ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»**

**ИНСТИТУТ ИНЖЕНЕРНЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ
КАФЕДРА ОБЩЕЙ МАТЕМАТИКИ**

Л.Н. Куртова

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

Учебно-методическое пособие

Белгород, 2018

УДК
ББК

Печатается по решению
редакционно-издательского совета
НИУ «БелГУ»

Рецензенты:

Доцент кафедры математики НИУ БелГУ, кандидат физико-математических наук Мотькина Н.Н.;

Доцент кафедры естественнонаучных дисциплин Белгородского университета кооперации, экономики и права, кандидат физико-математических наук Москаленко Н.И.

Куртова, Л.Н.

Основы комбинаторики и теории чисел: Учебное пособие / Л.Н. Куртова.– Белгород: Изд-во НИУ «БелГУ», 2018. – с. 50.

Излагаются основные теоретические сведения по комбинаторике и теории чисел, приведены примеры решения задач, представлены задания для самостоятельной работы. Пособие рекомендуется для всех интересующихся математикой. Представленные задания могут быть полезны школьникам при подготовке к олимпиадам.

УДК
ББК

© Куртова Л.Н., 2018

© Белгородский государственный университет, 2018

Содержание

Введение

В учебном пособии рассматриваются основные теоретические сведения по комбинаторике и теории чисел.

Пособие содержит следующие темы: основы комбинаторики, теория делимости, теория сравнений. В каждой теме даются краткие теоретические сведения, рассматриваются примеры решения задач, которые встречаются на математических олимпиадах различных уровней. В конце каждой темы приведены задания для самостоятельной работы.

Учебное пособие предназначено для школьников, обучающихся в классах с углубленным изучением математики, преподавателей и всех, кому будут интересны задачи по комбинаторике и теории чисел.

Тема 1. Основы комбинаторики

Основные определения и понятия

Часто при решении задач требуется определить, сколько различных комбинаций, удовлетворяющих каким-либо условиям, можно составить из заданных объектов. Раздел математики, занимающийся изучением этого вопроса, называют *комбинаторикой*.

Одними из важнейших правил комбинаторики являются правило суммы и правило произведения.

Правило суммы. Пусть объект A выбирается m способами, а объект B выбирается n способами, тогда выбрать «либо A, либо B» можно $m+n$ способами.

Правило произведения. Пусть объект A выбирается m способами, а объект B выбирается n способами, тогда выбрать пару (A, B) в указанном порядке можно $m \cdot n$ способами.

Используя правило произведения можно подсчитать количество способов выбора комбинаций из большего числа элементов.

Пусть присутствует k групп элементов, причем i-ая группа содержит n_i элементов, $1 \le i \le k$. Из каждой группы произведем выбор по одному элементу. Тогда общее число N способов выбора таких элементов равняется $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Пример. Две различные путевки между тремя сотрудниками можно распределить шестью способами. Действительно, первая путевка может достаться одному из трех сотрудников, т.е. существует три возможных исхода распределения первой путевки. Тогда вторая путевка может достаться одному из двух оставшихся сотрудников, т.е. существует два возможных исхода распределения второй путевки. Соответственно по правилу произведения две путевки между тремя сотрудниками можно распределить шестью способами.

Урновые модели. Пусть имеется некоторая урна, (то есть ящик), которая содержит n объектов, каждому из которых присвоен номер. Эти объекты будем считать шариками. Выберем из этой урны k шариков. Ставиться вопрос: сколькими способами можно осуществить выбор k шариков из n, или *сколько различных результатов* (то есть наборов, состоящих из k шариков) может получится?

Для ответа на этот вопрос нужно определиться с двумя важными составляющими:

1) с тем, как организован выбор (будут ли шарики возвращаться в урну или нет),
2) с тем, каким образом мы рассматриваем результаты выбора (в урне все шарики разные или одинаковые).

Существуют две возможные схемы выбора:

1. Выбор с возвращением: каждый выбранный шарик возвращается в урну, то есть каждый из k шариков выбирается из полной урны. В полученном наборе, состоящем из k номеров шариков, могут встречаться одни и те же номера. Назовем данный выбор *выборкой с повторениями*.

2. Выбор без возвращения: выбранные шарики в урну не возвращаются, и в полученном наборе не могут встречаться одни и те же номера. Назовем данный выбор *выборкой без повторений*.

В обоих случаях результатом выбора является набор из k номеров шариков. Будем считать, что шарики всегда выбираются последовательно, по одному (с возвращением или без).

Определимся, какие наборы выбранных шариков будем считать *различными*. Возможны два случая.

1. Выбор с учетом порядка: два набора номеров шариков считаются различными, если они отличаются составом или порядком номеров. Например, выбираем из урны, содержащей пять шариков, три шарика. Тогда наборы (1,3,4), (3,4,1), (1,4,5) различны.

2. Выбор без учета порядка: два набора номеров шариков считаются различными, если они отличаются составом. Наборы, отличающиеся лишь порядком следования номеров, считаются одинаковыми. В примере, рассмотренном выше, наборы (1,3,4), (3,4,1) являются одним и тем же результатом выбора, а набор (1,4,5) – другой результат выбора.

Таким образом, получили 4 урновые модели, представленные в таблице 1.1:

Возможность повторения элементов в выборке	Учет порядка элементов в выборке	
	Упорядоченные выборки	Неупорядоченные выборки
Без повторения	Перестановки без повторения	Сочетания без повторения
С повторением	Перестановки с повторением	Сочетания с повторением

Таблица 1.1. Урновые модели.

1) Урновая схема: перестановки без повторения

Общее количество выборок в схеме выбора k элементов из n без возвращения и с учетом порядка определяется формулой:

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

и называется *числом размещений из n элементов по k элементов*.

Доказательство. Существует n способов выбора первого шарика из урны. При каждом из этих способов существует $n-1$ способ выбрать второй шарик из урны, и т.д. Последний k-й шарик можно выбрать $(n-k+1)$ способом. По *правилу произведения*, общее число способов выбора равно $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$.

Пример. Число возможных слов из трех букв, которые выбираются из пяти различных букв, равно $A_5^3 = 5 \cdot 4 \cdot 3 = 60$.

Следствие. Число возможных перестановок множества из n элементов равно $P(n) = n!$.

Доказательство. Заметим, что перестановка – это выбор без возвращения и с учетом порядка всех n элементов из n. Так что общее число перестановок равно $P(n) = A_n^n = n!$.

Пример. Множество из трех элементов имеет $P_3 = 3! = 6$ перестановок.

Для приближенного вычисления факториала в случае больших значений аргумента используется формула Стирлинга: $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$.

2) Урновая схема: сочетания без повторения

Общее количество выборок в схеме выбора k элементов из n без возвращения и без учета порядка определяется формулой:

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k! \cdot (n-k)!}$$

и называется *сочетаниями из n различных элементов по m элементов* ($m \le n$).

Доказательство. Когда производится выбор без возвращений и без учета порядка, то можно образовать $k!$ выборок, отличающихся друг от друга только порядком элементов.

Таким образом, число выборок, которые различаются порядком, в $k!$ раз больше, чем число выборок, которые различаются только составом. Поделив A_n^k на $k!$, получим формулу для числа сочетаний.

Пример. Выбрать 2 ампулы из упаковки, содержащей 10 ампул можно $C_{10}^2 = \frac{10 \cdot 9}{2} = 45$ способами.

Отметим некоторые свойства сочетаний:

1. $C_n^n = 1$, $C_n^1 = n$, $C_n^2 = \frac{n \cdot (n-1)}{2}$.
2. Симметричность: $C_n^m = C_n^{n-m}$.

3. Рекуррентная формула: $C_n^m = C_{n-1}^{m-1} + C_{n-1}^m$.

3) Урновая схема: перестановки с повторением

Общее количество выборок в схеме выбора k элементов из n с возвращением и с учетом порядка равно n^k.

Доказательство. Существует n способов выбора первого шарика. При каждом из таких способов существует также n способов выбрать второй шарик, и так k раз.

4) Урновая схема: выбор с возвращением и без учета порядка

Общее количество выборок в схеме выбора k элементов из n с возвращением и без учета порядка определяется формулой:

$$C_{n+k-1}^k = C_{n+k-1}^{n-1}.$$

Бином Ньютона используется во многих разделах математики и ее приложениях. Эта формула дает правило для представления n-ой степени суммы двух слагаемых $(x+y)^n$ в виде суммы произведений степеней слагаемых x и y. Ее частными случаями при $n=2$ и $n=3$ являются известные формулы: $(x+y)^2 = x^2 + 2xy + y^2$, $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$.

Теорема 1. Для n-ой степени бинома, т.е. для $(x+y)^n$, при любом $n \in \mathrm{N}$ справедливо равенство

$$(x+y)^n = \sum_{m=0}^{n} C_n^m x^m y^{n-m}.$$

Отметим некоторые особенности биномиальной формулы Ньютона. Правая часть формулы содержит $n+1$ слагаемое. Сумма показателей степеней x и y в каждом члене разложения для $(x+y)^n$ равна n.

Треугольник Паскаля представлен на рисунке 1.2.

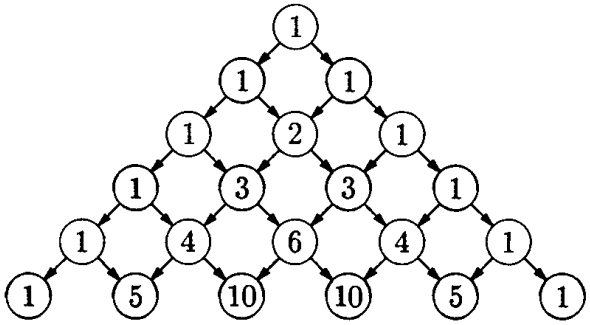

Рисунок 1.2. Треугольник Паскаля

Данный треугольник состоит из клеток и ветвей, входящих в клетку и выходящих из нее. Каждая клетка содержит число, которое показывывает, сколько существует путей из вершины треугольника, ведущих в эту клетку. Пути представляют собой ломанные, составленных из ветвей двух видов: идущих вправо-вниз и идущих влево-вниз. Числа, которые стоят в n-ой строке треугольника Паскаля, совпадают с коэффициентами бинома Ньютона $(x+y)^n$.

Не все задачи комбинаторики решаются с использованием основных теорем комбинаторики – правило суммы или правило произведения, число сочетаний, число перестановок, число размещений. В определенных случаях приходится действовать по другому и использовать «метод решета», который состоит в следующем: для нахождения числа элементов интересующего нас множества мы сначала находим число элементов некоторого большего множества, а потом «просеиваем» нужные элементы, постепенно отбрасывая лишние.

