Материалы летней школы «Матфак: предисловие»

под редакцией Хайдара Нурлигареева

Москва, август 2020 г.

Предисловие к летней школе 2020

Настоящее пособие представляет собой раздаточные материалы летней школы математического факультета «Матфак: предисловие 2020». О её целях и задачах будет подробно рассказано во Вступительном слове ниже, здесь же мы очертим структуру занятий, а также характерные особенности, присущие школе в 2020 году по причине коронакризиса.

Традиционно программа школы включает в себя следующие три вида деятельности.

1. **Просмотр видеолекций.** Каждый участник делает это самостоятельно в собственном ритме, в зависимости от своих потребностей и привычек. Полный список видеолекций 2020 года приведён в соответствующем разделе. Объём предлагаемого видеоматериала довольно большой — в 2020 году даже с учётом рекомендованной скорости воспроизведения он составлял около 10 часов. Поэтому в идеале мы бы настоятельно рекомендовали потенциальным участникам школы начать прорабатывать его заранее, хотя бы за две-три недели до старта школы. Это позволило бы во время занятий сосредоточиться на более детальном обдумывании сложных вопросов и на осмысленном решении задач.

2. **Семинарские занятия.** Все участники школы распределены по группам численностью 5-10 человек в соответствии со своим текущим уровнем подготовки, и семинары проводятся отдельно для каждой группы. В 2020 году наполненность групп составляла 6-8 человек в начале школы, а семинары проходили в формате видеоконференций при помощи платформ zoom и discord. Продолжительность одного семинарского занятия — 1 час 20 минут, посередине занятия предусмотрен пятиминутный перерыв.

3. **Математический практикум,** он же — приём задач. На наш взгляд, это наиболее важная активность школы, которая проводится в форме индивидуальных бесед с семинаристами и принимающими-волонтёрами из числа студентов и аспирантов математического факультета. В 2020 году для приёма задач использовалась платформа discord, в среднем на него отводилось полтора часа в день.

Нам бы хотелось особо подчеркнуть значимость математического практикума. К сожалению, часто случается, что участники недооценивают приносимую им пользу (и, как нам кажется, 2020 год не стал исключением). Однако как раз практикум является основным катализатором развития, поскольку именно во время вдумчивой беседы со старшим товарищем приходит осознание, как устроены те или иные аспекты теории, возникает внимание к деталям. Важно отметить, что начинать беседу с преподавателем стоит не только в тот момент, когда задача решена, но и тогда, когда усердные раздумия над ней не дали результата, а мозг поставлен в тупик. И уже тем более необходимо обратиться за помощью, если ощущения лучше всего характеризуются словами «ничего не понятно».

Опишем подробнее структуру настоящей брошюры. Непосредственно за Оглавлением следует Вступительное слово, из которого читатель в подробностях узнает о причинах возникновения летней школы «Матфак: предисловие» и её целях и задачах. Далее можно найти Список видеолекций 2020 года, снабжённый интерактивными ссылками на видео, размещённые на платформе youtube. Ниже даются задачи Вступительного теста, предлагавшегося участникам перед началом школы для распределения их по группам в соответствии с уровнем текущей подготовки. Основной объём брошюры составляют нумерованные главы, наполненные теоретическим и практическим материалом, и Математический практикум. Завершают брошюру Ответы и указания к упражнениям, а также Список рекомендованной литературы.

Каждая нумерованная глава содержит материал, относящийся к той или иной математической теме: логике, множествам, индукции и т.д. Первая часть такой главы — теоретическая и во многом повторяет лекционный материал. Таким образом, просмотр видеолекций можно дополнить и закрепить чтением теоретической части брошюры. Вторая часть состоит из задач, предназначенных для обсуждения на семинаре. Мы не предполагаем, что все эти задачи непременно должны быть разобраны в ходе семинарских занятий. Более того, мы не считаем, что обязательно ограничиваться только ими. Скорее, речь идёт о рекомендованном направлении, от которого допустимо отступать в зависимости от нужд аудитории. В том случае, когда задач по теме подобралось много, часть из них помечена специальными символами: так, символом **(T)** обозначается техническая задача, а **(C)** — это задача, предназначенная к первоочередному разбору на семинаре.

Особняком стоит глава, посвящённая математическому практикуму. В ней нет никакой теории, она состоит исключительно из задач, пробегающих все затронутые на школе темы и предназначенных для самостоятельного решения. Однако ошибочно было бы думать, что во время приёма задач участники школы обсуждают с принимающими лишь задачи из этой главы. Мы поощряем обсуждать с принимающими любые интересные или вызывающие ступор факты, будь то понятия из видеолекций, теоретические вопросы из брошюры или семинарские задачи.

Отметим, что в 2020 году в некоторых аспектах видеолекции довольно заметно отличались от теоретического материала брошюры. Это связано с тем, что большая часть видео записывалась, исходя из потребностей летней школы 2019 года, а внести в них изменения в связи с непростой эпидемиологической ситуацией возможности не было. В подобных случаях материал в брошюре изложен более подробно. Также нельзя обойти вниманием тот факт, что значительная часть брошюры версталась в условиях цейтнота прямо во время работы школы. Этим отчасти объясняются присущие ей недостатки.

В заключение хотелось бы выразить искреннюю признательность всем аспирантам и сотрудникам факультета математики ВШЭ и других учреждений, благодаря которым появление этой брошюры оказалось возможным. К сожалению, у нас нет уверенности в том, что приведённый ниже список полон, столь многие за прошедшие три года внесли свой вклад в развитие школы. Тем не менее, нам кажется важным перечислить приложивших к этому руку поимённо. Прежде всего, это авторы отдельных

разделов — Ренат Абугалиев, Владислав Балакирев, Арина Воорхаар, Юлия Горгинян, Евгений Красильников, Алексей Клименко, Иван Никитин и Анастасия Шепелевцева. В не меньшей степени нужно благодарить авторов видеоматериалов, на основе которых была написана брошюра, — Бориса Бычкова, Алексея Клименко, Марию Матушко, Дмитрия Минеева, Андрея Рябичева, Владлена Тиморина, Александра Тихомирова и особенно Александра Штерна, чьи записи послужили основой глав «Математическая логика» и «Математическая индукция». Также хотелось бы сказать спасибо всем тем, кто готовил материалы в предыдущие годы, заложив тем самым надёжный фундамент для нашей работы — это, помимо вышеперечисленных, Равиль Габдурахманов, Валентина Кириченко, Константин Козеренко, Андрей Кудинов, Григорий Мерзон, Алексей Пахарев и Владимир Шарич. Наконец, особую признательность хотелось бы выразить «отцу-основателю» и руководителю предыдущих школ Александру Эстерову, вдумчивое внимание и кропотливый труд которого послужили опорой не только для настоящей брошюры, но и для всей школы «Матфак: предисловие» в целом. Кроме того, мы благодарны Арине Банниковой, создавшей для этой брошюры яркую обложку, всем студентам математического факультета, оказавшим нам помощь на добровольных началах, а также участникам школы, высказавшим ряд ценных замечаний, которые помогут сделать летнюю школу, и, в частности, эту брошюру, лучше в будущем.

Хайдар Нурлигареев,
23 сентября 2020 года.

Оглавление

Вступительное слово

Давно замечено, что в начале обучения первокурсники, по независящим от них причинам, имеют очень разный уровень подготовки. Во многом это обусловлено тем фактом, что между любой университетской программой по специальности Фундаментальная Математика и нынешней школьной программой лежит «ничейная земля». К ней относятся, прежде всего, классические темы так называемой «олимпиадной математики» — индукция, комбинаторика, делимость целых чисел, многочлены и некоторые аспекты геометрии. Однако мы бы причислили к ней также начала анализа и логики, такие как язык теории множеств и базовые факты, относящиеся к построению действительных и комплексных чисел. Обозначенному выше кругу вопросов, на наш взгляд, во многих школах уделяют недостаточное внимание. Однако возможности задержаться на них подольше на первом курсе обычно нет: при глубоком и вдумчивом подходе это заняло бы слишком много времени. Так, в ведущих математических школах на освоение подобной программы обычно выделяется от трёх до пяти лет ([6],[7], [9], [18]). Не меньше времени тратит на решение математических задач и школьник, влившийся в олимпиадное движение и проходящий путь от вечерних математических кружков до выездных школ и сборов ([5], [10], [12]). Справедливости ради, нельзя не отметить, что использующаяся в ряде математических школ система Константинова предполагает не только насыщенную практическую часть, но и «переоткрытие» школьником теории, которая также даётся в виде задач. Это же в определённом смысле справедливо и для олимпиадых кружков, хотя они и не всегда претендуют на столь же фундаментальный подход к образованию.

Для того, чтобы нивелировать разницу в исходных позициях абитуриентов и помочь всем желающим освоить вышеупомянутую «ничейную землю», начиная с 2018 года математический факультет Высшей Школы Экономики проводит летнюю школу «Матфак: предисловие». Было бы наивно думать, что за две недели можно полноценно освоить материал, на который в математических школах тратят три года. К счастью, в подавляющем большинстве случаев речь не идёт об освоении с нуля. Почти всегда поступающие на факультет абитуриенты уже знакомы с теми или иными аспектами программы, а потому имеет смысл говорить, скорее, о восполнении лакун в уже существующих познаниях и формировании целостной картины мира. Не менее важными видятся и другие цели летней школы. По замыслу создателей двухнедельный интенсив должен позволить абитуриентам заранее почувствовать, что их ждёт во время обучения на математическом факультете, и втянуться в учебный процесс ещё до начала учебного года. Также нельзя недооценивать роль знакомства с коллективом. В условиях, когда олимпиадники и выпускники математических школ уже давно варятся в определённой среде и знакомы с частью преподавателей, аспирантов и студентов старших курсов ещё до поступления на факультет, человек извне может чувствовать себя если не посторонним, то по крайней мере «бедным родственником». Поэтому нам кажется крайне важным обеспечить для вновь принятого студента безболезненную адаптацию на новом месте. Предусмотренные летней школой активности — лекции, семинары и особенно

математический практикум, предполагающий индивидуальное взаимодействие со старшекурсниками или аспирантами, принимающими задачи, — отчасти выполняют и эту функцию тоже.

Особо отметим необходимое, на наш взгляд, исключение из процесса летней школы соревновательных и оценочных составляющих. Сбор информации о зачтённых задачах если и ведётся, то лишь с целью анализа подачи материала и дальнейшего его совершенствования. Точно так же финальные контрольные работы, в том случае, когда они проводятся, служат, прежде всего, для того, чтобы понять, насколько летняя школа удалась. С другой стороны, мы не можем отрицать того факта, что и для участников школы финальная работа может иметь несомненный интерес: с её помощью последние могут определить, чему им удалось научиться на школе, а каким разделам математики имеет смысл уделить дополнительное внимание в будущем. В конечном итоге реальный смысл для каждого имеет лишь сравнение с самим собой вчерашним, и если школа «Матфак: предисловие» поможет кому-то стать чуточку лучше и хоть немного приблизиться к своей цели, то мы уже с уверенностью сможем сказать, что наша работа была выполнена не зря.

В заключение хотелось бы подчеркнуть, что невозможность наверстать столь обширный материал за две недели — это не повод отчаиваться. Опыт показывает, что за время обучения на бакалавриате по специальности Фундаментальная Математика разница между многоопытными олимпиадниками и неискушёнными абитуриентами стирается. Во многом это происходит за счёт того, что по интенсивности погружения в науку четыре года бакалавриата значительно превосходят четыре года в математической школе. Это же соображение должно стать предостережением для выпускников математических классов: впечатление всезнания обманчиво, а соблазн почивать на лаврах кого-то раньше, кого-то позже неизбежно приведёт к печальному финалу. В конечном итоге на выходе решающую роль играет лишь то, насколько студент увлечён математикой и как много времени он уделяет учёбе. При этом первостепенное значение в достижении результата имеет потраченное время, а ключевой составляющей успеха являются мотивация и любовь к делу. Нам сложно представить первое без второго, и мы бы очень не рекомендовали заниматься математикой профессионально людям, которые не получают от этого удовольствия, поскольку это весьма трудозатратная и непростая деятельность. В частности, если в процессе учёбы студент поймёт, что математика не приносит ему удовольствия, и переведётся на другой, более привлекающий его факультет, — это тоже успех. Ведь чем раньше человек осознает, чем именно он хотел бы заниматься по жизни (или, хотя бы, чем заниматься точно не хотел бы), тем больше времени у него будет на самореализацию и исполнение заветных желаний, и тем счастливее в конечном счёте он будет.

Список видеолекций

Основные видеоматериалы.

1. Математическая логика (Александр Штерн)
   Рекомендованная скорость воспроизведения: 1.25.

2. Множества (Владлен Тиморин)
   Рекомендованная скорость воспроизведения: 1.25.

3. Отображения (Владлен Тиморин)
   Рекомендованная скорость воспроизведения: 1.25.

4. Математическая индукция (Александр Штерн)
   Рекомендованная скорость воспроизведения: 1.25.

