ВВЕДЕНИЕ В МАТЕМАТИКУ

листки с задачами
«100 урокам математики» Алексея Савватеева

составители: Н. Казимиров, П. Иванов, М. Бочкарев

Москва, 2020

АННОТАЦИЯ К СБОРНИКУ

Данный сборник задач может использоваться как приложение к конспекту «Введение в математику» Алексея Савватеева, а также как самостоятельный практикум для изучения основ математики. Нумерация глав-уроков в сборнике соответствует урокам онлайн-курса, подготовленным проектом «Дети и наука».

В каждом уроке даны ссылки на соответствующие видеоуроки и главы и разделы конспекта. Перед блоком задач даны краткие сведения из курса, содержащие необходимые определения и обозначения.

При составлении задачника было использовано несколько источников, в частности, задачи видеокурса по «100 урокам математики» проекта «Дети и наука», листки задач кружка Вечерней математической школы в 179 школе г. Москвы, листки задач для матшкольников из подборки Григория Мерзона.

Составители настоящего сборника: Николай Казимиров, Павел Иванов, Михаил Бочкарев.

29 ноября 2020 г.

УРОК 1

Числа, символы и фигуры

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 1. Числа, символы, фигуры.

Конспект: Глава 1, разделы 1.1 Запись действий с отрезками, 1.2 Понятие натурального числа, 1.3 Визуальные доказательства. Глава 7, раздел 7.1 Построение рациональных чисел.

Справочные сведения

Операции сложения и умножения мы визуально ассоциируем со смещением по прямой вправо или влево. Вправо — со знаком $+$, влево — со знаком $-$. Смещение на несколько единиц вправо или влево — это смещение на одноименное число шагов в данном направлении. В итоге операцию сложения или вычитания можно представить как путь по прямой дороге, который складывается из шагов, равных $+1$ или -1 в зависимости от направления.

Умножение задается с помощью прямоугольной сетки на плоскости. Имеем две координатные оси, на которых отложены, как и в одномерном случае, шаги-числа в обе стороны от точки O с соответствующими знаками. Откладываем перемножаемые числа по обеим осям, получаем прямоугольник, состоящий из единичных квадратов. Число этих квдаратов, т.е. площадь прямоугольника, и есть значение произведения (см. рис. 1.1).

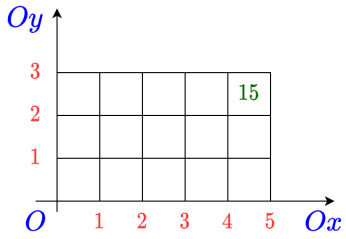


Рис. 1.1: Произведение $5 \cdot 3$.

В том случае, когда умножаются числа, оснащенные знаками, применяется правило ориентированной площади, т.е. знак выбирается в зависимости от направления оси наблюдателя, для которого порядок множителей всегда соответствует повороту против часовой стрелки (см. рис. 1.2).

Задачи

1.1. Нанести на прямой метки, соответствующие шагам вправо и влево, считая начальной точкой O, а все шаги равновеликими (т.е. каждый шаг равен выбранной единице длины). Дойти до точки 5, а затем от точки 5 до точки -5. Записать последовательность шагов с помощью ± 1, предполагая, что шаг вправо записывается как $+1$, шаг влево — как -1.

1.2. Описать в терминах одномерного путешественника операции сложения: $5+3$, $8-4$, $3-5$, $-2-6$. Сколько шагов и в какую сторону он прошел и в каком порядке? Записать в каждом

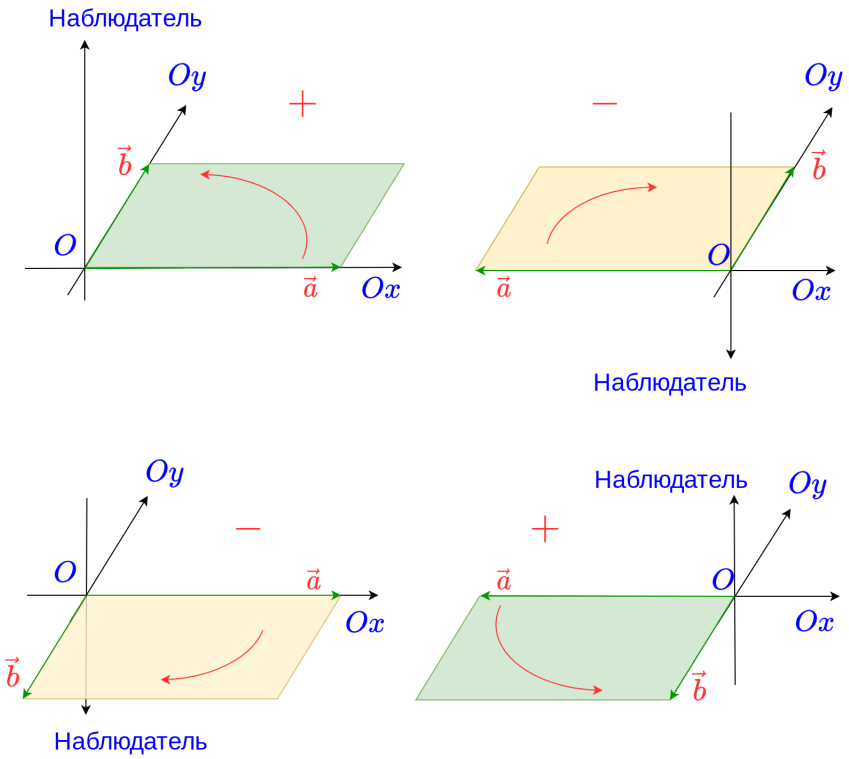


Рис. 1.2: произведение $a \cdot b$.

случае путь с помощью ± 1 и расставить скобки, объединяя в них указанные слагаемые.

1.3. *Путь* — это последовательность единичных шагов, обозначаемых $+1$ (шаг вправо) и -1 (шаг влево). Путь может начинаться в любой точке прямой. Записать пути, соответствующие операциям $-2+7$, $10-5$, $11-2-4$, $-8+3+10$.

1.4. Выберем точку O в качестве начала отсчета, затем нанесем на прямую точки, которые получаются в результате отсчета шагов влево и вправо, т.е. точки $\pm 1, \pm 2, \pm 3$ и т.д. Назовем эти точки *целыми*.

a) В какой точке окажется путешественник, если он стартует в точке -3 и проходит путь $4-1$? Изобразить графически.
b) В какой точке окажется путешественник, если он стартует в точке 1 и проходит путь $11-4+7$? Изобразить графически.

1.5. Два пути назовем *эквивалентными*, если, стартуя в одной и той же точке, они и закончатся в одной и той же точке. Эквивалентны ли пути $-2+7$, $10-5$, $11-2-4$, $-8+3+10$?

1.6. Путь a назовем *обратным* к пути b, если, стартовав там, где путь b заканчивается, он повторяет все шаги пути b в обратном порядке и с противоположным знаком (например, путь $1+1+1-1-1-1$ обратен к пути $-1-1-1+1+1+1$). Построить пути, соответствующие операциям $5+3$, $8-4$, $3-5$, $-2-6$, построить обратные к ним пути, выразить обратные пути в виде суммы или разности двух чисел (использовать те же цифры, что у исходного пути).

1.7. Изобразить ориентированные площади, соответствующие произведениям $3 \cdot 5$ и $5 \cdot 3$, $(-2) \cdot 6$ и $6 \cdot (-2)$, $(-3) \cdot (-4)$ и $(-4) \cdot (-3)$

УРОК 2

Соизмеримость отрезков

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 2. Соизмеримость и несоизмеримость отрезков.

Конспект: Глава 1, разделы 1.2 Понятие натурального числа, 1.4 Соизмеримость отрезков, алгоритм Евклида.

Справочные сведения

На этот раз у нас имеется два путешественника (кузнечика), каждый из которых имеет свою меру длины (длину шага), соответственно, у каждого из них получаются свои собственные ометки на прямой, расставленные через каждый шаг. Пусть у первого путешественника шаг равен a, а у второго — b. Таким образом, первый может придти в точки $\pm a, \pm 2a, \pm 3a$ и т.д., а второй — в точки $\pm b, \pm 2b, \pm 3b$ и т.д. Точка начала отсчета у них общая — точка O.

Длины шагов этих путешественников, т.е. числа a и b *соизмеримы*, если существует такая длина c (*общая мера отрезков* a и b), которая целое число раз укладывается в том и другом шаге: $a = nc$, $b = mc$.

Графический алгоритм Евклида: о прямоугольника со сторонами a и b отрезают квадраты со стороной, равной меньшей из длин a и b, столько раз, сколько возможно (будем называть это «операцией Евклида»). К оставшемуся прямоугольнику снова применяют операцию Евклида, и так далее (см. рис. 2.1).

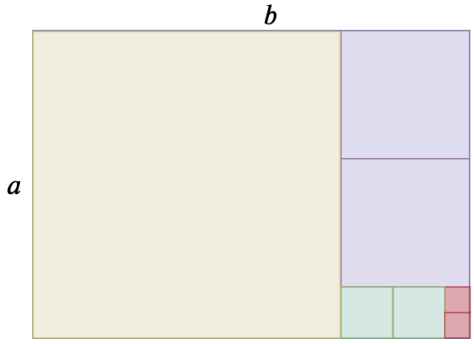


Рис. 2.1: Графический алгоритм Евклида.

Наибольший общий делитель целых чисел a и b — это наибольшее целое число, делящее a и b. Обозначение: НОД(a, b). Если НОД$(a, b) = 1$, то числа a и b называются *взаимно простыми* (обозначается так: $a \perp b$).

Задачи

2.1. Найти НОД$(10, 6)$, НОД$(11, 5)$, НОД$(12, 9)$ методом прямоугольников.

2.2. Сколько и каких шагов должны сделать 10- и 6-шаговые кузнечики, чтобы попасть в точку НОД(10,6)?

2.3. Доказать, что a и b соизмеримы тогда и только тогда, когда существует отрезок d такой, что отрезки a и b укладываются в нем целое число раз: $d = ka = lb$. Верно ли, что это также равносильно тому, что два путешественника могут встретиться в какой-то точке прямой, отличной от точки O?

2.4. Верно ли, что отрезки a и b соизмеримы тогда и только тогда, когда a и $2b$ соизмеримы?