Формула включений и исключений дает возможность находить число объектов, не обладающих ни одним из указанных свойств. Пусть дано N объектов и определенный набор свойств P_1, ..., P_n. Пусть N_i – число объектов, которые обладают свойством P_i, N_{ij} – число объектов, которые обладают свойствами P_i и P_j и т.д. Тогда число объектов, которые не обладают ни одним из свойств, равно

$$N - \sum N_i + \sum_{i_1<i_2} N_{i_1 i_2} - \sum_{i_1<i_2<i_3} N_{i_1 i_2 i_3} + \ldots + (-1)^n N_{123\ldots n}.$$

В этом случае предметы, обладающие указанными свойствами, удобно представлять в виде множеств. Для наглядности при рассмотрении множеств часто используют так называемые диаграммы Венна. Так на рисунке 1.3 представлена диаграмма Венна для формулы включений и исключений для множества объектов, которые обладают набором из трех свойств.

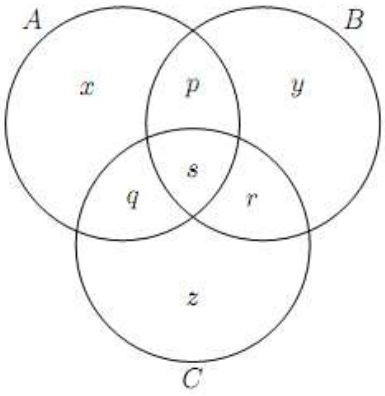

Рисунок 1.3. Диаграмма Венна для множества с набором из трех свойств.

Пример. Каждый ученик в классе ходил в воскресенье в зоопарк или в кино. В зоопарке были 18 человека. В кино посмотрели фильм 12 человек. И в зоопарке, и в кино были 6 человек. Сколько учеников в классе?

Решение. Найдём сумму $18+12$, тогда дважды были подсчитаны те ученики, которые в воскресенье побывали и в зоопарке и в кино. Например, если Максим был и в зоопарке, и в кино, то один раз он вошёл в эту сумму в числе тех 18 учеников, кто ходил в зоопарк, и второй раз – в числе 12 детей, кто ходил в кино. Поэтому эта сумма на 6 больше числа детей в классе. Следовательно, $18+12-6=24$ человека в классе.

Задача о беспорядках. Будем считать, что в перестановке $k_1k_2...k_n$ из 1, 2, …, n чисел число i стоит на своём месте, если $k_i=i$. Например, в перестановке {51342} тройка и четверка стоят на своём месте. Возникает вопрос: Сколько существует беспорядков? То есть, чему равно число перестановок, в которых ни одно из чисел не стоит на своём месте.

Число беспорядков N можно найти, если вычесть из общего количества перестановок, равного $n!$, количество тех перестановок, в

которых хотя бы одно из чисел стоит на своём месте. После применения формулы включений и исключений получаем, что

$$N = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Пример. Задача Леонардо Эйлера. Войдя в ресторан, n гостей оставили швейцару свои шляпы, а на выходе получили их обратно. Швейцар раздал шляпы случайным образом. Сколько существует вариантов, при которых каждый гость получит чужую шляпу?

Решение. В этой задаче необходимо подсчитать число беспорядков из n элементов, которое равно $N = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

Числа Стирлинга. Рассмотрим еще один пример, в котором используется формула включений и исключений. Далее предположим , что $m \geq n$.

Пример. Сколькими способами можно разложить m различных шаров по n различным ящикам так, чтобы ни один из ящиков не оказался пустым?

Решение. Если ящики могут быть пустыми, то получаем размещения с повторениями. Тогда общее число способов разложить m различных шаров по n различным ящикам равно n^m.

Пусть A_i – множество таких способов разложить шарики, при которых i-й ящик пуст ($i = 1, 2, ..., n$). Тогда искомое число $D(m,n)$ разложений шаров, при которых все ящики не будут пусты, равно:

$$D(m,n) = n^m - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - ... + (-1)^n |A_1 \cap ... \cap A_n|.$$

Можно доказать, что $|A_i| = (n-1)^m$, $|A_i \cap A_j| = (n-2)^m$ и так далее. Тогда:

$$D(m,n) = n^m - C_m^1 (n-1)^m + C_m^2 (n-2)^m - ... + (-1)^n \cdot 0 = \sum_{k=0}^{n} (-1)^k C_m^k (n-k)^m.$$

В предыдущем примере ящики различались. Рассмотрим случай, когда ящики не различаются. Имеем отдельную комбинаторную задачу, связанную с числом разбиений.

Пример. Сколькими способами можно разложить m различных шаров по n ящикам, которые не различаются, так, чтобы ни один из ящиков не оказался пустым? По-другому, сколькими способами можно представить m-элементное множество в виде объединения n непустых непересекающихся подмножеств?

Решение. Так как ящики не различаются, то любая перестановка n ящиков ничего не изменит, поэтому число $D(m,n)$ разложений m различных шаров по n различным ящикам нужно раз делить на число перестановок $n!$:

$$S(m,n)=\frac{D(m,n)}{n!}.$$

В итоге получили формулу для числа способов разложить m шаров по n неразличимым ящикам, или число способов представления m-элементного множества в виде объединения n непересекающихся непустых подмножеств. Числа $S(m,n)$ называются *числами Стирлинга второго рода*.

Числа Каталана. Во многих комбинаторных задачах решением является последовательность чисел Каталана:

$$\{c_n\}=\{c_0,\ c_1,\ ...,\ c_n\}=\{1,\ 1,\ 2,\ 5,\ 14,\ 42,\ ...\}.$$

Пусть имеются $n+1$ переменная $x_0,\ x_1,\ ...,\ x_n$. Чтобы вычислить их произведение, необходимо провести n умножений. Пусть c_n обозначает число способов расставить скобки в произведении $x_0\cdot x_1\cdot ...\cdot x_n$. При этом полностью определен порядок, с которым осуществляется процесс умножения. Например, при $n=2$ существует два способа: $x_0\cdot(x_1\cdot x_2)$ и $(x_0\cdot x_1)\cdot x_2$.

Одним из примеров использования чисел Каталана является разбиение многоугольника на треугольники непересекающимися диагоналями,

называемое *диагональной триангуляцией*. На рисунке 1.4 приведены четырехугольник и пятиугольник и все их различные диагональные триангуляции.

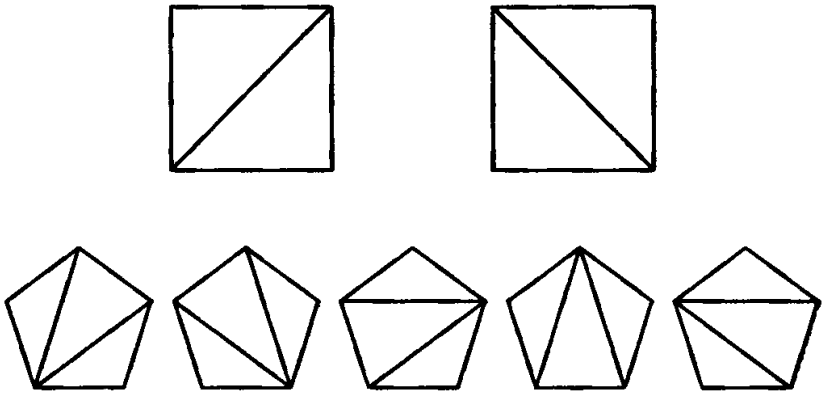

Рисунок 1.4. Диагональные триангуляции 4- и 5- угольника

Принцип Дирихле (принцип ящиков) заключается в следующем. Хотим распределить $n \cdot k + 1$ или более предметов по n ящикам. Тогда в каком-то ящике окажется не менее чем $k + 1$ предмет. Данное утверждение является весьма эффективным методом решения задач. Выбор предметов и ящиков не всегда очевиден. Далеко не всегда по виду задачи можно определить, что нужно воспользоваться принципом Дирихле. А главное, этот метод даёт неконструктивное доказательство, а попытка дать конструктивное доказательство, т. е. доказательство путём явного построения или указания требуемого объекта будет затруднено.

Пример. Класс, в котором 25 человек. Из любых случайно выбранных 3 учеников двое будут друзьями. Необходимо доказать, что в классе находится школьник, у которого больше 11 приятелей.

Решение. Для начала возьмем двух школьников, которые не дружат друг с другом (поскольку если бы все они дружили между собой, то в каждой тройке было бы три друга и каждый ученик дружил бы с 24 другими). Оставшиеся 23 одноклассника будут дружить с одним из нашей двойки, поскольку в противном случае нашлась бы тройка, где нет друзей (а это противоречит изначальному условию задачи). Получается, что один из двух школьников будет дружить как минимум с 12 учениками.

Правило крайнего заключается в том, чтобы рассмотреть тот элемент, для которого некая величина имеет наибольшее (или наименьшее) значение.

Пример. Семеро ребят вместе собрали 100 грибов, причем количество грибов у любых двоих из грибников различно. Докажите, что найдутся трое ребят, собравших вместе не менее 50 грибов.

Решение. Рассмотрим трех ребят, занявших в соревновании «кто больше соберет грибов», первые три места. Пусть они набрали соответственно x, y и z, грибов, причем $x > y > z$. Тогда, если $z \le 15$, то остальные четверо ребят набрали вместе не более, чем $14+13+12+11=50$, а три первых набрали не менее 50 грибов. Если же $z \ge 16$, то $x + y + ... + z \ge 16+17+18=51$.

Разложение неотрицательного числа. Найдем, сколькими способами можно представить число n в виде суммы неотрицательных слагаемых.

Два представления

$$n = a_1 + ... + a_k = b_1 + ... + b_k$$

будем считать различными, если $a_i \ne b_i$ хотя бы для одного индекса i, $1 \le i \le k$. Такое представление числа n будем называть его *разложением*.

Число различных разложений числа n в сумму k целых неотрицательных слагаемых равно C_{n+k-1}^{k-1}.

Доказательство. Представим себе число n в виде набора из n одинаковых шариков, лежащих на прямой. Каждому разложению числа n в сумму k слагаемых сопоставим расстановку $k-1$ палочки между шариками. Элемент a_i разложения равен числу шариков между палочками с номерами $i-1$ и i. Вместе палочки и шарики составляют $n+k-1$ предмет. При этом назначить $k-1$ предмет палочками можно ровно C_{n+k-1}^{k-1} различными способами.

Существует полезная геометрическая интерпретация разбиений. Каждое разбиение удобно представлять в виде диаграмма Ферре или

диаграммы Юнга. Изображенные на рисунке 1.5 диаграммы соответствуют разбиению 5 + 4 + 4 + 2+1 числа 16.