5. Делимость целых чисел – 1 (Борис Бычков)
   Рекомендованная скорость воспроизведения: 1.25.

6. Делимость целых чисел – 2 (Дмитрий Минеев)
   Рекомендованная скорость воспроизведения: 1.

7. Комбинаторика (Андрей Рябичев)
   Рекомендованная скорость воспроизведения: 1.5.

8. Делимость многочленов (Дмитрий Минеев)
   Рекомендованная скорость воспроизведения: 1.

9. Сравнения (Мария Матушко)
   Рекомендованная скорость воспроизведения: 1.5.

10. Действительные числа (Алексей Клименко)
    Рекомендованная скорость воспроизведения: 1.5.

11. Движения плоскости и векторы (Александр Тихомиров)
    Рекомендованная скорость воспроизведения: 1.75.

12. Комплексные числа (Александр Тихомиров)
    Рекомендованная скорость воспроизведения: 1.75.

Дополнительные видеоматериалы.

1. Математический уровень строгости (Андрей Кудинов)
   Рекомендованная скорость воспроизведения: 1.75.

2. Математическая индукция — дополнительные материалы (Александр Штерн)
   Рекомендованная скорость воспроизведения: 1.25.

3. Действительные числа — аксиоматический подход (Алексей Клименко)
   Рекомендованная скорость воспроизведения: 1.5.

4. Мера: длина, площадь, объём (Алексей Клименко)
   Рекомендованная скорость воспроизведения: 1.5.

Вступительный тест

Условия задач

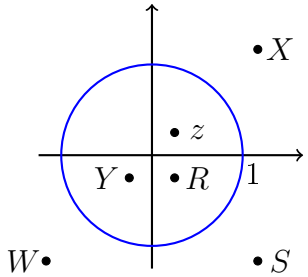
Задача 0.1. Найдите последнюю цифру числа $2^{2021} + 9^{2019}$.

Задача 0.2. Даны множества $A = \{1, 2, 3, 4\}$ и $B = \{x, y, z, w\}$. Сколько элементов в множестве $A \times B = \{(a, b) \mid a \in A, b \in B\}$?

Задача 0.3. Найдите сумму действительных корней уравнения $x^3 + 2x^2 + 3x + 2 = 0$.

Задача 0.4. Имеется 3 пары брюк, 4 рубашки и 5 шляп. Сколькими способами можно одеться?

Задача 0.5. Среди чисел X, Y, R, S и W выберите обратное к z.



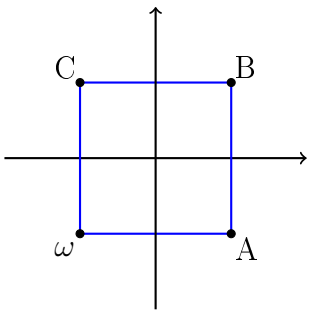
Задача 0.6. У числа 2020! посчитали сумму цифр, затем у получившегося числа тоже посчитали сумму цифр и так далее. Так продолжали до тех пор, пока не получилось однозначное (состоящее из одной цифры) число. Какое?

Задача 0.7. Из скольких элементов состоит пересечение множеств

$$\{0, 17, 36, 99, 127, 144, 243, 572\} \qquad \text{и} \qquad \{9n \mid n \in \mathbb{N},\ 1 \leqslant n \leqslant 15\}?$$

Задача 0.8. Найдите коэффициент при x^{2018} многочлена $(1 + x)^{2020}$.

Задача 0.9. Одна из вершин квадрата соответствует комплексному числу ω. Установите соответствие между множествами $\{A, B, C\}$ и $\{\bar{\omega}, -\omega, i\omega\}$.



Задача 0.10. Сколько подмножеств у множества $\{\{1\}, 0, 1, \{0\}, \varnothing\}$?

Задача 0.11. Найдите максимальное число n такое, что $40!$ делится на 2^n.

Задача 0.12. Вычислите сумму $C_{11}^0 + C_{11}^1 + C_{11}^2 + \ldots + C_{11}^{10} + C_{11}^{11}$.

Задача 0.13. Какое из приведённых ниже утверждений эквивалетно следующему: «Если A истинно, то B ложно»? Варианты ответа:

а) «Если A ложно, то B истинно».

б) «Если B истинно, то A истинно».

в) «Если B истинно, то A ложно».

г) «Если B ложно, то A истинно».

д) «A истинно или B истинно».

Задача 0.14. Найдите произведение комплексных корней уравнения $x^3+x^2+x+1=0$.

Задача 0.15. Какие из указанных чисел являются целыми? Укажите все варианты:

а) $\dfrac{n^m-1}{n-1}$,

б) $\dfrac{1000!}{(100!)^{10}}$,

в) $\dfrac{n^4+n^2+1}{n^2+n+1}$,

г) $[\log_{29}(n^3+1)]+0.01$,

д) $\dfrac{(1+\sqrt{2})^n}{2}+\dfrac{(1-\sqrt{2})^n}{2}$.

Задача 0.16. Найдите остаток от деления многочлена $f(x)=x^{150}+x+1$ на $(x-1)$.

Задача 0.17. Пусть A — множество учеников 8У класса, любящих футбол. Пусть, далее, B — множество учеников 8У класса, умеющих играть на скрипке. Наконец, пусть C — множество учеников 8У класса, у которых есть сестра. Какая из приведённых ниже формул описывает множество учеников 8У класса, у которых нет сестры, но которые любят футбол и умеют играть на скрипке? Варианты ответа:

а) $(A \setminus B) \cup (B \setminus C)$.

б) $(A \cap B) \setminus (B \cup C)$.

в) $(A \cap B) \setminus (A \cap B \cap C)$.

г) $(A \cap B \cap C) \cup (B \cap C)$.

Задача 0.18. Сколько существует одночленов полной степени d от n переменных?

Задача 0.19. Выберете из списка все верные утверждения.

а) Для любого комплексного числа z величина $z \cdot \bar{z}$ является вещественной.

б) Окружность радиуса 3 с центром в точке i можно задать как множество точек z, удовлетворяющих равенству $|z-i|=9$.

в) Если p — многочлен и $p(z)=i$, то и $p(\bar{z})=i$.

г) Для любого комплексного числа z его квадрат z^2 является вещественным числом.

д) Произведение всех корней седьмой степени из единицы равно единице, а их сумма равна минус единице.

е) Пусть точки X, Y и Z имеют комплексные координаты $27-4i$, $2-10i$ и $-4+15i$ соответственно. Тогда прямые XY и YZ перпендикулярны.

Задача 0.20. Перечислите движения, которые можно представить в виде композиции двух поворотов. Укажите все подходящие варианты.

а) Параллельный перенос.
б) Поворот.
в) Осевая симметрия.
г) Центральная симметрия.
д) Скользящая симметрия.

Задача 0.21. Найдите остаток от деления многочлена $x^{150}+1$ на x^2+x+1.

Задача 0.22. Пусть утверждения A и C истинны, а B ложно. Какие из выражений ниже истинны? Укажите все варианты ответа:

а) $A \to (B \wedge C)$.
б) $\neg(B \to (A \vee C))$.
в) $(\neg A \vee C) \wedge (\neg B)$.
г) $(\neg A) \wedge (\neg B) \wedge C$.

Задача 0.23. Справедливы ли приведённое ниже утвержение и его доказательство?
«Докажем по индукции, что если треугольник разбит на меньшие треугольники отрезками (не обязательно диагоналями), то хотя бы один из треугольников разбиения не остроугольный. Во-первых, заметим, что если треугольник разбит отрезком на два треугольника, то один из них не остроугольный. Далее, пусть некоторый треугольник разбит на n меньших треугольников. Проведём ещё один отрезок, разбив один из маленьких треугольников на два. Получим разбиение на $(n+1)$ треугольник, причём один из двух новых треугольников не остроугольный. По индукции теорема доказана.»
Варианты ответа.

а) Утверждение верное, доказательство верное.
б) Утверждение верное, но в базе индукции ошибка.
в) Утверждение верное, но в индукционном переходе ошибка.
г) Утверждение неверное, ошибка в базе индукции.
д) Утверждение неверное, ошибка в индукционном переходе.

Задача 0.24. Среди n рыцарей каждые двое — либо друзья, либо враги. У каждого из рыцарей ровно три врага, причём враги его друзей являются его врагами. При каких n такое возможно?

Задача 0.25. Уравнение $z^6+z^3+1=0$ имеет решение, аргумент которого лежит в промежутке $[\pi/2, \pi]$. Найдите аргумент этого решения.

Задача 0.26. На сколько частей 200 прямых общего положения (никакие 2 не параллельны и никакие 3 не проходят через одну точку) делят плоскость?

Задача 0.27. Число x даёт остаток 3 при делении на 8, остаток 1 при делении на 11, и остаток 12 при делении на 15. Сколько существует таких четырёхзначных положительных x?

Математическая логика

Теоретический материал

1.1. Высказывания и логические операции

Математика — строго дедуктивная наука. Никакие ссылки на наблюдения и опыт в ней не принимаются. В первом приближении (очень грубом) все высказывания в математике должны быть получены из определений и аксиом с помощью некоторого логического вывода. Мы не будем строго объяснять, что это значит, но попробуем описать некоторые важные элементы, из которых этот вывод складывается. В математике (как и везде) мы работаем с высказываниями.

Определение 1.1. *Высказывание* — повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности.

Пример 1.1.

- A : «Все лебеди белые»;
- B : «5 – нечётное число»;
- C : «Нью-Йорк – столица США».

Определение 1.2. Имеется два *истинностных значения* — «истина» (И) и «ложь» (Л). В разных источниках они могут обозначаться по-разному, например: (И/Л), (T/F), (1/0), ($\top/\bot$), и т.д.

Упражнение 1.1. *Установите истинностные значения высказываний из примера 1.1*

Определение 1.3. *Логическая операция* – способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний.

Основные логические операции:

• *конъюнкция* $X \wedge Y$ («X и Y») истинна тогда и только тогда, когда истинны оба высказывания X, Y;

• *дизъюнкция* $X \vee Y$ («X или Y») истинна тогда и только тогда, когда истинно хотя бы одно из высказываний X, Y;

• *отрицание* $\neg X$ («не X») истинно тогда и только тогда, когда X ложно.

Замечание. В отличие от математического языка, в естественном языке чаще используется так называемое «исключающее или». Иными словами, говоря «X или Y», мы имеем в виду, что истинно либо X, либо Y, но никак не оба высказывания.

Пример 1.2. Пусть высказывания X и Y таковы:

X: в четырёхугольнике $ABCD$ выполнено $AB \parallel CD$.

Y: в четырёхугольнике $ABCD$ выполнено $AD \parallel BC$.

Тогда:

$X \wedge Y$: четырёхугольник $ABCD$ — параллелограмм.

$X \vee Y$: четырёхугольник $ABCD$ — параллелограмм или трапеция.

Упражнение 1.2. *Рассмотрим следующую пару высказываний.*

X : *n – натуральное число, большее 2;*

Y : *n – натуральное число, меньшее 4.*

Что означают высказывания $X \wedge Y$ и $X \vee Y$?

1.2. Импликация и эквивалентность

Помимо основных связок «и», «или», «не» в речи мы часто используем и более сложные, например, связку «если ..., то ... ». Несомненно, в математическом языке такая операция была бы очень полезна. Однако, здесь стоит заметить, что используемая в естественном языке импликация «если X, то Y» *не является* логической операцией в смысле определения 1.1, так как истинность данного высказывания определяется не только истинностными значениями самих высказываний X и Y, но и наличием причинно-следственной связи между ними.

Поэтому в математическом языке мы считаем *импликацию* $X \to Y$ истинной тогда и только тогда, когда либо высказывание Y истинно, либо высказывание X ложно. Смысл очень простой: из истинного высказывания ложное не следует, а во всех остальных случаях импликация верна.

Определение 1.4. Высказывания X и Y *эквивалентны* ($X \Leftrightarrow Y$), если они следуют друг из друга, то есть, если истинно высказывание $(X \to Y) \wedge (Y \to X)$.

1.3. Пропозициональные формулы

Мы уже знаем из предыдущих разделов, что высказывания получаются из более простых с помощью логических операций (связок). Более того, мы уже видели первые примеры записи высказываний в виде формул — последовательностей букв (например, латинского алфавита), логических символов $\neg, \wedge, \vee, \to$ и скобок. Разумеется, таким образом можно получить далеко не любую последовательность указанного вида. Например, никакого смысла не имеет запись «$\wedge)X\neg$».

Определение 1.5. Элементарные высказывания, из которых строятся все остальные, называются *пропозициональными переменными*. Их мы обозначаем заглавными латинскими буквами.

Определение 1.6. *Пропозициональные формулы* строятся из пропозициональных переменных по следующим правилам:

1. всякая пропозициональная переменная является формулой;
2. если φ — пропозициональная формула, то $\neg\varphi$ — пропозициональная формула;
3. если φ и ψ — пропозициональные формулы, то $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ и $(\varphi \to \psi)$ тоже являются пропозициональными формулами.

