ВВЕДЕНИЕ В МАТЕМАТИКУ

листки с задачами
«100 урокам математики» Алексея Савватеева

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

Москва, 2021

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.

Сайт проекта: savvateev.xyz

24 февраля 2021 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).

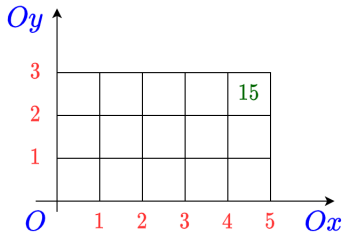


Рис. 1.1: Произведение $5 \cdot 3$.

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. 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.

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

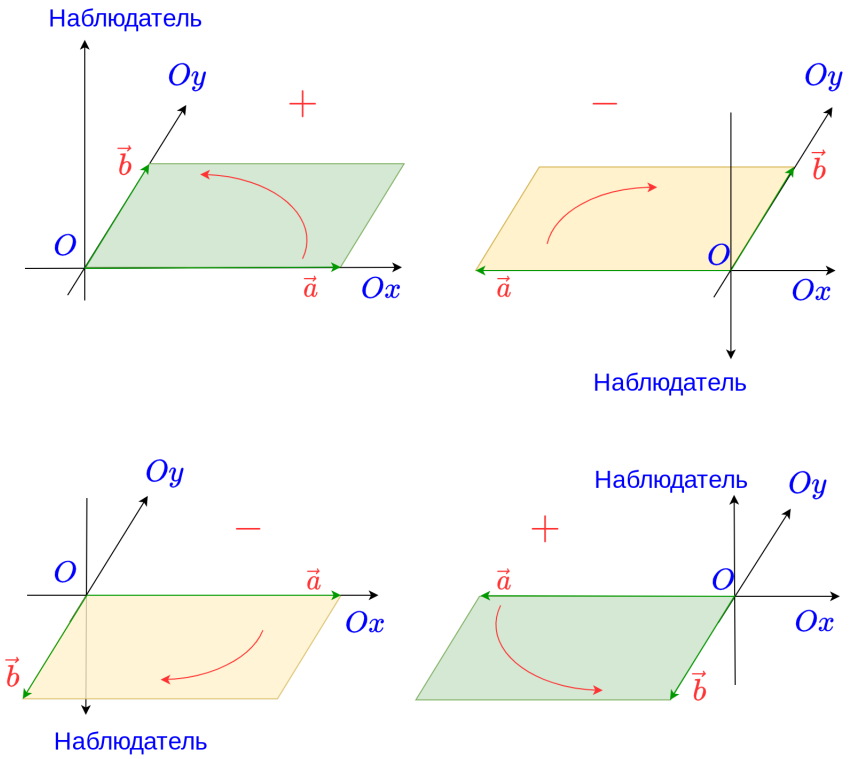


Рис. 1.2: произведение $a \cdot b$.

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

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 $-2+7$, $10-5$, $11-2-4$, $-8+3+10$.

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.

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 $-2+7$, $10-5$, $11-2-4$, $-8+3+10$?

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).

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).

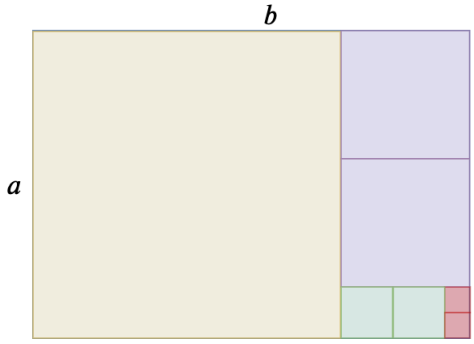


Рис. 2.1: Графический алгоритм Евклида.

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

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

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

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?

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

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?

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

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

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.

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

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

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

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

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

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

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).

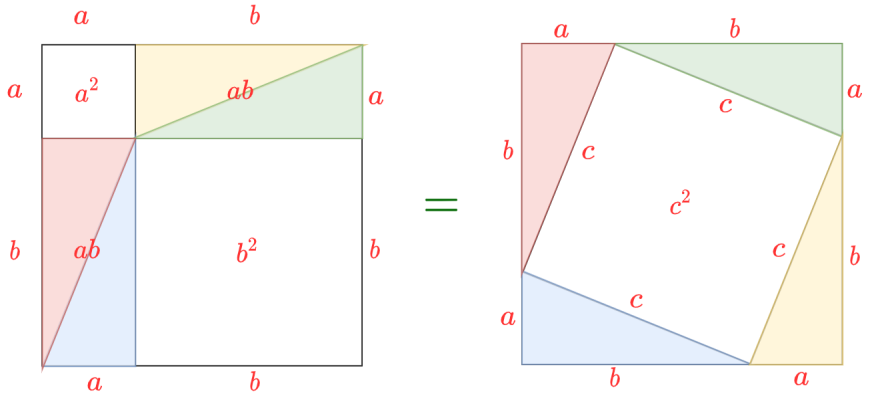


Рис. 3.1: $(a+b)^2 = a^2 + 2ab + b^2$ и $a^2 + b^2 = c^2$.

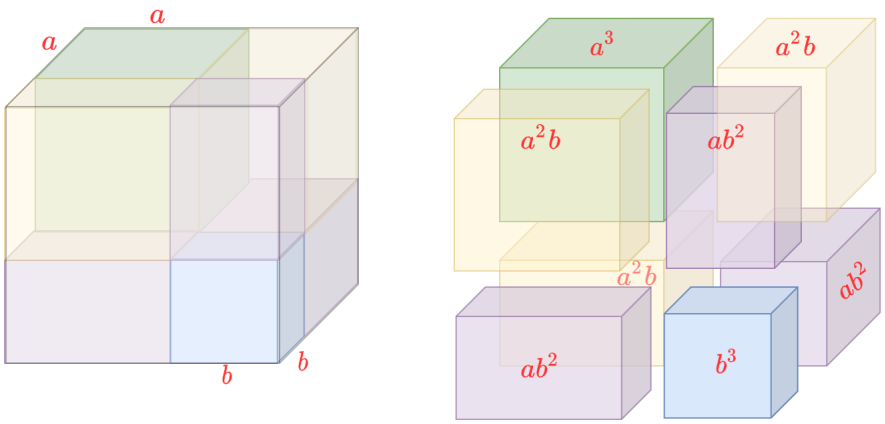


Рис. 3.2: $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^2$.

Задачи

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

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

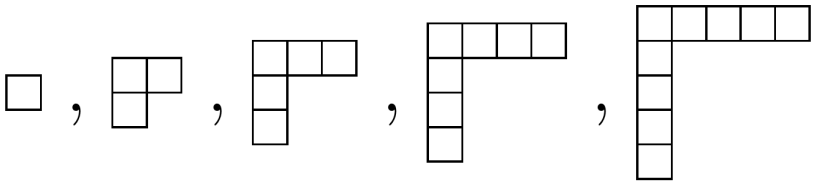
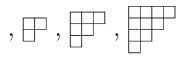


Рис. 3.3

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

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 $T_{n+m} = T_n + T_m + nm$.

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

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

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

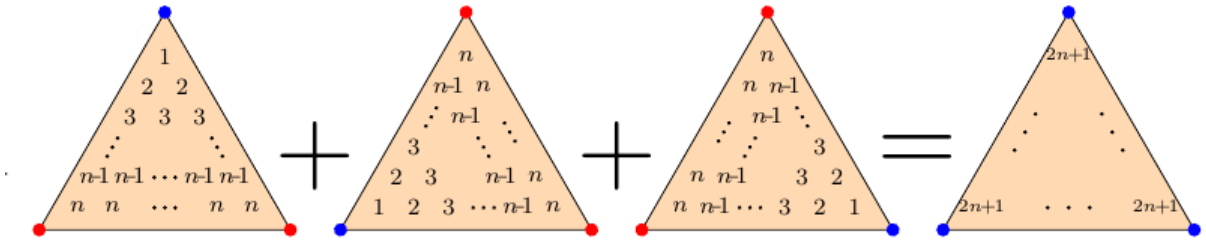


Рис. 3.4

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

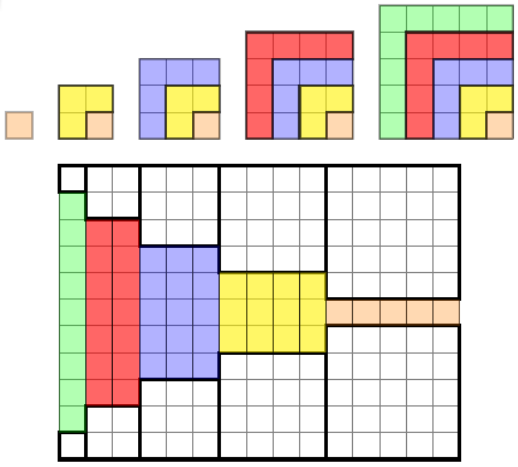


Рис. 3.5

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.

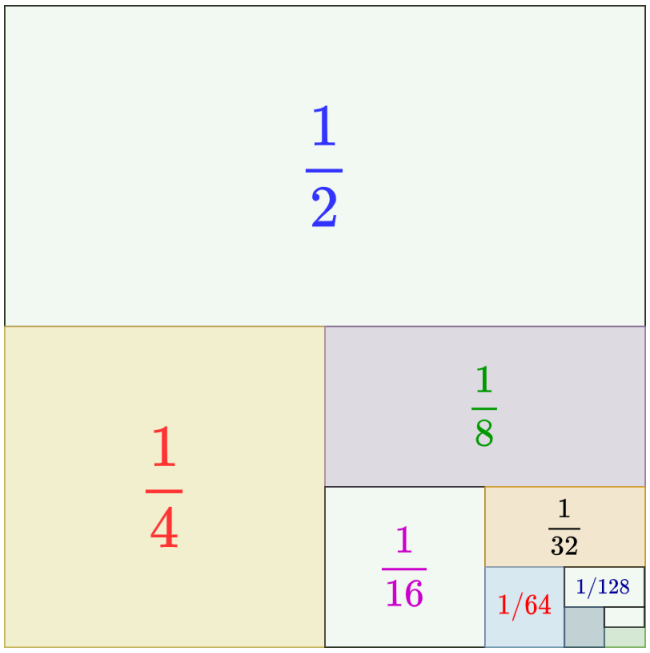


Рис. 4.1

Задачи

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) $\dfrac{1}{0.99} + \dfrac{1}{0.99^2} + \dfrac{1}{0.99^3} + \dots$.

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) $1 + \dfrac{2}{3} + \dfrac{3}{5} + \dfrac{5}{9} + \dots + \dfrac{n}{2n-1} + \dots$.

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. 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).

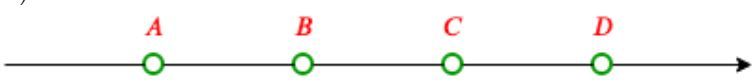


Рис. 5.1

1. Куда перейдет точка A при отражении S_B?
2. Куда перейдут точки B, C, D при преобразовании $T_{AB} \circ T_{CA}$?

3. Куда перейдут точки A, B, C при преобразовании $S_C \circ T_{AB}$?
4. Какое движение переводит A в C и B в D?
5. Существует ли движение, которое переводит A в B и B в D?
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.

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

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

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?

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

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. 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.

1. Какое движение получится при композиции

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

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

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.

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

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

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

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.

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

1. Доказать, что $\pi > 3$.
2. Пусть G — движение окружности. Сколько у G может быть неподвижных точек (имеется ввиду общее количество, найдите все возможные варианты)?
3. Пусть G — движение окружности. Известно, что $G(A) = A$ и $G(B) \neq B$. Какой вид может иметь G?
4. Пусть диаметры l и k перпендикулярны. Найдите $S_l \circ S_k$.
5. Известно, что точка A переходит при движении G окружности в точку A', диаметрально противоположную точке A. Каким может быть движение G?
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

1. Центральная симметрия — это какое движение?
2. Композицией каких отражений можно выразить центральную симметрию?
3. С помощью отражения относительно оси Ox (горизонтальной оси) и вращений выразить отражение относительно оси Oy (вертикальной оси).
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 $\varphi = \pi/2$, $\varphi = \pi$, $\pi = 2\pi$?
5. Построить поворот на угол 90^o при помощи двух отражений.
6. При каких n поворот на угол $n\varphi$ выражается в виде композиций S_0 и S_φ?
7. Пусть G и Q — движения окружности, причем $G \circ Q = Q \circ G$. Какими могут быть G и Q?
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 операцией называется *группой*, если:

G0 $a \circ b \in G$ для всех $a, b \in G$ (группоид);

G1 для любых $a, b, c \in G$ имеем тождество $(a \circ b) \circ c = a \circ (b \circ c)$ (ассоциативность);

G2 существует элемент $\mathrm{id} \in G$ такой, что $a \circ \mathrm{id} = \mathrm{id} \circ a = a$ для всех $a \in G$ (единица);

G3 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:

1. тривиальная подгруппа $\{\mathrm{id}\}$;
2. группа поворотов правильного n-угольника (включая случай вырожденного 2-угольника);
3. подгруппа одного отражения $\{\mathrm{id}, S_\varphi\}$;
4. группа движений правильного n-угольника (включает повороты, совмещающие углы многоугольника, и отражения относительно осей, проходящих через его вершины и центр окружности).

Задачи

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

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

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

	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						

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 $F \circ G$.

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.

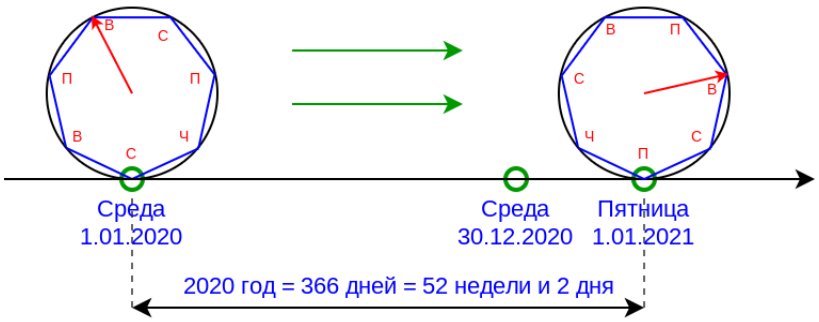


Рис. 11.1: Арифметика остатков по модулю 7.

Задачи

1. Отметить на числовой оси целые числа, которые при делении на 7 дают остаток 2 (на рисунке должны поместиться числа от -20 до 20).
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.)
3. Одному брату 6 лет, другому — 10. Значит, сумма из возрастов четная. Какой она будет в следующем году?
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)?
5. Найти день недели через месяц, квартал, полгода и год, отправляясь от текущей даты.
6. Поезд Москва–Владивосток отправляется из Москвы в 7:00 и находится в пути 166 часов. Определите время прибытия (московское) поезда во Владивосток.
7. Построить таблицы сложения для модулей: 2,3,4,5,6,10,11.
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.
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?
10. Что означает запись $a \equiv b \pmod 0$?
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).

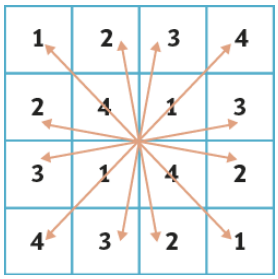


Рис. 12.1: Умножение по модулю 5.

Задачи

1. Целое положительное число увеличили на 1. Могла ли сумма его цифр (а) возрасти на 8? (б)Уменьшиться на 8? (в) Уменьшиться на 10?
2. Какие остатки может давать точный квадрат при делении на 4?
3. Последняя цифра точного квадрата равна 6. Доказать, что его предпоследняя цифра нечётна.
4. Остаток от деления простого числа на 30 — простое число или 1. Почему?
5. Какое наибольшее число различных целых чисел можно выбрать, если требуется, чтобы сумма и разность любых двух из них не делились на 15?
6. На какую цифру оканчивается число $33^{77} + 77^{33}$?
7. Могут ли среди m последовательных целых чисел какие-то два иметь равные остатки от деления на m?
8. Пусть $5x \equiv 6 \pmod 8$. Найти x.
9. Найти последнюю цифру 7^{100}, 7^{1942}.
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: $ka \equiv kb \pmod m$.

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

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

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

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

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

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

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

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

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

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

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

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?

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

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

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.)

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

1. Найти обратные остатки к $5, 9, 12, 25, 51, 88, 99, 100$ по модулю 101.
2. Найти (или доказать, что их не существует) обратные остатки к 10, 20, 30, 27, 51, 86 по модулю 2020. А по модулю 2021?
3. Докажите, что из любых n целых чисел всегда можно выбрать несколько, сумма которых делится на n (или одно число, делящееся на n).
4. Пусть m, n — целые, и $5m + 3n \vdots 11$. Докажите, что а) $6m + 8n \vdots 11$; б) $9m + n \vdots 11$.
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.
6. Найти цепную дробь для $\sqrt{3}$.
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

8. Даны 20 целых чисел, ни одно из которых не делится на 5. Докажите, что сумма двадцатых степеней этих чисел делится на 5.
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?
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.
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).
12. Сформулировать и доказать признаки делимости на 2, 4, 5, 8.
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.
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 $1 \dots 10 \dots 0$?
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

1. Написать на псевдоязыке алгоритм разложения числа по степеням простых.
2. *Оценить скорость алгоритма следующим образом: посчитать количество операций деления с остатком, производимых в ходе выполнения алгоритма.
3. Известно, что $n^2(m^2+1)(m+1) = 9999$ при некоторых целых n, m. Найдите эти числа.
4. Произведение возрастов Машиных братьев равно 1664. Младший из братьев вдвое моложе старшего. Сколько у Маши братьев?
5. Пусть a и b — натуральные числа, не делящиеся на 10, такие, что $ab = 10000$. Чему равна их сумма?
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

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

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

Задачи на делимость

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

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

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

$$N = 19202122\ldots909192.$$

На какую максимальную степень тройки оно делится?