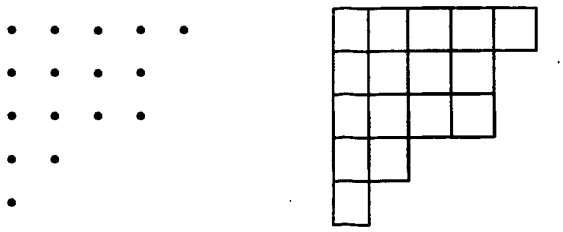

Рисунок 1.5. Диаграммы а) Ферре и б) Юнга

Каждая строчка диаграммы содержит столько элементов, каково соответствующее слагаемое разбиения.

Используя диаграммы Ферре или Юнга, можно доказывать различные свойства разбиений. Например, на диаграммах Юнга действует естественная инволюция — отражение относительно диагонали. Некоторые диаграммы при таком отражении переходят в себя. Такие диаграммы (и соответствующие им разбиения) будем называть *симметричными*.

Число симметричных разбиений числа n равно числу его разбиений на различные нечетные слагаемые.

Задачи для самостоятельной работы

1. Сколькими способами из 28 костей домино можно выбрать две кости так, чтобы их можно было приложить друг к другу (чтобы какое-то число очков встречалось на обеих костях)?

2. Группу из 20 студентов нужно разделить на 3 бригады, причем в первую бригаду должны входить 3 человека, во вторую – 5 и в третью – 12. Сколькими способами это можно сделать?

3. В Министерстве работают 67 человек. Из них 47 знают английский язык, 35 –французский язык и 23 – оба языка. Сколько человек в Министерстве не знают ни английского, ни немецкого языка?

4. Предприятие может предоставить работу по одной специальности 4 женщинами, по другой - 6 мужчинам, по третьей - 3 работникам независимо

от пола. Сколькими способами можно заполнить вакантные места, если имеются 14 претендентов: 6 женщин и 8 мужчин?

5. Сколько ожерелий можно составить из пяти белых и двух черных бусин?

6. Сколько различных дробей можно составить из чисел 3, 5, 7, 11, 13, 17 так, чтобы в каждую дробь входили 2 различных числа? Сколько среди них будет правильных дробей?

7. Сколько существует натуральных чисел, меньших 1000 которые не делятся ни на 5 ни на 7?

8. Сколько существует пар целых чисел x, y, заключенных между 1 и 1000, что $x^2 + y^2$ делится на 7?

9. Даны шесть цифр: 0, 1, 2, 3, 4, 5. Найдите количество всех четырехзначных четных чисел, которые можно написать этими цифрами (одна и та же цифра в числе может повторяться).

10. Докажите, что:

а) $C_n^0 + C_n^1 + ... + C_n^n = 2^n$;

б) $C_n^0 + C_n^2 + C_n^4 + C_n^6 + ... = C_n^1 + C_n^3 + C_n^5 + C_n^7 + ... = 2^{n-1}$;

в) $C_{2n}^n = (C_n^0)^2 + (C_n^1)^2 + ... + (C_n^n)^2$.

11. Докажите, что числа $(a+1)^{a^n} - 1$ и $(a-1)^{a^n} + 1$ делятся на a^{n+1} и не делятся на a^{n+2}.

12. Пусть $p_1 = 2$, $p_2 = 3$, … – последовательные простые числа. Докажите, что $p_1 \cdot ... \cdot p_k \le 4^{p_k}$.

13. Сколько существует целых чисел от 1 до 16 500, которые

а) не делятся на 5;

б) не делятся ни на 5 ни на 3;

в) не делятся ни на 5 ни на 3, ни на 11?

14. Староста класса дал следующие данные об учениках: «В классе учатся 45 школьников, в том числе 25 мальчиков. 30 школьников учатся на хорошо

и отлично, в том числе 16 мальчиков. Спортом занимаются 28 учеников, в том числе 18 мальчиков и 17 школьников, которые учатся на хорошо и отлично. 15 мальчиков учатся на хорошо и отлично, и в то же время занимаются спортом.» Через несколько дней его вызвал к себе классный руководитель и сообщил, что в сведениях ошибка. Найдите ее.

15. В классе 30 учеников. Сколькими способами они могут пересесть так, чтобы ни один не сел на свое место?

16. Сколькими способами можно расселить 15 гостей в четырех комнатах, если требуется чтобы ни одна из комнат не осталась пуста?

17. В саду у Ани и Вити росло 2006 розовых кустов. Витя полил половину всех кустов, и Аня полила половину всех кустов. При этом оказалось, что ровно три куста, самые красивые, были политы и Аней, и Витей. Сколько розовых кустов остались не политыми?

18. В кружок робототехники берут только те кто знает математику, физику или программирование. Известно, что 8 членов кружка знаю физику, 7 – математику, 11 – программирование. При этом известно, что не менее двоих знают одновременно физику и математику, не менее троих – математику и программирование и не менее четырёх – физику и программирование. Какое наибольшее количество участник кружка может быть при этих условиях?

19. На столе рубашкой вверх была разложена колода из 36 игральных карт. Лёша перевернул 30 карт, затем Макс перевернул 19 карт, а после этого Боря – 21 карту. В результате вся колода оказалась рубашкой вниз. Сколько карт было перевёрнуто трижды?

20. Уходя на работу, мама поручила Мише, Пете и Васе: а) подмести пол в прихожей; б) помыть посуду; в) купить хлеба; г) заплатить за электричество; д) вынести мусор; е) пропылесосить ковёр в гостиной. Сколькими различными способами они могут распределить задания так, чтобы каждое задание делал кто-то один из ребят и при условии, чтобы каждый что-нибудь делал?

21. Сколько последовательностей $\{a_1,\ a_2,\ ...,\ a_{2n}\}$, состоящих из +1 и –1, обладает свойством, что $a_1 + a_2 + ... + a_{2n} = 0$, а все их частичные суммы a_1, $a_1 + a_2$, …, $a_1 + a_2 + ... + a_{2n}$ неотрицательны?

22. Кассир, у которого в начальный момент времени денег нет, продаёт билеты по 50 рублей. Очередь состоит из $2n$ человек, у половины из которых есть только одна купюра 100 рублей, а у другой половины – 50 рублей. Докажите, что количество различных порядков очереди, для которых кассир сможет всем дать сдачу, равно c_n.

23. Докажите, что числа Каталана удовлетворяют рекуррентному соотношению: $c_n = c_0 \cdot c_{n-1} + c_1 \cdot c_{n-2} + ... + c_{n-1} \cdot c_0$.

24. В мешке 70 шаров, отличающихся только цветом: 20 красных, 20 синих, 20 желтых, остальные – черные и белые. Какое наименьшее число шаров надо вынуть из мешка, не видя их, чтобы среди них было не менее 10-ти шаров одного цвета?

25. Сто человек сидят за круглым столом, причем более половины из них – мужчины. Докажите, что какие-то двое из мужчин сидят друг напротив друга.

26. На складе имеется по 200 сапог 41, 42 и 43 размеров, причем среди этих 600 сапог 300 левых и 300 правых. Докажите, что из них можно составить не менее 100 годных пар обуви.

27. Несколько футбольных команд проводят турнир в один круг. Докажите, что в любой момент турнира найдутся две команды, сыгравшие к этому моменту одинаковое число матчей.

28. Есть 13 гирь, каждая из которых весит целое число граммов. Известно, что любые 12 из них можно так разложить на 2 чашки весов, по 6 гирь на каждой, что наступит равновесие. Докажите, что все гири одного веса.

29. Из чисел 1, 2, 3, 4, 5, 6, 7, …, 199, 200 произвольно выбрали 101 число. Докажите, что среди выбранных чисел найдутся два, одно из которых делится на другое.

30.Сколькими способами можно разменять рубль на монеты в 1,5, 10 и 50 копеек?

31.Сколькими способами можно выбрать путь из начала координат O(0,0) в точку B(6,4), если каждый шаг равен единице, но его можно совершать только вправо или вверх? Сколько таких путей проходит через точку A(2,3)?

32. Сколькими способами можно распределить 6 яблок, 8 груш и 10 слив между тремя детьми? Сколькими способами это можно сделать так, чтобы каждый ребенок получил по меньшей мере одно яблоко, одну сливу и одну грушу?

33. Сколько цифр в первом миллионе содержат цифру 5?

34. Сколько пятизначных цифр содержит в своей записи ровно три различные цифры?

35. В саду есть цветы десяти наименований (розы, флоксы, ромашки и т. д.). а) Сколькими способами можно составить букет из пяти цветков (не принимая во внимание совместимость растений и художественные соображения)? б) Сколькими способами можно составить букет из пяти различных цветков? в) Сколькими способами можно составить букет из пяти цветков так, чтобы в букете непременно было хотя бы по одному цветку двух определенных наименований?

Тема 2. Теория делимости

Основные определения и понятия

Делимость целых чисел. Запись $a|b$ означает, что существует целое число c, такое что $b=a\cdot c$. При этом a называется кратным b, а b – делителем a. Рассмотрим несколько свойств делимости:

1. $a|a$ при $a\neq 0$.
2. Если $a|b$ и $b|a$, то $a=\pm b$.
3. Если $a|b$ и $b|c$, то $a|c$.
4. Если $a|b$ и $a|c$, то $a|(b+c)$.
5. Если $a|b$, то $a|k\cdot b$.

Признаки делимости. Существуют несколько признаков, позволяющих сделать вывод о делимости числа на другое число.

- $2|a \Leftrightarrow$ последняя цифра числа a четна.
- $3|a \Leftrightarrow$ сумма всех цифр числа a делится на 3.
- $4|a \Leftrightarrow$ число, составленное из последних двух цифр его десятичной записи, идущих в том же порядке, делится на 4.
- $5|a \Leftrightarrow$ число a оканчивается на 0 или 5.
- $9|a \Leftrightarrow$ сумма всех цифр числа a делится на 9.
- $11|a \Leftrightarrow$ разность суммы цифр, стоящих на нечетных местах, считая справа в десятичной записи числа a, и суммы цифр, стоящих на четных местах, делится на 11.

Пример. Число, сумма цифр которого равна 2010, не может быть квадратом целого числа, так как это число делится на 3, но не делится на 9.

Простые и составные числа. Натуральное число, которое делится только на 1 и само себя, называется *простым*. Простых чисел бесконечно много. Числа, отличные от 1 и не являющиеся простыми, называются *составными*. 1 не является ни простым, ни составным числом, и стоит отдельно в ряду натуральных чисел. Если натуральное число n составное, то

его можно представить в виде произведения двух чисел $n = n_1 \cdot n_2$. Причем, наименьший из его делителей не превосходят $\sqrt{n}$ и является простым числом.