2.5. Сколько и каких квадратов получится в результате применения графического алгоритма Евклида к прямоугольнику со сторонами 75 и 21? а со сторонами 324 и 141?

2.6. Применяя операцию Евклида, прямоугольник разрезали на большой квадрат, два квадрата поменьше и два совсем маленьких. Найти отношение сторон исходного прямоугольника.

2.7. Доказать, что если стороны прямоугольника соизмеримы, то, применяя операцию Евклида, мы в конце концов разрежем его на квадраты (применить метод бесконечного спуска).

2.8. Доказать, что если применение графического алгоритма Евклида разрезает прямоугольник на некоторое конечное число квадратов, то стороны прямоугольника соизмеримы, и сторона самого маленького квадрата будет их наибольшей общей мерой.

2.9. Доказать, что любая общая мера соизмеримых отрезков a и b целое число раз укладывается в наибольшей общей мере отрезков a и b.

2.10. От прямоугольника отрезали квадрат и получили прямоугольник, подобный исходному. Соизмеримы ли стороны исходного прямоугольника? Чему равно отношение его сторон?

2.11. Докажите, что НОД(a, b) существует и единственный, если целые a и b не равны одновременно нулю.

2.12. Докажите, что НОД$(a, b) =$ НОД$(a - b, b) =$ НОД(r, b), где r — остаток от дееления a на b.

2.13. Найдите наибольшую общую меру отрезков $15/28$ и $6/35$.

2.14. Какие расстояния можно отложить на прямой, имея шаблоны 6 см и 15 см?

2.15. Найдите возможные значения а) НОД$(n, 12)$; б) НОД$(n, n + 1)$; в) НОД$(2n + 3, 7n + 6)$; г) НОД$(n^2, n + 1)$.

УРОК 3

Визуальная арифметика

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 3. Визуальное представление бинома Ньютона.
Конспект: Глава 1, раздел 1.3 Визуальные доказательства.

Справочные сведения

Теорема Пифагора (см. рис. 3.1) и куб суммы (см. рис. 3.2).

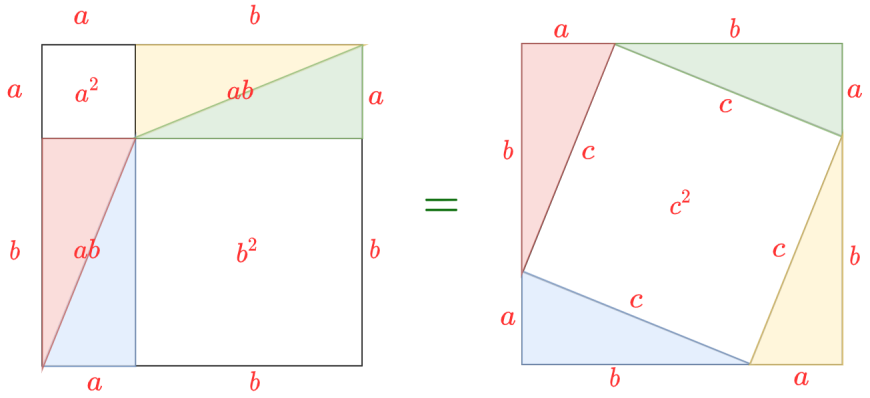


Рис. 3.1: $(a+b)^2 = a^2 + 2ab + b^2$ и $a^2 + b^2 = c^2$.

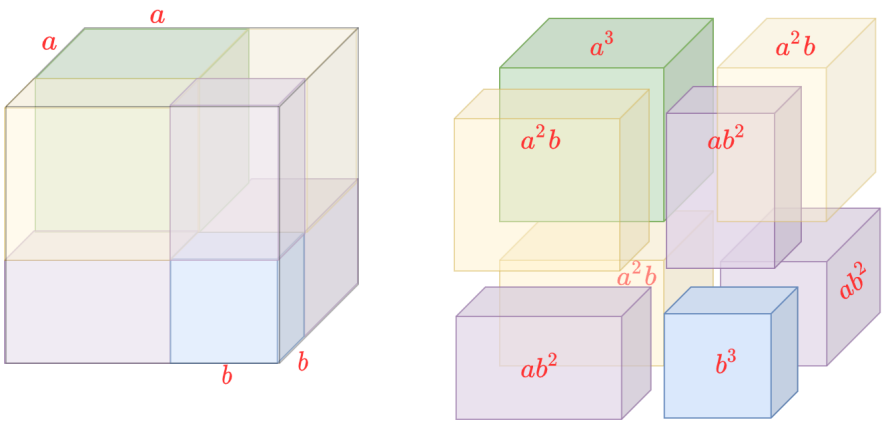


Рис. 3.2: $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^2$.

Задачи

3.1. Найти с помощью графического метода сумму подряд идущих нечетных чисел от 1 до n, где n — нечетное.

3.2. Рассмотрим последовательность уголков (см. рис. 3.3). Сколько клеток в k-м уголке? Чему равна суммарная площадь первый k уголков?

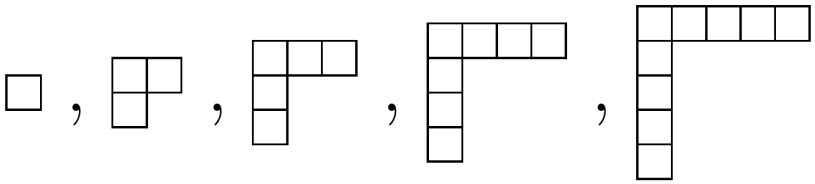
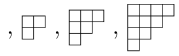


Рис. 3.3

3.3. Найти графически сумму первых k четных и первых k нечетных чисел.

3.4. Треугольные числа Диофанта  обозначим по порядку T_1, T_2, T_3, T_4 и т.д.

a) Сложите из двух последовательных треугольных чисел квадрат.
b) Что получится при сложении T_n с T_n?
c) Выразив T_n через n, найдите $1 + 2 + \cdots + n$.
d) Докажите геометрически, что $T_{n+m} = T_n + T_m + nm$.

3.5. Докажите геометрически, что $1 + 2 + \cdots + (n-1) + n + (n-1) + \cdots + 2 + 1 = n^2$.

3.6. Получите геометрически выражение для $(a + b + c)^2$, $(a + b + c)^3$.

3.7. Объясните равенство на рис. 3.4 и получите формулу для суммы квадратов $1^2 + 2^2 + 3^2 + \cdots + n^2$.

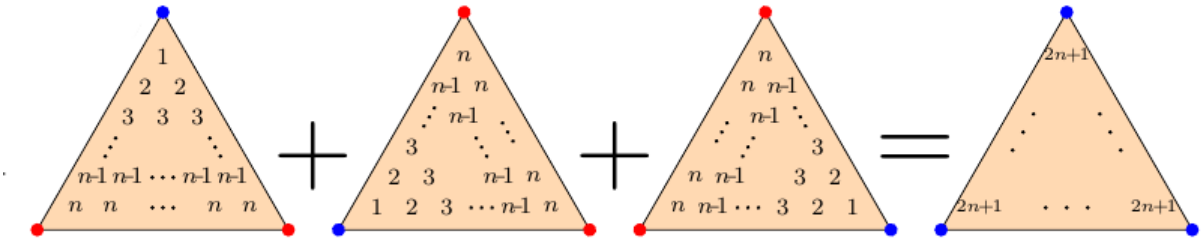


Рис. 3.4

3.8. С помощью рис. 3.5 получите еще один способ найти формулу для суммы квадратов.

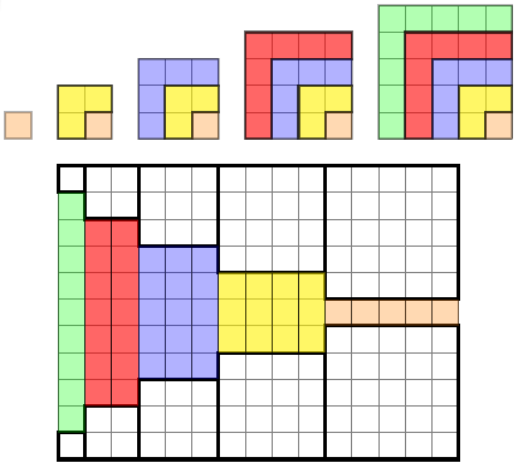


Рис. 3.5

УРОК 4

Бесконечные суммы

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 4. Бесконечные суммы.

Справочные сведения

В данном разделе мы рассматриваем только суммы *положительных* слагаемых.

Бесконечные суммы с положительными слагаемыми могут быть сходящимися и расходящисмися. Сходимость означает, что найдется такое число, что любой сколь угодно длинный конечный отрезок данной бесконечной суммы меньше этого числа. Например, сумму $1 + 1/2^2 + 1/3^2 + 1/4^2 + \dots$ можно оценивать так:

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

$$\frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} < \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} = \frac{1}{4},$$

и т.д. То есть, сумму можно разбить на отрезки длиной 2, 4, 8, 16 и т.д. слагаемых, причем сумма по каждому такому отрезку будет оцениваться сверху дробью $1/2^k$. Остается заметить, что ряд

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$$

сходится. А это легко обнаружить на картинке 4.1 последовательным делением квадрата 1×1 пополам. Таким образом, для суммы обратных квдаратов справедлива оценка:

$$1 + 1/2^2 + 1/3^2 + 1/4^2 + \dots \leqslant 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots \leqslant 2.$$

Обратно, для некоторых рядов можно найти такую оценку снизу, которая будет заведомо бесконечной, а значит, и сумма исходного ряда также будет бесконечной. Такое верно, например, для гармонического ряда:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots \geqslant 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + 4 \cdot \frac{1}{8} + 8 \cdot \frac{1}{16} + \dots,$$

а это — бесконечная сумма одинаковых слагаемых, равных $1/2$ (кроме первого слагаемого). Ясно, что какое бы большой число мы ни выбрали, можно взять столь много раз $1/2$, что их сумма будет больше выбранного числа. А значит, и сумма гармонического ряда равна бесконечности.