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

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.

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

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

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 значений выражения $m+xn$, где $m, n \in \mathbb{Z}$, $0 \leqslant m, n \leqslant \lfloor\sqrt{p}\rfloor$, найдутся два различных 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.

16. **a)** Пусть p простое и имеет вид $4k+3$. Найдется ли такое целое x, что $x^2 \equiv -1 \pmod{p}$? **b)** Докажите, что если x^2+1 делится на нечетное простое число p, то p имеет вид $4k+1$. **c)** Докажите, что простых чисел вида $4k+1$ бесконечно много. **d)** Пусть p простое и имеет вид $4k+1$. Найдите такое целое x, что $x^2 \equiv -1 \pmod{p}$.

17. *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

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?

2. Используя разложение на множители, решите уравнение:

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

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

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?

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

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

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

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

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

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

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

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.

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

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

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

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?

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

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

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 $(n \geqslant 1)$?

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

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

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) $19x + 17y = 15$.

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

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

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

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

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

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;

8. Пусть (x_0, y_0) — решение уравнения $ax + by = d$. Пусть a_0 и b_0 — такие числа, что $\text{НОД}(a, b)a_0 = a$, $\text{НОД}(a, b)b_0 = b$. 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.

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.

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

11. Доказать, что уравнение $ax + by = ab$, где $a, b > 0$ и $\text{НОД}(a, b) = 1$, 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

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

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$(2^m - 1, 2^n - 1)$.

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

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

5. Найти линейное представление НОД с помощью алгоритма Евклида и методом цепных дробей:
$$\text{НОД}(5, 9), \quad \text{НОД}(18, 15), \quad \text{НОД}(225, 81).$$

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

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

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

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

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

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

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.

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?

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.

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

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?

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:

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

1. При каком c прямая $ax + (\sqrt{3})y + c = 0$ пройдет через рациональную точку (x, y)?
2. Решить уравнение $(\sqrt{3})x - (\sqrt{12})y = \sqrt{75}$ в целых числах.
3. Имеет ли решения в целых числах следующее уравнения: $x\sqrt{6} + y\sqrt{24} = \sqrt{12}$?
4. Сколько решений в заисимости от c может иметь уравнение $x + y\sqrt{3} = c$?
5. Методом цепных дробей найти наилучшее приближение с точностью до 0.001 следующих иррацинальных чисел: $\sqrt{2}, \sqrt{3}, \sqrt{5}$.
6. Английский ярд составляет 0.914383 метра. Найти приближенное отношение метра к ярду.
7. Год равен 365.2422 суткам. Разложить эту дробь в цепную и найти первые четыре подходящие дроби.

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.

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

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

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.

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

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.

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.

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

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

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

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.

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

10. Докажите, что

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

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

12. Найдите совершенное число, кратное 16.

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

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.

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.

УРОК 21

Перестановки: первые шаги

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.2 Обозначения перестановок.

Справочные сведения

Перестановкой на множестве $\{1, \ldots, n\}$ называется всякое взаимно однозначное отображение этого множества в себя. Через S_n обозначим множество всех таких перестановок. Вместо чисел можно использовать любые другие n различных символов, объектов, фигур, но кодировать их проще всего числами от 1 до n.

Развернутая запись перестановки:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

где α_k — те же числа $1, \ldots, n$, только, возможно, в другом порядке.

Сокращенная запись через циклы:

$$\alpha = (\alpha_{11} \ldots \alpha_{1k_1}) \ldots (\alpha_{l1} \ldots \alpha_{lk_l}).$$

Цикл $(\alpha_{11} \ldots \alpha_{1k_1})$ следует читать слева направо: символ α_{11} переходит под действием перестановки α в символ α_{12}, который, в свою очередь, — в символ α_{13}, и т.д., а последний символ α_{1k_1} — в начальный символ α_{11}.

Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} = (142)(3)(5)$$

Циклы, состоящие из одного элемента обычно пропускаются, так что

$$(142)(3)(5) = (142).$$

Композиция перестановок $\alpha\beta$ — это перестановка, которая получается последовательным применением сначала перестановки β, а затем, к ее результату, — перестановки α. Например,

$$(123)(45)(135)(24) = (1)(25)(34) = (25)(34).$$

Перестановка вида (ij), где $i \neq j$, называется *транспозицией*.

Минимальное натуральное k такое, что α^k — тождественная перестановка, называется *порядком* перестановки α и обозначается $\operatorname{Ord} \alpha$.

Задачи

1. Докажите, что множество S_n содержит $n!$ элементов.

2. **a)** Сколько существует перестановок чисел $1, 2, \ldots, 5$? Сколько из них оставляют число 1 на месте? **b)** Сколько из них переводят 1 в 5? **c)** Для скольких из них $\sigma(1) < \sigma(2)$? **d)** Для скольких из них $\sigma(1) < \sigma(2) < \sigma(3)$?

3. Перед Петей на столе лежат в ряд n шариков, пронумерованные по порядку числами от 1 до n. Петя переставил местами шарики. Пусть α сопоставляет числу k число $\alpha(k)$ — номер места в ряду, на котором оказался шарик под номером k. **a)** Покажите, что α — перестановка из S_n. **b)** Затем Петя повторил движения рук (опять переставил шарики, даже не глядя на них). На этот раз шарик под номером k оказался на месте под номером $\beta(k)$. Выразите перестановку β через перестановку α.

4. Вычислить следующие перестановки:

   a) $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ **b)** $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ **c)** $\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&4&1&2\end{pmatrix}$

   d) $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}^2$ **e)** $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}^3$ **f)** $\begin{pmatrix}3&5&6&1&2&7&9&4&8\\1&2&3&4&5&6&7&8&9\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&5&6&1&2&7&9&4&8\end{pmatrix}$

5. **a)** Всегда ли $\sigma\tau = \tau\sigma$? **b)** Пусть $\sigma = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$, $\tau = \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$. Найти $\sigma\tau$ и $\tau\sigma$.

6. Докажите, что:

   a) для любых перестановок σ, τ, η выполненео равенство $(\sigma\tau)\eta = \sigma(\tau\eta)$;

   b) для любой перестановки σ справедливо равенство $(\sigma^{-1})^{-1} = \sigma$.

7. Найдите такую перестановку e, что $\mathsf{e}\alpha = \alpha\mathsf{e} = \alpha$ при всех α (она называется *тождественной*) и обозначается id. Докажите её единственность.

8. Для всякой перестановки α найдите такую перестановку α^{-1}, что $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \mathrm{id}$. Такая перестановка называется *обратной* к перестановке α. Докажите ее единственность.

9. Найдите α^{-1} для каждой α из S_3.

10. Пусть $\sigma = (123)$, $\tau = (34)$. Чему равно $\tau\sigma\tau^{-1}$?

11. Какой шарик стоит на месте k после применения перестановки α из задачи У21:3?

12. Пусть p — простое число, $\mathbb{Z}/p\mathbb{Z}$ — классы вычетов по модулю p. Докажите, что умножение на ненулевой остаток $a \in \mathbb{Z}/p\mathbb{Z}$ является перестановкой ненулевых остатков $\{1, 2, \ldots, p-1\}$, причём $a = 1$ соответствует тождественной перестановке, обратный элемент — обратной, а произведение — композиции.

13. Для скольких перестановок чисел $1, 2, 3, 4$ выполнено равенство **a)** $\sigma^2 = \mathrm{id}$? **b)** $\sigma = \sigma^{-1}$? **c)** $\sigma^2 = \sigma^{-1}$?

14. Во дворе стоят **a)** 17 **b)** 18 мальчиков. У каждого в руках мяч. Вдруг они одновременно кинули свои мячи друг другу. Петя и Вася наблюдали за ними. Петя утверждает, что может мысленно расположить мальчиков в круг так, что каждый кинул стоящему через одного по часовой стрелке. Аналогично Вася, но в кругу Васи каждый кидает стоящему через двух по часовой стрелке. Не врут ли Петя и Вася?

УРОК 22

Перестановки: циклы и транспозиции

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.2 Обозначения перестановок.

Справочные сведения

Циклы называются *независимыми* (или *непересекающимися*), если у них нет общих элементов, например: (123) и (678) — независимые циклы, в то время как циклы (123) и (345) зависмые.

Задачи

1. Какие перестановки из S_4 — не циклы? Разложите их в произведение независимых циклов.
2. Сколько всего различных циклов длины k в S_n?
3. Докажите, что любая перестановка из S_n однозначно, с точностью до порядка множителей, разлагается в произведение независимых циклов (циклы длины 1 обычно пропускают).
4. **a)** Докажите, что если циклы независимы, то они коммутируют. **b)** Верно ли обратное?
5. Текст на русском языке зашифрован программой, заменяющей взаимно однозначно каждую букву на некоторую другую. **a)** Докажите, что существует такое число k, что текст расшифровывается применением k раз шифрующей программы. **b)** Найдите хотя бы одно такое k.
6. Найдите порядки: **a)** перестановок из S_3; **b)** цикла длины k; **c)** перестановок задач У21:4 и У21:14.
7. Найдите все α из S_n, для которых $\alpha = \alpha^{-1}$.
8. Пусть α — это $(1\ 2 \dots n)^k$. На сколько независимых циклов раскладывается α, каковы их длины?
9. **a)** Докажите, что произвольный цикл в некоторой степени даст тождественную перестановку. **b)** Докажите, что любая перестановка в некоторой степени даст тождественную. **c)** Найти порядок цикла длины m. **d)** Найти все возможные порядки перестановок множества из 7 и 8 элементов.
10. Найдите максимальный возможный порядок перестановки **a)** из S_5; **b)** из S_{13}; **c)** *из S_n.
11. Докажите, что порядок перестановки из S_n делит $n!$. Может ли он быть равен $(n!)$?

12. Упростите (представьте в виде цикла или произведения независимых циклов):
a) $\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix}^{100}$; **b)** $(1\ k)(1\ k-1)\dots(1\ 3)(1\ 2)$; **c)** $(i+1\ i+2)(i\ i+1)(i+1\ i+2)$;
d) $(1\ 2\ \dots\ n)^{n-1}$; **e)** $(1\ 2\ \dots\ n)(1\ 2)(1\ 2\ \dots\ n)^{n-1}$.

13. Вычислите, чему равны следующие перестановки:
a) $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}^{100}$; **b)** $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}^{1000}$; **c)** $\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}^{-1000}$; **d)** $\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix}^{500}$;
e) $\begin{pmatrix}1&2&3&4&5&6\\4&5&2&6&3&1\end{pmatrix}^{-127}$; **f)** $\begin{pmatrix}1&2&3&4&5&6&7\\7&6&5&1&2&3&4\end{pmatrix}^{1001}$; **g)** $\begin{pmatrix}1&2&\dots&n\\n&n-1&\dots&1\end{pmatrix}^{n}$.

14. **a)** Пусть порядок перестановки равен двум. Разложим её в произведение независимых циклов. Какими могут быть длины этих циклов? **b)** Пусть σ — это k-я степень цикла $(1,2,\dots,n)$. На сколько независимых циклов раскладывается σ? Каковы длины этих циклов?

15. Докажите, что любая перестановка из S_n есть произведение

a) транспозиций;
b) *элементарных* транспозиций (то есть транспозиций вида $(i\ i+1)$, где $1 \leq i \leq n-1$);
c) транспозиций вида $(1\ k)$, где $2 \leq k \leq n$.

16. Пусть $n \geqslant 2$. Какие перестановки из S_n получаются композициями перестановок, каждая из которых — транспозиция $(1\ 2)$ или цикл $(1\ 2\ \dots\ n)$?

17. Сколько различных перестановок встречается среди степеней перестановки $(123)(4567)$?

18. *Несколько жителей города N хотят обменяться квартирами. У каждого есть по квартире, но каждый хочет переехать в другую (разные люди хотят переехать в разные квартиры). По законам города разрешены только парные обмены: если два человека обмениваются квартирами, то в тот же день они не участвуют в других обменах. Докажите, что можно устроить парные обмены так, что уже через два дня каждый будет жить в той квартире, куда хотел переехать.

Таблица 22.1: Таблица умножения симметрической группы S_4

Знакопеременная группа A_4											
Четверная группа Клейна											
e	(12)(34)	(13)(24)	(14)(23)	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(12)(34)	e	(14)(23)	(13)(24)	(243)	(143)	(234)	(134)	(142)	(132)	(124)	(123)
(13)(24)	(14)(23)	e	(12)(34)	(142)	(234)	(143)	(123)	(243)	(124)	(132)	(134)
(14)(23)	(13)(24)	(12)(34)	e	(134)	(124)	(132)	(243)	(123)	(234)	(143)	(142)
(123)	(134)	(243)	(142)	(132)	e	(13)(24)	(143)	(234)	(14)(23)	(12)(34)	(124)
(132)	(234)	(124)	(143)	e	(123)	(243)	(14)(23)	(12)(34)	(142)	(134)	(13)(24)
(124)	(143)	(132)	(234)	(14)(23)	(134)	(142)	e	(13)(24)	(243)	(123)	(12)(34)
(142)	(243)	(134)	(123)	(234)	(13)(24)	e	(124)	(132)	(12)(34)	(14)(23)	(143)
(134)	(123)	(142)	(243)	(124)	(14)(23)	(12)(34)	(234)	(143)	e	(13)(24)	(132)
(143)	(124)	(234)	(132)	(12)(34)	(243)	(123)	(13)(24)	e	(134)	(142)	(14)(23)
(234)	(132)	(143)	(124)	(13)(24)	(142)	(134)	(12)(34)	(14)(23)	(123)	(243)	e
(243)	(142)	(123)	(134)	(143)	(12)(34)	(14)(23)	(132)	(124)	(13)(24)	e	(234)
(12)	(34)	(1324)	(1423)	(23)	(13)	(24)	(14)	(1342)	(1432)	(1234)	(1243)
(13)	(1234)	(24)	(1432)	(12)	(23)	(1243)	(1423)	(34)	(14)	(1342)	(1324)
(14)	(1243)	(1342)	(23)	(1234)	(1324)	(12)	(24)	(13)	(34)	(1423)	(1432)
(23)	(1342)	(1243)	(14)	(13)	(12)	(1324)	(1432)	(1234)	(1423)	(34)	(24)
(24)	(1432)	(13)	(1234)	(1423)	(1342)	(14)	(12)	(1324)	(1243)	(23)	(34)
(34)	(12)	(1423)	(1324)	(1243)	(1432)	(1234)	(1342)	(14)	(13)	(24)	(23)
(1234)	(13)	(1432)	(24)	(1324)	(14)	(1342)	(34)	(1423)	(23)	(1243)	(12)
(1243)	(14)	(23)	(1342)	(1432)	(34)	(1423)	(13)	(24)	(1324)	(12)	(1234)
(1324)	(1423)	(12)	(34)	(14)	(1234)	(1432)	(23)	(1243)	(24)	(13)	(1342)
(1342)	(23)	(14)	(1243)	(24)	(1423)	(34)	(1234)	(1432)	(12)	(1324)	(13)
(1423)	(1324)	(34)	(12)	(1342)	(24)	(13)	(1243)	(23)	(1234)	(1432)	(14)
(1432)	(24)	(1234)	(13)	(34)	(1243)	(23)	(1324)	(12)	(1342)	(14)	(1423)

*Здесь особым фоном выделены элементы, образующие группу, изоморфную $\mathbb{Z}_3$, поскольку их 3-я степень равна e.

Таблица 22.2: Продолжение таблицы 22.1

(12)	(13)	(14)	(23)	(24)	(34)	(1234)	(1243)	(1324)	(1342)	(1423)	(1432)
(34)	(1432)	(1342)	(1243)	(1234)	(12)	(24)	(23)	(1423)	(14)	(1324)	(13)
(1423)	(24)	(1243)	(1342)	(13)	(1324)	(1432)	(14)	(34)	(23)	(12)	(1234)
(1324)	(1234)	(23)	(14)	(1432)	(1423)	(13)	(1342)	(12)	(1243)	(34)	(24)
(13)	(23)	(1423)	(12)	(1243)	(1234)	(1342)	(1324)	(24)	(34)	(1432)	(14)
(23)	(12)	(1432)	(13)	(1324)	(1342)	(34)	(24)	(1243)	(1234)	(14)	(1423)
(14)	(1324)	(24)	(1234)	(12)	(1243)	(1423)	(1432)	(1342)	(13)	(23)	(34)
(24)	(1342)	(12)	(1423)	(14)	(1432)	(23)	(34)	(13)	(1324)	(1234)	(1243)
(1234)	(14)	(34)	(1324)	(1342)	(13)	(1243)	(12)	(1432)	(1423)	(24)	(23)
(1243)	(34)	(13)	(1432)	(1423)	(14)	(12)	(1234)	(23)	(24)	(1342)	(1324)
(1342)	(1423)	(1234)	(24)	(34)	(23)	(1324)	(13)	(14)	(1432)	(1243)	(12)
(1432)	(1243)	(1324)	(34)	(23)	(24)	(14)	(1423)	(1234)	(12)	(13)	(1342)
e	(132)	(142)	(123)	(124)	(12)(34)	(234)	(243)	(13)(24)	(134)	(14)(23)	(143)
(123)	e	(143)	(132)	(13)(24)	(134)	(12)(34)	(124)	(243)	(234)	(142)	(14)(23)
(124)	(134)	e	(14)(23)	(142)	(143)	(123)	(12)(34)	(132)	(13)(24)	(234)	(243)
(132)	(123)	(14)(23)	e	(243)	(234)	(134)	(13)(24)	(124)	(12)(34)	(143)	(142)
(142)	(13)(24)	(124)	(234)	e	(243)	(14)(23)	(143)	(134)	(132)	(123)	(12)(34)
(12)(34)	(143)	(134)	(243)	(234)	e	(124)	(123)	(14)(23)	(142)	(13)(24)	(132)
(134)	(14)(23)	(234)	(124)	(12)(34)	(123)	(13)(24)	(132)	(142)	(143)	(243)	e
(143)	(243)	(13)(24)	(12)(34)	(123)	(124)	(142)	(14)(23)	(234)	e	(132)	(134)
(14)(23)	(124)	(243)	(134)	(132)	(13)(24)	(143)	(142)	(12)(34)	(123)	e	(234)
(234)	(142)	(12)(34)	(13)(24)	(134)	(132)	(243)	e	(143)	(14)(23)	(124)	(123)
(13)(24)	(234)	(123)	(142)	(143)	(14)(23)	(132)	(134)	e	(243)	(12)(34)	(124)
(243)	(12)(34)	(132)	(143)	(14)(23)	(142)	e	(234)	(123)	(124)	(134)	(13)(24)

Желтым фоном выделена таблица подгруппы 8 порядка. Данная подгруппа некоммутативна.