Основная теорема арифметики. Любое целое число ($n > 1$) может быть представлено в виде произведения простых чисел и при том единственным образом с точностью до порядка сомножителей.

Доказательство.

1) пусть $n > 1$ – простое число. Тогда запишем $n = p_1$, и теорема верна.

2) Пусть $n > 1$ – составное. Обозначим через p_1 положительный наименьший собственный делитель числа n, тогда $n = p_1 \cdot n_1$. А с числом n_1 проведем процедуру описанную в пунктах 1) и 2). Этот процесс конечен. Таким образом получим разложение $n = p_1 \cdot p_2 \cdot ... \cdot p_k$ и доказательство завершено.

Разложение $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, где $p_i \neq p_j$, называется *каноническим разложением* числа n.

Пример. Найдите наименьшее натуральное число, которое при делении на 5 дает остаток 4, при делении на 6 – остаток 5, при делении на 8 – остаток 7.

Решение. Пусть искомое число n, тогда $n+1$ делится нацело на 5, 6 и 7. $5 \cdot 6 \cdot 7 = 210$, поэтому $n = 209$.

НОД и НОК. Пусть даны два натуральных числа a и b. Число d называется *наибольшим общим делителем* чисел a и b, если $d \mid a$ и $d \mid b$ и каждый другой общий делитель a и b делит d. Обозначение: (a,b).

Если $(a,b) = 1$, то числа (a,b) будут взаимно простыми.

Справедливы следующие свойства:

1. Если $a \mid b \cdot c$ и $(a,b) = 1$, то $a \mid c$.
2. Если $p \mid b \cdot c$, где p – простое число, то $p \mid b$ или $p \mid c$.
3. $(a, k \cdot a) = a$, $(1, a) = 1$.

4. Если $b|a$, то совокупность общих делителей a и b совпадает с делителями b, $(a,b)=b$.

5. Если $a=b\cdot q+r$, то совокупность общих делителей a и b совпадает с совокупностью общих делителей b и c, $(a,b)=(b,c)$.

6. $(a\cdot m,b\cdot m)=(a,b)\cdot m$.

7. $\left(\frac{a}{m},\frac{b}{m}\right)=\frac{(a,b)}{m}$.

8. Если $(a,b)=1$, то $(ac,b)=(c,b)$.

Пусть даны два натуральных числа a и b. Число m называется *наименьшим общим кратным* чисел a и b, если $a|m$ и $b|m$ и каждое другое общее кратное a и b делится на m. Обозначение: $[a,b]$.

Справедливы следующие свойства:

1. Если $(a,b)=1$, то $[a,b]=a\cdot b$.

2. $[a,b]=\frac{a\cdot b}{(a,b)}$.

Алгоритм Евклида. Любое целое число a можно поделить с остатком на любое ненулевое число b. Таким образом, любое целое число a можно представить в виде $a=b\cdot q+r$, где $0\le r<|b|$, и это представление единственно. Число q называется неполным частным, число r – остатком от деления.

Сумма (произведение) чисел a и b дает тот же остаток при делении на число d, что и сумма (произведение) остатков чисел a и b при делении на число d.

Для целых чисел a и b можно проделать следующие действия:

$$a=b\cdot q_1+r_1,\ 0\le r_1<b;$$

$$b=r_1\cdot q_2+r_2,\ 0\le r_2<r_1;$$

$$r_1=r_2\cdot q_3+r_3,\ 0\le r_3<r_2;$$

…

$$r_{n-2} = r_{n-1} \cdot q_n + r_n,\ 0 \le r_n < r_{n-1};$$

$$r_{n-1} = r_n \cdot q_{n+1},\ r_{n+1} = 0.$$

В силу единственности представления числа в виде, содержащем неполное частное и остаток, такой алгоритм, который носит название *алгоритм Евклида*, будет единственен.

Последний не равный нулю остаток r_n в алгоритме Евклида для чисел a и b будет равен (a,b).

Пример. Найдем $(525,231)$ с помощью алгоритма Евклида. Имеем: $525 = 231 \cdot 2 + 63$, $231 = 63 \cdot 3 + 42$, $63 = 42 \cdot 1 + 21$, $42 = 21 \cdot 2$. Следовательно, $(525,231) = 21$.

Непрерывные и подходящие дроби и их связь с алгоритмом Евклида. Пусть α – действительное число. Обозначим через q_1 наибольшее целое, не превосходящее α. Тогда

$$\alpha = q_1 + \frac{1}{\alpha_2},\ \alpha_2 > 1.$$

Аналогично $\alpha_2 = q_2 + \frac{1}{\alpha_3}$, $\alpha_3 > 1$ и т.д.

Получаем следующее *разложение α в непрерывную дробь*:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}}.$$

Если α иррациональное, то в ряду α, α_2, ... не может встретиться целых чисел и указанный процесс можно неограниченно продолжить.

Если α рациональное, то в ряду α, α_2, ... обязательно встретиться целое число, и указанный процесс будет конечен.

Сам процесс разложения числа в непрерывную дробь основан на алгоритме Евклида. Действительно,

$$a = b \cdot q_1 + r_1,\ 0 \le r_1 < b;$$

$$b = r_1 \cdot q_2 + r_2,\ 0 \le r_2 < r_1;$$

$$r_1 = r_2 \cdot q_3 + r_3,\ 0 \le r_3 < r_2;$$

$$\dots$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n,\ 0 \le r_n < r_{n-1};$$

$$r_{n-1} = r_n \cdot q_{n+1},\ r_{n+1} = 0.$$

Откуда $\dfrac{a}{b} = q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3 + \ddots + \dfrac{1}{q_n}}}$. Числа $q_1,\ q_2,\ \ldots.$ называются *неполными частными*, а дроби $\delta_1 = q_1,\ \delta_2 = q_1 + \dfrac{1}{q_2},\ \delta_3 = q_1 + \dfrac{1}{q_2 + \dfrac{1}{q_3}},$ и т.д. – *подходящими дробями*.

Пример. Разложим число $\dfrac{105}{38}$ в непрерывную дробь. Имеем:

$$105 = 38 \cdot 2 + 29,$$

$$38 = 29 \cdot 1 + 9,$$

$$29 = 9 \cdot 3 + 2,$$

$$9 = 2 \cdot 4 + 1,$$

$$2 = 1 \cdot 2 + 0.$$

Тогда $q_1 = 2,\ q_2 = 1,\ q_3 = 3,\ q_4 = 4,\ q_5 = 2$.

$$\frac{105}{38} = 2 + \frac{1}{1 + \dfrac{1}{3 + \dfrac{1}{4 + \dfrac{1}{2}}}} = [2;1,3,4,2].$$

Легко вывести закон образования подходящих дробей, числители и знаменатели которых можно последовательно вычислять по формулам:

$$\delta_s = \frac{P_s}{Q_s} = \frac{q_s \cdot P_{s-1} + P_{s-2}}{q_s \cdot Q_{s-1} + Q_{s-2}}.$$

Такие вычисления удобно делать с помощью таблицы:

q_s		q_1	q_2	…			q_s
P_s	1	q_1	P_2	…	P_{s-2}	P_{s-1}	P_s
Q_s	0	1	Q_2	…	Q_{s-2}	Q_{s-1}	Q_s

Пример. Найдем шестую подходящую дробь для числа $\frac{5391}{3976}$. Значения q_s находим по алгоритму Евклида:

$$5391 = 3976 \cdot 1 + 1415,$$
$$3976 = 1415 \cdot 2 + 1146,$$
$$1415 = 1146 \cdot 1 + 269$$
$$1146 = 269 \cdot 4 + 70,$$
$$269 = 70 \cdot 3 + 59,$$
$$70 = 59 \cdot 1 + 11.$$

Тогда $q_1 = 1,\ q_2 = 2,\ q_3 = 1,\ q_4 = 4,\ q_5 = 3,\ q_6 = 1$. Составляем таблицу:

q_s		1	2	1	4	3	1
P_s	1	1	3	4	19	61	80
Q_s	0	1	2	3	14	45	59

Получаем, что $\delta_6 = \frac{80}{59}$.

Не рациональные корни уравнения $ax^2 + bx + c = 0$ с целыми коэффициентами называются *квадратичными иррациональностями*. Любая квадратичная иррациональность имеет вид $u \pm v\sqrt{N}$, где $u,\ v$ рациональные и N не является полным квадратом.

Квадратичные иррациональности только они могут быть представлены в виде бесконечной периодической обыкновенной непрерывной дроби (теорема Лагранжа).

Пример. Вычислим квадратичную иррациональность, представимую цепной дробью $[4;\overline{2,6}]$.

Можем записать следующее разложение для $x = [0;\overline{2,6}]$:

$$x = \frac{1}{2 + \dfrac{1}{6 + x}}.$$

Упрощая выражение, получаем, что x является корнем уравнения

$$x^2 + 6x - 3 = 0.$$

Тогда $x = -3 + 2\sqrt{3},\ 4 + x = 1 + 2\sqrt{3}$. Следовательно, $[4;\overline{2,6}] = 1 + 2\sqrt{3}$.

Важнейшие функции в теории чисел. Важную роль в теории чисел играет функция $[x]$, определенная для всех действительных x и равная наибольшему целому, не превосходящему x. Она называется *целой частью* числа x.

Примеры. $[7] = 7$, $[3{,}14] = 3$, $[-8{,}76] = -9$.

Наряду с целой частью числа рассматривается функция $\{x\} = x - [x]$, называемая *дробной частью* числа x.

Показатель, с которым данное простое число p входит в произведение $n!$, равен $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$.

Пример. Показатель числа 3 в 40! равен: $\left[\frac{40}{3}\right] + \left[\frac{40}{9}\right] + \left[\frac{40}{27}\right] = 13 + 4 + 1 = 18$.

Функция $\theta(x)$ называется *мультипликативной*, если выполнены следующие условия:

1. Функция $\theta(x)$ определена для всех натуральных x и $\theta(a) \neq 0$ хотя бы при одном значении a.

2. Для любых натуральных чисел a_1 и a_2, таких что $(a_1, a_2) = 1$ выполняется $\theta(a_1 \cdot a_2) = \theta(a_1) \cdot \theta(a_2)$.

Примером мультипликативной функции является функция $\theta(x) = x^s$, где s – любое (действительное или комплексное) число.

Свойства мультипликативных функций:

1. $\theta(1) = 1$.

2. Если $\theta_1(x)$ и $\theta_2(x)$ – мультипликативные функции, то $\theta(x)=\theta_1(x)\cdot\theta_2(x)$ – также мультипликативная функция.