Для того, чтобы у нас была возможность однозначно интерпретировать пропозициональные формулы, важно зафиксировать порядок выполнения логических операций. Приведём список логических операций в порядке их выполнения (от наибольшего приоритета к наименьшему):

1. отрицание ($\neg$);
2. конъюнкция ($\wedge$);
3. дизъюнкция ($\vee$);
4. импликация ($\to$);
5. эквивалентность ($\Leftrightarrow$).

Отметим, что порядок действий всегда можно изменить скобками.

Пример 1.3. $X \wedge Y \vee Z$ и $X \wedge (Y \vee Z)$ — разные высказывания (см. пример 1.5).

Упражнение 1.3. *Сколько существует пропозициональных формул от двух переменных, в которых используется две операции, каждая из которых является либо конъюнкцией, либо дизъюнкцией, либо отрицанием?*

1.4. Таблицы истинности

Ключевым свойством логических операций является то, что истинностное значение сложного высказывания полностью определяется истиностными значениями высказываний, из которых оно образовано. Следовательно, если вместо всех пропозициональных переменных, которые содержатся в формуле φ, всеми возможными способами подставить истинностные значения 0 и 1, то можно однозначно вычислить истинностные значения формулы φ. Результаты таких подстановок можно записать в таблицу, которая называется *таблицей истинности* формулы φ.

Пример 1.4. Приведем таблицы истинности известных нам формул: $\neg X$, $(X \wedge Y)$, $(X \vee Y)$, $(X \to Y)$. Для удобства объединим три из них в одну.

X	$\neg X$
0	1
1	0

X	Y	$(X \wedge Y)$	$(X \vee Y)$	$(X \to Y)$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

Определение 1.7. Формулы φ и ψ *эквивалентны*, если они истинны при одних и тех же значениях переменных.

Упражнение 1.4. *С помощью таблиц истинности докажите эквивалентность формул $X \wedge (X \to Y)$ и $X \wedge Y$.*

Пример 1.5. Построим и сравним таблицы истинности формул из примера 1.3. Начнём с формулы $X \wedge Y \vee Z$. Заметим, что таблицу истинности формулы можно строить поэтапно, учитывая способ, которым формула была получена. В данном случае, мы начали с формул X и Y. Далее, с помощью конъюнкции построили формулу $X \wedge Y$, а затем, взяв ещё одну формулу Z, дизъюнкцией получили $X \wedge Y \vee Z$.

Формула $X \wedge (Y \vee Z)$ была построена чуть-чуть иначе. Сначала из элементарных формул Y и Z дизъюнкцией была получена формула $Y \vee Z$, а затем, с помощью конъюнкции с X уже была получена интересующая нас формула.

Следовательно, искомые таблицы истинности устроены следующим образом.

X	Y	Z	$X \wedge Y$	$X \wedge Y \vee Z$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

X	Y	Z	$Y \vee Z$	$X \wedge (Y \vee Z)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Таким образом, мы вычислили, что первая формула ложна тогда и только тогда, когда одновременно ложны высказывание Z и хотя бы одно из высказываний X и Y. Вторая формула ложна, если X ложно, либо ложны оба высказывания Y и Z. Как можно видеть, данные формулы не эквивалентны.

Определение 1.8. Формула φ является *тавтологией*, если она истинна при любых значениях входящих в неё переменных.

Упражнение 1.5. *Докажите, что формула $(X \to Y) \vee (Y \to X)$ является тавтологией.*

Упражнение 1.6. *Докажите, что формулы φ и ψ эквивалентны тогда и только тогда, когда формула $(\varphi \to \psi) \wedge (\psi \to \varphi)$ является тавтологией.*

1.5. Дополнительные логические связки

Помимо операций $(\wedge, \vee, \neg)$ на практике удобно использовать дополнительные логические связки, упрощающие работу с формулами и сокращающие их запись.

Пример 1.6. Запись $X \to Y$ на самом деле является сокращением.

Упражнение 1.7. *Выразите импликацию $(\to)$ через основные логические связки, то есть через операции $(\wedge, \vee, \neg)$.*

Пример 1.7. Аналогично, запись $X \Leftrightarrow Y$, является сокращением более длинной записи $(X \to Y) \wedge (Y \to X)$, использующей операции $(\wedge, \to)$.

1.6. Прямое и обратное утверждение

Определение 1.9. Если некоторое утверждение имеет вид импликации $X \to Y$, то утверждение $Y \to X$ называется *обратным* к нему.

Замечание. Истинность обратного утверждения никак не связана с истинностью прямого утверждения.

Пример 1.8. Рассмотрим следующую пару высказываний:

X : «Данное целое число n оканчивается на 4»,

Y : «Данное целое число n чётно».

Высказывание $X \to Y$ означает следующее: «Если целое число n оканчивается на 4, то оно чётно». Обратное к нему высказывание $Y \to X$ означает «Если целое число n чётно, то оно оканчивается на 4».

В данном случае, $X \to Y$ истинно, а обратное к нему ложно.

Замечание. Более того, даже если обратное утверждение верно, его доказательство может существенно отличаться от доказательства прямого, как по сложности, так и по содержанию.

Пример 1.9. Рассмотрим (очень простое) утверждение «Если в бесконечной арифметической прогрессии, состоящей из натуральных чисел, есть простое число, отличное от её первого члена, то первый член и знаменатель взаимно просты». Утверждение, обратное к данному, есть знаменитая теорема Дирихле, весьма сложный и важный факт теории чисел.

Упражнение 1.8. *Докажите прямое утверждение из примера 1.9.*

1.7. Доказательство от противного

Предположим, мы хотим доказать некоторое утверждение X. Для этого достаточно доказать, что утверждение $\neg X$ ложно.

Допустим, из предположения об истинности $\neg X$ следует некоторое заведомо ложное утверждение Y. Тогда утверждение X истинно. Действительно, если Y ложно, то импликация $\neg X \to Y$ истинна тогда и только тогда, когда $\neg X$ ложно.

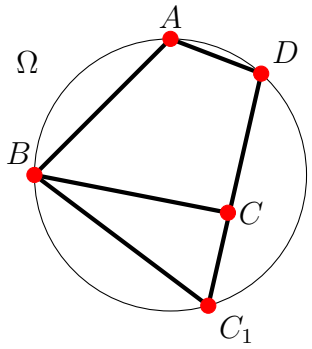
Определение 1.10. Рассмотренный выше метод доказательства называется *доказательством от противного.*

Пример 1.10. Если в выпуклый четырёхугольник можно вписать окружность, то суммы его противоположных углов равны. Докажем обратное утверждение от противного.

Утверждение. *Около четырёхугольника, сумма противоположных углов которого равна* $180°$, *можно описать окружность.*

Доказательство. Рассмотрим четырёхугольник $ABCD$. Пусть, без ограничения общности, $\angle BAD + \angle BCD = 180°$. Опишем окружность Ω около треугольника ABD. Предположим от противного, что точка C не лежит на этой окружности. Обозначим за C_1

точку пересечения прямой DC и окружности Ω. Тогда $\angle BC_1D + \angle BAD = 180°$. Поэтому $\angle BCD = \angle BC_1D$. Если точка C находится внутри окружности Ω, то угол BCD будет внешним в треугольнике BCC_1 и $\angle BCD = \angle BC_1D + \angle CBC_1$. Если же точка C находится снаружи Ω, то BC_1D – внешний угол в треугольнике BCC_1 и $\angle BC_1D = \angle BCD + \angle CBC_1$. В обоих случаях получаем противоречие.



Упражнение 1.9. *Пусть a и b — строго положительные вещественные числа. Докажите, что если выполнено равенство $\dfrac{a}{1+b} = \dfrac{b}{1+a}$, то $a = b$.*

Предостережение: не стоит пытаться доказывать все импликации от противного. Довольно часто оказывается, что даже если этот метод работает, он является далеко не самым оптимальным.

Пример 1.11. Рассмотрим следующее утверждение: «Если сумму в n тугриков можно разменять монетами в 10 и 15 тугриков, то n делится на 5 и $n > 5$.» Докажем обратное к нему утверждение. Придумать явный алгоритм размена в данном случае гораздо проще, чем доказать его от противного.

- Если $n > 5$ и $5 \mid n$, то $n = 5k$ для некоторого целого $k > 1$.
- Если $k = 2m$ (чётное), то $n = 10m$; значит, можно взять m монет в 10 тугриков.
- Если $k = 2m + 1$ (нечётное), то $n = 10(m - 1) + 15$. Значит, можно взять $(m - 1)$ монету в 10 тугриков и 1 монету в 15 тугриков.

1.8. Кванторы

В математике часто рассматриваются высказывания, которые начинаются со слов «для каждого» и «существует». Для них используются специальные символы $\forall$ и $\exists$ соответственно, называемые *кванторами*.

Пример 1.12. Запись $\forall n \in \mathbb{N}\ \exists m \in \mathbb{N} : m > n$ означает «Для любого натурального числа существует натуральное число, которое больше его».

Чрезвычайно важно следить за порядком, в котором идут кванторы.

Пример 1.13. Изменив порядок кванторов в предыдущем примере, получим формулу $\exists m \in \mathbb{N}\ \forall n \in \mathbb{N} : m > n$ («Существует натуральное число, которое строго больше любого натурального числа»).

Упражнение 1.10. *Какие из утверждений, рассмотренных в примерах 1.12 и 1.13, верны? Почему?*

1.9. Кванторы и отрицание

Операция отрицания связана с кванторами следующими правилами логического вывода. Пусть $P(x)$ — утверждение о переменной x. Тогда:

- $(\neg(\forall x P(x))) \quad \Leftrightarrow \quad (\exists x(\neg P(x)))$;
- $(\neg(\exists x P(x))) \quad \Leftrightarrow \quad (\forall x(\neg P(x)))$.

Так, согласно первому правилу, «Не все дома» $\Leftrightarrow$ «Существует кто-то, кто не дома». А согласно второму правилу, «Нет денег» $\Leftrightarrow$ «Всё, что есть, деньгами не является».

Пример 1.14. Построим отрицание следующего утверждения:

$$\exists m \in \mathbb{N}\, \forall n \in \mathbb{N} :\ m > n.$$

Используя правила построения отрицаний, получаем:

$$(\neg(\exists m \in \mathbb{N}\, \forall n \in \mathbb{N} :\ m > n)) \quad \Leftrightarrow \quad (\forall m \in \mathbb{N}\, \exists n \in \mathbb{N} :\ m \leqslant n).$$

Формула в правой части эквивалентна следующему высказыванию: «Для любого натурального числа существует натуральное число, большее или равное ему».

С помощью отрицания можно заменить кванторы в утверждении, тем самым заметно упростив его доказательство или опровержение.

Пример 1.15. Истинно ли следующее утверждение «Из любых 10 отрезков можно всегда выбрать 3 различных отрезка таким образом, чтобы из них можно было составить треугольник»?

Пытаться напрямую доказывать некоторое нетривиальное свойство для любых наборов из 10 отрезков, возможно, не самая разумная идея. Вместо этого сначала рассмотрим отрицание интересующего нас утверждения: «Существует набор из 10 отрезков такой, что ни из каких 3 отрезков данного набора нельзя составить треугольник».

Для того, чтобы доказать отрицание (если оно верно), нам достаточно найти один набор из 10 отрезков, не удовлетворяющий данному конкретному свойству. Иными словами, нам достаточно придумать набор из 10 длин отрезков, никакие 3 из которых не удовлетворяют неравенству треугольника.

Оказывается, что найти такой набор можно. Таковым, по определению, является набор из 10 идущих подряд чисел Фибоначчи $(1, 2, 3, 5, 8, 13, 21, 34, 55, 89)$, или, например, набор из 10 первых степеней двойки $(1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024)$.

Следовательно, мы доказали, что интересующее нас утверждение ложно, так как истинно его отрицание.

1.10. Литература для дальнейшего изучения

• *Верещагин Н.К., Шень А.*, Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления (4-е издание) — Москва, МЦНМО, 2012.

• *Успенский В.А.*, Простейшие примеры математических доказательств, Библиотека «Математическое просвещение», выпуск 34 (2-е издание) — Москва, МЦНМО, 2012.

Математическая логика

Задачи семинаров

Задача 1.1. Три студента то ли изучали логику, то ли не изучали. Высказывание X_k при каждом $k = 1, 2, 3$ утверждает, что k-й студент логику изучал. Известно, что истинно высказывание $(X_1 \to X_3) \wedge \neg(X_2 \to X_3)$. Кто из студентов изучал логику, а кто не изучал?

Задача 1.2. Убедитесь в справедливости *законов де Моргана*:

а) $\neg(X \wedge Y) \quad \Leftrightarrow \quad (\neg X \vee \neg Y)$;

б) $\neg(X \vee Y) \quad \Leftrightarrow \quad (\neg X \wedge \neg Y)$.