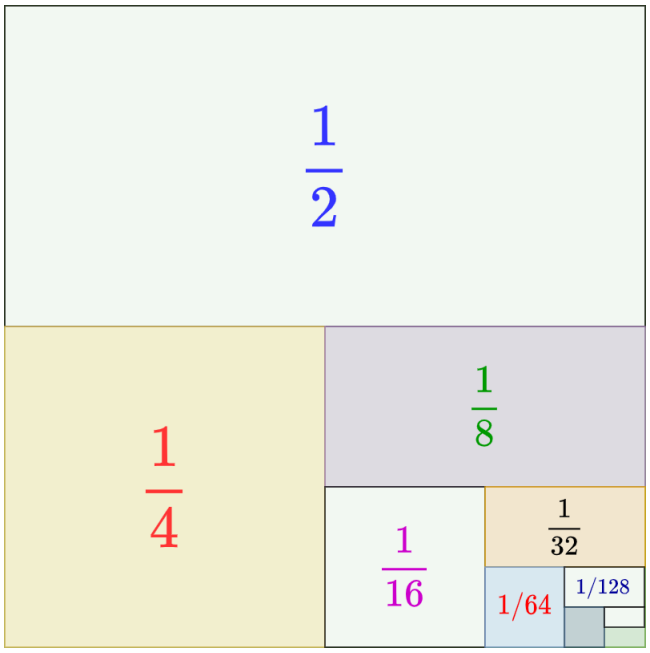


Рис. 4.1

Задачи

4.1. Выведите формулу суммы геометрической прогрессии $1 + x + x^2 + x^3 + \dots$ $(0 < x < 1)$ путем домножения этой суммы на x. Найти:

a) $\dfrac{1}{10} + \dfrac{1}{100} + \dfrac{1}{1000} + \dots$;
b) $1 + 0.2 + (0.2)^2 + (0.2)^3 + \dots$;
c) $\dfrac{1}{0.99} + \dfrac{1}{0.99^2} + \dfrac{1}{0.99^3} + \dots$.

4.2. Исследовать ряды на сходимость:

a) $1 + 1/3 + 1/5 + 1/7 + \dots$;
b) $1 + 1/3^2 + 1/5^2 + 1/7^2 + \dots$;
c) $\dfrac{1}{1001} + \dfrac{1}{2001} + \dfrac{1}{3001} + \dots + \dfrac{1}{1000n+1} + \dots$;
d) $1 + \dfrac{1}{2!} + \dfrac{1}{3!} + \dfrac{1}{4!} + \dots$;
e) $1 + \dfrac{2}{3} + \dfrac{3}{5} + \dfrac{5}{9} + \dots + \dfrac{n}{2n-1} + \dots$.

4.3. Доказать, что если ряды $\sum\limits_n a_n^2$ и $\sum\limits_n b_n^2$ сходятся, то сходятся также и ряды:

$$\sum_n a_n b_n, \quad \sum_n (a_n + b_n)^2.$$

Здесь все $a_n, b_n \geqslant 0$.

4.4. Доказать сходимость ряда

$$a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_n}{10^n} + \dots,$$

где $0 \leqslant a_n < 10$.

УРОК 5

Движения прямой: работа с понятием

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 5. Начальные представления о движении.
Конспект: Глава 2, разделы 2.1 Сдвиг, композиция сдвигов, группа и раздел 2.2 Отражение.

Справочные сведения

Движением называется такое преобразование (прямой, фигуры, плоскости, области пространства и т.д.), которое сохраняет расстояния. Т.е. если между точками A и B расстояние равно x, то между точками A' и B', в которые переходят исходные точки A и B при некотором движении, расстояние также будет равно x.

На прямой рассматриваются следующие два вида движений:

- Сдвиг на x, когда все точки, как по команде, сдвигаются на число x (если $x > 0$, то вправо, а если $x < 0$, то влево). Сдвиг на x обозначается за T_x. Сдвиг на вектор AB обозначается T_{AB}.
- Отражение относительно точки O, когда все точки переходят в симметричные себе относительно точки O. Отражение относительно точки O обозначается за S_O.

Частный случай сдвига — тождественное движение id, которое ничего не меняет (все точки остаются на своих местах). $\mathrm{id} = T_0$ (сдвиг на нулевой вектор).

Композиция движений G и Q записывается как $G \circ Q$, что означает последовательное применение движений: сначала ко всем точкам прямой применяется движение Q, а затем к результату предыдущего движения применяется движение G. Композиция движений есть движение.

Задачи

Пусть на прямой даны 4 точки A, B, C, D, поставленные друг за другом с одинаковым шагом (см. рис. 5.1).

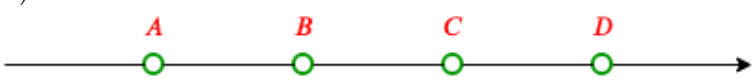


Рис. 5.1

5.1. Куда перейдет точка A при отражении S_B?

5.2. Куда перейдут точки B, C, D при преобразовании $T_{AB} \circ T_{CA}$?

5.3. Куда перейдут точки A, B, C при преобразовании $S_C \circ T_{AB}$?

5.4. Какое движение переводит A в C и B в D?

5.5. Существует ли движение, которое переводит A в B и B в D?

5.6. Опишите все движения, которые переводят A в C, используя только буквы A, B, C, D и обозначения сдвига и отражения.

УРОК 6

Движения прямой: классификация

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 6. Классификация движений прямой.
Конспект: Глава 2, раздел 2.4 Теорема о гвоздях, аналог теоремы Шаля.

Справочные сведения

Всякое движение прямой — это либо сдвиг, либо отражение. При этом любое движение — это либо одно отражение, либо композиция двух отражений.

Всякое движение прямой есть *взаимно однозначное соответствие* точек прямой, т.е. оно переводит разные точки в разные, и какова бы ни была точка прямой, найдется точка, переходящая в нее под действием движения.

Обратное движение для дивжения G — это такое движение G^{-1}, что $G \circ G^{-1} = G^{-1} \circ G = \mathrm{id}$.

Обращение композиции: $(G \circ Q)^{-1} = Q^{-1} \circ G^{-1}$.

Задачи

Введем координату на прямой, отметим там точки с целыми координатами: $\ldots, -2, -1, 0, 1, 2, \ldots$. Через S_n обозначим отражение относительно точки n, через T_n — сдвиг на число n.

6.1. Известно, что при некотором преобразовании G точка 0 переходит в 2, а 2 — в 3. Может ли оно быть движением? Каким?

6.2. Известно, что при некотором преобразовании G точка 0 переходит в 3, а 2 — в 1. Может ли оно быть движением? Каким?

6.3. Известно, что при некотором преобразовании G точка 0 переходит в 2, а при обратном преобразовании G^{-1} точка 3 переходит в -1. Может ли G быть движением? Каким?

6.4. Дано движение G. Известно, что $G^{-1}(0) = 1$ и при этом у G^{-1} нет неподвижных точек. Чему равно G?

6.5. Назовем *четностью движения* прямой четность количества отражений, с помощью которых это движение может быть выражено. Какова четность следующих движений: S_0, T_x, $T_x \circ T_y$, $S_0 \circ T_x$, $S_0 \circ S_1 \circ T_x \circ T_y$, T_x^{-1}, S_9^{-1}, $S_0 \circ S_1 \circ \cdots \circ S_n$?

6.6. Доказать, что

а) Четность обратного движения G^{-1} совпадает с четностью исходного движения G.

b) Четность композиции движений равна сумме четностей (по модулю 2) компонентов.
c) Четность движения не зависит от его представления в виде композиций каких-либо движений.

УРОК 7

Движения прямой: таблица композиций

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 7. Таблица композиций движений прямой.
Конспект: Глава 2, раздел 2.3 Таблица композиций движений прямой.

Справочные сведения

Таблица композиций отражений и сдвигов:

	T_a	S_O
T_b	T_{a+b}	$S_{O+b/2}$
S_C	$S_{C-a/2}$	T_{2OC}

Таблицу композиций следует читать слева наверх, т.е. если в левом столбце стоит движение F, а в верхней строке — движение G, то в соответствующей ячейке стоит композиция $F \circ G$.

Задачи

Введем координату на прямой, отметим там точки с целыми координатами: $\ldots, -2, -1, 0, 1, 2, \ldots$. Через S_n обозначим отражение относительно точки n, через T_n — сдвиг на число n.

7.1. Какое движение получится при композиции

a) $S_0 \circ S_1$?
b) $S_0 \circ S_1 \circ S_2$?
c) $S_0 \circ S_2 \circ S_1$?

7.2. Построить сдвиг на 7 единиц вправо с помощью композиции двух отражений.

7.3. Каким движением является следующая композиция?

$$S_n \circ S_{n-1} \circ \cdots \circ S_1 \circ S_0.$$

Ответ получить в зависимости от четности n.

7.4. При каких n сдвиг T_n выражается в виде композиций S_0 и S_1?

7.5. При каких n сдвиг S_n выражается в виде композиций S_0 и S_1?

7.6. Пусть G и Q — два движения прямой, причем $G \circ Q = Q \circ G$ и $G \neq Q$. Какими могут быть G и Q?

7.7. Пусть G и Q — два движения прямой, причем $G \circ Q = \mathrm{id}$ и $G \neq Q$. Какими могут быть G и Q?

7.8. Вывести равенства $S_C \circ T_a = S_{C-a/2}$ и $T_b \circ S_O = S_{O+b/2}$ из соотношения $S_C \circ S_O = T_{2OC}$ алгебраическим путем.

7.9. Доказать, что никакая композиция движений S_n и T_m с целыми индексами n, m не может быть равна сдвигу T_x с нецелым x и отражению S_y с неполуцелым y.

УРОК 8

Движения окружности: классификация

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 8. Движения окружжности.

Конспект: Глава 3, раздел 3.1 Движения окружности, раздел 3.2 Группа движений окружности, теорема Шаля.

Справочные сведения

Чтобы корректно говорить о движениях в криволинейном пространстве, нужно сначала договориться о метрике на нем. *Расстояние* (метрика) между двумя точка окружности — это длина меньшей из дуг данной окружности, соединяющих эти точки. Таким образом, движение окружности по определению должно сохранять длину дуги, переводя точки окружности в точки этой же окружности.

В отличие от прямой, на окружности расстояния имеют максимально допустимное значение, а именно, половину длины этой окружности. На масимальном расстоянии находятся диаметрально противоположные точки.

Движения на окружности являются:

- *Отражение относительно диаметра* (произвольного). Отражение обозначается S_l, где l — диаметр. Если на окружности зафиксировано нулевое положение диаметра, то любой диаметр можно определить через угол наклона относительно улевого диаметра (угол откладывается против часовой стрелки). Если диаметр l имеет наклон φ относительно нулевого диаметра ($0 \leqslant \varphi < \pi$), то отражение относительно данного диаметра мы также записваем как S_φ.