3. $\theta(p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k})=\theta(p_1^{\alpha_1})\cdot\ldots\cdot\theta(p_k^{\alpha_k})$, где $p_1,\ldots,p_k$ – простые числа.

4. Пусть $\theta(x)$ – мультипликативная функция и $x=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$ – каноническое разложение числа x. Обозначим через $\sum_{d|x}$ сумму всех делителей d числа x. Тогда

$$\sum_{d|x}\theta(d)=\left(1+\theta(p_1)+\theta(p_1^{\,2})+\ldots+\theta(p_1^{\,\alpha_1})\right)\cdot\ldots\cdot\left(1+\theta(p_k)+\theta(p_k^{\,2})+\ldots+\theta(p_k^{\,\alpha_k})\right).$$

Следствие. При $\theta(x)=x^s$ свойство 4. Имеет вид

$$\sum_{d|x}d^s=\left(1+p_1^{\,s}+p_1^{\,2^s}+\ldots+p_1^{\,\alpha_1 s}\right)\cdot\ldots\cdot\left(1+p_k^{\,s}+p_k^{\,2^s}+\ldots+p_k^{\,\alpha_k s}\right).$$

При $s=1$ получаем формулу для суммы $S(x)$ всех делителей числа x:

$$S(x)=\frac{p_1^{\,\alpha_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_k^{\,\alpha_k+1}-1}{p_k-1}.$$

При $s=0$ получаем формулу для числа $\tau(x)$ всех делителей числа x:

$$\tau(x)=(1+\alpha_1)\cdot\ldots\cdot(1+\alpha_k).$$

Пример. Число 3072 имеет 22 делителя, а их сумма равна 8188. Так как $3072=2^{10}\cdot 3$.

Примеры мультипликативных функций. Кроме числа делителей числа x – $\tau(x)$ и суммы всех делителей числа x – $S(x)$ существуют и другие мультипликативные функции, играющие важную роль в математике. *Функция Мебиуса* $\mu(x)$ является мультипликативной функцией и определяется следующим образом: если x делится на квадрат некоторого числа, отличного от 1, то $\mu(x)=0$; $\mu(x)=(-1)^k$, если x не делится на квадрат некоторого числа, отличного от 1. При этом k равно числу простых делителей числа x.

Свойства функции Мебиуса:

1. Пусть $\theta(x)$ – произвольная мультипликативная функция, $x = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$. Тогда

$$\sum_{d|x} \mu(d) \cdot \theta(d) = (1 - \theta(p_1)) \cdot ... \cdot (1 - \theta(p_k)).$$

2. Если $\theta(x) = 1$, то $\sum_{d|x} \mu(d) = \begin{cases} 0, & x > 0, \\ 1, & x = 1. \end{cases}$

3. Если $\theta(x) = \frac{1}{d}$, то $\sum_{d|x} \frac{\mu(d)}{d} = \begin{cases} \left(1 - \frac{1}{p_1}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right), & x > 0, \\ 1, & x = 1. \end{cases}$

Функция Эйлера и ее свойства. Функция Эйлера $\varphi(x)$ является мультипликативной функцией и определяется как число чисел ряда $0, 1, ..., x-1$, взаимно простых с x.

Пусть $x = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$, тогда:

1. $\varphi(x) = x \cdot \left(1 - \frac{1}{p_1}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right)$ (формула Эйлера);

2. $\varphi(x) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot ... \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$, в частности $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\varphi(p) = p - 1$.

3. $\varphi(x) = x \cdot \sum_{d|x} \frac{\mu(d)}{d}$.

4. $\sum_{d|x} \varphi(d) = x$.

Примеры. $\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 16$,

$\varphi(405) = \varphi(81) \cdot \varphi(5) = \left(3^4 - 3^3\right) \cdot 4 = 216$, $\varphi(30) = (2-1) \cdot (3-1) \cdot (5-1) = 8$.

Задачи для самостоятельной работы

1. В произведении семи натуральных чисел каждый сомножитель уменьшили на 3. Могло ли произведение при этом увеличиться ровно в 13 раз?

2. Докажите, что произведение любых пяти последовательных чисел делится на 30.

3. Можно ли в равенстве $1*2*3*...*10=0$ вместо звездочек поставить знаки плюс и минус так, чтобы получилось верное равенство?

4. Пусть m и n – целые числа. Докажите, что $mn(m+n)$ – четное число.

5. В десятичной записи целого числа есть 300 единиц, а остальные цифры – нули. Может ли это число быть полным квадратом?

6. Имеются семь жетонов с цифрами 1, 2, 3, 4, 5, 6, 7. Докажите, что ни одно семизначное число, составленное посредством этих жетонов, не делится на другое.

7. Каждый из людей, когда-либо живущих на земле, сделал определенное число рукопожатий. Докажите, что число людей, сделавших нечетное число рукопожатий – четно.

8. На доске написано 10 плюсов и 15 минусов. Разрешается стереть любые два знака и написать вместо них плюс, если они одинаковы, и минус в противном случае. Какой знак останется на доске после выполнения 24 таких операций?

9. Все косточки домино выложены в цепь. На одном конце оказалось 5 очков. Сколько очков на другом конце?

10.На столе стоят 7 стаканов— все вверх дном. Разрешается за один ход перевернуть любые 4 стакана. Можно ли за несколько ходов добиться того, чтобы все стаканы стояли правильно?

11. Ученик задумал простое трехзначное число, все цифры которого различны. На какую цифру оно может оканчиваться, если его последняя цифра равна сумме первых двух?

12. Существует ли число, которое является степенью 2 такое, что перестановкой его цифр можно получить другую степень 2?

13. Найдите наименьшее число, запись которого состоит лишь из нулей и единиц, делящееся без остатка на 225.

14. Найдите все такие трехзначные числа, которые в 12 раз больше суммы своих цифр.

15. При каких x и y число $xxyy$ является квадратом натурального числа?

16.Натуральные числа m и n таковы, что $m>n$, m не делится на n n и имеет от деления на n тот же остаток, что и $m+n$ от деления на $m-n$. Найдите отношение $\frac{m}{n}$.

17. Докажите, что если p – простое число и $1\le k\le p-1$, то C_p^k делится на p.

18. Докажите, что среди любых десяти последовательных натуральных чисел найдется число, взаимно простое с остальными.

19. Найдите все простые числа, которые отличаются на 17.

20. Докажите, что остаток от деления простого числа на 30 – простое число.

21. Докажите, что если число $n!+1$ делится на $n+1$, то $n+1$ – простое число.

22.Докажите, что 3, 5 и 7 являются единственной тройкой простых чисел-близнецов (чисел, отличающихся друг от друга на 2).

23. Пусть $p>3$ – простое число. Докажите, что p^2-1 делится на 24.

24. Докажите, что дробь $\frac{21n+4}{14n+3}$ несократима ни при каких натуральных n.

25. Пусть $b\cdot c$ делится на a и $(a,b)=1$. Докажите, что c делится на a.

26. В прямоугольнике с целыми сторонами m и n, нарисованном на клетчатой бумаге, проведена диагональ. Через какое число узлов она проходит? На сколько частей эта диагональ делится линиями сетки?

27. С 1 сентября четыре школьника начали посещать кинотеатр. Первый бывал в нем каждый четвертый день, второй – каждый пятый, третий –

каждый шестой и четвертый – каждый девятый. Когда второй раз все школьники встретятся в кинотеатре?

28. Найдите $(\underset{m}{1...1},\underset{n}{1...1})$.

29. Какое наибольшее значение может принимать наибольший общий делитель чисел a и b, если известно, что $a \cdot b = 600$?

30. Докажите, что если $(a,b)=1$, то $(2z+b, a(a+b))=1$.

31. Докажите, что если $(a,b)=1$, то наибольший общий делитель чисел $a+b$ и a^2+b^2 равен 1 или 2.

32. Докажите, что $\dfrac{[a,a+b]}{[a,b]} = \dfrac{a+b}{b}$.

33. Докажите, что число $\dfrac{1}{k} + \dfrac{1}{k+1} + ... + \dfrac{1}{k+n}$, где k и n – натуральные числа, не может быть целым.

34. Сколькими нулями оканчивается произведение всех целых чисел от 1 до 100 включительно?

35. Докажите, что $n!$ не делится на 2^n.

36. Найдите наибольшую степень двойки, на которую делится число $(n+1)\cdot(n+2)\cdot...\cdot 2n$.

37. Найдите все натуральные числа n, для которых $2^n - 1$ делится на 7.

38. Найдите наименьшее натуральное число, которое при делении на 5 дает остаток 4, при делении на 6 – остаток 5, при делении на 8 – остаток 7.

39. Разложите в цепные дроби числа $\dfrac{147}{13}$ и $\dfrac{129}{111}$.

40. Пусть $\dfrac{P_n}{Q_n} = [\underbrace{1;1,...,1}_{n}]$. Чему равны P_n и Q_n?

41. Докажите следующие свойства подходящих дробей:

а) $P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k a_k \ (k \geq 2)$;

б) $\dfrac{P_k}{Q_k} - \dfrac{P_{k-1}}{Q_{k-1}} = \dfrac{(-1)^{k+1}}{Q_k Q_{k-1}} \ (k \geq 1)$;

в) $Q_1 < Q_2 < ... < Q_n$.

42. Вычислите цепные дроби: $[5;\overline{1,2,1,10}]$, $[5;\overline{1,4,1,10}]$, $[2;\overline{1,1,3}]$.

43. Разложите в цепные дроби: $\sqrt{2}$, $\sqrt{3}$, $\frac{1}{2}+\sqrt{7}$.

44. Найдите наименьшее натуральное n, для которого существует такое m, что $\sqrt{2} < \frac{m}{n} < \frac{297}{210}$.

45. Докажите, что если квадратное уравнение с целыми коэффициентами имеет корень $[\overline{a;b}]$, то вторым корнем будет число $-\frac{1}{[\overline{a;b}]}$.

46. Найдите натуральное число n, зная, что оно имеет два простых делителя и удовлетворяет условиям $\tau(n)=6$, $\sigma(n)=28$.

47. Некоторое натуральное число n имеет два простых делителя. Его квадрат имеет а) 15; б) 81 делителей. Сколько делителей имеет куб этого числа?

48. Пусть $(m,n)>1$. Что больше $\tau(m\cdot n)$ или $\tau(m)\cdot\tau(n)$? Что больше $\sigma(m\cdot n)$ или $\sigma(m)\cdot\sigma(n)$?

49. Пусть a – действительное положительное число, d – натуральное. Докажите, что количество натуральных чисел, не превосходящих a и делящихся на d, равно $\left[\frac{a}{d}\right]$.

