Если  $m$  нечетное, то  $\alpha_1 = \alpha_2 = \dots = \alpha_k = 1$  (ибо правая часть написанного неравенства есть степень двойки):

$$(p_1 - 1)(p_2 - 1)\dots(p_k - 1) = 8.$$

Это возможно лишь при  $k = 2, p_1 = 3, p_2 = 5$ , т. е. при  $m = 15$ .

Пусть теперь число  $m$  четное. Положим для определенности  $p_1 = 2$ . Очевидно, по-прежнему  $\alpha_2 = \dots = \alpha_k = 1$ , и мы имеем

$$2^{\alpha_1-1}(p_2-1)\dots(p_k-1) = 8.$$

Очевидно,  $\alpha \leq 4$ . Если  $\alpha = 1$ , то случай подобен рассмотренному: написанное неравенство возможно также лишь при  $k = 3, p_2 = 3, p_3 = 5$ , т. е. при  $m = 30$ .

Если  $\alpha = 2$ , то  $k = 2, p_2 = 5$  и  $m = 20$ .

Если  $\alpha = 3$ , то  $k = 2, p_2 = 3$  и  $m = 24$ .

Если, наконец,  $\alpha = 4$ , то  $k = 1$  и  $m = 16$ .

Итак, решения нашей задачи:  $m_1 = 15, m_2 = 30, m_3 = 20, m_4 = 24, m_5 = 16$ .

54. Предположим, что

$$p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\dots p_k^{\alpha_k-1}(p_k-1) = 14.$$

Каждое из чисел вида  $p_i - 1$  есть либо единица, либо четное число, и потому не может быть семеркой. Будучи на единицу меньше простого числа, оно не может равняться 14. Значит, семеркой является одно из чисел  $p_i^{\alpha_i-1}$ . Но тогда  $p_i - 1 = 6$ , а 14 на 6 не делится.



55. Пусть  $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ . Рассмотрим сначала случай, когда  $m$  есть степень простого числа:  $m = p^\alpha$ . Для того чтобы некоторое число было взаимно простым с  $m$ , необходимо и достаточно, чтобы оно не делилось на  $p$ . Но среди чисел  $0, 1, 2, \dots, m - 1$  имеется всего  $\frac{m}{p}$  делящихся на  $p$  чисел. Следовательно, взаимно простых с  $p$  чисел в этом списке имеется столько:

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

Заметим теперь, что для взаимной простоты  $a$  и  $m$  необходимо и достаточно, чтобы с  $a$  был взаимно прост остаток от деления  $a$  на  $m$ .

По только что установленному число остатков от деления на  $p_i^{\alpha_i}$ , взаимно простых с  $p_i^{\alpha_i}$ , равно  $\varphi(p_i^{\alpha_i})$ . Но, как было выяснено в процессе решения задачи 28, из равноостаточности чисел при делении на все  $p_i^{\alpha_i}$  следует их равноостаточность при делении на  $m$ , и наоборот. Кроме того, для взаимной простоты некоторого числа с  $m$  необходимо и достаточно, чтобы оно было взаимно просто с каждым из чисел  $p_i^{\alpha_i}$ .

Следовательно, каждой комбинации остатков от деления на  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ , взаимно простых соответствующим делителям, соответствует ровно один остаток от деления на  $m$ , взаимно простой с  $m$ . Нам остается заметить, что число таких комбинаций остатков равно

$$\varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}) = \varphi(m).$$

56. Предоставляется читателю.

57.  $n^{13} - n = n(n^{12} - 1)$ . Но

$$n^{12} = n^{\varphi(13)} = n^{2\varphi(7)} = n^{3\varphi(5)} = n^{6\varphi(3)} = n^{12\varphi(2)}.$$

Поэтому либо  $n : p$ , либо  $n^{12} - 1 : p$  для  $p = 2, 3, 5, 7, 13$ . Остается сослаться на теорему 16.

58. Предоставляется сделать читателю самостоятельно.

59. Пусть наибольший общий делитель чисел  $a$  и  $b$  есть  $d$ . Если  $c$  не делится на  $d$ , то уравнение

$$ax + by = c$$

в целых числах неразрешимо. Если же  $c$  делится на  $d$ , то обе части уравнения можно сократить на  $d$ , и мы приходим к уже рассмотренному случаю.

60. Пусть  $A$  и  $B$  таковы, что

$$aA + bB = 1.$$

Положим

$$x_t = cA + bt,$$

$$y_t = c \frac{1 - aA}{b} - at.$$

Тогда

$$\begin{aligned} ax_t + by_t &= a(cA + bt) + b\left(c \frac{1 - aA}{b} - at\right) = \\ &= caA + abt + c(1 - aA) - abt = c, \end{aligned}$$

и  $(x_t, y_t)$  действительно является решением нашего уравнения.

61. а)  $x_t = 9 \cdot 5^5 + 7t = 28\,125 + 7t,$

$$y_t = 9 \frac{1 - 5^6}{7} - 5t = -20\,088 - 5t.$$

Поскольку свободные члены и коэффициенты при  $t$  в выражениях для  $x_t$  и  $y_t$ , так сказать, «примерно пропорциональны», мы можем надеяться получить представления наших решений в меньших числах. В самом деле, мы можем написать

$$x_t = 6 + 7(t + 4017),$$

$$y_t = -3 - 5(t + 4017),$$

или, полагая

$$t + 4017 = t',$$

мы получаем

$$x_{t'} = 6 + 7t',$$

$$y_{t'} = -3 - 5t'.$$

Заметим, что способ решения уравнений в целых числах, приведенный в задаче 60, позволяет обходиться меньшими числами, хотя и требует несколько более сложных вычислений.

б) Воспользуемся тем, что 25 по модулю 13 принадлежит показателю 2. Мы можем написать

$$x_t = 8 \cdot 25 + 13 = 200 + 13t,$$

$$y_t = 8 \frac{1 - 25^2}{13} - 25t = -384 - 25t,$$

или, после упрощений,

$$x_{t'} = 5 + 13t',$$

$$y_{t'} = -9 - 25t'.$$

62. Условие в) обеспечивается автоматически, а условие г) следует из теоремы 25.

63.	$m \mid 17$	19	27	29	31	49
	$k' \mid 12$ (или $-5$ )	2	19	3	28	(или $-3$ ) 5

64. Предоставляется читателю.

## СОДЕРЖАНИЕ

Предисловие . . . . .	3
§ 1. Делимость чисел . . . . .	7
§ 2. Делимость сумм и произведений . . . . .	24
§ 3. Признаки равноостаточности и признаки дели- мости . . . . .	29
§ 4. Делимость степеней . . . . .	44
Доказательства теорем . . . . .	49
Решения задач . . . . .	58