- *Поворот окружности* относительно ее центра. Поворот обозначается R_φ, где φ — угол поворота относительно центра окружности, осуществляемый против часовой стрелки, $0 \leqslant \varphi < 2\pi$.

В обоих случаях можно рассматривать и другие значения угла φ, приводя его по модулю π в случае отражений и по модулю 2π в случае поворотов, т.к. наклон диаметра на угол $\phi \pm \pi$ приводит к диаметру с углом φ, а поворот на угол $\pi \pm 2\pi$ — это поворот на угол φ.

Углы измеряются в радианах. 1 радиан — это угол, соответствующей дуге, длина которой равна радиусу окружности. Угол в 180^o, соответствующий дуге, равной половине длины окружности, он же — развернутый угол, — имеет радианную меру, равную числу π. Если окружность имеет радиус, равный 1, то мера угла в радианах численно совпадает с длиной соответствующей этому углу дуги данной окружности.

Частным случаем поворота является *тождественное движение* id, оставляющее все точки окружности на месте. $\mathrm{id} = R_0 = R_{2\pi k}$.

Других движений окружности не существует (теорема Шаля). Как и в случае прямой, любое движение окружности можно представить как композицию одного или двух отражений.

Задачи

8.1. Доказать, что $\pi > 3$.

8.2. Пусть G — движение окружности. Сколько у G может быть неподвижных точек (имеется ввиду общее количество, найдите все возможные варианты)?

8.3. Пусть G — движение окружности. Известно, что $G(A) = A$ и $G(B) \neq B$. Какой вид может иметь G?

8.4. Пусть диаметры l и k перпендикулярны. Найдите $S_l \circ S_k$.

8.5. Известно, что точка A переходит при движении G окружности в точку A', диаметрально противоположную точке A. Каким может быть движение G?

8.6. Движение назовем *четным*, если оно является композицией двух отражений, а в противном случае — *нечетным*. Верно ли, что:

a) Композиция четных движений — четное движение, композиция двух нечетных движений — четное движение, композиция четного движения с нечетным движением — нечетное движение?
b) G четно тогда и только тогда, когда G^{-1} нечетно?

УРОК 9

Движения окружности: таблица композиций

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 9. Таблица умножения движений окружности.
Конспект: Глава 3, раздел 3.2 Группа движений окружности, теорема Шаля.

Справочные сведения

Таблица композиций движений окружности:

	R_α	S_ψ
R_β	$R_{\alpha+\beta}$	$S_{\psi+\beta/2}$
S_φ	$S_{\varphi-\alpha/2}$	$R_{2(\varphi-\psi)}$

Таблицу композиций следует читать слева наверх, т.е. если в левом столбце стоит движение F, а в верхней строке — движение G, то в соответствующей ячейке стоит композиция $F \circ G$.

Задачи

9.1. Центральная симметрия — это какое движение?

9.2. Композицией каких отражений можно выразить центральную симметрию?

9.3. С помощью отражения относительно оси Ox (горизонтальной оси) и вращений выразить отражение относительно оси Oy (вертикальной оси).

9.4. Возьмем некоторый угол $\varphi > 0$. Найдите:

a) $S_0 \circ S_\varphi$;
b) $S_0 \circ S_\varphi \circ S_{2\varphi}$;
c) $S_0 \circ S_{2\varphi} \circ S_\varphi$;
d) $S_0 \circ S_\varphi \circ S_{2\varphi} \circ S_{3\varphi} \circ \cdots \circ S_{n\varphi}$.
e) Чему равно последнее выражение, если $\varphi = \pi/2$, $\varphi = \pi$, $\pi = 2\pi$?

9.5. Построить поворот на угол 90^o при помощи двух отражений.

9.6. При каких n поворот на угол $n\varphi$ выражается в виде композиций S_0 и S_φ?

9.7. Пусть G и Q — движения окружности, причем $G \circ Q = Q \circ G$. Какими могут быть G и Q?

9.8. Пусть G и Q — движения окружности, причем $G \circ Q = \mathrm{id}$. Какими могут быть G и Q?

УРОК 10

Конечные подгруппы движений прямой и окружности

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 10. Конечные подгруппы движений прямой и окружности.

Конспект: Глава 2, раздел 2.5 Все конечные подгруппы движений прямой, раздел 5.3 Подгруппы движений окружности.

Справочные сведения

Все движения прямой и все движения окружности образуют группы с операцией композиции. Напомним определение группы. Пусть на множестве G задана операция $\circ$. Множество G с данной опеарцией называется *группой*, если:

G1 $a \circ b \in G$ для всех $a, b \in G$ (группоид);

G2 для любых $a, b, c \in G$ имеем тождество $(a \circ b) \circ c = a \circ (b \circ c)$ (ассоциативность);

G3 существует элемент $\mathrm{id} \in G$ такой, что $a \circ \mathrm{id} = \mathrm{id} \circ a = a$ для всех $a \in G$ (единица);

G4 для всякого $a \in G$ существует обратный элемент $a^{-1} \in G$ такой, что $a \circ a^{-1} = a^{-1} \circ a = \mathrm{id}$ (обратный элемент).

Кроме того, группа называется *абелевой* (или *коммутативной*), если $a \circ b = b \circ a$ для всех $a, b \in G$. Количество элементов в группе называется ее ***порядком***.

Конечная подгруппа может быть определена следующим образом: это — *конечное подмножество группы, замкнутое относительно групповой операции*. Такого определения достаточно, чтобы вывести из него тот факт, что данное подмножество само по себе является группой, т.е. содержит единицу (исходной группы), обратные элементы, а также удовлетворяет требованию ассоциативности операции (т.к. операция та же самая).

Всякая конечная подгруппа группы движений прямой имеет вид либо $\{\mathrm{id}\}$, либо $\{\mathrm{id}, S_A\}$, где A — некоторая точка прямой.

Всякая конечная подгруппа группы движений окружности имеет один из видов:

10.1. тривиальная подгруппа $\{\mathrm{id}\}$;

10.2. группа поворотов правильного n-угольника (включая случай вырожденного 2-угольника);

10.3. подгруппа одного отражения $\{\mathrm{id}, S_\varphi\}$;

10.4. группа движений правильного n-угольника (включает повороты, совмещающие углы многоугольника, и отражения относительно осей, проходящих через его вершины и центр окружности).

Задачи

10.1. Выпишите все конечные подгруппы группы движений окружности порядка не выше 6, содержащие отражение S_0 (относительно горизонтальной оси).

10.2. Какова группа движений правильного треугольника, квдарата, пятиугольника?

10.3. Пусть задан правильный треугольник ABC с осями симметрии a, b, c и центром O. Заполните таблицу композиций движений данного треугольника: Таблицу композиций следует

	id	$R_{2\pi/3}$	$R_{4\pi/3}$	S_a	S_b	S_c
id						
$R_{2\pi/3}$						
$R_{4\pi/3}$						
S_A						
S_B						
S_C						

читать слева наверх, т.е. если в левом столбце стоит движение F, а в верхней строке — движение G, то в соответствующей ячейке стоит композиция $F \circ G$.

УРОК 11

Арифметика остатков

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 11. Введение в арифметику остатков.
Конспект: Глава 8, раздел 8.1 Арифметика остатков.

Справочные сведения

Посмотрим на шкалу целых чисел $0, \pm1, \pm2, \dots$ через некоторый трафарет. Этот трафарет является непрозрачной полоской, в которой проделаны дырки с шагом m друг от друга (где m — целое положительное число). Например, пусть $m = 7$, тогда если в одной дырке мы видим число 0, то в другой, справа от нее, — число 7, а слева — -7. Если мы сместим трафарет вправо на единицу, то увидим числа -6, 1 и 8, еще сдвинем — числа -5, 2 и 9, и т.д.

Таким образом, в массиве всех целых чисел мы сможем выделять такие числа, которые связаны друг с другом через этот трафарет. Например, все числа кратные 7, т.е. $0, \pm7, \pm14, \dots$. В другой класс войдут все числа, смещенные от них на 1 вправо, т.е. $1, \pm7 + 1, \pm14 + 1, \dots$. Эти классы называются *классами вычетов по модулю* m.

Если класс содержит число 0, то все числа из данного класса кратны шагу трафарета, т.е. модулю m. Действительно, ведь это числа $0, \pm m, \pm2m$ и т.д. Если класс не содержит нуля, то все числа в нем имеют слева соседа из нулевого класса на одном и том же расстоянии, т.к. это числа вида $k, k \pm m, k \pm 2m, \dots$, где $0 < k < m$. Число k является остатком от деления таких чисел на модуль m. Между классами и остатками от деления существует взаимно однозначное соответствие.

Простой иллюстрацией из жизни является пример с днями недели. Все понедельники отстоят друг от друга на кратное 7 число дней. Поэтому на шкале дней их можно увидеть через трафарет с шагом 7. Аналогично — все вторники, среды, четверги, пятницы, субботы и воскресенья. Если воскресенье обозначить за 0, понедельник — за 1, и т.д., то для любой даты можно определить ее класс, он же — остаток отделения на 7, т.е. день недели.

Как только мы отождествляем целые числа, входящие в один класс, их арифметика становится *модульной*. Это значит, что арифметические операции мы выполняем с точностью до класса. Так, если сложить $2 + 5$, то в обычной арифметике мы получим число 7, но оно находится в том же классе, что и число 0 по модулю $m = 7$, поэтому в модульной арифметике $2 + 5 = 0 \mod 7$. Проще говоря, в модульной арифметике мы всякий раз *вычитаем* максимально возможную часть числа, кратную модулю, и оставляем лишь *остаток* от деления на модуль. Поэтому она и называется арифметикой остатков.

Попадание чисел a и b в один класс по модулю m обозначается так: $a \equiv b \mod m$. Формально это означает, что $a - b = km$ при некотором целом k.

Если a делится на b (формально: существует целое k такое, что $a = kb$), то пишут $a \vdots b$, это равносильно записи $b|a$ (b делит a). Частный случай: $0 \vdots x$ и $x|0$ при любом целом x.