50. Докажите, что для действительного положительного a и натурального d всегда выполнено равенство $\left[\frac{a}{d}\right]=\left[\frac{[a]}{d}\right]$.

Тема 3. Теория сравнений

Основные определения и понятия

Остатки от деления. Будем рассматривать целые числа в связи с остатками от деления их на данное целое положительное число m, которое будем называть *модулем*. Каждому целому числу отвечает определенный остаток от деления его на m. Если двум целым числам a и b отвечает один и тот же остаток, то будем говорить, что они *сравнимы по модулю* m. Обозначение: $a \equiv b \pmod{m}$.

Сравнимость чисел a и b по модулю m равносильна равенству $a = b + m \cdot t$, где t – целое. Справедливо также утверждение, что m является делителем разности $a - b$.

Свойства сравнений:

1. Сравнения можно почленно складывать. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a + c \equiv b + d \pmod{m}$.

2. Два числа сравнимые с третьим, сравнимы между собой. Если $a \equiv b \pmod{m}$ и $c \equiv b \pmod{m}$, то $a \equiv c \pmod{m}$.

3. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть с противоположным знаком. Если $a \equiv b + c \pmod{m}$, то $a - b \equiv c \pmod{m}$.

4. К каждой части сравнения можно прибавлять (отнимать) любое число, кратное модулю. Если $a \equiv b \pmod{m}$, то $a \pm m \cdot k \equiv b \pmod{m}$.

5. Сравнения можно почленно перемножать. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $a \cdot c \equiv b \cdot d \pmod{m}$.

6. К обеим частям сравнения можно прибавлять (отнимать) одно и тоже число. Если $a \equiv b \pmod{m}$, то $a \pm c \equiv b \pm c \pmod{m}$.

7. Обе части сравнения можно умножать на одно и тоже число. Если $a \equiv b \pmod{m}$, то $a \cdot c \equiv b \cdot c \pmod{m}$.

8. Обе части сравнения можно сократить на одно и тоже число, взаимно простое с m. Если $a \equiv b \pmod{m}$ и $(c,m)=1$, то $\frac{a}{c} \equiv \frac{b}{c} \pmod{m}$.

9. Обе части сравнения можно возводить в одну и тоже степень. Если $a \equiv b \pmod{m}$, то $a^n \equiv b^n \pmod{m}$.

10. Обе части сравнения и модуль можно разделить на любой их общий делитель. Если $a \equiv b \pmod{m}$ и $d \mid a,\ d \mid b,\ d \mid m$, то $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

11. Если сравнение имеет место по нескольким модулям, то оно имеет место и по модулю, равному общему наименьшему кратному этих модулей. Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{[m_1,m_2]}$.

12. Если сравнение имеет место по модулю, то оно имеет место и по модулю, равному любому делителю исходного модуля. Если $a \equiv b \pmod{m_1}$ и $d \mid m$, то $a \equiv b \pmod{d}$.

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

Пример. Покажем, что квадраты натуральных чисел не дают остатка 2 при делении на 3. Действительно, если число n делится на 3, то n^2 также делится на 3, если остаток от деления n на 3 равен 1, то $n^2 = (3n_1+1)^2 \equiv 1 (\mathrm{mod}\, 3)$. Если $n \equiv 2 (\mathrm{mod}\, 3)$, то $n^2 = (3n_1+2)^2 \equiv 4 (\mathrm{mod}\, 3) \equiv 1 (\mathrm{mod}\, 3)$.

Пример. Докажем, что при любом натуральном n число $37^{n+2} + 16^{n+1} + 23^n$ делится на 7. Заметим, что $37 \equiv 2 \pmod{7}$, $16 \equiv 2 \pmod{7}$, $23 \equiv 2 \pmod{7}$, тогда первое сравнение возведем в степень $n+2$, второе – в степень $n+1$, третье – в степень n и сложим полученные сравнения:

$$37^{n+2} \equiv 2^{n+2} \pmod{7},\ 16^{n+1} \equiv 2^{n+1} \pmod{7},\ 23^n \equiv 2^n \pmod{7}.$$

Получаем, что $37^{n+2} + 16^{n+1} + 23^n \equiv 2^{n+2} + 2^{n+1} + 2^n \pmod{7} \equiv 2^n \cdot 7 \pmod{7}$. Тогда $37^{n+2} + 16^{n+1} + 23^n$ делится на 7 при любом натуральном n.

Отношение сравнимости по модулю m на множестве целых чисел является отношением эквивалентности и разбивает множество целых чисел на *классы эквивалентных элементов*. Любой представитель класса называется *вычетом* по модулю m. Множество всех вычетов по модулю m обозначаются $\mathbb{Z}_m = \{\bar{0},\ \bar{1},\ \bar{2},\ ...,\ \overline{m-1}\}$.

Существует точно m классов вычетов по модулю m. Никакие два класса вычетов по модулю m не пересекаются. Объединение всех классов вычетов по модулю m дает все множество целых чисел.

От каждого класса вычетов по модулю m выберем по одному представителю, тогда получаем *полную систему вычетов*. Таким образом, любые m чисел, попарно несравнимые по модулю m, образуют полную систему вычетов по этому модулю. Если $(a,m)=1$ и x пробегает полную систему вычетов по модулю m, то $ax+b$, где b – любое целое, тоже пробегает полную систему вычетов по модулю m.

Если в полной системе вычетов взяты все вычеты, взаимно простые с модулем, то система называется *приведенной*. Любые $\varphi(m)$ чисел, попарно не сравнимые по модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m. Если $(a,m)=1$ и x пробегает приведенную систему вычетов по модулю m, то ax также пробегает приведенную систему вычетов по модулю m.

Пример. Числа 0, 1, 2, 3, 4, 5 образуют полную систему вычетов по модулю 6. Приведенная система вычетов по модулю 6 содержит два класса вычетов $\bar{1},\ \bar{5}$, так как $\varphi(6)=\varphi(2\cdot 3)=\varphi(2)\cdot\varphi(3)=1\cdot 2=2$.

Теорема Эйлера. Пусть $m>1, (a,m)=1,\ \varphi(m)$ – функция Эйлера. Тогда:

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

Теорема Ферма. Пусть p – простое число, p не является делителем a. Тогда

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

Последнее сравнение можно переписать в виде: $a^p \equiv a \pmod{p}$.

Пример. Найдем остаток от деления 2^{1037} на 19. Для этого воспользуемся теоремой Эйлера. Так как $(2,19)=1$, то $2^{\varphi(19)} \equiv 1 \pmod{19}$. $2^{18} \equiv 1 \pmod{19}$. Найдем разложение 1037 по модулю 18. Имеем $1037 = 18 \cdot 57 + 11$. Тогда $2^{1037} \equiv 2^{18 \cdot 57 + 11} \pmod{19} \equiv (2^{18})^{57} \cdot 2^{11} \pmod{19} \equiv$ $\equiv 2^{11} \pmod{19} \equiv 2048 \pmod{19} \equiv 15 \pmod{19}$. Таким образом, остаток равен 15.

Сравнения первой степени. Сравнение вида

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

является *сравнением первой степени*. Класс вычетов

$$x \equiv x_0 \pmod{m}$$

является *решением сравнения*, если верно $ax_0 \equiv b \pmod{m}$.

Сравнение $ax \equiv b \pmod{m}$ имеет решение тогда и только тогда, когда $(a,m)=1$. Если сравнение разрешимо, то оно имеет единственное решение по модулю m.

Если $(a,m)=d$, то сравнение $ax \equiv b \pmod{m}$ не имеет смысла при $(b,d)=1$. При b кратном d, сравнение имеет d решений.

Существует несколько способов решения сравнений первой степени: по определению сравнения, с использованием линейного представления наибольшего общего делителя, через подходящие дроби для дроби $\frac{m}{a}$.

Если $ax \equiv b \pmod{m}$, то $x \equiv (-1)^{k-1} P_{k-1} b \pmod{m}$, где $\frac{m}{a} = \frac{P_k}{Q_k}$ – подходящая дробь.

Пример. Решим сравнение $111x \equiv 75 \pmod{321}$. Здесь $(111,\ 321)=3$ и 75 делится на 3. Поэтому сравнение имеет 3 решения. Разделим обе части сравнения на 3. Получим $37x \equiv 25 \pmod{107}$.

Используя алгоритм Евклида, найдем q_k:

$$107 = 37 \cdot 2 + 33,$$

$$37 = 33 \cdot 1 + 4,$$

$$33 = 4 \cdot 8 + 1$$

$$4 = 1 \cdot 4.$$

Тогда $q_1 = 2,\ q_2 = 1,\ q_3 = 8,\ q_4 = 4.$

Заполняем таблицу:

k		1	2	3	4
q_k		2	1	8	4
P_k	1	2	3	26	107

Получаем, что $k = 4$, $P_3 = 26$. Тогда $x \equiv -26 \cdot 25 \equiv 99 \pmod{107}$. Отсюда найдем решения исходного сравнения:

$$x \equiv 99;\ 99 + 107;\ 99 + 2 \cdot 107 \pmod{321}.$$

Решения сравнения будут иметь вид: $x \equiv 99;\ 206;\ 313 \pmod{321}$.

Системы сравнений. Рассмотрим систему, состоящую из двух сравнений первой степени:

$$\begin{cases} x \equiv a \pmod{m_1}, \\ x \equiv b \pmod{m_2}. \end{cases}$$

Можно доказать следующую теорему (*китайская теорема об остатках*). Для натуральных чисел m_1 и m_2 таких что $(m_1, m_2) = 1$ система сравнений разрешима и имеет единственное решение по модулю $m_1 \cdot m_2$. При этом решение системы является

$$x \equiv b \cdot m_1 \cdot u + a \cdot m_2 \cdot v \pmod{m_1 \cdot m_2},$$

где $m_1 \cdot u + m_2 \cdot v = 1$ – линейное представление $(m_1, m_2) = 1$.

Пример. Решим систему сравнений: $\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 8 \pmod{11}. \end{cases}$ Так как (5,11)=1, то можем использовать китайскую теорему об остатках. Для этого найдем линейное представление для (5,11)=1: $1 = 5 \cdot (-2) + 11 \cdot 1$. Тогда

$$x \equiv 8 \cdot 5 \cdot (-2) + 2 \cdot 11 \cdot 1 \pmod{5 \cdot 11},$$

$$x \equiv -58 \pmod{55},$$

$$x \equiv 52 \pmod{55}.$$

Системы сравнений можем решать и другим методом. Из определения сравнения можем найти решение первого сравнения, входящего в систему. А затем подставить это решение во второе уравнение системы и найти его решение, относительно новой переменной.