Задача 1.3. Постройте таблицу истинности для следующей пропозициональной формулы: $\neg(X \to Z) \vee \neg Y \wedge Z$.

Задача 1.4. Докажите, что любое правило, сопоставляющее каждому набору длины n из нулей и единиц значение 0 или 1, можно записать в виде пропозициональной формулы φ от n переменных.

Задача 1.5. Высказывание $X \uparrow Y$ означает, что ложно хотя бы одно из утверждений X, Y. Запишите, используя только знак $\uparrow$ и скобки, высказывания, эквивалентное высказываниям $X \vee Y$ и $X \wedge Y$.

Задача 1.6. Имеется некоторый список утверждений. Известно, что, если в этом списке есть утверждения A и B, то есть и утверждение $\neg(A \vee B)$. Докажите, что если в этом списке есть утверждения A и B, то есть и утверждение $A \vee B$.

Задача 1.7. Какие из следующих высказываний верны? Почему?

$X:\ \exists x\ \forall y:\ xy + 1 > y$;

$Y:\ \forall x\ \exists y:\ xy + 1 > y$;

$Z:\ \exists x\ \forall y:\ xy + 1 < y$;

$T:\ \forall x\ \exists y:\ xy + 1 < y$.

Задача 1.8. Пусть $Q_1, \ldots, Q_n$ — набор кванторов (каждый из них — либо $\forall$, либо $\exists$), а $P(x_1, \ldots, x_n)$ — утверждение о переменных $x_1, \ldots, x_n$. Докажите, что утверждение $\neg Q_1 x_1 \ldots Q_n x_n : P(x_1, \ldots, x_n)$ равносильно утверждению $\bar{Q}_1 x_1 \ldots \bar{Q}_n x_n : \neg P(x_1, \ldots, x_n)$, где черта сверху означает замену квантора противоположным ($\forall$ на $\exists$ и обратно).

Задача 1.9. Сформулируйте отрицание к следующему утверждению:

$$\forall x\ \exists n \in \mathbb{N}:\ \big((x \geqslant 1/n) \vee (x \leqslant 0)\big).$$

Что верно: исходное утверждение или его отрицание?

Задача 1.10. Пусть x, y, z, t — различные элементы множества $\{1, 2, 3, 4\}$. Найдите численные значения x, y, z, t, если истинны следующие высказывания:

$A:\ (x \neq 1) \to (z \neq 2)$;

$B:\ ((y = 2) \vee (y = 3)) \to (x = 1)$;

$C:\ (y \neq 3) \to (z = 4)$;

$D:\ (t = 2) \to (y \neq 1)$;

$E:\ (t \neq 1) \to (y = 1)$.

Множества и отображения

Теоретический материал

2.1. Понятия множества и элемента. Различные способы задания множеств.

Множество — это неопределяемое понятие. (Неформально можно представлять как совокупность *элементов*.) Множество можно задать перечислением всех его элементов.

Обозначения. $a \in A$ — элемент a принадлежит множеству A;
$a \notin A$ — элемент a не принадлежит множеству A.

Другой возможный способ задания множества — через описание свойств его элементов. То есть $B = \{a \in A \,|\, P(a)\}$ — это множество всех элементов a множества A, удовлетворяющих свойству $P(a)$.

Пример 2.1. Множество чётных чисел можно записать как
$\{x \in \mathbb{Z} \,|\,$ найдётся $y \in \mathbb{Z}$, такой, что $x = 2y\}$.

Пустое множество $\varnothing$ — это множество, не содержащее ни одного элемента.

Упражнение 2.1. *Сколько элементов в следующих множествах:*
а) $\{0\}$,
б) $\{0, \{0\}, \varnothing\}$,
в) $\{x \mid$ *буква* x *встречается в слове «крокодил»*$\}$*?*

Упражнение 2.2. *Какие числа принадлежат множеству* A*, заданному условием* $A = \{x \mid x \in \mathbb{N},\ x \leqslant 45,\ x$ *делится на* $5\}$*?*

2.2. Понятия подмножества. Критерий равенства множеств.

Определим важнейшие понятия, позволяющие нам, в некотором смысле, «сравнивать» множества:

• Множество A называется подмножеством множества B (пишем $A \subset B$), если каждый элемент множества A является также элементом множества B. Другими словами, $a \in A$ влечёт $a \in B$.

• Два множества A и B равны ($A = B$), если $x \in A$ влечёт $x \in B$ и $x \in B$ влечёт $x \in A$ для каждого элемента x.

Сформулируем также *критерий равенства* множеств в терминах подмножеств:

• Два множества A и B равны ($A = B$) тогда и только тогда, когда $A \subset B$ и $B \subset A$.

Упражнение 2.3. *Выпишите все подмножества множества* $\{\varnothing, \{0\}, 1\}$.

Упражнение 2.4. *Сколько различных подмножеств у множества из четырёх элементов? Обоснуйте ответ.*

2.3. Операции над множествами: объединение, пересечение, разность, декартово произведение.

Над множествами можно производить операции, в чём-то похожие на операции над числами. Определим основные из них:

• *Объединение* $A \cup B$ множеств A и B:

$$A \cup B = \{x \mid x \in A \text{ ИЛИ } x \in B\}.$$

• *Пересечение* $A \cap B$ множеств A и B:

$$A \cap B = \{x \mid x \in A \text{ И } x \in B\} = \{a \in A \mid a \in B\} = \{b \in B \mid b \in A\}.$$

• *Разность* $A \setminus B$ множеств A и B:

$$A \setminus B = \{a \in A \mid b \notin B\}.$$

• *Декартовым произведением* $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ множеств X и Y называется множество всех упорядоченных пар (x, y), таких, что $x \in X$ и $y \in Y$.

Упражнение 2.5. *Что является объединением множеств чётных и нечётных целых чисел? А пересечением?*

Упражнение 2.6. *Докажите, что для любых множеств A и B выполнено:*

а) $A \cup A = A, \quad A \cap A = A;$

б) $A \cup B = B \cup A, \quad A \cap B = B \cap A;$

в) $(A \backslash B) \cup B = A \cup B.$

2.4. Бинарные отношения. Отношение эквивалентности.

Формальное определение бинарных отношений может показаться слишком общим; интуитивно можно представлять себе задание «связи» между некоторыми его элементами, но при формальном задании этот «смысл» теряется. Этот вопрос подробно обсуждается в Видеолекции «Множества» начиная с 40 : 15.

• *Бинарное отношение* на множестве X — это подмножество R множества $X \times X$.

Обозначение. $x \sim y$, если $(x, y) \in X \times X$.

• Бинарное отношение называется *отношением эквивалентности*, если оно

а) *рефлексивно* (т.е. $x \sim x$ для каждого $x \in X$);

б) *симметрично* (т.е. $x \sim y$ влечёт $y \sim x$);

в) *транзитивно* (т.е. $x \sim y$ и $y \sim z$ влечет $x \sim z$).

Про элементы, связанные отношением эквивалентности, можно говорить, что они *эквивалентны*. Важным примером является *отношение равенства*.

Отношение эквивалентности позволяет классифицировать элементы множества по каким-либо свойствам. Полученные классы называются *классами эквивалентности*.

• *Классом эквивалентности* элемента $x \in X$ называется множество

$$C(x) = \{y \in X \mid x \sim y\}.$$

Сформулируем важную лемму и не менее важное следствие из неё:

Лемма 2.1. *Если $x \in C(y)$, то $C(x) = C(y)$.*

Следствие 2.2. *Классы эквивалентности либо не пересекаются, либо совпадают.*

Упражнение 2.7. *Убедитесь, что лемма 2.1 справедлива.*

Упражнение 2.8. *Дайте определение свободного вектора на плоскости как класса эквивалентности направленных отрезков.*

Упражнение 2.9. *Пусть m — ненулевое целое число. Определим отношение*

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

на множестве всех целых чисел следующим образом: $x - y$ делится на m. Докажите, что отношение $\equiv$ является отношением эквивалентности.

2.5. Понятия отображения, функции и их графика.

Неформально, мы хотим *сопоставлять* элементы множества X элементам множества Y. Тогда интуитивно мы можем понимать *отображение* как некоторый способ это сделать. Формально

• *Отображение* — это подмножество $f \subset X \times Y$ со следующим свойством: для каждого элемента $x \in X$ найдется единственный $y \in Y$ такой, что $(x, y) \in f$.

В смысле приведённого выше формального определения, функция — это то же самое, что её *график*. Таким образом, запись $y = f(x)$ эквивалентна записи $(x, y) \in f$. Иногда отображения называют *функциями* и обозначают как $f : X \to Y$.

2.6. Инъекция, сюръекция, биекция. Их описание в терминах образов и прообразов.

Отображение может обладать (или не обладать) следующими специальными свойствами:

• Отображение $f : X \to Y$ называется *инъективным* (или *инъекцией*, или *вложением*), если $f(x) = f(x')$ влечёт за собой $x = x'$.

• Отображение $f : X \to Y$ называется *сюръективным* (или *сюръекцией*, или *отображением НА*), если для всякого $y \in Y$ найдётся такой $x \in X$, что $f(x) = y$.

• Отображение называется *биективным* (или *биекцией*), если оно одновременно инъективно и сюръективно.

Биекции также называют *взаимно-однозначными соответствиями*.

Также введём важные понятия *образа* и *прообраза*: для отображения $f : X \to Y$ и всякого его подмножества $A \subset X$ определим $f(A)$ как $\{f(a) \mid a \in A\}$.

• Множество $f(A)$ называется *образом* подмножества A при отображении f.

Для всякого подмножества $B \subset Y$ определим $f^{-1}(B)$ как $\{x \mid f(x) \in B\} \subset X$.

• Множество $f^{-1}(B)$ называется *полным прообразом* подмножества B при отображении f.

Замечание. Когда множество B состоит из одного элемента, то есть если $B = \{y\}$, фигурные скобки обычно опускают и пишут $f^{-1}(y)$ вместо $f^{-1}(\{y\})$.

Оказывается, что свойства отображений связаны с этими понятиями, а именно:

• Отображение $f : X \to Y$ является *инъективным*, если и только если $f^{-1}(y)$ при $y \in Y$ не может содержать более одного элемента.

• Отображение $f : X \to Y$ является *сюръективным*, если и только если $f(X) = Y$ (эквивалентно, если и только если $f^{-1}(y)$ непусто для всякого $y \in Y$).

• Всегда $f^{-1}(Y) = X$ по определению отображения.

Также всегда верно, что $f(X) \subset Y$ и что $f^{-1}(\varnothing) = f(\varnothing) = \varnothing$.

Упражнение 2.10. *Постройте биекцию между множествами $A \times B$ и $B \times A$.*

Упражнение 2.11. *Перечислите все отображения из множества $\{7, 8, 9\}$ в множество $\{0, 1\}$. Сколько среди них сюръекций, инъекций, биекций?*

2.7. Композиция отображений. Тождественное, обратимое и обратное отображения. Критерий обратимости отображения.

Ещё одним важным понятием является *композиция отображений*. Неформально стоит понимать его как последовательное применение нескольких отображений. Формально, пусть $f : X \to Y$ и $g : Y \to Z$ — два отображения. Тогда

• *Композицией* отображений f и g называется отображение $g \circ f : X \to Z$, определенное формулой

$$(g \circ f)(x) = g(f(x))$$

для всякого $x \in X$.

Дадим определения ещё двух понятий: тождественного и обратного отображений.

• *Тождественное отображение* $\mathrm{id}_X : X \to X$ определяется формулой $f(x) = x$ для всякого $x \in X$.

• Отображение $f : X \to Y$ называется *обратным* к отображению $g : Y \to X$, если выполнены два условия: $g \circ f = \mathrm{id}_X$ и $f \circ g = \mathrm{id}_Y$

Если выполнено только

$$g \circ f = \mathrm{id}_X,$$

то g называется *левым* обратным к f;

если только

$$f \circ g = \mathrm{id}_Y,$$

то g называется *правым* обратным к f.

Эти понятия важны для доказательства нижеследующего критерия.

Теорема 2.3. *Отображение $f : X \to Y$ обладает* обратным *отображением тогда и только тогда, когда f —* биекция.

Упражнение 2.12. *Проверив инъективность и сюръективность для существования левого и правого обратных отображений соответственно, убедитесь, что теорема 2.3 справедлива.*

Упражнение 2.13. *Существует ли обратное к следующему отображению:*
$f : A = \{x \mid x \in \mathbb{N}, 1 \leqslant x \leqslant 45\} \to$ *остаток от деления числа x на 5?*
Существуют ли левое и правое обратное?

2.8. Равномощные множества. Счётные множества и их свойства.

Понятие *мощности* множества мы пока оставим без определения, но мы можем определить, что такое *равномощные* множества:

• Два множества X и Y имеют *одинаковую* мощность, если и только если существует *биекция* между X и Y.

Два конечных множества имеют одинаковую мощность, если и только если они состоят из одинакового числа элементов.