УРОК 23

Перестановки: четность

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.4 Знакопеременная группа.

Справочные сведения

В задаче У22:15 доказывалось, что любая перестановка есть композиция транспозиций (или просто транспозиция). В курсе мы доказываем теорему о том, что если перестановка предтавлена двумя разными способами в виде композиции транспозиций, то четность количества этих транспозиций будет одинаковой (либо их четный набор в обоих разложениях, либо нечетный — тоже в обоих разложениях).

Четность количества транспозиций в перестановке определяет четность самой перестановки. Если перестановка раскладывается в композицию четного числа транспозиций, то она называется ***четной***, в противном случае — ***нечетной***.

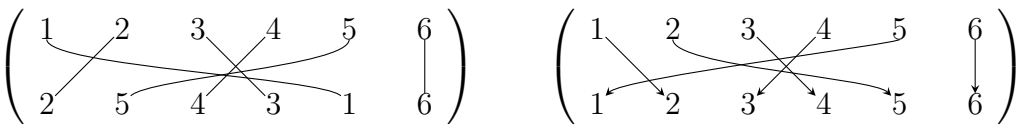
Четность перестановки совпадает с четностью количества инверсий данной перестановки. Под ***инверсией*** (или *беспорядком*) перестановки σ понимается пара индексов (i, j), для которых перестановка σ меняет порядок, т.е. если $i < j$, то $\sigma_i > \sigma_j$ и наоборот. У четной перестаноки количество инверсий четное, у нечетной — нечетное.

Множество всех четных пеерестановок группы S_n обозначается A_n и называется ***знакопеременной группой*** порядка n. Множество A_n образует нормальную подгруппу в S_n и содержит ровно половину элементов S_n.

Задачи

1. Докажите, что чётность перестановки при домножении на транспозицию меняется.

2. Чтобы увидеть число инверсий геометрически, на картинке, можно поступить двумя способами. Первый: в таблице, отвечающей перестановке α, соединим нитями одинаковые элементы (картинка слева). Второй: нарисуем таблицу с двумя одинаковыми верхними строками — 1, 2, ..., n, — и каждый элемент i верхней строки соединим нитью с элементом $\alpha(i)$ во второй строке (картинка справа).



   a) Как увидеть количество инверсий на этой картинке (можно дать ответ для одного способа)?
   b) Сделайте это для (2 3 4) и (14)(23) из S_4.
   c) Изменится ли чётность числа инверсий, если в нижней строке таблицы поменять два элемента местами?

3. **a)** Какие перестановки в S_3 четные? **b)** Какие из перестановок задачи У21:4 четные

4. Сколько инверсий у перестановки

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}?$$

5. Можно ли сказать, сколько инверсий у перестановки σ^{-1}, зная лишь число инверсий у σ?

6. Для каких k в S_n существует перестановка, у которой ровно k инверсий?

7. Доказать, что чётных перестановок столько же, сколько нечётных.

8. Докажите, что чётность цикла зависит только от его длины. Как?

9. **a)** Как выражается чётность $\sigma\tau$ через чётности σ и τ? **b)** Как выражается чётность σ^n через чётности σ и n?

10. В таблице n строк и m столбцов. *Горизонтальный ход* — это любая перестановка элементов таблицы, при которой каждый элемент остается в той же строке, что и до перестановки. Аналогично определяется *вертикальный ход*. За какое наименьшее число горизонтальных и вертикальных ходов всегда удастся получить любую перестановку элементов таблицы?

11. У отца было 7 дочерей. Всякий раз, когда одна выходила замуж, каждая ее старшая сестра, оставшаяся в невестах, жаловалась отцу, что нарушен обычай выходить замуж по старшинству. После того, как вышла замуж последняя дочь, оказалось, что отец услышал всего 7 жалоб. В каком порядке дочери могли выходить замуж (приведите пример)? Сколько всего таких порядков?

12. В каждой клетке таблицы $2 \times n$ стоит одно из целых чисел от 1 до n, причем в каждой строке стоят разные числа, и в каждом столбце стоят разные числа. Сколько таких таблиц?

13. *Докажите, что если в игре в «пятнашки» поменять местами фишки с номерами 14 и 15, то, следуя правилам, невозможно получить первоначальное расположение фишек.

14. *Каждому из n мудрецов написали на лбу число и выдали две варежки: чёрную и белую. По сигналу все мудрецы одновременно надевают варежки. После этого их строят в шеренгу в порядке возрастания написанных на их лбах чисел и просят соседей взяться за руки. Как мудрецам надевать варежки, чтобы в результате каждая белая варежка взялась за белую, а каждая чёрная — за чёрную? (Мудрец видит все числа, кроме своего; все написанные на лбах числа различны.)

15. *Пусть $n > 3$. Докажите, что A_n — это в точности множество перестановок из S_n, которые можно разложить в произведение циклов длины 3 (повторения разрешаются).

16. *Пусть s_l — количество перестановок с числом инверсий l. Покажите, что

$$1 + s_1 x + s_2 x^2 + s_3 x^3 + \dots = (1+x)(1+x+x^2)\dots(1+x+\dots+x^{n-1}).$$

УРОК 24

Множества

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.1 Теория множеств: отношения и функции.

Справочные сведения

Под *множеством* мы пока понимаем произвольную совокупность объектов без повторений и порядка («коробка с карандашами»).

Пустое множество $\emptyset$ — множество без элементов.

Множества задаются перечислением своих элементов $\{a, b, \ldots, c\}$ или с помощью логического описания элементов $\{x \mid \varphi(x)\}$, где $\varphi(x)$ — некоторое утверждение про объект x. Например, $\{x \mid x^2 = 1,\ x \in \mathbb{Z}\}$ — множество всех целых чисел, квадрат которых равен 1, т.е. попросту множество $\{-1, 1\}$. Пустое множество в скобочной записи имеет вид $\emptyset = \{\}$.

Стандартные обозначения множеств: $\mathbb{N}$ (натуральные числа), $\mathbb{Z}$ (целые числа), $\mathbb{Q}$ (рациональные числа), $\mathbb{R}$ (действительные числа), $\mathbb{C}$ (комплексные числа).

$a \in A$ — a есть *элемент множества* A; $A \subseteq B$ — множество A *подмножество множества* B.

Множества *равны* ($A = B$), если они состоят из одних и тех же элементов (т.е. $x \in A$ эквивалентно $x \in B$).

Объединением (или логической суммой) *множеств* A и B называется множество $A \cup B = \{x \mid x \in A \vee x \in B\}$. Здесь символ $\vee$ обозначает логическое ИЛИ.

Пересечением множеств A и B называется множество $A \cap B = \{x \mid x \in A \wedge x \in B\}$. Здесь символ $\wedge$ обозначает логическое И.

Разностью множества A и B называется множество $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

Задачи

1. Докажите, что для любых множеств A, B и C: **a)** $A \subseteq A$; **b)** если $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$; **c)** $A = B$ тогда и только тогда, когда $A \subseteq B$ и $B \subseteq A$.

2. Докажите, что **a)** пустое множество является подмножеством любого множества; **b)** пустое множество единственно.

3. Для каждого из множеств $\{0\}, \emptyset, \{\emptyset\}, \{1, 2\}, \{1, 2, 3\}, \{\{1, 2, 3\}\}, \{\{1, 2\}, 3\}$ найдите количество его **a)** элементов; **b)** подмножеств.

4. Может ли у множества быть ровно **a)** 0; **b)** 7; **c)** 16 подмножеств?

5. Сколько подмножеств у множества, содержащего ровно n элементов?

6. Может ли у множества A быть ровно на 2014 подмножеств больше, чем у множества B?

7. Пусть $a = \{b, c\}$, $b = \{\}$, $d = \{c, e\}$, $e = \{b\}$. Определите истинность высказываний: **a)** $a \in e$; **b)** $e \in b$; **c)** $b \in d$; **d)** $(a \in c \vee c \in d)$; **e)** $(b \in c \to a \in a)$; **f)** $(e \in d \leftrightarrow d \in e)$; **g)** $(e \in c \wedge a \in c)$; **h)** $\forall x\ x \notin b$; **i)** $\forall q\ (q \in c \to q \in a)$; **j)** $\exists k\ k \in d$; **k)** $\forall s \exists t\ (s \in t)$; **l)** $\forall s \exists t\ (t \in s)$.

8. Пусть во всей вселенной есть только множества: $a = \{\}$, $b = \{a\}$, $c = \{a, e\}$, $d = \{a, e, c\}$, $e = \{a\}$, $f = \{a, b, c, d, e\}$. Чему может быть равно множество x, удовлетворяющее условию: **a)** $x \in e$; **b)** $x \notin f$; **c)** $d \subseteq x$; **d)** $f \subseteq x$; **e)** $\forall y\ y \notin x$; **f)** $x = \{\{\}\}$; **g)** $b = \{a, x\}$; **h)** $(x \in b \wedge x \notin d)$; **i)** $(x \in c \not\to x \in b)$; **j)** $\forall n\ n \not\subset x$?

   Здесь символ $\subset$ обозначает *собственное вложение*, т.е $A \subset B$, если $A \subseteq B$ и $A \neq B$.

9. Пусть $A = \{57, 91, 179, 239\}, B = \{91, 239, 2014\}, C = \{2, 57, 239, 2014\}, D = \{2, 91, 2014, 2017\}$. Найдите следующие множества: **a)** $A \cup B$; **b)** $A \cap B$; **c)** $(A \cap B) \cup D$; **d)** $C \cap (D \cap B)$; **e)** $(A \cup B) \cap (C \cup D)$; **f)** $(A \cap B) \cup (C \cap D)$; **g)** $(D \cup A) \cap (C \cup B)$; **h)** $(A \cap (B \cap C)) \cap D$; **i)** $(A \cup (B \cap C)) \cap D$; **j)** $(C \cap A) \cup ((A \cup (C \cap D)) \cap B)$.

10. Докажите, что для любых множеств A, B, C выполнены равенства: **a)** $A \cup A = A$, $A cap A = A$; **b)** $A \cup B = B \cup A, A \cap B = B \cap A$; **c)** $A \cup (B \cup C) = (A \cup B) \cup C, A \cap (B \cap C) = (A \cap B) \cap C$; **d)** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

11. Для множеств A, B, C, D из задачи У24:9 найдите следующие множества: **a)** $(A \cup B) \setminus (C \cap D)$; **b)** $(A \cup D) \setminus (B \cup C)$; **c)** $A \setminus (B \setminus (C \setminus D))$; **d)** $D \setminus ((B \cup A) \setminus C)$; **e)** $((A \setminus (B \cup D)) \setminus C) \cup B$.

12. Верно ли, что для любых множеств A, B, C: **a)** $(A \setminus B) \cup B = A$; **b)** $A \setminus (A \setminus B) = A \cap B$; **c)** $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$; **d)** $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$; **e)** $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$; **f)** $(A \setminus B) \cup (B \setminus A) = A \cup B$?

13. *Приведите пример такого множества из четырёх элементов, что для каждых двух его элементов один из них является элементом другого.

14. *Сколько различных множеств можно получить из множеств A, B, C, D задачи У24:9 при помощи операций **a)** $\cup, \cap, \setminus$; **b)** $\cup, \cap$; **c)** $\cup, \setminus$; **d)** $\cap, \setminus$?

УРОК 25

Прямое произведение, отношения, мощность

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.1 Теория множеств: отношения и функции.

Справочные сведения

Упорядоченной парой называется символ (a, b), для которого верно утверждение: $(a, b) = (c, d)$ тогда и только тогда, когда $a = c$ и $b = d$.

Множество всех пар $\{(a, b) \mid a \in A, b \in B\}$ называется *прямым (декартовым) произведением множеств* A и B и обозначается $A \times B$.

Подмножество $R \subseteq A \times B$ называется *отношением между множествами* A и B (в случае, когда $A = B$, — отношением на множестве A). Если $(x, y) \in R$, то говорят, что x и y связаны отношением R и пишут xRy (например, $x < y$ или $x = y$).

Виды отношений на A:

R1 рефлексивное: xRx для всех $x \in A$;

R2 симметричное: если xRy, то yRx для всех $x, y \in A$;

R3 транзитивное: если xRy и yRz, то xRz для всех $x, y, z \in A$;

R4 эквивалентности: рефлексивное симметричное транзитивное отношение (пример — сравнимость по модулю).

Мощностью множества A называется количество его элементов. Обозначение: $|A|$. Множества конечной мощности называются *конечными*.

Классом эквивалентности элемента a в множестве A при заданном на нем отношении эквивалентности E называется множество $[a]_E = \{x \mid x \in A \wedge xRa\}$, т.е. множество всех эквивалентных a элементов. Множество всех классов эквивалентности множества A по отношению эквивалентности E называется *фактор-множеством* множества A и обозначается $A/_E$.

Задачи

1. Из каких элементов состоят следующие множества: **a)** $\{0, 1\} \times \{9\}$; **b)** $\{0, 1\} \times \{0, 1\}$; **c)** $\emptyset \times \emptyset$; **d)** $\{5, 7\} \times \{1, 3, 17\}$; **e)** $\{16, 41\} \times \emptyset$?

2. Верно ли, что для всех множеств A, B, C, D выполняются равенства **a)** $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$; **b)** $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$?

3. Когда $A \times B = B \times A$?

4. Покажите, что $|A \times B| = |A| \cdot |B|$ для конечных множеств A и B.

5. (*Принцип включения-исключения*) **a)** Докажите, что

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

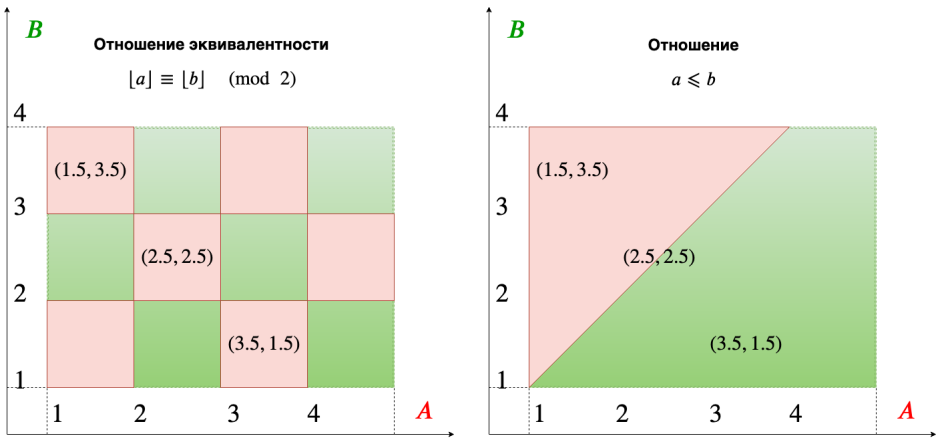
b) *Сформулируйте и докажите аналогичное утверждение для n множеств.

6. Упорядоченной парой a и b *по Куратовскому* называется множество $\{\{a\}, \{a, b\}\}$. Докажите, что **a)** $\{\{a\}, \{a, b\}\} \neq \{\{b\}, \{b, a\}\}$, если $a \neq b$; **b)** $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ тогда и только тогда, когда $a = c$ и $b = d$, т.е. такая конструкция реализует упорядоченную пару.

7. Постройте все возможные отношения на множестве **a)** $\emptyset$; **b)** $\{0\}$; **c)** $\{1, 2\}$. К какому виду относится каждое из полученных отношений?

8. Какова мощность **a)** множества всех отношений, заданных на множестве мощности n; **b)** множества всех отношений между множествами мощности m и n?

9. Изучить картинки с примерами отношений. Какой цвет и почему соответствует указанным отношениям? Функция $\lfloor x \rfloor$ обозначает целую часть числа.



10. Докажите, что отношение сравнимости по любому заданному модулю является отношением эквивалентности на множестве целых чисел. Что представляют собой классы эквивалентности в этом случае?