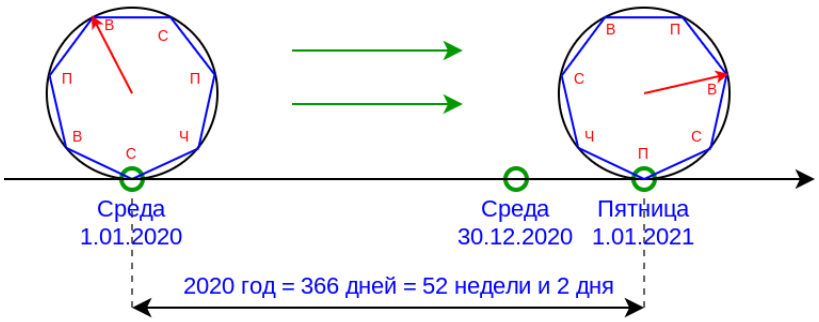


Рис. 11.1: Арифметика остатков по модулю 7.

Задачи

11.1. Отметить на числовой оси целые числа, которые при делении на 7 дают остаток 2 (на рисунке должны поместиться числа от -20 до 20).

11.2. Книги на столе пытались связывать в пачки по 2, по 3, по 4 и по 5 книг, и каждый раз оставалась одна лишняя. Сколько книг было на столе? (Известно, что их было не больше 100.)

11.3. Одному брату 6 лет, другому — 10. Значит, сумма из возрастов четная. Какой она будет в следующем году?

11.4. Если сегодня понедельник, то какой день недели будет через 10 дней, через 90 дней, через 2 года (рассмотреть случай без високосных лет и с високосным годом)?

11.5. Найти день недели через месяц, квартал, полгода и год, отправляясь от текущей даты.

11.6. Поезд Москва–Владивосток отправляется из Москвы в 7:00 и находится в пути 166 часов. Определите время прибытия (московское) поезда во Владивосток.

11.7. Построить таблицы сложения для модулей: 2,3,4,5,6,10,11.

11.8. Найти число, которое при делении на 2 даёт остаток 1, при делении на 3 остаток 2, при делении на 4 остаток 3, при делении на 5 остаток 4, при делении на 6 остаток 5 и при делении на 7 даёт остаток 6.

11.9. Верно ли, что а) если $n \vdots k$ и $k \vdots n$, то $n = \pm k$; б) если $a|b$ и $b|c$, то $a|c$; в) если $b \vdots a$ и $c \vdots a$, но $d \not\vdots a$, то $(b+c) \vdots a$, но $(b+d) \not\vdots a$; г) если a и b не делятся на c, то ab не делится на c^2?

11.10. Что означает запись $a \equiv b \pmod 0$?

11.11. Обозначим за $\oplus$ сложение по модулю 2, т.е. $a \oplus b = a + b \pmod 2$, если $a, b \in \{0, 1\}$. Для битовых последовательностей эта операция применяется попозиционно (например, $110 \oplus 101 = 011$).

Алиса и Боб придумали следующий алгоритм шифрования. Каждый из них сгенерил случайную последовательность длины n: A и B соответственно. Алиса передает Бобу сообщение m длиной в n битов следующим способом: она отправляет ему сообщение $m_1 = m \oplus A$, в ответ Боб отправляет ей $m_2 = m_1 \oplus B$, затем Алиса отправляет Бобу $m_3 = m_2 + A$.

Как Боб сможет прочесть сообщение m, зная алгоритм и сообщение m_3? Как Ева, перехватившая сообщения m_1, m_2, m_3, сможет прочесть исходное сообщение m ?

УРОК 12

Таблицы умножения остатков

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 12. Таблицы умножения остатков.

Конспект: Глава 8, раздел 8.1 Арифметика остатков, раздел 8.2 Свойства арифметики остатков.

Справочные сведения

Умножение остатков производится также по модулю m, т.е. после умножения отбрасываем часть, кратную m, и оставляем остаток от деления на m (см. рис. 12.1).

Таблица умножения по модулю m обладает следующими свойствами:

- Она центрально симметрична (на картинке 12.1 мы убрали строку и столбец, соответствующие умножению на ноль).
- Если модуль — простое число, то нулей в таблице нет (кроме тривиальных строк и столбца).

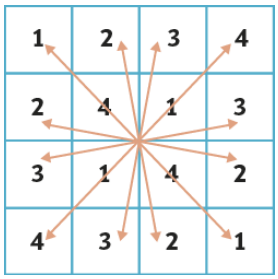


Рис. 12.1: Умножение по модулю 5.

Задачи

12.1. Целое положительное число увеличили на 1. Могла ли сумма его цифр (а) возрасти на 8? (б)Уменьшиться на 8? (в) Уменьшиться на 10?

12.2. Какие остатки может давать точный квадрат при делении на 4?

12.3. Последняя цифра точного квадрата равна 6. Доказать, что его предпоследняя цифра нечётна.

12.4. Остаток от деления простого числа на 30 — простое число или 1. Почему?

12.5. Какое наибольшее число различных целых чисел можно выбрать, если требуется, чтобы сумма и разность любых двух из них не делились на 15?

12.6. На какую цифру оканчивается число $33^{77} + 77^{33}$?

12.7. Могут ли среди m последовательных целых чисел какие-то два иметь равные остатки от деления на m?

12.8. Пусть $5x \equiv 6 \pmod 8$. Найти x.

12.9. Найти последнюю цифру 7^{100}, 7^{1942}.

12.10. Пусть $a \equiv b \pmod m$, $c \equiv d \pmod m$. Докажите, что сравнения по одному и тому же модулю

a) можно складывать и вычитать: $a + c \equiv b + d \pmod m$, $a - c \equiv b - d \pmod m$;
b) можно перемножать: $ac \equiv bd \pmod m$;
c) можно возводить в натуральную степень n: $a^n \equiv b^n \pmod m$;
d) можно домножать на любое целое число k: $ka \equiv kb \pmod m$.

12.11. Найдите остаток от деления ***а)*** числа $1 + 31 + 331 + \cdots + 3333333331$ на 3; ***б)*** 6100 на 7.

12.12. Найдите остаток от деления числа $1 - 11 + 111 - 1111 + \cdots - 1111111111$ на 9.

12.13. Найдите остаток от деления ***а)*** 10! на 11; ***б)*** 11! на 12.

12.14. ***а)*** Какой цифрой оканчивается 8^{18}? ***б)*** При каких натуральных k число $2^k - 1$ кратно 7?

12.15. Найдите три последние цифры числа 1999^{2000}.

12.16. Найти ***а)*** $3^{31} \pmod 7$, ***б)*** $2^{35} \pmod 7$, ***в)*** $128^{129} \pmod{17}$.

12.17. Докажите, что ***а)*** $30^{99} + 61^{100}$ делится на 31; ***б)*** $43^{95} + 57^{95}$ делится на 100.

12.18. Докажите, что $1^n + 2^n + \cdots + (n-1)^n$ делится на n при нечётном n.

12.19. Числа x и y целые, причем $x^2 + y^2$ делится на 3. Докажите, что x и y делятся на 3.

12.20. Какие целые числа дают при делении на 3 остаток 2, а при делении на 5 — остаток 3?

12.21. Докажите, что остаток от деления простого числа на 30 есть или простое число или 1.

12.22. (а) Квадрат целого положительного числа оканчивается на ту же цифру, что и само число. Что это за цифра? (Указать все возможности.) (б) Квадрат целого положительного числа оканчивается на те же две цифры, что и само число. Что это за цифры? (Указать все возможности.) (в) Пятая степень числа оканчивается на ту же цифру, что и само число. Почему? Для каких ещё степеней это верно?

12.23. Доказать, что для любого целого a число 10a даёт при делении на 9 тот же остаток, что и само a.

12.24. Доказать, что число и его сумма цифр дают одинаковые остатки при делении на 3 и 9.

12.25. *Сколько есть способов записать 2018 как сумму натуральных слагаемых, любые два из которых равны или различаются на 1? (Способы лишь с разным порядком слагаемых считаем равными.)

12.26. *Докажите, что из любых n целых чисел всегда можно выбрать несколько, сумма которых делится на n (или одно число, делящееся на n).

УРОК 13

Умножение по простому модулю

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 13. Основная теорема арифметики. Часть 1.

Конспект: Глава 4, раздел 4.2 Кузнечик НОД и алгоритм Евклида, раздел 4.3 Простые числа и ОТА, Глава 8, раздел 8.1 Арифметика остатков, раздел 8.2 Свойства арифметики остатков.

Справочные сведения

Для произвольной строки (столбца) таблица умножения остатков по модулю m эквивалентны следующие утверждения:

- В строке (столбце) отсутствует ноль;
- Номер строки (столбца) взаимно прост с модулем m;
- В строке (столбце) встречаются все числа от 1 до $m-1$;
- В строке (столбце) встречается 1.

Натуральное число p — *простое*, если оно имеет ровно два положительных делителя (1 и p).

Таблица умножения остатков по простому модулю p не содержит нулей (кроме строки и столбца с умножением на ноль) и все строки и столбцы являются перестановками множества $\{1,\ldots,p-1\}$.

В таблице умножения остатков по простому модулю p номер k любой строки взаимно прост с модулем: НОД$(k,p)=1$. Отсюда следует, что при некоторых целых n,m имеем $mp-nk=1$, а по модулю p это равенство принимает вид $nk\equiv 1$, т.е. число n обратно к k по модулю p. Таково же и число $n \mod p$. Иначе говоря, равенство $mp-nk=1$ позволяет найти обратный к остатку k остаток по модулю p.

Коэффициенты n,m можно найти методом цепных дробей. Например, пусть $p=101$, $k=77$. Найдем обратный к нему остаток. Для этого используем цепную дробь

$$\frac{101}{77}=1+\frac{1}{3+\frac{1}{5-\frac{1}{5}}}\approx 1+\frac{1}{3+\frac{1}{5}}=\frac{21}{16}.$$

откуда видим, что $77\cdot 21-101\cdot 16=1$. Поэтому $77\cdot 21\equiv 1 \pmod{101}$, т.е. остаток 21 обратен к 77.

При решении сравнений и доказательстве теорем о сравнениях часто очень полезен ***принцип Дирихле***: если $n+1$ шарик разложен по n ящикам, то по крайней мере в одном ящике есть как минимум два шарика.

В частности, среди m натуральных чисел либо одно из них делится на m, либо есть два такие, разность которых делится на m.

Задачи

13.1. Найти обратные остатки к $5, 9, 12, 25, 51, 88, 99, 100$ по модулю 101.