Удивительным фактом является то, что бывают бесконечные множества разной мощности. Неформально, одно бесконечное множество может быть «больше» другого. Мы введём определение одной конкретной мощности. Множества такой мощности называются *счётными*. Неформально говоря, счётное множество — это то множество, которое можно перенумеровать натуральными числами. Формально

• Множество X называется *счётным*, если существует биекция между X и множеством $\mathbb{N}$ всех натуральных чисел.

Важными примерами счётных множеств являются следующие множества:

Пример 2.2. Множества целых чисел $\mathbb{Z}$ и рациональных чисел $\mathbb{Q}$ счётны.

Упражнение 2.14. *Постройте биекции:*
а) между множествами $\mathbb{Z}$ и $\mathbb{N}$;
б) между множествами $\mathbb{N} \times \mathbb{N}$ и $\mathbb{N}$.

Счётным множествам присущ ряд важных свойств. Перечислим некоторые из них.

Теорема 2.4. *Всякое подмножество счётного множество конечно или счётно.*

Теорема 2.5. *Объединение конечного или счётного числа счётных множеств счётно. Если A и B — счётные множества, то $A \times B$ — тоже счётное множество.*

Ключевым фактом, использующимся в доказательстве теоремы 2.4, является принцип минимального элемента (см. раздел 3.1). Теорема 2.5 доказывается непосредственно, конструктивным построением биекций.

Упражнение 2.15. *Убедитесь, что теоремы 2.4 и 2.5 справедливы.*

Упражнение 2.16. *Покажите, что множество рациональных чисел $\mathbb{Q}$ счётно.*

2.9. Несчётные множества: $\mathcal{P}(\mathbb{N})$ и последовательности из 0 и 1. Канторов диагональный процесс.

Следующие разделы являются дополнительными. К ним стоит переходить после уверенного освоения всех предыдущих.

Пусть A — множество.

• Рассмотрим *множество $\mathcal{P}(A)$ всех подмножеств* множества A.

Существование множества $\mathcal{P}(A)$ фактически является аксиомой. Иногда его обозначают как 2^A, так как если A состоит из n элементов, то $\mathcal{P}(A)$ состоит из 2^n элементов.

Упражнение 2.17. *Приведите пример множества A из трёх элементов, для которого $A \subset \mathcal{P}(A)$.*

Теорема 2.6. *Множество $\mathcal{P}(\mathbb{N})$ всех подмножеств множества $\mathbb{N}$ несчётно.*

Доказательство. [приведённое в лекции] Пусть $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ — биекция. Рассмотрим подмножество $A = \{n \in \mathbb{N} \,|\, n \notin f(n)\} \subset \mathbb{N}$. Допустим, $A = f(m)$. Спросим, верно ли, что $m \in A$. Не сможем ответить ни ДА, ни НЕТ. □

Сейчас мы рассмотрим альтернативное доказательство, для которого нам потребуется следующая теоерема:

Теорема 2.7. [Кантор] *Множество бесконечных последовательностей нулей и единиц несчётно.*

Доказательство. Проведем доказательство от противного: пусть оно счётно, тогда все его элементы (последовательности) можно пронумеровать натуральными числами. Обозначим n-ную последовательность как (a_{ni}), $i \in \mathbb{N}$, элементы $a_{ni} \in \{0, 1\}$. Запишем эти последовательности одна под другой в виде таблицы:

$$\begin{array}{lcccc} (a_{1i}): & a_{11} & a_{12} & a_{13} & \dots \\ (a_{2i}): & a_{21} & a_{22} & a_{23} & \dots \\ (a_{3i}): & a_{31} & a_{32} & a_{33} & \dots \\ & \vdots & \vdots & \vdots & \vdots \end{array}.$$

Рассмотрим «диагональную» последовательность в этой таблице, то есть последовательность

$$a_{11}a_{22}a_{33}a_{44}a_{55}\dots.$$

Заменим в этой последовательности каждый элемент на «противоположный», то есть 0 на 1 и наоборот. Полученная последовательность является последовательностью нулей и единиц, таким образом она должна принадлежать нашему исходному множеству. Но её нет в таблице последовательностей, так как она отличается от любой последовательности (a_{ni}) в n-й позиции. Противоречие. Следовательно, множество бесконечных последовательностей нулей и единиц несчётно. □

Теперь, пользуясь теоремой Кантора, мы можем доказать несчётность множества подмножеств натуральных чисел. Для этого нам необходимо построить биекцию между подмножествами множества натуральных чисел и последовательностями из нулей и единиц.

Утверждение 2.8. *Существует биекция между подмножествами множества натуральных чисел и последовательностями из нулей и единиц.*

Доказательство. Подмножество мы будем кодировать следующим образом: на i-том месте в последовательности мы ставим 1, если i принадлежит данному подмножеству, и 0, если не принадлежит. Это соответствие взаимно-однозначно. □

Итого, множество всех подмножеств множества натуральных чисел несчётно.

2.10. Парадоксы теории множеств.

Почему так важна аксиоматика, упомянутая в предыдущем разделе? Оказывается, её отсутствие приводит к парадоксам, примеры которых мы сейчас рассмотрим.

Парадокс (Рассел-Цермело): Большинство «нормальных» множеств не являются собственными элементами. Скажем, что X *обычное*, если $X \notin X$, и *странное*, если $X \in X$. Рассмотрим множество всех обычных множеств $U = \{x \mid x \notin x\}$. Спросим, верно ли, что $U \in U$. Если да, то U странное, но тогда по определению $U \notin U$. Если нет, то U обычное, но тогда по определению $U \in U$.

Вообще, рассмотрение *множества всех множеств* приводит к парадоксам. Например, из него можно было бы выделить множество U в качестве подмножества.

Рассмотренный парадокс связан с явлением *автореферентности*, то есть ситуации, когда описание некоторого объекта ссылается на сам этот объект. Современный подход к теории множеств включает в себя попытку избежать автореферентности именно благодаря аксиоматике.

• Самый известный парадокс, основанный на этом принципе — это *парадокс лжеца*:

Пусть человек говорит «Я лгу». Может ли данное утверждение быть правдой или ложью?

• Другая обёртка того же парадокса — это *парадокс брадобрея*:

Брадобрей вывешивает объявление: «Брею всех тех и только тех, кто не бреется сам». Нужно ли ему бриться самому? Ответ на данный вопрос невозможно получить.

Заключение: Отчасти для того, чтобы избежать подобных парадоксов, но, что более важно, чтобы установить чёткие правила, математики стоят теорию множеств на чётких логических основаниях и аксиомах теории множеств. Разбор этих аксиом является материалом для более полного курса, в данных материалах были упомянуты лишь некоторые из них. Но для последующего изучения важно понимать, что упомянутые аксиомы являются именно аксиомами, на которых в том числе и строится вся разобранная здесь теория.

2.11. Литература для дальнейшего изучения

• *Верещагин Н.К., Шень А.*, Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств (4-е издание) — Москва, МЦНМО, 2012.

• *Виленкин Н.Я.*, «Рассказы о множествах» (3-е издание) — Москва, МЦНМО, 2005.

Множества и отображения

Задачи семинаров

2.1. Понятия множества и элемента, способы задания множеств

Задача 2.1. (С) а) Старейший математик среди шахматистов и старейший шахматист среди математиков — это один или тот же человек или (возможно) разные?

б) Лучший математик среди шахматистов и лучший шахматист среди математиков — это один или тот же человек или (возможно) разные?

в) Каждый десятый математик — шахматист, а каждый шестой шахматист — математик. Кого больше — математиков или шахматистов — и во сколько раз?

2.2. Понятие подмножества, критерий равенства множеств

Задача 2.2. (С) Верно ли, что множество летающих крокодилов является подмножеством множества ботинков на левую ногу? Обоснуйте ответ.

Задача 2.3. (С) Может ли такое быть, что $A \subset B$ и одновременно $A \in B$? Приведите пример или докажите невозможность.

2.3. Операции над множествами: объединение, пересечение, разность, декартово произведение

Задача 2.4. (Т) Пусть $A = \{57, 91, 179, 239\}$, $B = \{91, 239, 2014\}$, $C = \{2, 57, 239, 2014\}$, $D = \{2, 91, 2014, 2017\}$ Найдите следующие множества:

а) $A \cup B$,
б) $A \cap B$,
в) $(A \cap B) \cup D$,
г) $C \cap (D \cap B)$,
д) $(A \cap B) \cup (C \cap D)$,
е) $(A \cup (B \cap C)) \cap D$,
ж) $(C \cap A) \cup ((A \cup (C \cap D)) \cap B)$,
з) $(A \cup B) \backslash (C \cap D)$,
и) $A \backslash (B \backslash (C \backslash D))$,
к) $((A \backslash (B \cup D)) \backslash C) \cup B$.

Задача 2.5. (Т) Из каких элементов состоят следующие множества: $\{0, 1\} \times \{9\}$, $\{0, 1\} \times \{0, 1\}$, $\varnothing \times \varnothing$, $\{5, 7\} \times \{1, 3, 17\}$, $\{16, 41\} \times \varnothing$?

Задача 2.6. (С) Докажите, что для любых множеств A, B, C выполняется равенство $(A \cap B) \setminus C = (A \setminus C) \cap B$.

Задача 2.7. Существуют ли такие множества A, B, C, для которых одновременно выполнялись бы равенства $A \cap B \neq \varnothing$, $A \cap C = \varnothing$, $(A \cap B) \setminus C = \varnothing$? Приведите пример или докажите, что таких множеств не существует.

Задача 2.8. Обозначим

- через A множество всех целых чисел от 0 до 20;
- через B множество всех двузначных чисел;
- через C множество всех чётных чисел;
- через D множество всех простых чисел.

Выпишите все элементы множества $A \cap (B \setminus (C \cup D))$.

2.4. Бинарные отношения, отношение эквивалентности

Задача 2.9. (С) Выполнены ли свойства рефлексивности, симметричности и транзитивности для следующих отношений:
а) $x \sim y$, если x и y взаимно просты, на множестве целых чисел $\mathbb{Z}$;
б) $x \sim y$, если $10(x - y) \in \mathbb{Z}$, на множестве рациональных чисел $\mathbb{Q}$;
в) $x \sim y$, если $x^2 + y^2$ рационально, на множестве действительных чисел $\mathbb{R}$?
Является ли каждое из рассмотренных отношений отношением эквивалентности?

Задача 2.10. Является ли отношение $x < y$ на множестве всех действительных чисел отношением эквивалентности? Объясните ответ.

Задача 2.11. Постройте бинарное отношение C на 3-элементном множестве $\{x, y, z\}$ такое, что C рефлексивно и симметрично, но не транзитивно.

Задача 2.12. Сколько всего различных отношений эквивалентности на множестве из пяти элементов?

2.5. Понятия отображения, функции и их графика

Задача 2.13. (С) Множество A состоит из $n > 0$ элементов, а множество B состоит из $m > 0$ элементов. Найдите количество отображений из A в B.

2.6. Инъекция, сюръекция и биекция; образы и прообразы

Задача 2.14. (Т) Укажите все биекции из множества $\{1, 2, 3\}$ в себя.

Задача 2.15. Постройте биекцию между множествами $(A \times B) \times C$ и $A \times (B \times C)$.

Задача 2.16. (С) Множество A состоит из a элементов, а множество B — из b элементов. При каких соотношениях на a и b существует инъекция из A в B? Сюръекция? Биекция? Сторого обоснуйте ответы.

Задача 2.17. Может ли для некоторого отображения $f : X \to Y$ и некоторых подмножеств A, $B \subset X$ быть так, что $A \cap B = \varnothing$, но при этом $f(A) = f(B)$? Докажите невозможность или приведите пример.

Задача 2.18. (С) Пусть $f : X \to Y$ — отображение, $A, B \subset X$. Всегда ли верно, что

а) если $f(A) \subset f(B)$, то $A \subset B$,

б) $f(A \cap B) = f(A) \cap f(B)$,

в) $f(A \cup B) = f(A) \cup f(B)$,

г) $A = f^{-1}(f(A))$?

Для каждого пункта докажите или приведите контрпример.

Задача 2.19. Пусть $f : X \to Y$ — отображение, $C, D \subset Y$. Всегда ли верно, что

а) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$,

б) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$,

в) $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$,

г) $C = f(f^{-1}(C))$?

Для каждого пункта докажите или приведите контрпример.

2.7. Композиция отображений и обратимые отображения

Задача 2.20. (С) Пусть $f : X \to Y$ и $g : Y \to Z$ — отображения, а $C \subset Z$ — некоторое подмножество. Всегда ли верно, что $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$? Строго обоснуйте ответ.

Задача 2.21. Отображение $f : \mathbb{R} \to \mathbb{R}$ определяется формулой $f(x) = x^2$. Найдите образ $f(\mathbb{R})$, а также полный прообраз $f^{-1}(x)$ для каждой точки $x \in \mathbb{R}$.

Задача 2.22. (С) Докажите, что следующее свойство отображения $f : X \to Y$ эквивалентно биективности: существует отображение $g : Y \to X$ со свойствами $g \circ f = \mathrm{id}_X$, $f \circ g = \mathrm{id}_Y$.