11. Постройте фактормножество множества $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ по отношению сравнимости по модулю 3.

12. Что представляет собой фактор-множество произвольного множества X по отношению равенства? Рассмотрите также случай $X = \emptyset$.

13. Докажите что два класса эквивалентности либо не пересекаются, либо совпадают. Что можно сказать о сумме мощностей классов эквивалентности конечного множества?

14. *Разбиением множества* A называется такое множество непустых множеств $\{A_n\}$, что $A_i \cap A_j = \emptyset$ для всех i, j $(i \neq j)$ и, кроме того A есть объединение всех A_n. Докажите, что **a)** фактор-множество является разбиением; **b)** всякому разбиению соответствует единственное отношение эквивалентности, фактор-множество по которому совпадает с данным разбиением.

15. Числом Бэлла B_n для натурального n называется количество всех разбиений множества, состоящего из n элементов. Найдите B_5 и B_7.

УРОК 26

Функции и равномощность

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.1 Теория множеств: отношения и функции, Глава 15, раздел 15.1 Мощности множеств.

Справочные сведения

Отношение $R \subseteq A \times B$ называется **a)** *однозначным*, если из $(aRb \wedge aRc)$ следует $b = c$, **b)** *всюду определенным*, если $\forall a \in A\ \exists b \in B\ (aRb)$, **c)** *всюду значным*, если $\forall b \in B\ \exists a \in A\ (aRb)$, *обратно однозначным*, если из $(aRb \wedge cRb)$ следует $a = c$.

Функция $f : A \to B$ — это всюду определенное однозначное отношение f между A и B. Иначе говоря, функция f каждому элементу из A ставит в соответствие единственный элемент из B. Функция называется **d)** *инъекцией*, если она является также обратно однозначным отношением, **e)** *сюръекцией* — если она является также всюду значным отношением, **f)** *биекцией* — если она сюръекция и инъекция одновременно.

Если $f : A \to B$ и $(a, b) \in f$, то пишут $b = f(a)$.

Множества A и B *равномощны*, если между ними существует биекция. Равномощность множеств A и B записывается так: $|A| = |B|$.

Отношение $R^{-1} = \{(b, a) \mid (a, b) \in R\}$ называется *обратным* к отношению R. Если f — сюръекция из A в B и отношение f^{-1} является функцией из B в A, то f^{-1} называется *обратной функцией* к функции f.

Пусть задано отношение $R \subseteq A \times B$. И пусть $X \subseteq A$, $Y \subseteq B$. Образом множества X по отношению R называется множество $R[X] = \{b \mid aRb \wedge a \in X\}$. Прообразом множества Y по отношению R называется множество $R^{-1}[Y] = \{a \mid aRb \wedge b \in Y\}$.

Внимание! При записи образа и прообаза множества мы используем *квадратные скобки*, не следует путать их с круглыми, включающими аргумент функции.

Множество называется *конечным*, если оно равномощно множеству $\{1, 2, \ldots, n\}$ для некоторого натурального n или пусто. Говорят, что множество *бесконечно*, если оно не является конечным.

Множество называется *счётным*, если оно равномощно множеству натуральных чисел $\mathbb{N}$. Говорят, что множество не более чем счётно, если оно конечно или счётно. Множество называется *несчётным*, если оно бесконечно и не является счётным.

Задачи

1. Рассмотрим соответствие множества людей и множества всех возрастов (целых лет). В каком направлении соответствие между ними является функцией?

2. Рассмотрим соответствие множества людей и банковских счетов. Является ли это соответствие функцией хоть в каком-то направлении?

3. Доказать, что функция $f(x) = 3x - 7$ биективно отображает $\mathbb{R}$ в $\mathbb{R}$.

4. Доказать, что функция $g(x) = x^2 + 3x - 6$ действует инъективно при $x \in [-3/2, +\infty)$.

5. Доказать, что прообраз Y — это образ Y для обратного отношения.

6. Пусть $R \subseteq A \times B$ и $X_1, X_2 \subseteq A$, $Y_1, Y_2 \subseteq B$. Проверьте, что

   a) $R[X_1 \cup X_2] = R[X_1] \cup R[X_2]$;

   b) $R^{-1}[Y_1 \cup Y_2] = R^{-1}[Y_1] \cup R^{-1}[Y_2]$;

   c) $R[X_1 \cap X_2] \subseteq R[X_1] \cap R[X_2]$;

   d) $R^{-1}[Y_1 \cap Y_2] \subseteq R^{-1}[Y_1] \cap R^{-1}[Y_2]$.

   Что изменится, если R будет функцией? инъекцией? биекцией?

7. Привести примеры, когда $f[X_1 \cap X_2] \neq f[X_1] \cap f[X_2]$, если $f : A \to B$.

8. Что можно сказать **a)** о равенстве множеств X и $f^{-1}[f[X]]$; **b)** о равенстве множеств Y и $f[f^{-1}[Y]]$, если такие множества определены?

9. Докажите, что равномощность является отношением эквивалентности, то есть **a)** $|A| = |A|$; **b)** если $|A| = |B|$, то $|B| = |A|$; **c)** если $|A| = |B|$ и $|B| = |C|$, то $|A| = |C|$.

10. Докажите, что для любых множеств X и Y выполнено $|X \times Y| = |Y \times X|$.

11. Верно ли, что если $|A| = |B|$ и $|C| = |D|$, то **a)** $|A \times C| = |B \times D|$; **b)** $|A \cup C| = |B \cup D|$; **c)** $|A \cap C| = |B \cap D|$?

12. Докажите, что следующие множества являются счётными: **a)** множество чётных натуральных чисел; **b)** множество нечётных натуральных чисел; **c)** множество натуральных чисел без числа 2015; **d)** множество целых чисел $\mathbb{Z}$.

13. Докажите, что всякое подмножество счётного множества не более чем счётно.

14. Докажите, что если X счётно, а Y конечно и непусто, то $X \times Y$ счётно.

15. Докажите, что следующие множества являются счётными: **a)** объединение конечного числа счётных множеств; **b)** прямое произведение двух счётных множеств; **c)** объединение счётного числа различных конечных множеств; **d)** объединение счётного числа счётных множеств.

16. Докажите, что множество рациональных чисел $\mathbb{Q}$ является счётным.

17. *Верно ли, что следующие множества являются счётными: **a)** множество всевозможных конечных последовательностей нулей и единиц; **b)** множество всевозможных русских «слов»; **c)** множество конечных подмножеств множества $\mathbb{N}$?

УРОК 27

Группы: основы

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 2, раздел 2.1 Сдвиг, композиция сдвигов, группа, Глава 10, раздел 10.3 Пара слов о конечных группах.

Справочные сведения

Пара $(G, \circ)$, где функция $\circ : G \times G \to G$, называется *группой*, если

G1 $(a \circ b) \circ c = a \circ (b \circ c)$ для любых $a, b, c \in G$ (ассоциативность);

G2 существует элемент $\mathsf{e} \in G$ такой, что $a \circ \mathsf{e} = \mathsf{e} \circ a = a$ для любого $a \in G$ (единица);

G3 для всякого $a \in G$ существует элемент $a^{-1} \in G$ такой, что $a \circ a^{-1} = a^{-1} \circ a = \mathsf{e}$ (обратный элемент).

Группа называется *абелевой* (*коммутативной*), если групповая операция коммутативна, т.е. $a \circ b = b \circ a$ для всех $a, b \in G$.

Обозначение групповой операции по умолчанию будем пропускать, записывая $a \circ b$ как ab.

H — *подгруппа* группы G, если $H \subseteq G$, H замкнуто относительно групповой операции группы G и групповая операция группы G является групповой операцией в H. Множество $gH = \{gh \mid h \in H\}$ называется *левым классом смежности* подгруппы H, множество $Hg = \{hg \mid h \in H\}$ — *правым классом смежности*.

Порядок группы — это количество ее элементов.

Индексом подгруппы H в группе G называется количество различных смежных классов. Обозначение: $|G : H|$.

Задачи

1. Показать, что единица и обратный элемент в группе определяются однозначно.
2. Ассоциативна ли операция $\circ$ на множестве M, если **a)** $M = \mathbb{N}$, $x \circ y = x^y$; **b)** $M = \mathbb{Z}$, $x \circ y = x^2 + y^2$; **c)** $M = \mathbb{R}$, $x \circ y = \sin x \cdot \sin y$?
3. Пусть на множестве X задана операция $x \circ y$ и для нее выполняются тождества: $\forall x, y \in X$ $(x \circ y) \circ y = x$ и $y \circ (y \circ x) = x$. Доказать, что данная операция коммутативна, т.е. $x \circ y = y \circ x$.
4. Пусть на $\mathbb{Z}$ задана операция $n \circ m = n + m + nm = (1 + n)(1 + m) - 1$. Каким аксиомам группы она удовлетворяет? Существует ли единица этой операции и как она выглядит? Существуют ли обратные элементы и для каких элементов?
5. Пусть G — группа и непустое множество $H \subseteq G$. Доказать, что если множество H замкнуто относительно групповой операции и конечно, то оно является подгруппой группы G.

6. Доказать, что множество всех биекций на множестве X образует группу с операцией композиции функций: $(f \circ g)(x) = f(g(x))$.

7. Доказать, что пересечение произвольного множества подгрупп группы G является подгруппой группы G.

8. Доказать, что в произвольной группе правый и левый смежные классы подгруппы равномощны этой подгруппе.

9. Вывести из предыдущего утверждения ***теорему Лагранжа***: порядок подгруппы делит порядок группы. Предполагается, что группа — конечная.

10. Какое отношение эквивалентности соответствует разбиению группы G на **a)** правые; **b)** левые классы смежности?

11. Доказать, что $m\mathbb{Z}$ является подгруппой в $\mathbb{Z}$ с операцией сложения. Найти все смежные классы этой подгруппы. Найти индекс подгруппы $m\mathbb{Z}$ в группе $\mathbb{Z}$, т.е. вычислить $|\mathbb{Z} : m\mathbb{Z}|$.

12. Доказать, что $\mathbb{Q}$ не содержит собственных подгрупп конечного индекса.

13. Доказать следующее обобщение теоремы Лагранжа. Пусть A, B — подгруппы группы G, и $A \subseteq B$. Индексы $|G : B|$ и $|B : A|$ конечны тогда и только тогда, когда $|G : A|$ конечен и $|G : A| = |G : B| \cdot |B : A|$.

14. Проверить, что $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ является подгруппой группы S_4 перестановок на 4 символах. Каков ее индекс в S_4? Найдите ее правые и левые смежные классы в группе S_4.

15. В группе $\mathbb{Z}_8^*$ найти обратные элементы: $3^{-1}, 5^{-1}, 7^{-1}$.

УРОК 28

Циклические группы

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 2, раздел 2.1 Сдвиг, композиция сдвигов, группа; Глава 10, раздел 10.3 Пара слов о конечных группах.

Справочные сведения

Традиционные обозначения и термины. Если групповая операция обозначается как '$+$', то группа называется *аддитивной*, при этом нейтральный элемент обозначается за 0, а обратный элемент к элементу g называется *потивоположным* и записывается как $-g$. Обычно абелевы группы считаются аддитивными. Если групповая операция обозначается как '$\cdot$', то группа называется *мультипликативной*, а знак операции, как правило, пропускается в записи формул, при этом нейтральный элемент обозначается за 1, а обратный элемент к элементу g записывается как g^{-1}. Если группа состоит из отображений, а групповой операцией является композиция отображений, то нейтральный элемент обозначается id, в остальном нотация соответствует мультипликативному варианту.

Кратную групповую операцию будем записывать с помощью натуральных чисел:

$$ng = \underbrace{g + \cdots + g}_{n \text{ раз}}, \quad g^n = \underbrace{g \cdot \ldots \cdot g}_{n \text{ раз}},$$

где $n \in \mathbb{N}$, причем $0g = 0$ и $g^0 = 1$ (в общем случае $g^0 = \mathsf{e}$, где e — нейтральный элемент). Для отрицательных коэффициентов полагаем:

$$(-n)g = -(ng), \quad g^{-n} = (g^{-1})^n,$$

где $n \in \mathbb{N}$.

Группа G *порождается* множеством $S \subseteq G$, если всякий элемент $g \in G$ можно представить в виде

$$g = s_1^{\delta_1} s_2^{\delta_2} \ldots s_n^{\delta_n},$$

где $s_k \in S$, $\delta_k \in \mathbb{Z}$. В случае аддитивной группы данное представление принимает вид $g = \delta_1 s_1 + \delta_2 s_2 + \cdots + \delta_n s_n$.

Обозначение: $G = \langle S \rangle$ — множество S порождает группу G. Если S состоит из одного элемента s (т.е. G порождается степенями одного своего элемента), то пишут $G = \langle s \rangle$, при этом группа называется *циклической*.

Порядок элемента группы — это его минимальная положительная степень, в которой данный элемент равен e. Если такой степени не существует, то данный элемент имеет бесконечный порядок.

Задачи

1. Доказать свойства степеней в группе:

$$g^m g^n = g^{m+n}, \quad (g^m)^n = g^{mn}$$

(соответственно, $mg + ng = (m+n)g$ и $n(mg) = (nm)g$).

2. Доказать. что если G — конечная группа, то $g^n = g^{n \bmod m}$, где m — порядок элемента g в группе G.

3. Доказать, что если группа $G = \langle S \rangle$ конечная, то любой элемент $g \in G$ имеет представление $s_1^{m_1} \dots s_n^{m_n}$ для некоторых $s_k \in S$, где все m_k — неотрицательные целые числа.

4. Доказать, что в конечной группе порядок всякого элемента делит порядок группы.

5. Доказать, что группа G четного порядка $|G| = 2n$ обязательно содержит элемент $g \neq \mathsf{e}$ порядка 2. *Указание: представить G как объединение пар g, g^{-1}.*

6. Является ли циклической группа **a)** $(\mathbb{Z}, +)$; **b)** $(\mathbb{Z}, \cdot)$?

7. Найдите порядок элемента R_φ в группе вращений окружности, если **a)** $\varphi = \pi$; **b)** $\varphi = \pi/3$; **c)** $\varphi = \pi/6$; **d)** $\varphi = 32\pi/63$; **e)** $\varphi = \pi\sqrt{2}$; **f)** $\varphi = 0$.

8. Существует ли конечное множество образующих у следующих групп: **a)** группа движений прямой; **b)** группа движений окружности; **c)** группа движений правильного многогранника;

9. Доказать, что перестановочные элементы g, h произвольной группы G, имеющие взаимно простые порядки m, n, порождают в G циклическую подгруппу H порядка mn, где $H = \langle g, h \rangle = \langle gh \rangle$. *Указание: использовать равенство НОД$(m, n) = km + ln$.*

10. Показать, что $\mathsf{S}_n = \langle (12), (13), \dots, (1n) \rangle$.

11. Показать, что $\mathsf{S}_n = \langle (12), (123\dots n) \rangle$.

12. Показать, что знакопеременная группа A_n, $n \geqslant 3$, порождается циклами длины 3, причем

$$A_n = \langle (1\,2\,3), (1\,2\,4), \dots, (1\,2\,n) \rangle.$$

13. Показать, что порядок перестановки $\sigma \in \mathsf{S}_n$ (порядок циклической группы $\langle \sigma \rangle$) равен НОК длин независимых циклов, входящих в разложение σ.

14. Какую систему образующих можно предложить для мультипликативной группы $(\mathbb{Q}^+, \cdot)$ положительных рациональных чисел? *Указание: использовать ОТА.*

15. Показать, что все группы порядка 4 абелевы. *Указание: если для всех $x \in G$ имеем $x^2 = \mathsf{e}$, то $abab = \mathsf{e}$ и, следовательно, $ab = ba$.*

УРОК 29

Нормальные подгруппы. Гомоморфизмы

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 2, раздел 2.1 Сдвиг, композиция сдвигов, группа; Глава 10, раздел 10.3 Пара слов о конечных группах.

Справочные сведения

Подгруппа H группы G называется *нормальной*, если ее правые и левые смежные классы совпадают, т.е. $gH = Hg$ при любом $g \in G$. Обозначение: $H \triangleleft G$. Группа G называется *простой*, если она не имеет нетривиальных (отличных от $\{\mathsf{e}\}$ и G) нормальных подгрупп.

Множество классов смежности по нормальной подгруппе H с операцией умножения $(g_1H)(g_2H) = (g_1g_2)H$ образует группу, которая называется *факторгруппой* группы G по нормальной подгруппе H и обозначается G/H. Единицей факторгруппы является подгруппа H.

Гомоморфизмом группы G в группу G' называется всякая функция $f : G \to G'$, сохраняющая групповую операцию, т.е. $f(ab) = f(a)f(b)$ для всех $a, b \in G$. *Ядро гомоморфизма* — это прообраз единицы: $\operatorname{Ker} f = \{x \mid f(x) = \mathsf{e}'\}$, где e' — нейтральный элемент группы G'.

Ядро гомоморфизма $f : G \to G'$ является нормальной подгруппой в группе G. Обратно: каждой нормальной подгруппе $H \triangleleft G$ соответствует гомоморфизм $f(a) = aH$, действующий из G в G/H, для которого $\operatorname{Ker} f = H$.

$f : G \to G'$ называется *изоморфизмом* групп G и G', если f — гомоморфизм и биекция.