13.2. Найти (или доказать, что их не существует) обратные остатки к 10, 20, 30, 27, 51, 86 по модулю 2020. А по модулю 2021?

13.3. Докажите, что из любых n целых чисел всегда можно выбрать несколько, сумма которых делится на n (или одно число, делящееся на n).

13.4. Пусть m, n — целые, и $5m + 3n \vdots 11$. Докажите, что а) $6m + 8n \vdots 11$; б) $9m + n \vdots 11$.

13.5. Пусть в некоторой стране имеют хождение монеты достоинством только 14 и 23 тугрика. Продавец должен выдать сдачу покупателю в размере 1 тугрик. Считая, что у обоих имеется достаточное количество монет того и другого достоинства, указать способ, которым должен воспользоваться продавец для выдачи сдачи.

13.6. Найти цепную дробь для $\sqrt{3}$.

13.7. С помощью цепной дроби найти дробь

$$\frac{k}{r} \in \left[\frac{165}{256} - \frac{1}{512}; \frac{165}{256} + \frac{1}{512}\right]$$

при условии, что $r < 16$.

Еще задачи на остатки

13.8. Даны 20 целых чисел, ни одно из которых не делится на 5. Докажите, что сумма двадцатых степеней этих чисел делится на 5.

13.9. Число a даёт остаток 5 при делении на 9, число b даёт остаток 7 при делении на 9. Можно ли по этим данным определить, какой остаток дают числа $a + b$ и ab при делении на 9?

13.10. Докажите, что из любых 52 целых чисел всегда можно выбрать два таких числа, что ***а)*** их разность делится на 51; ***б)*** их сумма или разность делится на 100.

13.11. Докажите, что а) $\overline{aaa}$ делится на 37 (черта означает позиционную запись числа цифрами); б) $\overline{abc} - \overline{cba}$ делится на 99 (где a, b, c — цифры).

13.12. Сформулировать и доказать признаки делимости на 2, 4, 5, 8.

13.13. Из числа $\overline{a_n \dots a_1 a_0}$ вычли сумму его цифр $a_n + \dots + a_1 + a_0$. а) Докажите, что получилось число, кратное 9. б) Выведите отсюда признаки делимости на 3 и на 9.

13.14. **а)* Докажите, что для любого натурального N существует делящееся на N натуральное число, все цифры которого только 0 и 1. ***б)*** Найдётся ли такое число вида $1 \dots 10 \dots 0$?

13.15. *Шайка из K разбойников отобрала у купца мешок с N монетами. Каждая монета стоит целое число грошей. Оказалось, что какую монету ни отложи, оставшиеся монеты можно поделить между разбойниками так, что каждый получит одинаковую сумму. Докажите, что $N - 1$ делится на K.

УРОК 14

Основная теорема арифметики

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 14. Основная теорема арифметики. Часть 2.

Конспект: Глава 4, раздел 4.3 Простые числа и ОТА, Глава 8, раздел 8.1 Арифметика остатков, раздел 8.2 Свойства арифметики остатков.

Справочные сведения

Всякое положительное число N имеет единственное представление в виде

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

где $p_1, \dots, p_k$ — некоторые простые числа, целые $\alpha_1, \dots, \alpha_k > 0$.

НОД(a, b) — наибольшее целое число, одновременно делящее a и b, НОК(a, b) — наименьшее целое положительное число, одновременно делящееся на a и b.

Теорема Вильсона: если p — простое число, то $(p-1)! \equiv -1 \pmod{p}$.

Задачи

14.1. Написать на псевдоязыке алгоритм разложения числа по степеням простых.

14.2. *Оценить скорость алгоритма следующим образом: посчитать количество операций деления с остатком, производимых в ходе выполнения алгоритма.

14.3. Известно, что $n^2(m^2+1)(m+1) = 9999$ при некоторых целых n, m. Найдите эти числа.

14.4. Произведение возрастов Машиных братьев равно 1664. Младший из братьев вдвое моложе старшего. Сколько у Маши братьев?

14.5. Пусть a и b — натуральные числа, не делящиеся на 10, такие, что $ab = 10000$. Чему равна их сумма?

14.6. В силу ОТА будем записывать положительное натуральное число m как последовательность $\overline{m}$ степеней простых:

$$m = p_0^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k} \dots \iff \overline{m} = (\alpha_0, \alpha_1, \dots, \alpha_k, \dots),$$

где $p_0 < p_1 < p_2 < \dots$ — все простые числа, начиная с 2.

Докажите, что если $\overline{m} = (\alpha_0, \alpha_1, \dots, \alpha_k, \dots)$ и $\overline{n} = (\beta_0, \beta_1, \dots, \beta_k, \dots)$, то

$$\begin{aligned}
\overline{nm} &= (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \dots, \alpha_k + \beta_k, \dots) \\
\overline{\text{НОД}(n,m)} &= (\min(\alpha_0, \beta_0), \min(\alpha_1, \beta_1), \dots, \min(\alpha_k, \beta_k), \dots), \\
\overline{\text{НОК}(n,m)} &= (\max(\alpha_0, \beta_0), \max(\alpha_1, \beta_1), \dots, \max(\alpha_k, \beta_k), \dots).
\end{aligned}$$

14.7. Докажите, что НОД(n, m)НОК$(n, m) = nm$.

Задачи на делимость

14.8. Переставив цифры в числе N, получили в 3 раза меньшее число. Докажите, что $N \vdots 27$.

14.9. Верен ли такой признак делимости на 27: число делится на 27 тогда и только тогда, когда сумма его цифр делится на 27?

14.10. Запись числа N составлено из записей подряд идущих чисел от 19 до 92:

$$N = 19202122\ldots909192.$$

На какую максимальную степень тройки оно делится?

14.11. Докажите, что число $11\ldots11$, запись которого состоит из 3^n единиц, делится на 3^n.

14.12. Докажите, что число делится на 11 тогда и только тогда, когда сумма его цифр, стоящих в четных разрядах, и сумма его цифр, стоящих в нечетных разрядах, отличаются на число, кратное 11.

14.13. Может ли $n!$ оканчиваться ровно на 4 нуля? А ровно на 5 нулей?

14.14. Пусть p — простое число вида $4k+1$, и пусть $x = (2k)!$. Докажите, что $x^2 \equiv -1 \pmod{p}$.

14.15. Пусть p — простое число вида $4k+1$, и пусть x удовлетворяет сравнению $x^2 \equiv -1 \pmod{p}$. Докажите, что

a) $(a+xb)(a-xb) \equiv a^2+b^2 \pmod{p}$ при $a, b \in \mathbb{Z}$;
b) среди чисел вида $m+xn$, где $m, n \in \mathbb{Z}$, $0 \leqslant m, n \leqslant \lfloor\sqrt{p}\rfloor$, найдутся два с равными остатками от деления на p;
c) найдется ненулевое число $a+bx$, делящееся на p, где $a, b \in \mathbb{Z}$, причем $|a| < \sqrt{p}$ и $|b| < \sqrt{p}$;
d) p представимо в виде суммы двух квадратов целых чисел.

14.16. *Докажите, что существует бесконечно много натуральных чисел, не представимых как сумма трёх или менее точных квадратов.

УРОК 15

Следствия ОТА

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 15. Основная теорема арифметики. Следствия.
Конспект: Глава 4, раздел 4.2 Кузнечик НОД и алгоритм Евклида.

Справочные сведения

Кузнечик умеет прыгать одной ногой на a (в обе стороны), другой ногой — на b (в обе стороны). Здесь a, b — целые числа. Тогда он может попасть во все целые точки, кратные НОД(a, b), и только в них.

Лемма Евклида: если простое число p делит произведение целых чисел ab, то p делит a или p делит b.

Задачи

15.1. В какую ближайшую к нулю точку может попасть кузнечик, умеющий делать прыжки по числовой прямой длины 37 и 777, если он стартует в нуле?

15.2. Используя разложение на множители, решите уравнение:

$$n^3(n+1)^3 3 = 1728$$

15.3. Кузнечик делает по числовой прямой прыжки длины 11 и 1331. Укажите точки, в которых он может оказаться: 99, 999, 1, 11, 111.

15.4. Два кузнечика на числовой прямой, стартуя из нуля, могут совершать любые комбинации прыжков: первый — длины 16 и 28, а второй — длины 9 и 15. В какой ближайшей к нулю точке они могут встретиться?

15.5. При каком минимальном целом $n > 0$ уравнение $120n = x^3$ будет иметь целочисленное решение?

15.6. Доказать, что любое простое число $p > 3$ имеет вид $6k + 1$ или $6k + 5$.

15.7. Доказать, что квадрат простого числа $p > 3$ при делении на 12 дает остаток 1.

15.8. Доказать, что любое общее кратное чисел a и b делится на их НОК.

15.9. Про натуральные числа a и b известно, что их НОД равен 15, а НОД равен 840. Найти a и b.

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

15.11. Какие натуральные числа делятся на 30 и имеют ровно 20 положительных делителей?

15.12. Рассмотрим целое число $n > 0$. Докажите, что количество упорядоченных пар натуральных чисел (u, v) таких, что $\text{НОК}(a, b) = n$, равно количеству натуральных делителей у числа n^2.

15.13. Существуют ли целые x, y, для которых ***(а)*** $x^2 + y^2 = 99$? ***(b)*** $x^2 + y^2 = 33333$? (c) $x^2 + y^2 = 5600$?

15.14. ***(а)*** [Решето Эратосфена] Выпишем целые числа от 2 до n. Подчеркнём 2 и сотрём числа, кратные 2. Первое неподчёркнутое число подчеркнём и сотрём кратные ему, и т. д., пока каждое число от 2 до n не будет подчёркнуто или стёрто. Докажите, что мы подчеркнём в точности простые числа от 1 до n. ***(б)*** Пусть очередное число, которое мы хотим подчеркнуть, больше $\sqrt{n}$. Докажите, что нестёртые к этому моменту числа от 2 до n простые. ***(в)*** Какие числа, меньшие 100, простые?

15.15. Числа a, b, c, n натуральные, $\text{НОД}(a, b) = 1$, $ab = c^n$. Найдется ли такое целое x, что $a = x^n n$?

15.16. Решите в натуральных числах уравнение $x^{42} = y^{55}$.

15.17. Найдутся ли такие 10 разных целых чисел, ни одно из которых не квадрат целого числа, со свойством: квадратом целого числа будет произведение ***(а)*** любых двух из них; ***(б)*** любых трёх них?