Пример. Решим систему сравнений: $\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 8 \pmod{11}. \end{cases}$ Из первого сравнения получаем, что $x = 2 + 5t$. Подставим это решение во второе сравнение системы: $2 + 5t \equiv 8 \pmod{11}$ и решим его.

$2 + 5t \equiv 8 \pmod{11}$, $5t \equiv 6 \pmod{11}$, $5t \equiv -5 \pmod{11}$, $t \equiv -1 \pmod{11}$, $t \equiv 10 \pmod{11}$. Тогда $t = 10 + 11k$. Следовательно, $x = 2 + 5(10 + 11k) = 52 + 55k$, т.е. $x \equiv 52 \pmod{55}$.

Диофантовы уравнения. Уравнение вида $f(x, y, ...) = 0$, в котором все переменные принимают целочисленные значения, называются *уравнениями в целых числах* или *диофантовыми уравнениями*. Набор целочисленных значений переменных, при подстановке которых в уравнение получается верное равенство, называется *решением диофантова уравнения*.

Уравнение вида

$$ax + by = c$$

называется *линейным диофантовым уравнением*.

Такое уравнение имеет решение в целых числах тогда и только тогда, когда $(a,b)|c$. В этом случае можно разделить оба коэффициента и свободный член уравнения на (a,b) и решать более простое уравнение.

Если пара чисел $(x_0;y_0)$ является решение такого уравнения, то все решения можно получить по формулам:

$$\begin{cases} x = x_0 + t \cdot \dfrac{b}{(a,b)}, \\ y = y_0 + t \cdot \dfrac{a}{(a,b)} \end{cases} \qquad (t \text{ – целое}).$$

Обычно указанную пару находят подбором, подставляя вместо одной переменной остатки от деления на коэффициент при другой.

Пример. Решим уравнение $31x-23y=11$. Если $y=13$, то $x=(11+23\cdot 13)\div 31=10$. Тогда общее решение можно имеет вид: $x=10+23t$, $y=13+31t$, где t – целое.

Можно находить решение линейного диофантова уравнения, использую линейное представление для наибольшего общего делителя. Если $(a,b)=1$, то существуют такие числа x_1, y_1, что выполнено условие:

$$ax_1+by_1=1.$$

Умножаем обе части уравнения на c. Тогда решение уравнения можно записать в виде $x=x_1\cdot c+b\cdot t$, $y=y_1\cdot c+a\cdot t$, где t – целое.

Пример. Решим уравнение $31x-23y=11$. Найдем x_1, y_1, такие, что $31x_1-23y_1=1$. Используем алгоритм Евклида:

$$31=23\cdot 1+8,$$
$$23=8\cdot 2+7,$$
$$8=7\cdot 1+1$$
$$7=1\cdot 7.$$

Тогда получим линейное представление: $1=8-7\cdot 1=8-(23-8\cdot 2)=8\cdot 3-23=(31-23\cdot 1)\cdot 3-23=31\cdot 3-23\cdot 4$. И, следовательно, $31\cdot 3\cdot 11-23\cdot 4\cdot 11=11$. Таким образом, $x_1=3,\ y_1=4$ и общее решение уравнения имеет вид: $x=33+23t$, $y=44+31t$, где t – целое.

Также мы можем использовать непрерывные дроби.

Предположим, что $\frac{P_k}{Q_k}$ – последняя подходящая дробь в представлении дроби $\frac{a}{b}$, где $(a,b)=1$. Тогда $a=P_k$ и $b=Q_k$. Используя рекуррентные соотношения:

$$P_k=q_k\cdot P_{k-1}+P_{k-2},$$

$$Q_k=q_k\cdot Q_{k-1}+Q_{k-2},$$

$$P_0=1,\ P_1=q_1,$$

$$Q_0=0,\ Q_1=1,$$

находим одно решение уравнения $ax+by=1$:

$$x_0=(-1)^{k-1}\cdot Q_{k-1},\ y_0=(-1)^{k-1}\cdot P_{k-1}.$$

Остальные решения имеют вид:

$$x=(-1)^{k-1}\cdot Q_{k-1}+b\cdot t,\ y=(-1)^{k-1}\cdot P_{k-1}+a\cdot t,$$

где t – целое.

Пример. Решим уравнение $31x-23y=11$. Так как $(31,23)=1$, то решение существует. Значения q_k находим по алгоритму Евклида:

$$31=23\cdot 1+8,$$

$$23=8\cdot 2+7,$$

$$8=7\cdot 1+1$$

$$7=1\cdot 7.$$

Тогда $q_1=1,\ q_2=2,\ q_3=1,\ q_4=7$.

Заполняем таблицу:

k		0	1	2	3
q_k		1	2	1	7
P_k	1	1	3	4	31
Q_k	0	1	2	3	23

Получаем, что $k=3$, $P_2=4$, $Q_2=3$. Тогда $x=(-1)^2\cdot 3\cdot 11+23\cdot t=33+23t$, $y=(-1)^2\cdot 4\cdot 11+31\cdot t=44+31t$, где t – целое.

Для диофантовых уравнений более высоких степеней не существует единых и действенных алгоритмов решения. Более того, существуют различные классы уравнений, которые не имеют решений.

Одним из способов решения диофантовых уравнений степени ≥ 2 является метод перебора корней. Проводятся преобразования уравнения, чаще всего связанные с разложением на множители. В итоге возникают ограничения на переменные, и остается выполнить перебор тех пар решений, которые удовлетворяют этим ограничениям.

Пример. Решить уравнение $xy+2x+3y=7$ в целых числах.

Решение. Представим левую часть уравнения в виде $xy+2x+3y=(x+3)(y+2)$. Тогда $(x+3)(y+2)=13$. Число 13 можно разложить в произведение целых чисел четырьмя различными способами: $13=13\cdot 1=1\cdot 13=(-13)\cdot(-1)=(-1)\cdot(-13)$. Получаем следующие системы уравнений:

$$\begin{cases} x+3=1, \\ y+2=13, \end{cases} \quad \begin{cases} x+3=13, \\ y+2=1, \end{cases} \quad \begin{cases} x+3=-1, \\ y+2=-13, \end{cases} \quad \begin{cases} x+3=-13, \\ y+2=-1. \end{cases}$$

В итоге имеем: $(-2;11)$, $(10,-1)$, $(-4;-15)$, $(-16,-3)$.

Пример. Решить в натуральных числах уравнение $\frac{1}{x}+\frac{1}{y}=\frac{1}{p}$, где p – простое число.

Решение. Из уравнения следует, что оба неизвестных больше p. Приведем в левой части к общему знаменателю. Получим

$$xy = p(x+y).$$

Это уравнение можно записать в виде

$$(x-p)(y-p) = p^2.$$

Тогда получаем следующие три системы уравнений:

$$\begin{cases} x-p=1, \\ y-p=p^2, \end{cases} \qquad \begin{cases} x-p=p, \\ y-p=p, \end{cases} \qquad \begin{cases} x-p=p^2, \\ y-p=1. \end{cases}$$

В итоге получаем следующие решения: $(p+1; p^2+p),\ (2p; 2p),\ (p^2+p; p+1)$.

Доказательство факта, что уравнение не имеет решений, может основываться на рассмотрении остатков по какому-либо модулю. Иногда этот же прием позволяет находить решение уравнения, которое будет единственным. А затем обязательно проводиться доказательство, что других решений нет.

Пример. Решим уравнение $3^x + 7 = 2^y$ в целых числах. Подбором находим, что пара $(2;4)$ является решением данного уравнения. Докажем, что других решений нет.

Перепишем уравнение в виде: $3^x = 4^m - 7$. Так как $4^m - 7 \equiv 1 \pmod 4$, а $3^{2n} \equiv 1 \pmod 4$, $3^{2n+1} \equiv 3 \pmod 4$, то x – четное число, т.е. $x = 2n$. Получаем, то $3^{2n} + 7 = 2^{2m}$, следовательно, $7 = 2^{2m} - 3^{2n} = \left(2^m - 3^n\right)\left(2^m + 3^n\right)$. Тогда $2^m + 3^n = 7$, а $2^m - 3^n = 1$, и получаем единственное решение $(2;4)$.

При решении диофантовых уравнений могут использоваться различные оценки и неравенства.

Пример. Найдем целые решения уравнения: $x^2+4xy+13y^2=58$. Преобразуем левую часть уравнения, выделив полный квадрат относительно переменной x:

$$x^2+4xy+13y^2=(x+2y)^2+(3y)^2.$$

Тогда исходное уравнение примет вид

$$(x+2y)^2+(3y)^2=58.$$

Откуда следует, что $(3y)^2\le 58$, $|y|\le 2$. Поэтому y может равняться одному из чисел $-2,\ -1,\ 0,\ 1,\ 2$.

Если $y=-2$, то уравнение $x^2-8x-4=0$ не имеет целых корней.

Если $y=-1$, то уравнение $x^2-4x-45=0$ имеет целые корни $x=-5$ и $x=9$.

Если $y=0$, то уравнение $0=58$ не имеет решений.

Если $y=1$, то уравнение $x^2+4x-45=0$ имеет целые корни $x=5$ и $x=-9$.

Если $y=2$, то уравнение $x^2+8x-4=0$ не имеет целых корней.

Следовательно, целыми решения уравнения являются $(5;1),\ (-9;1),\ (-5,-1),\ (9;-1)$.

Пример. Найдем целые решения уравнения $x(x+1)=4y(y+1)$. Данное уравнение равносильно уравнению $x^2+x+1=(2y+1)^2$.

Если $x\ge 1$, то $x^2<(2y+1)^2<(x+1)^2$ и уравнение не имеет решений.

Если $x\le -2$, то $(x+1)^2<x^2+x+1=(2y+1)^2<x^2$ и уравнение не имеет решений.

Получается, что x может принимать значения $x=0$ и $x=-1$.

Следовательно, будет имеет следующие целые решения: $(0;0),\ (0;1),\ (-1,0),\ (-1;-1)$

Одним из примеров диофантова уравнения второй степени является уравнение вида:

$$x^2 + y^2 = z^2 .$$

Натуральные числа $a,\ b,\ c$, являющиеся решением данного уравнения, называются *пифагоровой тройкой*. Простейшая пифагорова тройка – $(3;4;5)$. Пифагорову тройку $a,\ b,\ c$ называют *примитивной*, если $(a,b,c)=1$.

Пример. Решите в натуральных числах уравнение $3^x + 4^y = 5^z$.