Задачи

1. Найти факторгруппы: **a)** $\mathbb{Z}/n\mathbb{Z}$; **b)** $4\mathbb{Z}/12\mathbb{Z}$.
2. Доказать, что $\operatorname{Ker} f \triangleleft G$, если $f : G \to G'$ — гомоморфизм.
3. Доказать, что любая подгруппа абелевой группы нормальна.
4. Доказать, что $A_n \triangleleft \mathsf{S}_n$.
5. Доказать, что $\mathbb{Z}/p\mathbb{Z}$ — простая группа, если p — простое число.
6. Доказать, что если $|G : H| = 2$, то $H \triangleleft G$.
7. Доказать, что в группе $\mathbb{Q}/\mathbb{Z}$: **a)** каждый элемент имеет конечный порядок; **b)** для каждого натурального n имеется в точности одна подгруппа порядка n.
8. Пусть $H \triangleleft G$ и $f : G \to G/H$ — естественный гомоморфизм, т.е. $f(g) = gH$. Доказать, что f — гомоморфизм, *эпиморфизм* (т.е. сюръективный гомоморфизм), а также, что $\operatorname{Ker} f = H$.

9. Найти все нетривиальные подгруппы S_3 Какие из них являются нормальными? Каким группам $\mathbb{Z}_m$ изоморфны факторы по данным нормальным подгруппам?

10. Показать, что *группа Клейна* $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ является нормальной в S_4.

11. Рассмотрим на прямой точки X, A, B, C, D, предполагая, что все они попарно различны. Обозначим за a разность точек $A - X$, которая равна длине отрезка XA, взятой со знаком направления (если A справа от X, то с плюсом, иначе — с минусом), а также $b = B - X$, $c = C - X$, $d = D - X$. Запишем *двойное отношение*

$$\lambda = [A; B; C; D] = \frac{(c-a)(d-b)}{(c-b)(d-a)}.$$

    Докажите, что двойное отношение не зависит от выбора точки X.

12. Пусть точки A, B, C, D пронумерованы цифрами $1, 2, 3, 4$. Через $\lambda(\sigma)$ обозначим двойное отношение $[\sigma(A); \sigma(B); \sigma(C); \sigma(D)]$, где $\sigma \in \mathsf{S}_4$, т.е. является перестановкой на 4 символах. Покажите, что

$$\lambda(\sigma) \in \Lambda = \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, 1-\frac{1}{\lambda}, \frac{\lambda}{1-\lambda}\right\}$$

    при любом σ.

13. Показать, что если на множестве Λ ввести операцию композиции (т.е. рассматривать его элементы как функции от аргумента λ и подставлять одну в другую), то получится группа, изоморфная S_3. Что в этой группе является единицей?

14. Покажите, что перестановки S_4, сохраняющие двойное отношение, — это перестановки группы Клейна V_4.

15. Какой группе изоморфна группа S_4/V_4? Как это связать со свойствами двойного отношения? Какой эпиморфизм $\mathsf{S}_4 \to \mathsf{S}_3$ можно задать с помощью двойного отношения?

16. Рассмотрим группу движений правильного n-угольника. Два движения будем называть эквивалентными, если их композиция является поворотом (или id). Докажите, что это и в самом деле отношение эквивалентности, постройте классы эквивалентности, постройте факторгруппу на этих классах. Какова ее таблица умножения?

УРОК 30

Сопряжение

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 10, раздел 10.3 Пара слов о конечных группах.

Справочные сведения

Для группы G и двух ее элементов $x, g \in G$ элемент $x^{-1}gx$ называется *сопряженным* g *при помощи* x и обозначается g^x. При этом элементы g и h называются *сопряженными*, если при некотором x имеет место равенство $g^x = h$. Пишем: $g \sim h$.

Классом сопряженности элемента g называется множество $g^G = \{g^x \mid x \in G\}$.

Критерий нормальной подгруппы. Пусть H — подгруппа группы G, тогда $H \triangleleft G$ тогда и только тогда, когда H есть объединение некоторых классов сопряженности. Отсюда, в частности, следует, что нормальные подгруппы следует искать только среди объединений классов сопряженности (в конечной группе: если такое объединение замкнуто относительно групповой операции, то оно является нормальной подгруппой).

Задачи

1. Доказать свойства сопряжения: **a)** $g^{xy} = (g^x)^y$; **b)** $(gh)^x = g^x h^x$; **c)** $(g^{-1})^x = (g^x)^{-1}$;
2. Доказать, что отношение сопряженности элементов является отношением эквивалентности и классы сопряженности либо не пересекаются либо совпадают.
3. Доказать, что g^x, как функция от g, является автоморфизмом G при любом x.
4. Доказать, что если $f : G \to G'$ гомоморфизм и $g \in \operatorname{Ker} f$ и $g \sim h$, то $h \in \operatorname{Ker} f$.
5. Опишите перестановки, сопряженные переперестановке $(13)(24)$ в группе S_4.
6. Доказать, что при сопряжении при помощи **a)** перестановки (12); **b)** любой транспозиции; **c)** любой перестановки цикловая структура перестановки (т.е. количество циклов определенной длины) не меняется. **d)** Обратно: если перестановки имеют одинаковую цикловую структуру, то они сопряжены.
7. Опишите классы сопряженности в группе **a)** S_3; **b)** S_4
8. Пусть $\sigma \in \mathsf{S}_n$. И пусть $\tilde{\sigma}(\tau) = \tau^\sigma = \sigma^{-1}\tau\sigma$. Из задачи У30:3 следует, что $\tilde{\sigma}$ — автоморфизм S_n, т.е. биекция, т.е. $\tilde{\sigma} \in \mathsf{S}(\mathsf{S}_n)$.

   a) Что представляет собой автоморфизм $\tilde{\mathrm{id}}$?
   b) Занумеруем элементы S_3 числами от 1 до 6 в каком-либо порядке. Тогда автоморфизм $\tilde{\sigma}$ можно записать как элемент $\varphi(\sigma) \in \mathsf{S}_6$. Какая перестановка $\varphi(\sigma)$ из S_6 соответствует **a)** $\sigma = (12)$; **b)** $\sigma = (13)$; **c)** $\sigma = (123)$?
   c) Доказать, что $\tilde{\sigma}(\alpha \circ \beta) = \tilde{\sigma}(\alpha)\tilde{\sigma}(\beta)$. Сравнить с У30:1.

d) Доказать, что соответствие $\sigma \mapsto \varphi(\sigma)$, определенное выше и действующее из S_n в $\mathsf{S}_{n!}$, является гомоморфизмом при любом выборе нумерации элементов S_n.

9. Гомоморфизм $\varphi(\sigma) : \mathsf{S}_n \to \mathsf{S}_{n!}$, определенный в предыдущей задаче, можно рассматривать не на всем S_n, а только на перестановках, в ходящих в один класс сопряженности K. Доказать, что сужение $\varphi|_K$ является гомоморфизмом из S_n в $\mathsf{S}_{|K|}$, где $|K|$ — мощность множества K.

10. Пусть $K = (12)^{\mathsf{S}_3}$. Доказать, что $\varphi|_K : \mathsf{S}_3 \to \mathsf{S}_3$ — изоморфизм.

11. Пусть $K = (123)^{\mathsf{S}_3}$. Доказать, что $\varphi|_K : \mathsf{S}_3 \to \mathsf{S}_2$ — отображение знака, т.е. четным перестановкам сопоставляется id, а нечетным — транспозиция.

12. Найти ядра гомоморфизмов из задач У30:10 и У30:11.

13. Найти ядро гомоморфизма $\varphi|_K : \mathsf{S}_4 \to \mathsf{S}_{24}$, если $K = ((12)(34))^{\mathsf{S}_4}$.

14. Доказать, что если $f : \mathsf{S}_n \to \mathsf{S}_m$ — гомоморфизм и $(12) \in \operatorname{Ker} f$, то $\operatorname{Ker} f = \mathsf{S}_n$.

УРОК 31

Движения плоскости: определения

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 11, раздел 11.1 Виды движений плоскости. Теорема Шаля.

Справочные сведения

Движение плоскости — это всякое отображение $x \mapsto f(x)$, которое точкам плоскости ставит в соответствие точки плоскости, причем с сохранением расстояния, т.е. $|AB| = |f(A)f(B)|$ (отрезок AB переходит в равный ему по длине отрезок $f(A)f(B)$).

Виды движений плоскости:

P1 T_v: параллельный перенос (для краткости — сдвиг) на вектор v;

P2 R_α^O: поворот с центром O на угол α;

P3 S_l: отражение относительно прямой l (частный случай T_vS_l при $v = 0$);

P4 T_vS_l: скользящая симметрия со сдвигом на вектор v и симметрий относительно прямой $l \parallel v$.

Задачи

1. Докажите, что **a)** параллельный перенос; **b)** поворот; **c)** осевая симметрия является движением.
2. Доказать, что параллельные переносы образуют группу.
3. Каковы конечные подгруппы группы параллельных переносов плоскости?
4. Доказать, что концентрические повороты плоскости образуют группу.
5. Каковы конечные подгруппы группы концентрических поворотов плоскости?
6. Доказать, что скользящие симметрии с параллельными осями отражения образуют группу.
7. Каковы конечные подгруппы группы скользящих симметрий с параллельными осями?
8. Назовем движение собственным, если оно сохраняет ориентацию. Какие движения являются собственными? Доказать, что собственные движения образуют нормальную подгруппу в группе движений.

9. Движение G переводит точку $(0,0)$ в точку $(1,0)$, а точку $(1,0)$ — в $(1,1)$. Может ли G быть **a)** параллельным переносом; **b)** поворотом; **c)** скользящей симметрией? Укажите параметры соответствующих движений.

10. Вычислить движения:

    a) сдвиг на вектор $(1,0)$ с последующим поворотом относительно $O=(0,0)$ на угол π;

    b) сдвиг на вектор $(0,1)$ с последующей скользяшей симметрией с осью Ox и сдвигом на вектор $(a,0)$;

    c) сдвиг на вектор $(1,1)$ с последующим поворотом на угол π относительно точки $(0.5,0.5)$;

    d) поворот на угол $\pi/2$ относительно O с последующим сдвигом на вектор $(1,1)$;

    e) поворот на угол $\pi/3$ относительно O с последующей скользящей симметрией с осью OA, где $A=(1,0.5)$ и сдвигом на вектор $(-1,0)$;

    f) поворот на угол $\pi/3$ относительно O с последующим поворотом на угол $\pi/3$ относительно $(0.5,1)$.

11. Представить движение в виде композиции симметрий:

    a) параллельный перенос на вектор $(2,2)$;

    b) поворот на угол $\pi/2$ относительно точки $(1,1)$;

    c) скользящая симметрия с осью Oy и сдвигом вдоль нее на вектор $(-1,0)$.

12. Доказать, что движение **a)** прямую переводит в прямую; **b)** треугольник переводит в треугольник; **c)** окружность переводит в окружность; **d)** отрезок переводит в отрезок (при этом внутренние точки — во внутренние).

УРОК 32

Движения плоскости: продолжение

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 11, раздел 11.1 Виды движений плоскости. Теорема Шаля.

Справочные сведения

Теорема Шаля: любое движение плоскости есть либо параллельный перенос, либо поворот, либо скользящая симметрия.

Таблица композиций движений плоскости:

id	T_u	R_α^O	S_l	$T_u S_l$
T_u	T_{u+v}	$R_\alpha^{O_1}$	$T_{\mathrm{Pr}_l v} S_{l+v/2}$	$T_{\mathrm{Pr}_l[u+v]} S_{l+(u+v)/2}$
R_β^A	$R_\beta^{A_1}$	$R_{\alpha+\beta}^C$ $(\alpha+\beta\neq 0)$ T_w $(\alpha+\beta=0)$	$T_w S_{l+\beta/2}$ $(A\notin l)$ $S_{l+\beta/2}$ $(A\in l)$	$T_w S_{l+\beta/2}$ $(A_1\notin l)$ $S_{l+\beta/2}$ $(A_1\in l)$
S_m	$T_{\mathrm{Pr}_l u} S_{m-u/2}$	$T_w S_{m-\alpha/2}$ $(O\notin m)$ $S_{m-\alpha/2}$ $(O\in m)$	$R_{2\angle lm}^{l\cap m}$ $(l\not\parallel m)$ $T_{2(m-l)}$ $(l\parallel m)$	$R_{2\angle lm}^{O}$ $(l\not\parallel m)$ $T_{2(m-l)+u}$ $(l\parallel m)$
$T_v S_m$	$T_{\mathrm{Pr}_l[u+v]} S_{m-(u+v)/2}$	$T_w S_{m-\alpha/2}$ $(O_1\notin m)$ $S_{m-\alpha/2}$ $(O_1\in m)$	$R_{2\angle lm}^{O}$ $(l\not\parallel m)$ $T_{2(m-l)+v}$ $(l\parallel m)$	$R_{2\angle lm}^{O}$ $(l\not\parallel m)$ $T_{2(m-l)+u+v}$ $(l\parallel m)$

Задачи

1. Вывести формулы таблицы композиций (хотя бы частично).
2. Найти композиции движений:

$$T_v S_l \circ T_v S_l; \quad T_v S_l \circ T_v S_l \circ T_v S_l.$$

3. Всегда ли $U\circ V = V\circ U$, если U, V — движения плоскости? Привести поясняющие примеры.
4. Всегда ли композиция движений есть движение?
5. Пусть $W = U\circ V$, где V — поворот на угол $\pi/3$ с центром O, а U — сдвиг на вектор v. Найти такую точку x, что $W(x) = O$.
6. Пусть теперь $W = V\circ U$, где U, V — из предыдущей задачи. Решите уравнение $W(x) = O$.

7. К какому классу относятся движения W из двух предыдущих задач?

8. Пусть даны поворот R^O_α и сдвиг $T_{\vec{v}}$, $\alpha \neq 0$, $\vec{v} \neq 0$.

   1) Построить такой равнобедренный треугольник $\triangle OAB$ с вершиной O, что $R^O_\alpha(A) = B$ и $BA = \vec{v}$;
   2) Доказать, что A является неподвижной точкой композиции $T_{\vec{v}} \circ R^O_\alpha$;
   3) Доказать, что B является неподвижной точкой композиции $R^O_\alpha \circ T_{\vec{v}}$.

9. Найдите обратное преобраазование к $R^O_\alpha \circ T_v$ и $T_v \circ R^O_\alpha$. Какие точки x при этих обратных преобразованиях пеереходят в точку O?

10. Чем является композиция двух осевых симметрий относительно **a)** двух перпендикулярных прямых; **b)** двух параллельных прямых; **c)** двух прямых, образующих угол $\pi/3$?

11. Докажите, что композиция отражения относительно прямой l и параллельного переноса на вектор v является **a)** осевой симметрией, если $v \perp l$; **b)** скользящей симметрией в любом случае.

12. Чем является композиция поворота с центром O на угол α и отражения относительно прямой l, если $O \in l$?

13. Найти композицию отражения относительно вертикальной оси и поворота на 180^o относительно точки, не лежащей на оси симметрии.

14. (Теорема Наполеона) Пусть дан произвольный треугольник $\triangle ABC$. На его сторонах построим правильные треугольники и назовем их центры A', B', C'. Доказать, что полученный треуголник $\triangle A'B'C'$ — правильный. *Указание*: рассмотреть два вращения $R^{120^o}_{A'}$ и $R^{120^o}_{B'}$ и доказать, что $R^{120^o}_{B'} \circ R^{120^o}_{A'}(C') = C'$.

УРОК 33

Подобия прямой и плоскости

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 13, раздел 13.1 Преобразования, раздел 13.2 Подобия прямой и плоскости.

Справочные сведения

видел ***Подобие*** — такое преобразование $x \mapsto f(x)$, при котором сохраняется отношение расстояний $|f(A)f(B)|/|AB|$. Такое отношение называется коэффициентом подобия. Коэффициент подобия всегда отличен от нуля. Если коэффициент равен 1, то подобие является движением.

Если композиция параллельных перенесов соответствует сумме векторов, то композиция подобий соответствует произведению коэффициентов подобия.

Частный случай подобия: ***гомотетия*** H_O^k с центром O и коэффициентом k, которая каждой точке A ставит в соответствие точку $O + k\vec{OA}$, причем число k может быть и отрицательным (но не нулевым).

Поворотная гомотетия: композиция гомотетии H_O^k с поворотом R_α^O.

Задачи

1. В каких случаях гомотетия является движением?
2. Коммутирует ли гомотетия с поворотом, **a)** если их центры идентичны; **b)** если их центры различны? Коммутируют ли гомотетии с разными центрами?
3. Вычислить композиции: **a)** $H_O^2 \circ H_A^{1/2}$; **b)** $H_O^2 \circ R_O^{\pi/2} \circ H_O^{-1/2}$; $T_{OA} \circ H_A^{-1}$; **c)** $H_O^2 \circ H_A^3$ $(A \neq O)$.
4. Доказать, что подобия прямой — это либо гомотетия, либо сдвиг (при $k = 1$).
5. Проверить, что подобия прямой и плоскости образуют группу с операцией композиции.
6. Найти все конечные подгруппы подобий прямой.
7. Доказать, что при подобии **a)** прямая переходит в прямую; **b)** окружность — в окружность; **c)** отрезок — в отрезок (с сохранением внутренних точек); **d)** треугольник — в треугольник (вершины — в вершины).
8. Пусть дан треугольник $\triangle ABC$, и в нем проведены биссектрисы углов. Затем через середины его сторон провели прямые, параллельные этим биссектрисам (через середину BC провели прямую, параллельную биссектрисе $\angle A$, и т.д.). Доказать, что эти прямые пересекаются в одной точке. *Указание*: использовать гомотетию с центром в точке пересечения медиан $\triangle ABC$.