15.18. Найдите разложение по степеням простых числа ***(а)*** 2021; ***(б)*** 17!; ***(в)*** $\binom{20}{10}$.

15.19. При каких натуральных k число $(k-1)!$ не делится на k?

15.20. ***(а)*** [Теорема Лежандра] Докажите, что простое число p входит в разложение по степеням простых числа $n!$ в степени $\lfloor n/p \rfloor + \lfloor n/p^2 2 \rfloor + \lfloor n/p^3 \rfloor + \ldots$ (где $\lfloor x \rfloor$ — это целая часть числа x). С какого момента слагаемые в этой сумме станут равными нулю? ***(б)*** Сколько у 2000! нулей в конце его десятичной записи? ***(в)*** Может ли $n!$ делиться на 2^n $(n \geqslant 1)$?

15.21. Докажите, что существует бесконечное число простых чисел вида ***(а)*** $3k + 2$; ***(б)*** $4k + 3$.

15.22. Сократить дробь $\frac{8547}{4144}$.

УРОК 16

Линейные уравнения в целых числах

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 16. Решение линейных уравнений в целых числах. Часть 1.
Конспект: Глава 6, раздел 6.2 Линейные уравнения в целых числах.

Справочные сведения

Уравнение вида $ax + by = c$, где a, b, c — некоторые целые числа, а x, y — переменные, пробегающие целые числа, называется линейным уравнением в целых числах. Задача: отыскать все возможные пары (x, y), удовлетворяющие данному уравнению.

Шаг 1. Находим НОД(a, b) и проверяем, делится ли c на НОД(a, b). Если не делится, то решений нет.

Шаг 2. Если делится, то сокращаем все уравнение на НОД(a, b), получаем эквивалентное уравнение такого же вида, только с условием НОД$(a, b) = 1$.

Шаг 3. Ищем общее решение однородного уравнения: $ax + by = 0$ (здесь уже считаем НОД$(a, b) = 1$). Это решение имеет вид

$$x = bk, \quad y = -ak, \quad k \in \mathbb{Z}.$$

Шаг 4. Ищем частное решение уравнения $ax + by = 1$ (например, с помощью цепной дроби для a/b). Это решение существует в силу алгоритма Евклида. Обозначим это решение за (x_0, y_0). Тогда (x_0c, y_0c) будет частным решением уравнения $ax + by = c$.

Шаг 5. Общее решение уравнения $ax + by = c$ (НОД$(a, b) = 1$) записывается в виде

$$x = bk + x_0c, \quad y = -ak + y_0c, \quad k \in \mathbb{Z}.$$

Задачи

16.1. Решите в целых числах уравнения:

a) $6x - 5y = 0$;
b) $6x - 6y = 2$;
c) $6x - 5y = 3$;
d) $4x + 7y = 41$;
e) $7x - 5y = 21$;
f) $19x + 17y = 15$.

16.2. Найти все решения линейного уравнения в целых числах или доказать что их нет: ***(а)*** $5x - 9y = 2$; ***(б)*** $225x + 81y = 18$; ***(в)*** $10x - 18y = 3$.

16.3. Решите уравнения: ***(а)*** $121x + 91y = 1$; ***(б)*** $-343x + 119y = 42$; ***(в)*** $111x - 740y = 11$.

16.4. Разложить в цепную дробь числа ***(а)*** 15/4; ***(б)*** 42/31; ***(в)*** 13/9; ***(г)*** 6/5.

16.5. Используя разложение в цепную дробь решить уравнение в целых числах ***(а)*** $57x - 89y = 16$; ***(б)*** $13x - 10y = 27$.

16.6. Докажите, что уравнение $ax + by = d$ имеет решение в целых числах тогда и только тогда, когда НОД$(a, b)|d$. В частности, НОД(a, b) — это наименьшее натуральное число, представимое в виде $ax + by$.

16.7. Кузнечик может прыгать на расстояние 15 и 7. Изначально он находится в точке 0. ***(а)*** Найдите, как следует прыгать кузнечику, чтобы оказаться в точке 3. ***(б)*** Найдите, за какое наименьшее число прыжков он может попасть в точку 6;

16.8. Пусть (x_0, y_0) — решение уравнения $ax + by = d$. Пусть a_0 и b_0 — такие числа, что НОД$(a, b)a_0 = a$, НОД$(a, b)b_0 = b$. Покажите, что каждое решение уравнения $ax + by = d$ имеет вид $x = x_0 + b_0 \cdot t$, $y = y_0 - a_0 \cdot t$, где t — целое число.

16.9. Известно, что пары чисел (x_1, y_1) и (x_2, y_2) являются решением уравнения $ax + by + c = 0$, где a, b, c — некоторые неизвестные целые коэффициенты. Найдите, выразив через (x_1, y_1) и (x_2, y_2), чему равно a/b.

16.10. Решите в целых числах уравнение $2x + 3y + 5z = 1$.

16.11. Доказать, что уравнение $ax + by = ab$, где $a, b > 0$ и НОД$(a, b) = 1$, неразрешимо в натуральных числах.

УРОК 17

Алгоритм Евклида

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 17. Решение линейных уравнений в целых числах. Часть 2.
Конспект: Глава 6, раздел 6.2 Линейные уравнения в целых числах.

Справочные сведения

Алгоритм Евклида последовательного деления с остатком. Пусть даны целые числа a и b, причем $a > b > 0$. Делим a/b с остатком:

$$a = bk_0 + r_0, \quad 0 \leqslant r_0 < b.$$

Далее делим b/r_0 с остатком, получаем равенство $b = r_0k_1 + r_1$, где $0 \leqslant r_1 < r_0$. Затем делим с остатком r_0 на r_1, и так далее. То есть делим каждый предыдущий остаток на текущий. Рано или поздно мы получим $r_n = 0$, на этом алгоритм останавливается.

При этом, последний ненулевой остаток есть не что иное как НОД(a, b). Если сразу же получаем $r_0 = 0$, то НОД$(a, b) = b$.

Затем можно начать раскручивать полученные равенства в обратном направлении, чтобы выразить НОД(a, b) через a и b. Отсюда получаем представление

$$\text{НОД}(a, b) = an + bm, \quad n, m \in \mathbb{Z}.$$

Например, найдем НОД$(16, 6)$ и его линейное представление.

$$\begin{aligned} 16 &= 6 \cdot 2 + 4 \\ 6 &= 4 \cdot 1 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

Отсюда НОД$(16, 6) = 2$. Из второго равенства получаем, что $2 = 6 - 4 \cdot 1$, куда подставляем 4, и получаем

$$2 = 6 - (16 - 6 \cdot 2) \cdot 1 = 16 \cdot (-1) + 6 \cdot 3,$$

т.е. $n = -1, m = 3$.

Задачи

17.1. Написать реализацию алгоритма Евклида на псевдоязыке программирования. А также алгоритм, выводящий линейное представление НОД через исходные два числа.

17.2. Вычислите при помощи алгоритма Евклида: ***(а)*** НОД$(91, 147)$; ***(б)*** НОД$(-144, -233)$; ***(в)*** НОД$(525, 231)$; ***(г)*** НОД$(7\,777\,777, 7\,777)$; ***(д)*** НОД$(10946, 17711)$; ***(е)*** НОД$(2^m - 1, 2^n - 1)$.

17.3. Доказать, что все остатки r_k в алгоритме Евклида можно представить в виде линейной комбинации $ax + by$, подобрав подходящие целые x, y.

17.4. Покажите, как при помощи алгоритма Евклида можно по произвольным a и b найти такие k и l, что $ak + bl = \text{НОД}(a, b)$.

17.5. Найти линейное представление НОД с помощью алгоритма Евклида и методом цепных дробей:

$$\text{НОД}(5, 9), \quad \text{НОД}(18, 15), \quad \text{НОД}(225, 81).$$

17.6. Доказать, что алгоритм Евклида, описанный выше, завершается за конечное число шагов для любых стартовых целых положительных чисел a и b.

17.7. Докажите, что $\text{НОД}(a, b)$ делится на любой общий делитель чисел a и b.

17.8. С помощью представления НОД в виде линейной комбинации исходных чисел докажите, что если $\text{НОД}(a, b) = 1$ и $ac \vdots b$, то $c \vdots b$.

17.9. Какие расстояния можно отложить от данной точки на прямой, пользуясь двумя шаблонами (без делений) длины a см и b см (где $\text{НОД}(a, b) = d$)?

УРОК 18

Метод цепных дробей

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 18. Метод цепных дорбей.

Конспект: Глава 6, раздел 6.2 Линейные уравнения в целых числах, Глава 7, раздел 7.2 Соизмеримость. Иррациональности.

Справочные сведения

Равенства, используемые в алгоритме Евклида, соберем в одно выражение для исходной дроби a/b, введя обозначения $a = r_0$, $b = r_1$.

$$\frac{r_0}{r_1} = \frac{k_1 r_1 + r_2}{r_1} = \boxed{k_1} + \frac{1}{\frac{r_1}{r_2}} = \boxed{k_1} + \frac{1}{\frac{k_2 r_2 + r_3}{r_2}} =$$

$$= \boxed{k_1} + \frac{1}{\boxed{k_2} + \frac{1}{r_3/r_2}} = \boxed{k_1} + \frac{1}{\boxed{k_2} + \frac{1}{\boxed{k_3} + \ddots \frac{1}{\boxed{k_n} + r_{n+1}/r_n}}},$$

где $r_0 > r_1 > r_2 > \cdots > r_n > r_{n-1}$.

Такле разложение называется ***цепной дробью***.

Разложение дроби a/b в цепную дробь конечно тогда и только тогда, когда дробь a/b рациональна, т.е. числа a и b *соизмеримы*.

Цепная дробь помогает решать линейные уравнения вида $ax + by =$ в целых числах.

Пусть дано уравнение

$$112x - 34y = 16.$$

Предположим, что мы не знаем НОД(112,34), и не будем сокращать на него уравнение.