Задача 2.23. В цепочке отображений $A \to B \to C$ первое сюръективно, а второе не инъективно. Верно ли, что их композиция сюръективна? Не инъективна?

Задача 2.24. (Т) Пусть отображения $f : \mathbb{R} \to \mathbb{R}$ и $g : \mathbb{R} \to \mathbb{R}$ заданы формулами $f(x) = -x$ и $g(x) = x + 1$ соответственно. Найдите $f \circ g$ и $g \circ f$.

Задача 2.25. Пусть $f : \mathbb{R} \to \mathbb{R}$ — отображение, заданное формулой $f(x) = 2x^2$. Найдите композицию $f^{\circ n}$ (композицию n копий отображения f).

Задача 2.26. Пусть A — конечное множество.

а) Докажите, что для любого отображения $f : A \to A$ найдутся различные натуральные числа m и n такие, что итерации $f^{\circ m}$ и $f^{\circ n}$ совпадают.

б) Докажите, что для любой биекции $f : A \to A$ найдётся такое натуральное число n, для которого $f^{\circ n} = \mathrm{id}_A$.

Задача 2.27. При каких условиях на действительные числа $a, b, c \in \mathbb{R}$ отображение $f : \mathbb{R} \to \mathbb{R}$, заданное формулой $f(x) = ax^2 + bx + c$ является инъекцией? Сюръекцией? Биекцией?

2.8. Равномощные множества, счётные множества и их свойства

Задача 2.28. (С) Про каждые два из следующих множеств выясните, существует ли между ними биекция:

1. множество натуральных чисел $\mathbb{N}$;
2. множество чётных натуральных чисел;
3. множество натуральных чисел без числа 3;
4. множество целых чисел $\mathbb{Z}$.

Задача 2.29. Постройте биекцию между множеством $\mathbb{N} \times \mathbb{N}$ и множеством всех положительных чисел, которые делятся на 2 и 3 и не делятся на другие простые числа.

2.9. Дополнительные задачи: множество всех подмножеств

Задача 2.30. Для любых множеств A, B проверьте, верно ли равенство
а) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$,
б) $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$.
Как и выше, через $\mathcal{P}(A)$ обозначается множество всех подмножеств множества A.

Задача 2.31. Для каких множеств A, B выполнено равенство $\mathcal{P}(A \cup B) = \mathcal{P}(A) \times \mathcal{P}(B)$? Строго обоснуйте ответ.

Математическая индукция

Теоретический материал

3.1. Принцип минимального элемента

Мы принимаем за аксиому следующее утверждение, называемое *принципом минимального элемента*: каждое непустое подмножество множества натуральных чисел (в том числе, бесконечное) имеет минимальный элемент.

Замечание. Бесконечное подмножество множества натуральных чисел не имеет максимального элемента.

Пример 3.1. Подмножество $S \subset \mathbb{N}$, состоящее из чётных чисел, имеет минимальный элемент — это 2.

3.2. Метод математической индукции

Метод математической индукции, которому посвящён этот раздел, очень полезен для доказательства различных результатов и является следствием принципа минимального элемента. Что мы доказываем по индукции?

Утверждение, содержащее параметр n, который может принимать любые натуральные значения. Либо утверждения, которые изначально выглядят не так, но могут быть переформулированы таким образом.

Пример 3.2. При любом натуральном $n > 4$ выполнено неравенство $2^n > n^2$.

Пример 3.3. Число, десятичная запись которого состоит из 3^n единиц, делится на 3^n.

Пример 3.4. Пусть на всех сторонах и диагоналях многоугольника расставлены стрелки. Тогда найдётся вершина, из которой можно добраться до любой другой, двигаясь по стрелкам.

Итак, простейшая схема метода математической индукции такова.

• *База индукции*: доказываем первое утверждение из последовательности.

• *Индукционный переход*: доказываем, что каждое из этих утверждений является следствием предыдущего.

После этого, чтобы убедиться в справедливости каждого из утверждений, достаточно сослаться на принцип минимального элемента. Более строго это формулируется так.

Теорема 3.1. *Пусть имеется последовательность утверждений $A_1, A_2, A_3, \ldots$, пронумерованная натуральными числами, такая, что*

• *утверждение A_1 истинно,*

• *для любого $k \in \mathbb{N}$ из истинности утверждения A_k следует истинность утверждения A_{k+1}.*

Тогда все утверждения $A_1, A_2, A_3, \ldots$ истинны.

Доказательство. В множестве $\{A_1, A_2, A_3 \ldots\}$ рассмотрим подмножество M, состоящее из ложных утверждений. Предположим, что оно непусто. Тогда по принципу минимального элемента найдётся ложное утверждение $A_k \in M$, индекс k которого минимален. Ясно, что $k \neq 1$, поскольку утверждение A_1 истинно по условию. Утверждение A_{k-1} в таком случае является истинным (в самом деле, A_k — ложное утверждение с минимальным индексом, значит, все утверждения с меньшими индексами истинны). Но по условию из истинности A_{k-1} следует истинность A_k, поэтому $M = \varnothing$, что и требовалось доказать. □

На практике нумерация утверждений часто начинается не с единицы, как можно видеть, скажем, в примере 3.2, однако метод принципиально не меняется — изменения, которые нужно сделать в доказательстве, очевидны.

Упражнение 3.1. *Докажите утверждения из примеров 3.2, 3.3 и 3.4, используя метод математической индукции.*

3.3. Разбор базовых примеров

Для начала вернемся к примерам из предыдущего раздела.

Пример 3.2. При любом натуральном $n > 4$ выполнено неравенство $2^n > n^2$.
► Итак, утверждение A_n звучит следующим образом: $2^n > n^2$. Это как раз тот случай, когда нумерация начинается не с единицы, а именно, база индукции доказывается для $n = 5$. Утверждение A_5 очевидно: $32 > 25$. Осталось научиться выводить неравенство $2^{n+1} > (n+1)^2$ из неравенства $2^n > n^2$. Это делается так:

$$2^n > n^2 \quad \to \quad 2^{n+1} > 2n^2 > (n+1)^2.$$

Последнее неравенство сводится к $n^2 > 2n + 1$, что очевидно при $n > 2$. ◄

Пример 3.3. Число, десятичная запись которого состоит из 3^n единиц, делится на 3^n.
► Сформулируем искомое утверждение как задачу о последовательностях. Утверждение A_n будет звучать следующим образом: член последовательности $x_n = 11\ldots11$ (состоящий из 3^n единиц) делится на 3^n. База индукции ясна: $111 = 3 \cdot 37$. Для того чтобы вывести импликацию, удобно перейти к *рекуррентному заданию последовательности* (выражаем член последовательности через предыдущие):

$$x_{n+1} = x_n + x_n \cdot 10^n + x_n \cdot 10^{2n} = x_n(1 + 10^n + 10^{2n}).$$

Поскольку выражение в скобках делится на 3 (например, в силу соответствующего признака делимости, см. утверждение 4.3) импликацию можно считать доказанной: каждый член последовательности содержит в разложении на множители на одну тройку больше, чем предыдущий. ◄

Замечание. 1) Из приведённого утверждения ссылку на принцип математической индукции можно и убрать. В самом деле, первый член последовательности содержит

в разложении одну тройку, а каждый следующий на одну тройку больше. Поэтому член с номером n содержит $1 + (n - 1) = n$ троек. Это — типичный пример задачи, в которой ссылка на принцип математической индукции может быть заменена аккуратно проведённым суммированием.

2) В этом решении мы сделали довольно странную на первый взгляд вещь: перешли от задания последовательности общей формулой к *рекуррентной* (выражающей член последовательности через предыдущий). Казалось бы, общая формула лучше, но в задачах на индукцию *переход к рекуррентной формуле* очень часто помогает.

Пример 3.4. Пусть на всех сторонах и диагоналях многоугольника расставлены стрелки. Тогда найдётся вершина, из которой можно добраться до любой другой, двигаясь по стрелкам.

► Будем называть вершину, из которой можно добраться до любой другой, *корнем*. Тогда утверждение A_n означает, что для любой конфигурации стрелок на сторонах и диагоналях n-угольника найдётся корень. В этом примере нумерация начинается не с единицы, а с $n = 3$. Утверждение A_3 легко доказывается: либо найдётся вершина, из которой выходит две стрелки (и тогда она является корнем), либо из каждой вершины выходит одна стрелка, а конфигурация является циклом (тогда в качестве корня можно взять любую вершину). Докажем импликацию $A_k \to A_{k+1}$. Итак, мы умеем искать нужную вершину на сторонах и вершинах любого n-угольника со стрелками, а нам нужно сделать то же самое для $(n + 1)$-угольника. Что же сделать? Уберём мысленно одну из вершин вместе со всеми входящими в неё и выходящими из неё стрелками. Тогда в получившемся n-угольнике искать корень мы умеем. Теперь вспомним об $(n + 1)$-ой вершине. Если стрелка из корня ведёт в неё, то всё прекрасно. Если же стрелка ведёт из неё в корень, то эту последнюю вершину и нужно объявить корнем вместо имеющегося корня. ◄

Замечание. Только что проделанный нами приём обычно называют термином *спуск*. Убрав один из элементов системы, мы получаем систему с меньшим числом параметров, то есть попадаем в уже изученную ситуацию. Но какой именно элемент убирать, чтобы можно было благополучно вернуться назад? В предыдущей задаче это было неважно, но часто без правильного выбора такого параметра упрощения индукционное рассуждение провести невозможно. Прекрасным примером является следующая задача.

Пример 3.5. Некоторые населённые пункты соединены дорогами с двусторонним движением. При этом из каждого города по дорогам можно доехать до любого другого и ни в какой город нельзя вернуться, не разворачиваясь. Докажите, что число дорог на 1 меньше числа городов.

► Идея решения заключается в том, чтобы убирать не совсем уж произвольный город, а тот, который находится «с краю». Осталось понять, что это значит и почему «крайний» город всегда есть. ◄

Упражнение 3.2. *Доведите решение задачи из примера 3.5 до конца.*

3.4. Нестандартные индуктивные схемы

В некоторых задачах простейшая схема математической индукции не проходит и её приходится модифицировать. Обычно это не приводит к существенным дополнительным сложностям, но быть готовым к такой ситуации надо.

Пример 3.6. *Индукция от всех меньших значений.*

• Задача. Число x подобрано так, что число $x+\frac{1}{x}$ является целым. Докажите, что при любом натуральном n число $x^n+\frac{1}{x^n}$ тоже является целым.

• Решение. Выкладка

$$x^n+\frac{1}{x^n}=\left(x^{n-1}+\frac{1}{x^{n-1}}\right)\left(x+\frac{1}{x}\right)-\left(x^{n-2}+\frac{1}{x^{n-2}}\right)$$

показывает, что утверждение A_n здесь следует не из предыдущего утверждения A_{n-1}, а из двух предыдущих утверждений по логической схеме $(A_{n-1}\wedge A_{n-2})\to A_n$. В этом случае ссылка на принцип минимального элемента позволяет обосновать все утверждения цепочки, начиная с третьего. Справедливость утверждений A_1 и A_2, в свою очередь, нужно заносить в базу индукции и проверять отдельно. Утверждение A_1 верно по условию, а утверждение A_2 легко проверяется той же выкладкой:

$$x^2+\frac{1}{x^2}=\left(x+\frac{1}{x}\right)^2-2.$$

Замечание. Если мы выводим истинность утвреждения A_n не из двух, а из k предыдущих утверждений, то и в базу индукции придётся заносить доказательство k первых утверждений.

Пример 3.7. *Индукция с нееединичным шагом.*

• Задача. Докажите, что при $n>5$ любой квадрат можно разрезать на n меньших квадратов (не обязательно одинаковых).

• Решение. Разрезая квадрат на 4 одинаковые части, мы добавляем к имеющемуся числу квадратов ещё 3. Таким образом, здесь индукционный переход легко сделать по схеме $A_{n-3}\to A_n$. Но для того, чтобы ссылка на принцип минимального элемента сработала, как и в предыдущем случае придётся доказать не одно, а три базовых утверждения. С учётом ограничения $n>5$ можно взять утверждения A_4, A_6, A_8. Утверждение A_4 очевидно, A_6 получается разбиением квадрата на 9 одинаковых клеток и взятием одного квадрата 2×2 клетки и пяти оставшихся клеток 1×1, а A_8 — разбиением на 16 одинаковых клеток и взятием одного квадрата 3×3 и семи оставшихся клеток 1×1.

Пример 3.8. *Введение дополнительных гипотез.*

• Задача. Докажите неравенство

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\ldots+\frac{1}{n^2}<2.$$

• Решение. Совершенно непонятно, как в этой задаче сделать переход индукции. Однако если вместо исходного неравенства сначала доказать, что

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{(n-1)\cdot n}\leqslant\frac{n-1}{n},$$

то с учётом неравенства $\frac{1}{n^2}<\frac{1}{n(n-1)}$ доказательство исходного утверждения проясняется:

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\ldots+\frac{1}{n^2}<1+\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{(n-1)\cdot n}\leqslant 1+\frac{n-1}{n}<1+1<2.$$

Упражнение 3.3. *Докажите, что в действительности справделиво даже большее:*

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

Обратите внимание, что здесь база индукции $n=2$.