9. Взяли карту в одном масштабе, уменьшили ее (сделали масштаб более мелким) и положили на исходную карту так, что уменьшенная карта оказалась полностью внутри исходной. Доказать, что существует точка на карте, которая при этом совместилась сама с собою.

10. Вычислить, нарисовать на плоскости и указать модуль и аргумент следующих комплексных чисел:

$$i^2,\ i^3,\ i^4,\ 1/i,\ (1+2i)(2-i),\ (1+i)(1+2i)(1+3i),\ \frac{1}{1+i},\ \frac{5}{2-i}.$$

УРОК 35

Комплексные числа. Часть 1

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Справочные сведения

$z = x + iy$ — вектор на плоскости с координатами (x, y). При вычислениях пользуемся правилом: $i^2 = -1$. Арифметика:

1. $(a + ib) + (c + id) = (a + c) + i(b + d)$;
2. $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$;
3. $1/(a + bi) = (a - ib)/(a^2 + b^2)$.

Модуль комплексного числа: $|z| = \sqrt{x^2 + y^2}$.
Сопряжение комплексного числа: $\overline{z} = x - iy$. $|z|^2 = z\overline{z}$.

Задачи

1. Доказать, что $z + w = z + w$ и что $zw = zw$.
2. Докажите, что если $zw = 0$, то либо $z = 0$, либо $w = 0$.
3. Докажите, что если и сумма, и произведение двух комплексных чисел вещественны, то либо оба этих числа вещественны, либо сопряжены.
4. Вычислить $(-i)2$, $i10$, $(1 + i)10$, $(1 - i)10$, $(1 + i)101$.
5. Вычислить $(2+3i)+(7-i)$, $(2+3i)(7-i)$, $(1+i)(1-i)$, $(2-3i)(3+2i)$ и $2(4+3i)-3(2-i)$.
6. Найти два комплексных числа, сумма и произведение которых равны 2.
7. Найти комплексное число z, для которого $z(1 + i) = 1$.
8. Найти комплексное z, при котором $z(2 + 3i) = 3 - 2i$.
9. Найти комплексное z, при котором $z(1 + i) = 3 + 4i$.
10. Доказать, что $|z|^2 = z \cdot \overline{z}$.
11. Вывести формулу для расстояния между числами z и w.
12. Найти z, при котором $z(2 + 3i) = 5 + 4i$.
13. Найти сумму $1 + i + i2 + i3 + \cdots + i100$.
14. Найти z, для которого **a)** $z^2 = 2$; **b)** $z^2 = -2$; **c)** $z^2 = 2i$.

15. Найти z, для которого $z^2 = 1 + i$.
16. Найти z, для которого $z^2 + 2z + 2 = 0$.
17. Найти все $z = a + bi$, для которых $z^3 = -1$.

УРОК 36

Комплексные числа. Часть 2

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Справочные сведения

Для комплексного числа $z = x + iy$ определяется ***аргумент*** $\varphi = \arg z$ и модуль $r = |z|$. Аргумент — угол между осью Ox и вектором (x, y), отложенный в положительном направлении (против часовой стрелки). Через аргумент комплексное число записывается как $re^{i\varphi}$ с полной поддержкой арифметических правил.

Имеет место ***формула Эйлера***: $e^{i\varphi} = \cos(\varphi) + i\sin(\varphi)$.

Обозначения действительной и мнимой частей: $\mathsf{Re}\, z = x$, $\mathsf{Im}\, z = y$.

Задачи

1. **a)** Каков геометрический смысл суммы комплексных чисел? **b)** Сравните $|z+w|$ и $|z|+|w|$ для $z, w \in \mathbb{C}$.

2. Найдите модуль и аргумент чисел: **a)** -4, $1+i$, $1-i\sqrt{3}$, $\sin\alpha + i\cos\alpha$; **b)** $1+\cos\alpha+i\sin\alpha$.

3. Рассмотрим умножение точек комплексной плоскости на $\cos\varphi + i\sin\varphi$ как преобразование f этой плоскости, переводящее z в $(\cos\varphi + i\sin\varphi)z$. Куда при этом преобразовании перейдут

   a) точки действительной оси;

   b) точки мнимой оси?

   c) Докажите, что f — поворот против часовой стрелки на угол φ вокруг начала координат.

   d) Пусть $z, w \in \mathbb{C}$. Выразите $|zw|$ и $\arg(zw)$ через $|z|$, $|w|$, $\arg(z)$, $\arg(w)$.

   e) Выведите из предыдущего пункта формулы для косинуса суммы и синуса суммы.

4. **a)** Из любого ли комплексного числа можно извлечь квадратный корень?

   b) Решите уравнение $z^2 = i$. **c)** Найдите ошибку: $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = i \cdot i = i^2 = -1$.

5. Докажите, что если и m и n — суммы двух квадратов целых чисел, то и mn — тоже.

6. (Формула Муавра) Пусть $z = r(\cos\varphi + i\sin\varphi)$, $n \in \mathbb{N}$. Докажите: $z^n = r^n(\cos n\varphi + i\sin n\varphi)$.

7. Вычислите **a)** $(\sqrt{3}+i)^{30}$; **b)** $(1+i)^{333}$; **c)** $(1+i\sqrt{3})^{150}$. **d)** Выразите $\cos nx$ и $\sin nx$ через $\cos x$ и $\sin x$ ($n \in \mathbb{N}$).

8. **a)** Выразите $|\overline{z}|$, $\arg(\overline{z})$ через $|z|$, $\arg(z)$. Докажите: **b)** $|z|^2 = z\overline{z}$; **c)** $z+w = z+w$, $zw = zw$; **d)** если $P(x)$ — многочлен с вещественными коэффициентами и $P(z) = 0$, то $P(\overline{z}) = 0$.

УРОК 37

Комплексные числа. Часть 3

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Задачи

1. Вычислить действительную и мнимую части суммы и произведения чисел $a+bi$ и $c+di$.
2. Доказать, что для любого z сумма $z+\overline{z}$ и произведение $z\overline{z}$ действительны, то есть имеют нулевую мнимую часть.
3. Вычислить $(1+i)/(1-i)$ и $(8+i)/(1+2i)$.
4. Найти общую формулу для частного $(a+bi)/(c+di)$.
5. **a)** вычислите $\frac{(5+i)(7-6i)}{3+i}$; **b)** вычислите $\frac{(1+i)^5}{(1-i)^3}$;
6. Для каких z найдётся такое w, что $zw=1$?
7. Доказать, что если $z^2=w^2$, то $z=w$ или $z=-w$.
8. Найти все комплексные числа, для которых $z^2=2i$.
9. Доказать, что $\overline{z/w}=\overline{z}/\overline{w}$.
10. Как найти модуль и аргумент частного z/w, зная модули и аргументы комплексных чисел z и w?
11. Доказать тождество $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$.
12. Доказать, что если два целых числа представимы в виде суммы двух квадратов (например, $2=1^2+1^2$ и $13=2^2+3^2$), то их произведение обладает этим же свойством.
13. Доказать, что число $2a$ представимо в виде суммы двух квадратов тогда и только тогда, когда в этом виде представимо число a.
14. Доказать, что если сумма и произведение двух комплексных чисел вещественны, то эти числа либо оба вещественны, либо сопряжены.
15. Найти все комплексные числа z, для которых $z^2+z+1=0$.
16. Найти все комплексные числа z, для которых $z^3=1$.
17. Нарисуйте: **a)** $\{z\in\mathbb{C}\mid z^n n+1=0\}$; **b)** $\{z\in\mathbb{C}\mid 2>|z-i|\}$; **c)** $\{z\in\mathbb{C}\mid \mathrm{Re}\,\frac{1}{z}=1\}$; **d)** $\{\frac{1+ti}{1-ti}\mid t\in\mathbb{R}\}$.

УРОК 38

Геометрия комплексных чисел
Часть 1

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Справочные сведения

Арифметические операции над комплексными числами можно рассматривать как преобразования плоскости. Сложение — как *параллельный перенос*, умножение — как *поворотную гомотетию*, сопряжение — как *отражение*.

Задачи

1. Доказать, что для любого комплексного α преобразование $z \mapsto \alpha z$ увеличивает все расстояния в одно и то же число раз, и найти это число.
2. Что можно сказать о преобразовании $z \mapsto \alpha z$, если число α действительное?
3. Что можно сказать о преобразовании $z \mapsto \alpha z$, если $|\alpha| = 1$?
4. При каком числе α преобразование $z \mapsto \alpha z$ будет поворотом на 30^o вокруг начала координат?
5. Доказать, что преобразование $z \mapsto \alpha z$ есть композиция гомотетии с коэффициентом $|\alpha|$ и поворота на угол $\arg \alpha$.
6. Доказать, что преобразование поворота на угол φ вокруг начала координат задаётся формулой $z \mapsto z(\cos\varphi + i\sin\varphi)$.
7. Куда переходит точка $z = 1$ при повороте на угол φ, а затем на угол ψ в том же направлении? Вывести формулы для $\cos(\varphi+\psi)$ и $\sin(\varphi+\psi)$.
8. **a)** Докажите, что $e^{i\varphi}e^{i\psi} = e^{i(\varphi+\psi)}$. **b)** Можно ли найти $e^{i\varphi} + e^{i2\varphi} + \cdots + e^{in\varphi}$ по формуле суммы геометрической прогрессии?
9. Найдите: **a)** $\sin\varphi + \sin 2\varphi + \cdots + \sin n\varphi$; **b)** $\binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \binom{n}{7} + \ldots$; **c)** $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \binom{n}{12} + \ldots$
10. Какое преобразование плоскости переводит **a)** z в $2z$; **b)** z в $z+1$; **c)** z в $\overline{z}$; **d)** z в $-z$; **e)** z в $-\overline{z}$; **f)** z в iz?
11. Опишите геометрически преобразование плоскости, заданное формулой: **a)** $z \mapsto z + w$, где w — комплексное число; **b)** $z \mapsto kz$, где k — вещественное число; **c)** $z \mapsto 2z + 1$; **d)** $z \mapsto \overline{z}$; **e)** $z \mapsto e^{i\alpha}z$, где $0 \leqslant \alpha < 2\pi$; **f)** $z \mapsto wz$, где w — произвольно.
12. Где находятся точки z, для которых $z + \overline{z} = 1$?

13. Где находятся точки z, для которых $z \cdot \overline{z} = 1$?

14. Где находятся числа z, для которых **a)** $|z| = 1$; **b)** $|z - 1| = 1$; **c)** $|z| = |z + 1|$?

15. Доказать, что $|z \cdot w| = |z| \cdot |w|$ для любых комплексных z и w.

16. Найти действительную и мнимую части числа z, если $|z| = 2$ и $\arg z = 60^o$. Найти действительную и мнимую части чисел z^2 и z^3.

17. Вывести формулы для действительной и мнимой частей числа с модулем r и аргументом φ.

18. Для данного z найти w, при котором точки $0, z, iz$ и w лежат в вершинах квадрата.

19. Решите уравнения: **a)** $z^2 = e^{i\pi/3}$; **b)** $z^2 = 5 - 12i$; **c)** $z^2 + (2i - 7)z + 13 - i = 0$; **d)** $\overline{z} = z^2$; **e)** $\overline{z} = z^3$; **f)** $z3 + z2 + z + 1 = 0$.

20. Запишите как функцию комплексной переменной (можно использовать переменную z, комплексные числа и операции сложения, вычитания, умножения, деления, сопряжения)

    a) симметрию относительно оси y;
    b) ортогональную проекцию на ось x;
    c) центральную симметрию с центром A;
    d) поворот на угол φ относительно точки A;
    e) гомотетию с коэффициентом k и центром A;
    f) скользящую симметрию относительно прямой $y = 3$ со сдвигом на 1 влево;
    g) поворот, переводящий ось Ox в прямую $y = 2x + 1$;
    h) симметрию относительно прямой $y = 2x + 1$.

УРОК 39

Геометрия комплексных чисел
Часть 2

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Справочные сведения

Для комплексных чисел z_1, z_2, z_3 определим их ***простое отношение***:

$$\frac{z_1 - z_3}{z_2 - z_3}.$$

Для комплексных чисел z, w, z_1, w_1 определим их ***двойное отношение***:

$$[z, w, z_1, w_1] = \frac{z_1 - z}{z_1 - w} \cdot \frac{w_1 - w}{w_1 - z}.$$

Задачи

1. Доказать, что точки $0, 1/z$ и $\overline{z}$ лежат на одной прямой.
2. Доказать, что точки z, для которых $z + \overline{z} = z \cdot \overline{z}$, лежат на одной окружности, и найти её центр и радиус.
3. Доказать, что точки, для которых число $z/(z-1)$ является чисто мнимым, лежат на одной окружности, и найти её центр и радиус.
4. Найти все z, для которых $|z - 3| \leqslant 2$ и $|z + 4i|le3$.
5. Найти комплексное число α, при котором преобразование $z \mapsto \alpha z$ есть поворот на 45^o. Чему равен квадрат этого числа?
6. Доказать, что преобразование $z \mapsto (1 + i)z$ увеличивает все расстояния в одно и то же число раз, и найти это число.
7. Как найти четвёртую вершину параллелограмма, если три его вершины совпадают с точками u, v и w комплексной плоскости? Указать все возможности.
8. Где находится точка пересечения медиан треугольника, вершинами которого являются точки u, v и w комплексной плоскости?
9. Вывести формулу для преобразования комплексной плоскости, являющегося симметрией относительно прямой $\mathsf{Re}\, z = \mathsf{Im}\, z$.

10. Пусть z и w — ненулевые различные комплексные числа. Верно ли, что точки $z, w, 1/z, 1/w$ лежат на одной окружности?

11. Даны два комплексных числа a и b. Опишите множество таких $z \in \mathbb{C}$, что $(z-a)/(z-b)$ — **a)** вещественное число; **b)** чисто мнимое число. **c)** Каков геометрический смысл аргумента этого числа? **d)** Докажите, что треугольники $\triangle z_1 z_2 z_3$ и $\triangle w_1 w_2 w_3$ подобны тогда и только тогда, когда простые отношения точек z_1, z_2, z_3 и w_1, w_2, w_3 равны или сопряжены.

12. Рассмотрим двойное отношение:

$$\lambda = [z, w, z_1, w_1] = \frac{z_1 - z}{z_1 - w} \cdot \frac{w_1 - w}{w_1 - z}.$$

Найти все значения двойного отношения $[z, w, z_1, w_1]$ при перестановках символов внутри обозначения $[z, w, z_1, w_1]$, выразить через данное λ.

13. Каким будет число λ, если все точки двойного отношения лежат **a)** на одной прямой; **b)** на одной окружности?

14. Докажите с помощью комплексных чисел, что **a)** композиция двух поворотов является поворотом или параллельным переносом; **b)** композиция поворота на ненулевой угол и параллельного переноса является поворотом.

УРОК 40

Геометрия комплексных чисел
Часть 3

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Задачи

1. (Эйлер) Докажите, что сумма квадратов длин сторон четырёхугольника отличается от суммы квадратов диагоналей на учетверённый квадрат длины отрезка, соединяющего середины диагоналей.

2. Пусть M — точка на плоскости, S — окружность, AB — её диаметр. Докажите, что величина $|MA|^2 + |MB|^2$ не зависит от выбора диаметра AB окружности S.

3. Докажите теорему косинусов $|BC|^2 = |AB|^2 + |AC|^2 - 2 \cdot |AB| \cdot |AC| \cos\alpha$, расположив вершины треугольника ABC в точках $0, z$ и w соответственно, где w вещественно.

4. На плоскости даны точки A, B, C. Пусть A_1 — образ точки C при повороте вокруг A на 90^o против часовой стрелки, B_1 — образ точки C при повороте вокруг B на 90^o по часовой стрелке, K — середина A_1B_1, M — середина AB. Докажите, что отрезки M и AB перпендикулярны. Как соотносятся их длины?

5. На сторонах треугольника $A_1A_2A_3$ во внешнюю сторону построены квадраты с центрами B_1, B_2, B_3. Докажите, что отрезки B_1B_2 и A_3B_3 равны по длине и перпендикулярны.

6. Пусть $A_1A_2A_3$ и $B_1B_2B_3$ — правильные треугольники, и их вершины занумерованы против часовой стрелки. Докажите, что середины отрезков A_1B_1, A_2B_2 и A_3B_3 — вершины правильного треугольника.

7. Доказать, что комплексные числа z, для которых $z^3 = 1$, являются вершинами правильного треугольника.

8. Доказать, что для любого целого $n > 2$ и любого комплексного α корни уравнения $z^n = \alpha$ являются вершинами правильного n-угольника.

9. Докажите, что три точки z_1, z_2, z_3 являются вершинами правильного треугольника тогда и только тогда, когда $z_1^2 + z_2^2 + z_3^2 = z_1z_2 + z_1z_3 + z_2z_3$.

10. Докажите, что **a)** три различные точки z_1, z_2, z_3 лежат на одной прямой тогда и только тогда, когда их простое отношение вещественно; **b)** прямая, проходящей через точки z_1 и z_2, задаётся уравнением $(z_1 - z)(\overline{z}_2 - \overline{z}) = (\overline{z}_1 - \overline{z})(z_2 - z)$; **c)** каково уравнение перпендикуляра к этой прямой, проходящего через w?