Решение. Выражение 5^z дает при делении на 4 остаток 1, тогда и выражение $3^x + 4^y$ должно давать такой же остаток при делении на 4. Следовательно, x четно. Обозначим $x = 2m$, где m – натуральное число. Рассмотрим остатки от деления на 3 исследуемых выражений. $3^x + 4^y$ при всех натуральных x и y дает остаток 1, а 5^z дает остаток 1 только при четных z, тогда $z = 2k$, где k – натуральное число. Тогда исходное уравнение можно переписать в виде

$$3^{2m} + 2^{2y} = 5^{2k},\ 5^{2k} - 2^{2y} = 3^{2m}.$$

Разложим левую часть уравнения по формуле разности квадратов, получаем

$$\left(5^k - 2^y\right)\left(5^k + 2^y\right) = 3^{2m}.$$

Так как правая часть содержит только тройки, то каждая скобка в левой части должна быть неотрицательной степенью тройки. Разность между скобками $5^k + 2^y - (5^k - 2^y) = 2 \cdot 2^y$ не делится на 3, то это возможно только в случае, когда

$$5^k - 2^y = 1 \text{ и } 5^k + 2^y = 3^{2m}.$$

Тогда $5^k = 2^y + 1$ и $5^k + 2^y = 2^y + 1 + 2^y = 3^{2m}$.

Получаем, что $3^{2m} - 1 = 2^{y+1}$. Опять раскладываем левую часть по формуле разности квадратов, получаем:

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

Значит, оба сомножителя в левой части являются степенями двойки, отличающимися на 2. Следовательно,

$3^m - 1 = 2$ и $3^m + 1 = 4$. Тогда $m = 1$, а $2^{y+1} = 8,\ y = 2$.

Получаем, что $x = 2,\ y = 2$ и $3^2 + 4^2 = 5^z,\ z = 2$.

Уравнение Пелля. Уравнение вида

$$x^2 - Ny^2 = 1,$$

где N – число, которое не содержит квадратов чисел, называется *уравнением Пелля*. Уравнение Пелля имеет бесконечно много решений. Существует решение $(x_1; y_1)$ такое, что каждое другое решение связано с $(x_1; y_1)$ равенством:

$$x_k + y_k\sqrt{N} = \pm(x_1 + y_1\sqrt{N})^k.$$

Решение $(x; y)$ больше, чем решение $(u; v)$, если $x + y\sqrt{N} > u + v\sqrt{N}$. Наименьшее решение $(x; y)$ с $x > 0,\ y > 0$ называется *фундаментальным*. Его можно получит с помощью *метода Браункера*, раскладывая $\sqrt{N}$ в непрерывную дробь.

Если n – нечетное, решение является пара $(P_n; Q_n)$. Если n – четное, решение будет пара $(P_{2n+1}; Q_{2n+1})$.

Пример. Найдем наименьшее решение уравнения $x^2 - 34y^2 = 1$. Раскладываем $\sqrt{34}$ в непрерывную дробь

$$\sqrt{34} = 5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{10 + \ldots}}}},$$

где $a_0 = 5,\ a_1 = 1,\ a_2 = 4,\ a_3 = 1,\ n = 3$ – нечетное.

$$\frac{P_0}{Q_0} = \frac{5}{1},\ \frac{P_1}{Q_1} = \frac{6}{1},\ \frac{P_2}{Q_2} = \frac{39}{5},\ \frac{P_3}{Q_3} = \frac{35}{6}.$$

Получаем наименьшее положительное решение $(35; 6)$.

Задачи для самостоятельной работы

1. Докажите, что остатки от деления на n чисел $a \pm b$ и $a \cdot b$ однозначно задаются остатками от деления на n чисел a и b.

2. Пусть p – простое число, и число a не делится на p. Докажите, что все остатки от деления на p чисел a, $2a$, ..., $(p-1)a$ попарно различны.

3. Докажите, что если p – простое число, а числа a и b не делятся на p, то остаток от деления на p числа a однозначно определяется остатками от деления чисел b и ab на p.

4. Докажите, что существует бесконечно много простых чисел вида $4k-1$.

5. Пусть $p = 4k+3$ – простое число. Докажите, что если $a^2 + b^2$ на p, то оба числа a и b делятся на p.

6. Пусть p – простое число. Докажите, что если q – простой делитель числа $2p-1$, то $q-1$ делится на p.

7. Докажите, что $2^{41} - 1$ делится на 83.

8. Докажите, что $2^{70} + 3^{70}$ делится на 13.

9. Докажите, что $11^{10} - 1$ делится на 100.

10. У Ивана-царевича есть два волшебных меча. Первый меч может отрубить 21 голову у Змея Горыныча, а второй – 4 головы. Но если Иван-царевич отрубает головы вторым мечом, на их месте вырастает еще 1999 голов. Может ли Иван отрубить у Змея Горыныча все головы, если в начале боя у него было 100 голов? (Если голов меньше 4, то рубить их нельзя).

11. Проводится игра, в которой из 100 камней каждый игрок поочередно берет от 1 до 5 камней. Проигрывает тот, кто взял последний камень. Определите выигрышную стратегию первого игрока.

12. Составьте список остатков, которые получаются при делении числа n^2 на 4, 5, 6, …, 9.

13.В магазин привезли 6 ящиков яблок с массами: 15, 16, 18, 19, 20 и 31 килограммов. Две фирмы купили 5 ящиков, причем одна из них взяла ящики яблок, масса которых в два раза больше массы ящиков яблок, которые взяла другая фирма. Какой ящик не был куплен?

14. Найдите остатки от деления числа 2^{2001} на 3, 5, 7, …, 17.

15. Найдите остаток от деления на 17 числа $2^{1999}+1$.

16. При каких целых n число $5n^2+10n+8$ делится на 3? На 4?

17. Найдите все такие целые числа x, что $x \equiv 3 \pmod 7$, $x^2 \equiv 44 \pmod{7^2}$, $x^3 \equiv 111 \pmod{7^3}$.

18. Решите сравнения:

а) $8x \equiv 3 \pmod{13}$; б) $17x \equiv 1 \pmod{37}$; в) $7x \equiv 2 \pmod{11}$.

19. Докажите, что уравнения не имеют решений в целых числах:

а) $x^2+y^2=2003$; б) $12x+5=y^2$; в) $8y^3-13y^3=17$.

20. Найдите такое n, чтобы число 10^n-1 делилось на 7; 13; 91.

21. Для каких n число $n^{2001}-n^4$ делится на 11?

22. Докажите, что $7^{51}-1$ делится на 103.

23. Пусть числа a, b, c – составляют пифагорову тройку. Докажите, что одно из них делится на 3, другое (или то же самое) делится на 4, третье – на 5.

24. Пусть числа a, b, c составляют примитивную пифагорову тройку. Докажите, что одно из чисел a или b чётно, а другое нечётно.

25. Пусть числа a, b, c составляют примитивную пифагорову тройку. Докажите, что $a \cdot b$ делится на 12.

26. Решите в целых числах уравнения: а) $xy+3x-5y=-3$; б) $x+y=x^2-xy+y^2$.

27. Найдите натуральные решения уравнения: а) $2^x+7=y^2$; б) $2^n+1=3^m$.

28. Найдите натуральные решения уравнения: а) $x!-1=y^2$; б) $x!+12=y^2$.

29. Пусть n – натуральное число. Докажите, что количество решений уравнения $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$ в натуральных числах равно количеству делителей числа n^2.

30. Найдите натуральные решения уравнения: $\frac{1}{x}+\frac{1}{y}=\frac{1}{239}$.

31. Найдите все натуральные числа $x,\ y,\ z$, для которых $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1$.

32. Найдите натуральные решения уравнения: $x+\frac{1}{y+\frac{1}{z}}=\frac{10}{7}$.

33. Найдите целые решения уравнения: $1+x+x^2+x^3=2^y$.

34. Найдите натуральные решения уравнения: $a^2b^2+a^2+b^2=1969$.

35. Найдите все а) натуральные, б) рациональные решения уравнения $x^y=y^x$.

36. Решите в натуральных числах системы уравнений:

а) $\begin{cases} x+y=180, \\ (x,y)=30; \end{cases}$ б) $\begin{cases} 7x=11y, \\ (x,y)=45; \end{cases}$ в) $\begin{cases} xy=720, \\ (x,y)=4. \end{cases}$

37.Найдите целые решения уравнения:

а) $45x-37y=25$; б)$109x+89y=1$; в) $19x+95y=1995$.

Если уравнения имеют несколько решений, то укажите все из них.

38. Существует ли в сутках момент, когда расположенные на общей оси часовая, минутная и секундная стрелки правильно идущих часов образуют попарно углы в 120^0?

39. Найдите все взаимно простые a и b, для которых $\frac{a+b}{a^2-ab+b^2}=\frac{3}{13}$.

40. Найдите наименьшее c, при котором уравнение $7x+9y=c$ имело бы ровно 6 целых положительных решений.

Список литературы

1. Алфутова Н.Б., Устинов А.В. Алгебра и теория чисел. Сборник задач для математических школ. – М.: МЦНМО, 2002. – 264 с.
2. Банникова Т.М., Баранова Н.А. Основы теории чисел: учебно-методическое пособие. – Ижевск, 2009. – 95 с.
3. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с.
4. Василенко О.Н., Галочкин А.И. Сборник задач по теории чисел. – М.: Изд-во Моск. ун-та, 1995. – 128 с.
5. Виленкин Н.Я. Комбинаторика. – М.: Наука, 1969. – 328 с.
6. Виноградов И.М. Основы теории чисел. – СПб-М.: Лань, 2004. – 167 с.
7. Ежов И.И., Скороход А.В., Ядренко М.И. Элементы комбинаторики. М.: Наука, 1977. – 80 с.
8. Кофман А. Введение в прикладную комбинаторику. – М.: Наука, 1975. – 480 с.
9. Крупинин В.Г., Павлов А.Л., Попов Л.Г. Высшая математика. Теория вероятностей, математическая статистика, случайные процессы. Сборник задач с решениями: Учебное пособие. – М.: Издательский дом МЭИ, 2013. – 386 с.
10. Кудреватов Г.А. Сборник задач по теории чисел. – М.: Просвещение, 1970. – 128 с.
11. Ландо С.К. Лекции о производящих функциях. – М.: МЦНМО, 2004. – 144 с.
12. Прасолов В.В. Задачи по алгебре, арифметике и анализу: Учебное пособие. – М.: МЦНМО, 2007. 608 с.
13. Серпинский В. О решении уравнений в целых числах. – М.: Изд-во физ.-мат. лит., 1961. – 90 с.
14. Серпинский В. 250 задач по элементарной теории чисел. – М.: Просвещение, 1968. – 160 с.