3.5. Индукция как обоснование алгоритма

Сфера применимости метода математической индукции чрезвычайно широка. Одной из важных областей её использования является *обоснование корректной работы различных алгоритмов*. В разделах 4.2 и 4.3 мы увидим это на примере деления с остатком и алгоритма Евклида. Здесь же обсудим, почему любой многоугольник можно разбить диагоналями на треугольники — подобные разбиения называются *правильными триангуляциями*.

Утверждение 3.2. *Любой многоугольник (не обязательно выпуклый) обладает правильной триангуляцией.*

Доказательство. Для того, чтобы доказать существование триангуляции, достаточно предъявить алгоритм её построения для каждого n-угольника. В нашем случае, можно воспользоваться следующим *рекурсивным* (то есть ссылающимся на себя) алгоритмом:

- Если $n=3$ — ничего не делать.
- Если $n>3$ — провести внутреннюю диагональ и применить алгоритм к каждому из получившихся многоугольников.

Покажем при помощи индукции, почему работа этого алгоритма завершится и даст правильную триангуляцию. База индукции: $n=3$ — в этом случае исходный треугольник совпадает со своей триангуляцией, и алгоритм сразу остановится. Индукционный переход: допустим, при всех $n\leqslant k$ алгоритм корректно заканчивает свою работу для любого n-угольника. Рассмотрим какой-нибудь $(k+1)$-угольник. Применяя алгоритм к нему, мы должны разделить его диагональю на два меньших многоугольника, а затем

к каждому их них применить всё тот же алгоритм. Но к меньшим многоугольникам применимо предположение: число их сторон не превышает k, а значит, для них алгоритм завершит свою работу правильно. Поэтому и для исходного $(k+1)$-угольника мы получим правильную триангуляцию.

Остаётся объяснить, почему в каждом многоугольнике можно провести внутреннюю диагональ — диагональ, лежащую целиком внутри этого многоугольника. Для выпуклых многоугольников это очевидно: любая диагональ будет внутренней по определению выпуклости. Если же многоугольник невыпуклый, у него найдётся вершина, внутренний угол при которой больше развёрнутого. Рассмотрим множество исходящих из этой вершины лучей, которые идут внутрь данного многоугольника, и для каждого такого луча определим ближайшую сторону многоугольника, которую луч пересекает. Среди определённых сторон хотя бы две различных (иначе лучи заполняют угол, меньший π), а пограничный между ними луч как раз и задаёт внутреннюю диагональ. □

Упражнение 3.4. *а) Докажите, что количество треугольников в произвольной триангуляции n-угольника не зависит от триангуляции и равно $(n-2)$.*

б) Выведите из предыдущего пункта, что сумма углов n-угольника равна $(n-2)\pi$.

3.6. Литература для дальнейшего изучения

• *Головина Л.И., Яглом И.М.*, Индукция в геометрии (Выпуск 21 из серии «Популярные лекции по математике») — Москва, Физматгиз, 1961.

• *Курант Р., Робинс Г.*, Что такое математика? (3-е издание) — Москва, МЦНМО, 2001.

• *Соминский И.С.*, Метод математической индукции (Выпуск 3 из серии «Популярные лекции по математике») — Москва, Наука, 1965.

• *Успенский В.А.*, Простейшие примеры математических доказательств, Библиотека «Математическое просвещение», выпуск 34 (2-е издание) — Москва, МЦНМО, 2012.

• *Шень А.*, Математическая индукция (5-е издание) — Москва, МЦНМО, 2016.

Математическая индукция

Задачи семинаров

3.1. Тождества и неравенства

Задача 3.1. (Т) Докажите, что для любого натурального n справедливо тождество

а) $1+2+3+4+\ldots+n=\dfrac{n(n+1)}{2}$;

б) $1+2^2+3^2+4^2+\ldots+n^2=\dfrac{n(n+1)(2n+1)}{6}$;

в) $1+2^3+3^3+4^3+\ldots+n^3=\dfrac{n^2(n+1)^2}{4}$;

г) $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)=\dfrac{n(n+1)(n+2)}{3}$;

д) $1\cdot 1!+2\cdot 2!+3\cdot 3!+\ldots+n\cdot n!=(n+1)!-1$;

е) $\dfrac{1}{1\cdot 2\cdot 3}+\dfrac{1}{2\cdot 3\cdot 4}+\ldots+\dfrac{1}{n(n+1)(n+2)}=\dfrac{n(n+3)}{4(n+1)(n+2)}$;

ж) $\dfrac{1}{1\cdot 3}+\dfrac{1}{2\cdot 4}+\dfrac{1}{3\cdot 5}+\ldots+\dfrac{1}{n(n+2)}=\dfrac{3}{4}-\dfrac{1}{2n+2}-\dfrac{1}{2n+4}$.

Задача 3.2. Пусть $s_1, s_2, \ldots$ последовательность чисел такая, что $s_1 = 2$, а каждое следующее выражается через предыдущее по формуле

$$s_{n+1}=\frac{1}{2}\left(s_n+\frac{2}{s_n}\right).$$

Докажите, что для всех натуральных n выполнено неравенство $1 \leqslant s_n \leqslant 2$.

Задача 3.3. (С) Докажите, что при любого действительного числа $\alpha > -1$ и любого натурального числа $n > 1$ выполнено *неравенство Бернулли*: $(1+\alpha)^n > 1+n\alpha$.

Задача 3.4. Докажите, что при $n > 1$ выполняется неравенство:

а) $\dfrac{1}{\sqrt{1}}+\dfrac{1}{\sqrt{2}}+\ldots+\dfrac{1}{\sqrt{n}}>\sqrt{n}$;

б) $\dfrac{1\cdot 2\cdot 3\cdot\ldots\cdot 2n}{(1\cdot 2\cdot 3\cdot\ldots\cdot n)^2}>\dfrac{4^n}{n+1}$.

3.2. Правдоподобные рассуждения

Задача 3.5. (Т) Найдите ошибку в следующем доказательстве.

Утверждение: все натуральные числа равны между собой.

Доказательство: база выполняется — одно число равно самому себе. Предположим, утверждение справедливо для любых k чисел. Рассмотрим $k+1$ число. Если отбросить первое число, то все оставшиеся по предположению индукции будут равны между собой. Если отбросить второе число, то все оставшиеся числа также будут равны между собой, в частности, равны первому числу. Итак, все натуральные числа равны.

Задача 3.6. (Т) Найдите ошибку в следующем доказательстве.

Утверждение: для любого $n \in \mathbb{N}$ произвольные n точек лежат на одной прямой.

Доказательство: база при $n = 1$, разумеется, выполняется — одна точка лежит на одной прямой. Предположим, утверждение верно для $n = k$. Тогда при $n = k + 1$ рассмотрим произвольные n точек $X_1, X_2, \ldots, X_k, X_{k+1}$. Точки $X_1, X_2, \ldots, X_k$ лежат на одной прямой по предположению индукции; точки $X_2, X_3, \ldots, X_{k+1}$ также лежат на одной прямой. Это означает, что все точки $X_1, X_2, \ldots, X_k, X_{k+1}$ лежат на единственной прямой, проходящей через точки $X_1, X_2, \ldots, X_k$.

Задача 3.7. (С) Справедливы ли следующее утверждение и его доказательство?

Утверждение: если треугольник разбит на меньшие треугольники отрезками (не обязательно диагоналями), то хотя бы один из треугольников разбиения не остроугольный.

Доказательство: Если треугольник разбит отрезком на два треугольника, то один из них не остроугольный (ясно). Пусть некоторый треугольник разбит на n меньших треугольников. Проведём ещё один отрезок, разбив один из маленьких треугольников на два. Получим разбиение на $(n + 1)$ треугольник, причём один из двух новых треугольников не будет остроугольным. По индукции утверждение доказано.

3.3. Суммирование и рекуррентные формулы

Задача 3.8. Найдите явную формулу для a_n, если известно, что

а) $a_1 = 1$ и $a_{n+1} = a_n + 3$ при всех натуральных n;

б) $a_0 = 2$, $a_1 = 3$, а также $a_{n+1} = 3a_n - 2a_{n-1}$ при всех натуральных $n > 1$.

Задача 3.9. Про последовательность (a_n) известно, что $a_1 = 1$, $a_2 = 2$, а также что при всех натуральных $n > 1$ выполнено $a_{n+1} = a_n - a_{n-1}$. Докажите, что $a_{n+6} = a_n$ для всех $n \in \mathbb{N}$.

Задача 3.10. (С) Несколько прямых называются *прямыми общего положения*, если никакие 2 из них не параллельны и никакие 3 не пересекаются в одной точке. Найдите количество частей, на которые n прямых общего положения делят плоскость.

а) Выпишите пять первых членов.

б) Найти рекуррентную формулу для этой последовательности.

в) Найдите формулу общего члена.

3.4. Обоснование алгоритма и конструирование

Задача 3.11. Докажите, что квадрат $2^n \times 2^n$, из которого вырезана произвольная клетка, можно разрезать на «уголки» из трёх клеток («уголок» — это квадрат 2×2 без одной клетки).

Задача 3.12. Имеется куча из n камней. Петя и Вася по очереди забирают из неё по 1, 2 или 3 камня; тот, кто не может сделать ход — проигрывает. Кто выигрывает при правильной игре, если начинает Петя?

Задача 3.13. 2020 человек не знакомы между собой. Докажите, что их можно перезнакомить так, что ни у каких трёх людей не будет одинакового числа знакомых.

Задача 3.14. Плоскость разбита на части прямыми и окружностями. Докажите, что полученную карту можно раскрасить в два цвета так, что области, граничащие по дуге или отрезку, будут иметь разный цвет.

3.5. Дополнительные задачи

Задача 3.15. Непустое множество целых чисел называется числовой группой, если оно содержит разность любых двух своих элементов. Докажите, что любая числовая группа состоит из всех целых чисел, делящихся на некоторое натуральное число n.

Задача 3.16. Поезд ехал через тоннель и n среди сидящих в одном купе мудрецов запачкались. Заметив это, проводник сказал: «Господа, среди вас есть запачкавшиеся». Мудрецы ленивые и ходят умываться только на остановках и только тогда, когда точно поймут, что запачкались. Зеркал в купе нет, а умывальник вмещает произвольное число пассажиров. Докажите, что на остановке с номером n все запачкавшиеся мудрецы одновременно пойдут умываться.

Задача 3.17. Восьми мудрецам показали 5 красных, 4 синих и 2 белых колпака. В темноте на них надели 4 красных, 2 синих и 2 белых колпака. Через некоторое время один из мудрецов правильно назвал цвет своего колпака. Какой на нём был колпак?

Задача 3.18. Докажите, что любое натуральное число можно представить как сумму

а) нескольких различных степеней двойки (возможно, включая нулевую степень);

б) нескольких различных чисел Фибоначчи (последовательность *чисел Фибоначчи* (f_n) задаётся начальными условиями $f_0 = f_1 = 1$, а также рекуррентной формулой $f_{n+1} = f_n + f_{k-1}$ при всех натуральных $n > 1$).

Задача 3.19. Дано натуральное число n. Выпишем все дроби вида $\frac{1}{pq}$, для которых числа p и q являются взаимно простыми и удовлетворяют неравенствам $0 < p < q \leqslant n$ и $p + q > n$. Чему равна сумма всех дробей такого вида?

Задача 3.20. Рассмотрим всевозможные наборы чисел из множества $1, 2, 3, \ldots, n$, не содержащие двух соседних чисел. Найдите сумму квадратов произведений чисел в этих наборах.

Задача 3.21. На небе бесконечное число звёзд. У каждой звезды есть размер и яркость, причём и то, и другое — натуральные числа. Известно, что любые две звезды отличаются хотя бы по одному из этих двух параметров. Докажите, что найдутся две звезды, первая из которых не меньше второй ни по яркости, ни по размеру.

Задача 3.22. Имеется таблица из трёх строк и бесконечного числа столбцов. В каждой клетке таблицы стоит натуральное число. Докажите, что можно так выбрать два столбца в таблице, что в каждой из строк число, стоящее в первом столбце, будет не больше числа, стоящего во втором столбце.

Задача 3.23. Докажите, что любые $n > 4$ точек можно так соединить стрелками, что из каждой точки в каждую можно попасть, пройдя последовательно либо по одной стрелке, либо по двум.

Делимость целых чисел

Теоретический материал

4.1. Основные определения и свойства

Целые числа знакомы читателю еще со школы. В этом разделе мы напомним основные определения и обозначения, связанные с целыми числами.