11. Докажите, что **a)** $(z_1 - z_2)(z_4 - z_3) + (z_2 - z_3)(z_4 - z_1) = (z_2 - z_4)(z_3 - z_1)$; **b)** в любом четырехугольнике произведение длин диагоналей не превосходит сумму произведений длин противоположных сторон; **c)** (теорема Птолемея) для четырехугольника, вписанного в окружность, достигается равенство. **d)** Верно ли, что если равенство достигается, то четырехугольник вписанный?

12. Докажите, что прямая, проходящая через точки a и b единичной окружности $z\overline{z} = 1$, имеет уравнение $z + ab\overline{z} = a + b$, а касательная в точке p этой окружности имеет уравнение $p\overline{z} + p\overline{z} = 2$.

13. **a)** Пусть z_1 и z_2 — точки на единичной окружности $z\overline{z} = 1$. Докажите, что точка пересечения касательных к этой окружности, проходящих через z_1 и z_2, — это точка $2z_1z_2/(z_1 + z_2)$ **b)** (Задача Ньютона) В описанном около окружности четырехугольнике середины диагоналей и центр окружности лежат на одной прямой.

14. **a)** Пусть a, b, c, d — различные точки на единичной окружности $z\overline{z} = 1$. Докажите, что секущая, проходящая через a и b, и секущая, проходящая через c и d, пересекаются в точке, сопряжённой к $\frac{(a+b)-(c+d)}{ab-cd}$.

УРОК 41

Геометрия комплексных чисел
Часть 4

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Задачи

1. При каких a и b преобразование $z \mapsto az + b$ является поворотом на 45^o вокруг точки $1 = 1 + 0i$?
2. Числа 0 и z являются вершинами правильного треугольника. Где может находиться третья его вершина?
3. Числа 0 и z являются вершинами квадрата. Где могут находиться две другие его вершины?
4. Найти все корни уравнения $z^5 = 1$. *Указание*: в ответе могут остаться квадратные корни, но не должно быть синусов и косинусов.
5. Доказать, что сумма всех n корней уравнения $z^n = 1$ равна нулю.
6. Найти произведение всех n корней уравнения $z^n = 1$.
7. Доказать, что все корни уравнения $z^n = 1$ являются степенями некоторого из них. *Замечание*: корень с таким свойством называется ***первообразным корнем***.
8. Проверить, что корни уравнения $z^n = 1$ образуют группу по умножению. Какой известной вам группе данная группа изоморфна? Чем является первообразный корень в теоретико-групповой терминологии?
9. Сколько существует первообразных корней степени 12 из единицы?
10. Сколько существует первообразных корней степени 1001 из единицы?
11. При каких a и b преобразование $z \mapsto az + b$ является **a)** поворотом; **b)** параллельным переносом; **c)** осевой симметрией?
12. При каких a и b преобразование $z \mapsto a\overline{z} + b$ является осевой симметрией?
13. Найти все значения корня: **a)** $\sqrt[3]{-i}$; **b)** $\sqrt[4]{-16}$; **c)** $\sqrt[5]{1+i}$.

УРОК 42

Комплексные числа: разное

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.1 Алгебра комплексных чисел.

Задачи

1. Докажите, что многочлен степени n с коэффициентами из $\mathbb{C}$ имеет не более n корней из $\mathbb{C}$.

2. **a)** Найдите и нарисуйте все корни из 1 степеней 2, 3, 4, 5 и 6. **b)** Сколько всего корней из 1 степени n? Найдите их произведение и сумму их s-х степеней для каждого $s \in \mathbb{N}$.

3. Пусть P — многочлен степени k с коэффициентами из $\mathbb{C}$. Докажите, что среднее арифметическое значений P в вершинах правильного n-угольника равно значению P в центре многоугольника, если $n > k$.

4. *Вершины правильного n-угольника покрашены в несколько цветов так, что точки одного цвета — вершины правильного многоугольника. Докажите: среди этих многоугольников есть равные.

5. **a)** Пусть $z = (3+4i)/5$. Найдется ли такое $n \in \mathbb{N}$, что $z^n = 1$? **b)** Докажите, что $\frac{1}{\pi}\operatorname{arctg}\frac{4}{3} \notin \mathbb{Q}$.

6. *Можно ли сравнивать комплексные числа так, чтобы сохранились основные свойства неравенств (домножение на число, большее 0, не меняет знак неравенства и т.п.)? Верно ли, что $i > 0$, или что $i < 0$?

7. Что можно сказать о расположении точек z, z_1, w, w_1 на плоскости, если их двойное отношение — вещественное?

8. *Каждую сторону n-угольника продолжили на её длину (обходя по часовой стрелке). Пусть концы построенных отрезков образуют правильный n-угольник. Докажите, что и исходный n-угольник правильный.

9. *Пусть вписанная окружность треугольника ABC задаётся уравнением $z\overline{z} = 1$ и касается его сторон в точках p, q, r. Докажите, что **a)** $\frac{2pqr(p+q+r)}{(p+q)(p+r)(q+r)}$ — центр описанной окружности треугольника ABC; **b)** $\frac{(pq+pr+qr)^2}{(p+q)(p+r)(q+r)}$ — центр окружности Эйлера треугольника ABC; **c)** точка $\frac{pq+pr+qr}{p+q+r}$ лежит и на вписанной окружности, и на окружности Эйлера (окружность 9 точек) треугольника ABC; **d)** (теорема Фейербаха) вписанная окружность и окружность Эйлера треугольника ABC касаются друг друга.

10. (*Теорема Паскаля) Докажите, что точки пересечения прямых, содержащих противоположные стороны вписанного шестиугольника, лежат на одной прямой.

УРОК 43

Гауссовы целые числа
Часть 1

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.2 Гауссовы целые числа.

Справочные сведения

Гауссовы целые числа — это комплексные числа вида $m + ni$, где $m, n \in \mathbb{Z}$. Обозначение: $\mathbb{Z}[i]$, т.е. расширение кольца целых чисел присоединением мнимой единицы.

Операции сложения и умножения наследуются от комплексных чисел.

Деление в $\mathbb{Z}[i]$ не всегда возможно, поэтому оно порождает теорию делимости, аналогичную таковой в целых числах.

Все гауссовы числа делятся на $\pm 1, \pm i$. Эти четыре числа называются ***обратимыми***. Для каждого числа $z \in \mathbb{Z}[i]$ его делимость на какое-либо гауссово число w эквивалентно делимости чисел $z, -z, iz, -iz$ на $\pm w, \pm iw$.

Числа $\pm z, \pm iz$ называются ***ассоциированными***.

Нормой гауссова числа $z = m + ni$ называется целое неотрицательное число $N(z) = |z|^2 = n^2 + m^2$. Делимость гауссовых чисел тесно связана с деимостью их норм в обычных целых числах.

Гауссово число называется ***простым***, если оно имеет ровно 8 делителей: 1 и все с ней ассоциированные, само себя и все ассоциированные. Простое целое число не обязано быть простым в гауссовых числах. Например, 5 делится на $2 + i$ в гауссовых числах, хотя является простым в целых.

Задачи

1. Что с точки зрения движений плоскости представляют собой ассоциированные числа?

2. Покажите, что в $\mathbb{Z}[i]$ сложение и умножение не выходит за рамки $\mathbb{Z}[i]$.

3. **a)** Покажите, что $\pm 1, \pm i$ обратимы, т.е. для каждого из них в $\mathbb{Z}[i]$ существует обратный по умножению. **b)** Покажите, что обратимые элементы образуют группу по умножению, изоморфную циклической группе из 4 элементов (группе вращения квадрата).

4. Нарисуйте на комплексной плоскости: **a)** числа $\mathbb{Z}[i]$; **b)** числа, на которые делится z и **c)** числа, коротые делятся на z для $z = 1 + i, 2 + i, 3 + i, 3 + 2i$.

5. Докажите свойства нормы:

   a) $N(z) = 0$ тогда и только тогда, когда $z = 0$;
   b) $N(z) = N(\overline{z})$;

c) Если норма $N(z)$ — нечетное число, то она имеет вид $4k+1$, никакая норма не может иметь вид $4k+3$;
d) $N(zw) = N(z)N(w)$.
e) z делит $N(z)$;
f) если z делит w, то $N(z)$ делит $N(w)$.

6. Для следующих пар чисел выясните, делится ли какое-либо из них на другое, и найдите частное: $1+i$ и 8; $2+i$ и $3+i$; $4-3i$ и $3+4i$.

7. Докажите, что для гауссовых чисел x и y следующие свойства эквивалентны: (1) Множество делителей x совпадает с множеством делителей y; (2) x делит y и y делит x; (3) $x = ry$, где $N(r) = 1$.

8. Показать, что норма $z = a + bi$ четна тогда и только тогда, когда $(1+i)|z$, в частности, если a и b имеют разную четность, то z не делится на $1+i$.

9. **a)** Докажите, что обратимые числа в точности числа с нормой 1. **b)** Докажите, что гауссово число $z \neq 0$ является простым тогда и только тогда, когда для любого разложения $z = wr$ какое-то из чисел w, r обратимо.

10. Являются ли простыми следующие гауссовы числа: $-i, 2, 3, 1+i, 2+i, 1+2i$?

11. Докажите, что гауссово число с простой нормой является простым.

12. Докажите, что простые натуральные числа разбиваются на два непересекающиеся множества: простые гауссовы числа и числа, которые являются нормой простых гауссовых чисел.

13. **a)** Докажите, что простое натуральное число p является нормой гауссового числа тогда и только тогда, когда $p = a^2 + b^2$ для натуральных a, b. **b)** Какие простые числа $p \leqslant 29$ являются простыми гауссовыми? **c)** Сформулируйте гипотезу об этих числах в общем виде и докажите её (*Указание*: используйте задачу У14:16).

УРОК 44

Гауссовы целые числа
Часть 2

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 12, раздел 12.2 Гауссовы целые числа.

Справочные сведения

НОД гауссовых чисел определяется с точностью до ассоциированности, т.е. в качестве НОД(z,w) выбирается любой представитель множества таких гауссовых чисел r, что $r|z$ и $r|w$ и норма r при этом максимально возможная. Слово «наибольший» здесь означает наибольшую норму.

Деление с остатком: при делении z на w ищем представление $z = wq + r$, где $N(r) < N(w)$. При этом q называется неполным частным, а r — остатком.

Гауссовы числа называются ***взаимно простыми***, если их НОД обратим. Обозначение: $z \perp w$.

Задачи

1. Пусть $z, w \in \mathbb{Z}[i]$, причем $w \neq 0$. **a)** Докажите, что существуют $q, r \in \mathbb{Z}[i]$ такие, что $z = wq+r$ и $N(r) < N(w)$. **b)** Сколькими способами можно выбрать такую пару гауссовых чисел?

2. **a)** Докажите, что НОД определен однозначно с точностью до умножения на обратимые. **b)** Докажите, что в гауссовых числах алгоритм Евклида для чисел z, w останавливается, в конце получается общий делитель d чисел z, w, который линейно выражается через изначальные два числа.

3. Найдите **a)** НОД$(7+9i, 10+2i)$; **b)** НОД$(7-i, -4+7i)$; **c)** НОД$(5+3i, 6-4i)$; **d)** НОД$(7, 3+i)$; **e)** НОД$(10+i, 3+4i)$.

4. Найдите НОД$(z, \overline{z})$ для произвольного $z \in \mathbb{Z}[i]$.

5. Разложите следующие гауссовы числа в произведение простых: $7+i$; $11+2i$.

6. Пусть a, b, c — такие взаимно простые целые числа, что $a^2+b^2 = c^2$. Докажите, что $c = |z|^2$ для некоторого $z \in \mathbb{Z}[i]$. (*Указание*: воспользуйтесь задачей У14:15)

7. Укажите все тройки целых чисел $a, b, c \in \mathbb{Z}$, таких что $a^2 + b^2 = c^2$. (То есть напишите формулу, которая дает все такие тройки при подстановке в нее целых чисел)

8. **a)** Верно ли, что целые числа a и b взаимно просты (как целые), если они взаимно просты как гауссовы? **b)** Верно ли обратное? **c)** Верно ли, что $z, w \in \mathbb{Z}[i]$ — гауссовы взаимно

простые числа, если $N(z)$ и $N(w)$ — взаимно просты (как натуральные)? **d)** Верно ли обратное?

9. Докажите, что если гауссово простое делит произведение zw, то оно делит либо z, либо w.

10. Сформулируйте и докажите основную теорему арифметики для гауссовых чисел.

УРОК 51

Многочлены, кольца и поля

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 4, раздел 4.1 Целые числа. Кольцо, Глава 9. Многочлены.

Справочные сведения

Многочлен (полином) степени n (где $n \in \mathbb{N}$) от одной переменной x — это формальная запись вида

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

где x — переменная, пробегающая некоторую числовую структуру (кольцо, поле и т.п.), $a_n, a_{n-1}, \ldots, a_0$ — некоторые числа (коэффициенты) из той же числовой структуры, причем $a_n \neq 0$.

Если многочлены задаются над кольцом K, то множество всех многочленов от переменной x над K обозначается $K[x]$.

Многочлены можно складывать, вычитать и умножать. Полагая $Q(x) = \sum_k b_k x^k$, определим операции:

$$(P+Q)(x) = \sum_k (a_k + b_k) x^k; \quad (PQ)(x) = \sum_k \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Мы намеренно не указываем пределы суммирования, чтобы упростить запись. Вместо этого мы предполагаем, что для всех $k > \deg P$ коэффициенты $a_k = 0$ (аналогично — для второго многочлена).

Степенью многочлена называется старший показатель n, степень многочлена P обозначается $\deg P$. Многочлен нулевой степени — это любая константа $a_0 \neq 0$. Число 0 является многочленом степени $-\infty$.

Если рассматривать степень многочлена как норму на множестве многочленов, то многочлены можно делить с остатком подобно гауссовым числам. Для многочленов деление P на Q с остатком означает найти такие многочлены S и R, что $P = QS + R$, где $\deg R < \deg Q$. Если $\deg R = -\infty$, то говорят, что P делится на Q, что записывается как $P \vdots Q$ или $Q | P$.

Множество K с заданными на нем двумя бинарными операциями $+$ и $\cdot$ называется ***кольцом***, если K является абелевой группой с операцией $+$, полугруппой с операцией $\cdot$, и обе операции связывает дистрибутивный закон (левый и правый):

R1 $a + b$, $ab \in K$, если $a, b \in K$;

R2 $(a + b) + c = a + (b + c)$ и $(ab)c = a(bc)$, если $a, b, c \in K$;

R3 существует элемент 0 такой, что: $a + 0 = a = 0 + a$, если $a \in K$;

R4 для всякого $a \in K$ существует $-a$ такой, что $a + (-a) = (-a) + a = 0$;

R5 $a(b+c) = ab + ac$ и $(a+b)c = ac + bc$, если $a, b, c \in K$;

R6 $a + b = b + a$, если $a, b \in K$.

Кольцо K называется ***кольцом с единицей***, если оно является моноидом по умножению, т.е. существует элемент $1 \in K$ такой, что $a \cdot 1 = 1 \cdot a = a$ для любого $a \in K$.

Кольцо K называется ***коммутативным кольцом***, если умножение в нем коммутативно, т.е. $ab = ba$ для всех $a, b \in K$.

Если не указано иное, мы будем считать, что кольцо K, над которым мы рассматриваем многочлены вида $P(x)$, является *коммутативным кольцом с единицей*.

Коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим (относительно операции умножения), называется ***полем***. Над полем обычно рассматриваются ***приведенные многочлены***, т.е. такие, у которых коэффициент при старшей степени равен 1.

Соответственно, вводится понятие ***подкольца*** — подмножество кольца, замкнутое относительно операций кольца и само являющееся кольцом с этими операциями.

Задачи

1. Доказать, что в любом кольце (даже некоммутативном и без единицы) выполняется аксиома нуля: $a \cdot 0 = 0 \cdot a = 0$.
2. Доказать, что $K[x]$ является кольцом (с единицей, коммутативным), если K — кольцо (с единицей, коммутативное).
3. Если K — поле, то будет ли $K[x]$ полем?
4. Доказать, что $\mathbb{Z}[i]$ (гауссовы числа, не путать с кольцом многочленов $\mathbb{Z}[x]$!) является кольцом.
5. Проверить, что $\mathbb{Z}/m\mathbb{Z}$ удовлетворяет аксиомам кольца.
6. Опишите группу остатков по сложению и умножению по модулю от 2 до 10.
7. При каких m кольцо $\mathbb{Z}/m\mathbb{Z}$ будет полем?
8. Докажите, что $m\mathbb{Z}$ — подкольцо (без единицы) кольца $\mathbb{Z}$, т.е. в нем также можно складывать, вычитать и умножать, m — произвольное целое положительное число.
9. Решите уравнение $x^2 = 1$ в $\mathbb{Z}/m\mathbb{Z}$ для $2 \leqslant m \leqslant 10$.
10. Разделите многочлен $5x^5 - x^3 + 3x - 2$ на $x - 3$ в $\mathbb{Z}/m\mathbb{Z}$ для $m = 7, 11, 13, 17, 19$.
11. Доказать, что если $P \vdots Q$ над полем, то либо $P = 0$, либо $\deg Q \leqslant \deg P$.
12. *Установить коммутативность произвольного кольца, в котором каждый элемент x удовлетворяет уравнению $x^2 = x$.

УРОК 52

Многочлены: делимость

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 9. Многочлены.