Ищем приближение дроби $112/34$ следующим способом:

$$\frac{112}{34} = 3 + \frac{10}{34} = 3 + \frac{1}{3 + \frac{4}{10}} = 3 + \frac{1}{3 + \frac{1}{2+2/4}} = 3 + \frac{1}{3 + \frac{1}{2+1/2}}$$

Как только мы дошли до хвоста вида $1/k$, мы останавливаемся, отбрасываем этот хвост и сворачиваем дробь обратно, получая приближение исходной дроби:

$$\frac{112}{34} \approx 3 + \frac{1}{3 + \frac{1}{2}} = \frac{23}{7}.$$

Далее, перемножая накрест эти дроби, получаем представление для НОД:

$$\text{НОД}(112, 34) = 112 \cdot 7 - 34 \cdot 23 = 2.$$

Таким образом, мы нашли НОД(112,34) и одновременно — коэффициенты для общего и частного решения.

Искомые коэффициенты: $n = 7$, $m = 23$. Общее решение уравнения, таким образом, получаем в виде

$$\begin{cases} x = (34/2)k + (16/2) \cdot 7, \\ y = (112/2)k + (16/2) \cdot 23, \end{cases}$$

где k — любое целое число.

Задачи

18.1. Разложить в цепную дробь отношения: 36/25, 111/34, 12/8, 1024/333.

18.2. Решить уравнение в целых числах методом цепных дробей: $100x+77y = 1$, $355x+113y = 1$, $271x - 100y = 7$, $707x + 500x = 10$.

18.3. Маша продавала на школьной ярмарке плетеные мандалы по 135 рублей, а потом купила несколько фенечек по 40 рублей, после чего у нее осталось 5 рублей. Пользуясь методом цепных дробей, найдите, сколько фенечек купила Маша.

18.4. ***(а)*** В фирме 28 служащих с большим стажем и 37 — с маленьким. Хозяин фирмы выделил некую сумму для подарков служащим на Новый год. Бухгалтер подсчитал, что есть только один способ разделить деньги так, чтобы все служащие с большим стажем получили поровну и все с маленьким — тоже поровну (все получают целое число рублей, большее 0). Какую наименьшую и какую наибольшую сумму мог выделить хозяин на подарки? ***(б)**** А если ещё требуется, чтобы служащий с большим стажем получил больше денег, чем служащий с маленьким стажем?

18.5. Натуральные числа a и b взаимно просты. Докажите, что уравнение $ax + by = c$

a) при любом целом c имеет такое решение в целых числах x и y, что $0 \leqslant x < b$;
b) имеет решение в *целых неотрицательных* числах x и y, если c целое, большее $ab-a-b$;
c) *при целых c от 0 до $ab-a-b$ ровно в половине случаев имеет целое неотрицательное решение, причем если для $c = c_0$ такое решение есть, то для $c = ab - a - b - c_0$ таких решений нет.

18.6. *Слонопотам типа (p, q) ходит по бесконечной клетчатой доске, сдвигаясь за ход на p клеток по любому направлению «горизонталь-вертикаль» и на q клеток по перпендикулярному. (Шахматный конь — слонопотам типа $(1, 2)$.) Какие слонопотамы могут попасть на соседнее с собой поле? m + 179n

18.7. *Натуральные числа m и n взаимно просты. Известно, что дробь $\dfrac{m + 179n}{179m + n}$ можно сократить на число k. Каково наибольшее возможное значение k?

18.8. *Есть шоколадка в форме равностороннего треугольника со стороной n, разделенная бороздками на равносторонние треугольники со стороной 1. Играют двое. За ход можно отломить от шоколадки треугольный кусок вдоль бороздки, съесть его, а остаток передать противнику. Тот, кто получит последний кусок — треугольник со стороной 1, — победитель. Тот, кто не может сделать ход, досрочно проигрывает. Кто выигрывает при правильной игре?

УРОК 19

Итоги арифметических исследований

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 19. Итоги арифметических исследований. Часть 1..

Конспект: Глава 6, раздел 6.2 Линейные уравнения в целых числах, Глава 7, раздел 7.2 Соизмеримость. Иррациональности.

Справочные сведения

Линейное уравнение $ax+by+c=0$ можно решать в целых числах, даже если коэффициенты a, b, c не являются целыми.

Отрезки a и b называются *соизмеримыми*, если существует третий отрезок c, который укладывается в a и в b целое число раз без остатка, т.е. $a = cn$ и $b = cm$ для некоторых натуральных n, m.

Обобщение линейного уравнения в целых числах:

19.1. уравнение с рациональными коэффициентами $ax + bx + c = 0$ — сводится к уравнению в целых числах, если все коэффициенты умножить на общий знаменатель;

19.2. уравнение $ax + bx + c = 0$ с соизмеримыми коэффициентами a и b — сводится к случаю уравнения в целых числах, если c также соизмеримо с a (или с b), и не имеет решений в противном случае.

В обоих случаях мы ищем решение (x, y) с целыми координатами x и y.

Задачи

19.1. При каком c прямая $ax + (\sqrt{3})y + c = 0$ пройдет через рациональную точку (x, y)?

19.2. Решить уравнение $(\sqrt{3})x - (\sqrt{12})y = \sqrt{75}$ в целых числах.

19.3. Имеет ли решения в целых числах следующее уравнения: $x\sqrt{6} + y\sqrt{24} = \sqrt{12}$?

19.4. Сколько решений в заисимости от c может иметь уравнение $x + y\sqrt{3} = c$?

19.5. Методом цепных дробей найти наилучшее приближение с точностью до 0.001 следующих иррацинальных чисел: $\sqrt{2}, \sqrt{3}, \sqrt{5}$.

19.6. Английский ярд составляет 0.914383 метра. Найти приближенное отношение метра к ярду.

19.7. Год равен 365.2422 суткам. Разложить эту дробь в цепную и найти первые четыре подходящие дроби.

19.8. Разность между последней и предпоследней подходящими дробями равна $1/42$. Подберите два-три набора пар чисел, которые могли бы быть, соответственно, числителями и знаменателями этих подходящих дробей.

19.9. Разложите в цепную дробь число $43/40$. Найдите все ее подходящие дроби. Чему равна разность между последгней и предпоследней дробями?

19.10. Решить уравнения в целых числах

a) $12x = 42y$;
b) $ax + by = 0$, где НОД$(a, b) = d$;
c) $2x + 3y = 1$;
d) $4x + 6y = 2$;
e) $4x + 6y = 5$;
f) $20x + 21y = 2021$.

УРОК 20

Делимость и простые числа

Связь с онлайн курсом и главами конспекта:

«Дети и наука»: Урок 20. Итоги арифметических исследований. Часть 2..
Конспект: Глава 4, раздел 4.3 Простые числа и ОТА.

Справочные сведения

Количество положительных делителей числа m обозначим за $\tau(m)$.

Сумму всех положительных делителей числа m обозначим за $\sigma(m)$.

Количество всех положительных чисел, меньших m и взаимно простых с m, обозначим за $\varphi(m)$.

Теорема Эйлера: если a и m взаимно просты, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Задачи

20.1. Найти $\tau(p^k)$, где p — простое число. Верно ли, что $\tau(ab) = \tau(a)\tau(b)$ при условии НОД$(a, b) = 1$. Найти $\tau(n)$, если

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

— разложение числа n по степеням простых.

20.2. Напишите на псевдоязыке алгоритм вычисления $\tau(n)$ для любого положительного целого числа.

20.3. Найти $\sigma(p^k)$, где p — простое число, k — целое положительное, $\sigma(m)$ — сумма всех положительных делителей числа m. Верно ли, что $\sigma(ab) = \sigma(a)\sigma(b)$ при условии НОД$(a, b) = 1$? Найдите $\sigma(n)$, где

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

— разложение числа n по степеням простых.

20.4. Натуральное число называется ***совершенным***, если сумма всех его делителей, меньших его, равно ему самому. Например, 6 и 28 — совершенные числа. Докажите, что число $2^{n-1}(2^n - 1)$ будет совершенным, если $2^n - 1$ — простое число.

20.5. Напишите на псевдоязыке алгоритм вычисления $\sigma(n)$ для любого положительного целого числа.

20.6. Вычислите значения функций φ, τ и σ для чисел 999, 512, 5!.

20.7. Напишите на псевдоязыке алгоритм вычисления $\varphi(n)$ для любого положительного целого числа.

20.8. Доказать, что $2^n - 1$ кратно трем тогда и только тогда, когда n — четное, и $2^n + 1$ кратно трем тогда и только тогда, когда n — нечетное.

20.9. Доказать, что если $2^n + 1$ — простое число, то n является степенью двойки.

20.10. Докажите, что

$$\text{НОД}(kn, km) = k\text{НОД}(n, m), \quad \text{НОК}(kn, km) = k\text{НОК}(n, m).$$

20.11. Написать алгоритм вычисления последней десятичной цифры выражения a^b на основе последней цифры числа a и представления числа b в виде $b = 4k + r$.

20.12. Найдите совершенное число, кратное 16.

20.13. Сколько существует различных разложений в виде суммы двух простых чисел для числа 22?

20.14. Пифагор назвал содружественными числа a и b такие, что a является суммой всех делителей числа b (без самого числа b), а число b является суммой всех делителей числа a (без самого числа a). Найдите число, содружественное числу 220.

20.15. Боб хочет послать Алисе сообщение, выраженное числом m. На этот раз они используют алгоритм шифрования RSA.

RSA устроен так.

A1) Берем некоторое большое число N (все сообщения должны быть остатками по модулю N), которое плохо раскладывается на простые множители (например, полупростое, т.е. $N = pq$, где p, q — большие числа, обычно 1024 или 2048-битные).
A2) Берем также некоторое число $e < \varphi(N)$, взаимно простое с $\varphi(N)$.
A3) Находим $d = e^{-1}$ по модулю $\varphi(N)$, т.е. такое, что $e \cdot d \equiv 1 \pmod{\varphi(N)}$.
A4) Пара (e, N) называется *открытым ключом*, пара (d, N) — *закрытым*.
A5) Сообщение m, которое должно быть взаимно просто с N, кодируем числом $m_1 = m^e \pmod{N}$.
A6) Чтобы расшифровать сообщение, пользуемся закрытым ключом d:

$$m_1^d = m^{e \cdot d} = m^{\varphi(N)k+1} \equiv m \pmod{N}$$

в силу теоремы Эйлера.

Алиса и Боб заранее обмениваются закрытым ключом d. Сообщение m пересылается в зашифрованном виде Алисе, а вместе с ним открытый ключ ($e = 53, N = 299$). Зашифрованное сообщение $m^e \pmod{N}$ равно числу 171. Эти данные (открытый ключ и кодированное сообщение) перехватывает Ева.

Опишите действия Евы по расшифровке сообщения m и найдите число m.