Справочные сведения

Мнгочлен $P \in K[x]$ называется ***неприводимым*** над K, если его невозможно представить в виде произведения многочленов более низких степеней, т.е. в виде $P = QR$, где $\deg Q, \deg R < \deg P$. Неприводимость формального многочлена над одним кольцом (полем) не означает его неприводимость над другим кольцом (полем). Неприводимый многочлен — это аналог простого числа в обычной арифметике (с тем отличием, что константа неприводима, а единица в арифметике не относится к простым числам).

Если многочлен R делит многочлены P и Q и никакой другой многочлен более высокой степени их не делит, то R называется ***наибольшим общим делителем*** P и Q.

Если НОД многочленов есть константа, то многочлены называются ***взаимно простыми*** ($P \perp Q$).

Задачи

1. Докажите, что (x^2-1) не делится на x^3. Перечислите все делители многочлена (x^2-1).
2. Пусть $P, Q, R \in \mathbb{R}[x]$. Докажите, что

   a) если $P \vdots R$ и $Q \vdots R$, то $(P \pm Q) \vdots R$;

   b) если $P \vdots R$ и Q — произвольный многочлен, то $PQ \vdots R$;

   c) если $P \vdots Q$ и $Q \vdots R$, то $P \vdots R$.
3. Верно ли, что любые многочлены удовлетворяют следующим свойствам:

   a) если P делится на R, а Q не делится на R, то $(P+Q)$ не делится на R;

   b) если P делится на Q, а Q не делится на R, то P не делится на R;

   c) если PQ делится на R^2 , то P делится на R или Q делится на R?
4. **a)** Остаток от деления $A(x)$ на $x-1$ равен 5, а на $x-3$ равен 6. Найдите остаток от деления $A(x)$ на $(x-1)(x-3)$. **b)** Найдите остаток от деления x^{1000} на x^2+x-1.
5. Найдите неполные частные и остатки от деления **a)** 10305 на 102; **b)** x^4+3x^2+5 на x^2+2; **c)** x^4+3x^2+5 на x^2+x+2; **d)** x^4+3x^2+5 на $x-1$; **e)** x^4+3x^2+5 на $x-c$, где $c \in \mathbb{R}$.
6. Найдите НОД многочленов над полем: **a)** $x(x-1)^3(x+2)$ и $(x-1)^2(x+2)^2(x+5)$; **b)** $3x^3-2x^2+x+2$ и x^2-x+1; **c)** x^m-1 и x^n-1; **d)** x^m+1 и x^n+1.

7. Разложите на неприводимые множители над $\mathbb{R}$ и на неприводимые множители над $\mathbb{Q}$: **a)** $5x+7$; **b)** x^2-2; **c)** x^3+x^2+x+1; **d)** $x^3-6x^2+11x-6$; **e)** x^3+3; **f)** x^4+4.

8. Разложите x^4-1 на неприводимые множители над кольцами $\mathbb{Z}/m\mathbb{Z}$ при $m = 2,3,4,5,6,7,8,9,10$.

9. Пусть K — поле и $P,Q \in K[x]$, причем $P \neq 0$ или $Q \neq 0$. Обозначим через $\mathcal{M}$ множество всех многочленов, представимых в виде $PU+QV$, где $U,V \in \mathbb{R}[x]$. Пусть D — один из многочленов наименьшей степени в $\mathcal{M}$.

   a) Докажите, что каждый многочлен из $\mathcal{M}$ делится на любой общий делитель многочленов P и Q.

   b) Докажите, что каждый многочлен из $\mathcal{M}$ делится на D.

   c) Докажите, что НОД(P,Q) всегда существует, причём определен лишь с точностью до множителя-константы.

   d) Сформулируйте и докажите алгоритм Евклида для многочленов.

   e) Докажите, что НОД(P,Q) делится на любой другой общий делитель этих многочленов.

   f) Докажите, что существуют $U,V \in \mathbb{R}[x]$ такие, что НОД$(P,Q) = PU+QV$.

10. Найдите НОД(P,Q), если **a)** $P(x) = x^2-4x+3$ и $Q(x) = 2x^2+4x-6$; **b)** $P(x) = \frac{2}{3}x^4 + x^3 - \frac{1}{4}x^2 + 1$ и $Q(x) = x^2 - x + \frac{1}{2}$;

11. Найдите НОД(P,Q) и его линейное выражение через $P,Q \in \mathbb{R}[x]$, если **a)** $P(x) = x^4+x^3-3x^2-4x-1$ и $Q(x) = x^3+x^2-x-1$; **b)** $P(x) = x^4+2x^3-x^2-4x-2$ и $Q(x) = x^4+x^3-x^2-2x-2$.

12. **a)** Докажите, что если P и Q — произвольные многочлены, а R — такой неприводимый многочлен, что $PQ \vdots R$, то либо $P \vdots R$, либо $Q \vdots R$. **b)** Сформулируйте и докажите основную теорему арифметики для многочленов.

УРОК 53

Многочлены: сравнения, теорема Безу

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 9. Многочлены.

Справочные сведения

Если разность многочленов $P - Q$ делится на многочлен R, то говорят, что P и Q ***сравнимы по модулю*** R ($P \equiv Q \pmod{R}$).

Пусть K — коммутативное кольцо с единицей, тогда имеет место ***теорема Безу́***: для любого многочлена $P \in K[x]$ и любой константы $c \in K$ имеет место представление

$$P(x) = (x - c)Q(x) + P(c),$$

причем $\deg Q = \deg P - 1$ ($\deg Q = -\infty$, если $\deg P = 0$).

Задачи

1. Пусть $P, Q, R \in \mathbb{R}[x]$, причём $R \neq 0$. Докажите, что $P \equiv Q \pmod{R}$ тогда и только тогда, когда многочлены P и Q имеют одинаковые остатки при делении на R.

2. Пусть $P_1, Q_1, P_2, Q_2, R, S \in \mathbb{R}[x]$, причем $R, S \neq 0$. Докажите следующие свойства сравнений:

   a) если $P_1 \equiv Q_1 \pmod{R}$ и $P_2 \equiv Q_2 \pmod{R}$, то $P_1 \pm P_2 \equiv Q_1 \pm Q_2 \pmod{R}$;

   b) если $P_1 \equiv Q_1 \pmod{R}$ и $P_2 \equiv Q_2 \pmod{R}$, то $P_1 P_2 \equiv Q_1 Q_2 \pmod{R}$;

   c) если $P_1 \equiv Q_1 \pmod{R}$, а $k \in \mathbb{N}$, то $P_1^k \equiv Q_1^k \pmod{R}$;

   d) если $P_1 \equiv Q_1 \pmod{RS}$, то $P_1 \equiv Q_1 \pmod{R}$.

3. Известно, что $P(x) \equiv x^2 \pmod{x^4 - x^3}$. Какой остаток даст x при делении на $(x - 1)$, x, $(x^2 - x)$ и x^3?

4. Какой остаток может дать $P(x)$ при делении на $(x^4 - x^3)$, если известно, что **a)** $P(x) \equiv x^2 \pmod{x^3}$ и $P(x) \equiv 1 \pmod{x - 1}$; **b)** $P(x) \equiv x \pmod{x^2 - x}$ и $P(x) \equiv 0 \pmod{x^2}$?

5. Рассмотрим кольцо многочленов над полем. Доказать ***теорему Безу***. Доказать, что $P(x)$ делится на $(x - c)$ тогда и только тогда, когда $P(c) = 0$.

6. Докажите, что число различных корней ненулевого многочлена над полем не превышает его степень.

7. Пусть $P \in \mathbb{Z}[x]$ и $m, n \in \mathbb{Z}$. Докажите, что число $P(m) - P(n)$ делится на число $m - n$.

8. В выражении $(x^5 - 6x^4 + 5x^2 + 1)^{2021}$ раскрыли скобки и привели подобные. Найдите: **a)** коэффициент при x^0 (свободный член); **b)** сумму всех коэффициентов; **c)** *сумму коэффициентов при четных степенях получившегося выражения.

9. *Сформулируйте и докажите признак делимости многочлена **a)** на $(x^3 - 1)$; **b)** на $(x^2 + x + 1)$.

УРОК 54

Многочлены и целые числа

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 9. Многочлены.

Задачи

1. Коэффициенты многочленов P и Q целые. Коэффициенты их произведения делятся на 5. Докажите, что либо коэффициенты P, либо коэффициенты Q делятся на 5.

2. На графике многочлена из $\mathbb{Z}[x]$ отмечены две точки с целыми координатами. Докажите, что если расстояние между ними — целое число, то у них одинаковые ординаты.

3. Пусть $P(x)$ — многочлен с целыми коэффициентами. **a)** Докажите, что $a-b$ делит $P(a)-P(b)$ при любых различных целых числах a и b. **b)** Пусть уравнения $P(x)=1$ и $P(x)=3$ имеют целое решение. Может ли уравнение $P(x)=2$ иметь два различных целых решения?

4. Пусть $P(x)$ — непостоянный многочлен с целыми коэффициентами. **a)** Докажите, что при любом целом числе n либо $P(n)$ делит $P(n+P(n))$, либо $P(n)=P(n+P(n))=0$. **b)** Могут ли все числа $P(0), P(1), P(2), \ldots$ быть простыми?

5. Квадратный трехчлен ax^2+bx+c при всех целых x принимает целые значения. Верно ли, что среди его коэффициентов **a)** хотя бы один — целое число; **b)** все — целые числа?

6. Докажите, что для любого многочлена $P(x)$ степени n, принимающего при всех целых x целые значения, существуют такие целые числа $b_0, b_1, \ldots, b_n$, что

$$P(x) = b_n\binom{x}{n} + b_{n-1}\binom{x}{n-1} + \cdots + b_1\binom{x}{1} + b_0.$$

   Указание: $P(x+1)-P(x)$ тоже многочлен, принимающий целые значения при целых x, но он меньшей степени.

7. Многочлен $P(x)$ степени $n-1$ принимает целые значения при n последовательных целых значениях x. Докажите, что $P(x)\in\mathbb{Q}[x]$ и $P(k)\in\mathbb{Z}$ при всех $k\in\mathbb{Z}$.

8. Докажите, что многочлен $(x-a_1)\ldots(x-a_n)-1$ не раскладывается в произведение двух многочленов меньшей степени из $\mathbb{Z}[x]$ при любых попарно различных целых числах $a_1, \ldots, a_n$.

УРОК 55

Многочлены: теорема Виета

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 9. Многочлены.

Справочные сведения

Для многочленов над полем существует понятие ***нормированного*** (или приведенного) многочлена — такого, у которого коэффициент при старшей степени равен 1. Ясно, что всякий многочлен над полем можно нормировать, что никак не влияет на делимость многочлена и поиск его корней. Поэтому многие утверждения проще формулировать именно для нормированных многочленов, в частности, теорему Виета: пусть

$$P(x) = (x - a_1)\dots(x - a_n) = x^n + x^{n-1}k_{n-1} + \dots + k_0,$$

тогда корни и коэффициенты этого многочлена связаны следующми равенствами:

$$\begin{aligned}
k_0 =& (-1)^n a_1 \dots a_n \\
k_1 =& (-1)^{n-1} a_1 \dots a_n \left(\frac{1}{a_1} + \dots + \frac{1}{a_n}\right) \\
k_2 =& (-1)^{n-2} a_1 \dots a_n \left(\frac{1}{a_1 a_2} + \dots + \frac{1}{a_{n-1}a_n}\right) \\
& \dots\dots \\
k_{n-2} =& (a_1 a_2 + \dots + a_{n-1}a_n) \\
k_{n-1} =& -(a_1 + \dots + a_n)
\end{aligned}$$

Задачи

1. **a)** Пусть многочлен $P(x) = x^3 + ax^2 + bx + c$ раскладывается на линейные множители (то есть многочлены первой степени): $P(x) = (x - a_1)(x - a_2)(x - a_3)$. Докажите, что справедливы формулы Виета: $a_1 + a_2 + a_3 = -a$, $a_1a_2 + a_2a_3 + a_3a_1 = b$, $a_1a_2a_3 = -c$. **b)** Доказать теорему Виета.

2. **a)** Пусть $a + b + c > 0$, $ab + bc + ac > 0$, $abc > 0$. Докажите, что a, b, c положительны. **b)** Пусть $a + b + c < 0$, $ab + bc + ac < 0$, $abc < 0$. Какие знаки могут иметь числа a, b, c?

3. **a)** Пусть число $c \neq 0$. Докажите, что многочлен $x^5 + ax^2 + bx + c$ не может раскладываться на пять линейных множителей. **b)** Та же задача для многочлена $x^5 + ax^4 + bx^3 + c$.

4. **a)** Коэффициенты многочлена $(x-a)(x-b)$ целые. Докажите, что $a^n + b^n$ целое при $n \in \mathbb{N}$. **b)** Найдите первые n цифр после запятой в десятичной записи числа $(\sqrt{26} + 5)^n$.

5. Целые числа a, b, c таковы, что числа $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ и $\frac{a}{c} + \frac{c}{b} + \frac{a}{b}$ целые. Докажите, что $|a| = |b| = |c|$.

УРОК 56

Многочлены: разное

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 9. Многочлены.

Задачи

1. Выполните действия с многочленами:

   a) $(1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16})$;

   b) $(1+x+x^2+x^3+\cdots+x^9)^2$;

   c) $(x^4-9x^3+16x^2+36x-80)/(x^2-4)$;

   d) $(x^{56}+x^{55}+x54+\cdots+x^2+x+1)/(x^{18}+x^{17}+\cdots+x+1)$.

2. Многочлены $P(x)$ и $Q(x)$ имеют целые коэффициенты, причем каждый из них имеет хотя бы один нечётный коэффициент. Докажите, что у произведения $P(x)Q(x)$ также есть хотя бы один нечётный коэффициент.

3. Делится ли **a)** $x^{1000}+x^{999}+\cdots+x+1$ на $x^5+x^4+x^3+x^2+x+1$; **b)** x^4+x-2 на $x+2$; **c)** 57 на $x-2$?

4. Пусть $P(x)$ — многочлен степени n, и пусть a — некоторое число. Докажите, что $P(x)$ можно записать в виде $c_0+c_1(x-a)+\cdots+c_n(x-a)^n$, подобрав подходящие числа $c_0,\ldots,c_n$.

5. Многочлен P таков, что $P(x^n)$ делится на $x-1$. Докажите, что $P(x^n)$ делится на x^n-1.

6. Даны многочлены положительной степени $P(x)$ и $Q(x)$, причём выполнены тождества $P(P(x))=Q(Q(x))$ и $P(P(P(x)))=Q(Q(Q(x)))$. Обязательно ли $P(x)$ и $Q(x)$ совпадают?

7. Барон Мюнхгаузен попросил задумать непостоянный многочлен $P(x)$ с целыми неотрицательными коэффициентами и сообщить ему только значения $P(2)$ и $P(P(2))$. Барон утверждает, что лишь по этим данным всегда может восстановить задуманный многочлен. Не ошибается ли барон?

8. Существует ли такой многочлен $P(x)$, что у него есть отрицательный коэффициент, а у каждой его степени $(P(x))^n$, где $n>1$, все коэффициенты положительны?

9. Существуют ли такие многочлены $P(x)$ и $Q(x)$ из $\mathbb{R}[x]$, что каждое рациональное число r представимо в виде $r=P(k)/Q(k)$ для некоторого целого числа k?

УРОК 57

Малая теорема Ферма
критерий Вильсона

Связь с онлайн курсом и главами конспекта:

Конспект: Глава 9. Многочлены.

Справочные сведения

Малая теорема Ферма: $n^{p-1} \equiv 1 \pmod{p}$, если $n \perp p$ (т.е. они взаимно просты).

Задачи

1. Число p простое. Докажите, что $\binom{p}{k}$ делится на p, если $0 < k < p$.
2. (Малая теорема Ферма). Пусть p — простое, n — целое. **a)** Докажите индукцией по n, что $n^p - n$ делится на p. **b)** Докажите, что если $n \perp p$, то $n^{p-1} - 1$ делится на p.
3. Пусть $a \perp p$ и p — простое. **a)** Докажите, что числа $a, 2a, \ldots, (p-1)a$ имеют разные ненулевые остатки от деления на p. **b)** Выведите отсюда малую теорему Ферма.
4. Докажите, что $2222^{5555} + 5555^{2222}$ делится на 7.
5. **a)** Числа p и q простые, $2p-1$ делится на q. Докажите, что $q-1$ делится на p. **b)** Простое ли $2^{13} - 1$? **c)** Простое ли число $257^{60} + 60$?
6. Пусть p не равно 5. Докажите, что среди чисел, записываемых только единицами, есть число, которое делится на p.
7. Пусть p простое. **a)** Докажите, что для каждого ненулевого остатка a от деления на p найдётся такой остаток b от деления на p, что $ab \equiv 1 \pmod{p}$. **b)** Для каких a из предыдущего пункта $b = a$? **c)** Докажите, что сравнение $x^2 \equiv a \pmod{p}$ имеет не больше двух корней. **d)** Что будет с этим сравнением в случае не простого модуля m? **e)** Решите сравнение $x^2 \equiv 1 \pmod{p}$. **f)** [*Критерий Вильсона*] Докажите, что $(p-1)! + 1$ делится на p тогда и только тогда, когда p — простое.
8. (Второе доказательство критерия Вильсона). Рассмотрим многочлен $x^{p-1} - 1$ как многочлен в $\mathbb{Z}/p\mathbb{Z}$. **a)** Все ненулевые остатки являются его корнями. **b)** Произведение остатков равно -1.
9. Пусть p — простое вида $4k+1$, и пусть $x = (2k)!$. Докажите, что $x^2 \equiv -1 \pmod{p}$.