Множество целых чисел обозначается символом $\mathbb{Z}$ и состоит из элементов вида

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}.$$

Множество неотрицательных целых чисел обозначают символом $\mathbb{Z}_+$:

$$\mathbb{Z}_+ = \{0, 1, 2, \ldots\} \subset \mathbb{Z}.$$

На множестве целых чисел имеется естественное отношение порядка $\leqslant$. Подобно натуральным числам, $\mathbb{Z}_+$, обладает тем важным свойством, что любое его подмножество содержит минимальный элемент. Это наблюдение может показаться очевидным, но оно постоянно используется в доказательствах.

Упражнение 4.1. *Является ли отношение порядка рефлексивным? Симметричным? Транзитивным?*

Определение 4.1. Пусть $a, b \in \mathbb{Z}$ — целые числа. Говорят, что a *делится на* b и пишут $a \vdots b$, если существует такое $k \in \mathbb{Z}$, что

$$a = k \cdot b.$$

Про элемент b в этом случае говорят, что *он делит* a и пишут $b \mid a$. Если же b не делит a, то пишут $b \nmid a$.

Пример 4.1. $8 \vdots 2$, поскольку $8 = 2 \cdot 4$, но $3 \nmid 16$.

Упражнение 4.2. *Докажите, что если* $n \mid a$ *и* $n \mid b$, *то* $n \mid (a + b)$ *и* $n \mid (a - b)$ *для любой тройки* $n, a, b \in \mathbb{Z}$.

Упражнение 4.3. *Пусть целые числа* $n, a, b \in \mathbb{Z}$ *таковы, что* $n \mid a$ *и* $n \nmid b$. *Докажите, что в этом случае* $n \nmid (a + b)$.

Упражнение 4.4. *Докажите, что для любых* $a, b, c \in \mathbb{Z}$, *если* $a \vdots b$ *и* $b \vdots c$, *то* $a \vdots c$.

Напомним всем знакомую *десятичную запись целого числа* (о десятичной записи действительных чисел, а также о записях с другими основаниями будет подробно рассказано в главе Действительные числа). Целые числа в десятичной системе исчисления записываются последовательностью цифр $0,\ 1,\ 2, \ldots 9$. Это запись означает следующее

$$\overline{a_n a_{n-1} a_{n-2} \ldots a_0} := a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_0.$$

Здесь a_i — (не обязательно различные) цифры, а черта нужна для того, чтобы отличать эту запись от перемножения.

Пример 4.2. $1467 = 1 \cdot 1000 + 4 \cdot 100 + 6 \cdot 10 + 7 = 1 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 7$.

В терминах десятичной записи можно сформулировать признаки делимости на разные числа.

Утверждение 4.2.

- *Число делится на* 2, *если и только если его последняя цифра делится на 2.*
- *Число делится на 4, если и только если число, составленное из его последних цифр делится на 4.*
- *Число делится на 5, если и только если последняя цифра в его записи* — 0 *или* 5.

Упражнение 4.5. *а) Докажите утверждение 4.2.*

б) Сформулируйте аналогичные признаки делимости на $8, 25, 16, 125$.

Утверждение 4.3.

- *Число делится на* 3, *если и только если сумма его цифр делится на* 3.
- *Число делится на* 9, *если и только если сумма его цифр делится на* 9.

Упражнение 4.6. *Докажите утверждение 4.3.*

4.2. Деление с остатком

Определение 4.4. Пусть $a, b \in \mathbb{Z}$ — целые числа. Говорят, что a *делится с остатком* на b, если существуют $q, r \in \mathbb{Z}$ такие, что

$$a = qb + r, \qquad 0 \leqslant r < |b|.$$

В таком случае q называют *(неполным) частным*, а r — *остатком.*

Теорема 4.5. *Целые числа можно делить с остатком. А именно, для любых целых чисел* a *и* $b \neq 0$ *существует единственная пара целых чисел* q *и* r *такая, что*

$$a = qb + r, \qquad 0 \leqslant r < |b|,$$

Замечание. Обратите внимание, что $r \geqslant 0$, — это условие нужно для единственности.

Мотивировка. Данное рассуждение нельзя считать честным доказательством, но ознакомиться с ним весьма полезно. Предположим сначала, что $b > 0$, и рассмотрим множество $\{nb \mid n \in \mathbb{Z}\}$. Точки этого множества разбивают числовую прямую на равные отрезки (точнее, полуинтервалы) длины b. Ясно, что число a должно находиться в одном из них:

$$bn \leqslant a < b(n+1).$$

Вычитая из всех частей этого двойного неравенства bn, получаем

$$0 \leqslant a - bn < b.$$

Остаётся положить $q = n$ и $r = a - bn$.

Если же $b < 0$, то $-b > 0$ и число $-a$ представимо в виде

$$-a = q'(-b) + r'.$$

Отсюда видно, что если $r' = 0$, то достаточно взять $q = -q'$. В противном случае положим $q = q' + 1$ и $r = -b - r'$.

Упражнение 4.7. *Покажите, что при $b < 0$ указанные числа q и r действительно являются неполным частным и остатком при делении a на b.*

Доказательство. Приведём строгое доказательство теоремы 4.5. Начнём с единственности. Пусть существует две пары чисел (q_1, r_1) и (q_2, r_2), удовлетворяющих условиям теоремы, то есть

$$a = q_1 b + r_1, \quad 0 \leqslant r_1 < |b|, \qquad \text{и} \qquad a = q_2 b + r_2, \quad 0 \leqslant r_2 < |b|.$$

Тогда

$$q_1 b + r_1 = q_2 b + r_2 \qquad \Longrightarrow \qquad (q_1 - q_2)b = r_2 - r_1.$$

Заметим, что, с одной стороны,

$$(r_2 - r_1) \vdots b \qquad \Longrightarrow \qquad |r_2 - r_1| \vdots |b|.$$

С другой стороны,

$$|r_2 - r_1| < |b|.$$

Таким образом, $r_2 - r_1$ должно быть равно 0, а значит, и $b(q_1 - q_2) = 0$. Поскольку по условию теоремы $b \neq 0$, имеем $q_1 = q_2$ и $r_1 = r_2$, что и хотелось доказать.

Перейдём к доказательству существования. Мы ограничимся случаем $a \geqslant 0$, $b > 0$, оставив остальное в качестве упражнения. Для доказательства воспользуемся индукцией по a. Заметим, что случай $a < b$ тривиален, а именно, достаточно положить $q = 0$ и $r = a$. Тем самым, база индукции доказана. Пусть теперь $a \geqslant b$ и утверждение верно для всех $0 \leqslant a_0 < a$. Положим

$$a_0 = a - b.$$

Тогда $0 \leqslant a_0 < a$, и по предположению индукции найдутся q_0 и r_0 такие, что

$$a_0 = q_0 b + r_0, \qquad 0 \leqslant r_0 < b.$$

Таким образом,

$$a = q_0 b + b + r_0 = (q_0 + 1)b + r_0,$$

и остаётся положить $q = q_0 + 1$ и $r = r_0$. Теорема доказана $\square$

Упражнение 4.8. *Проверьте существование в остальных случаях.*

Упражнение 4.9. *Пусть $n \in \mathbb{Z}$. На какие цифры может оканчиваться десятичная запись числа n^2?*

Упражнение 4.10. *Найдите остатки от деления а) 2^{2020} на 3; б) 3^{777} на 5.*

4.3. Алгоритм Евклида

• Пусть $a, b \in \mathbb{Z}$ — целые числа. Будем называть их *общим делителем* такое число $n \in \mathbb{Z}$, что $a \vdots n$ и $b \vdots n$. Ясно, что любые два числа имеют хотя бы один общий делитель: таковым, например, является число 1.

Упражнение 4.11. *Пусть $a \in \mathbb{Z}$, причём $a \neq 0$, и $a \vdots n$. Покажите, что $|n| \leqslant |a|$.*

• *Наибольший общий делитель (НОД)* чисел $a, b \in \mathbb{Z}$ — это, как следует из названия, наибольший из их общих делителей. Применяют два основных обозначения:

$$d = \text{НОД}(a, b) \qquad \text{или просто} \qquad d = (a, b).$$

Оба они означают, что d является наибольшим общим делителем чисел a и b.

Из упражнения 4.11 вытекают следующие факты.

• Множество делителей ненулевого целого числа конечно.

• Множество общих делителей конечного набора различных целых чисел конечно.

Поскольку в любом непустом конечном подмножестве целых чисел обязательно есть максимальный элемент, отсюда следует, что определение наибольшего общего делителя чисел a и b корректно, коль скоро они оба не равны нулю.

• Если $(a, b) = 1$, то числа a и b называются *взаимно простыми*.

Замечание. Можно было бы определить (a, b) как число d, обладающее следующими двумя свойствами:

1) $a \vdots d$ и $b \vdots d$;

2) если $a \vdots n$ и $b \vdots n$, то $d \vdots n$.

Это определение, однако, не определяет наибольший общий делитель однозначно, а лишь с точностью до умножения на ± 1.

Опишем алгоритм, позволяющий находить НОД для любой пары целых чисел, не равных нулю одновременно. Согласно этому алгоритму, известному в литературе как *алгоритм Евклида*, НОД (a, b) вычисляется при помощи последовательности шагов:

$$\begin{aligned} a &= q_0 b + r_0 && \text{нулевой шаг} \\ b &= q_1 r_0 + r_1 && \text{первый шаг} \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n && n\text{-й шаг} \\ r_{n-1} &= q_{n+1} r_n && (n+1)\text{-й шаг} \end{aligned}$$

где r_n – последний ненулевой остаток. Отметим, что алгоритм завершит свою работу корректно, поскольку последовательность целочисленных остатков

$$|b| > |r_0| > |r_1| > \ldots > |r_n|$$

строго убывает. В частности, в какой-то момент предпоследний полученный остаток будет нацело делиться на последний.

Пример 4.3. Воспользуемся алгоритмом Евклида, чтобы вычислить НОД$(351, 120)$.

$$351 = 2 \cdot 120 + 111,$$
$$120 = 1 \cdot 111 + 9,$$
$$111 = 12 \cdot 9 + 3,$$
$$9 = 3 \cdot 3.$$

Таким образом, $(351, 120) = 3$.

Прежде, чем обосновывать корректность работы алгоритма Евклида, мы докажем небольшую, но важную лемму.

Лемма 4.6. *Пусть $a = qb + r$. Тогда $(a, b) = (b, r)$.*

Доказательство. Введём обозначения $d = (a, b)$ и $d' = (b, r)$. Заметим, что с одной стороны, согласно упражнению 4.2,

$$a = qb + r \qquad \Longrightarrow \qquad a \vdots d'.$$

Отсюда следует, что $d \geqslant d'$, поскольку d' — общий делитель чисел a и b, а d — их наибольший общий делитель. С другой стороны, очевидно,

$$r = a - qb \qquad \Longrightarrow \qquad r \vdots d.$$

Совершенно аналогичным образом это влечёт $d' \geqslant d$. Таким образом, $d_1 = d$. □

Теорема 4.7. [Алгоритм Евклида] *Последний остаток r_n в описанном выше алгоритме — это в точности НОД(a, b).*

Доказательство. Благодаря лемме 4.6 имеем $(a, b) = (b, r_0) = (r_0, r_1) = \ldots = (r_n, 0)$. Остаётся заметить, что $(r_n, 0) = r_n$. □

Замечание. В доказательстве теоремы используется индукция, хоть и в немного непривычном виде: по количеству шагов в алгоритме. В качестве базы выступает равенство $(r_n, 0) = r_n$, а индукционный переход проводится при помощи леммы 4.6.

Упражнение 4.12. *С помощью алгоритма Евклида найдите НОД* $(69, 372)$.

Пример 4.4. Из алгоритма Евклида можно вывести так называемое *линейное представление* наибольшего общего делителя. Мотивировку и более общее доказательство мы отложим до следующего раздела, а здесь обсудим конкретный пример: представим $(351, 120) = 3$ в виде $3 = 351x + 120y$. В примере 4.3 мы убедились, что наибольший общий делитель чисел 351 и 120 действительно равен 3. Чтобы получить желаемый результат, нужно в некотором смысле пройти по алгоритму в обратную сторону:

$$3 = 111 - 12 \cdot 9 =$$
$$= 111 - 12 \cdot (120 - 111) = 13 \cdot 111 - 12 \cdot 120 =$$
$$= 13 \cdot (351 - 2 \cdot 120) - 12 \cdot 120 = 13 \cdot 351 - (13 \cdot 2 + 12) \cdot 120 =$$
$$= 13 \cdot 351 - 38 \cdot 120.$$

Итого $x = 13$, а $y = -38$.

4.4. Линейное представление НОД

Для пары целых чисел $a, b \in \mathbb{Z}$ определим множества

$$\mathbb{Z}(a,b) = \{ax + by \mid x, y \in \mathbb{Z}\}, \qquad \text{и} \qquad \mathbb{Z}(d) = \{dm \mid m \in \mathbb{Z}\}, \quad \text{где} \quad d = (a,b).$$

Основная цель этого раздела — доказать, что эти множества совпадают. Но прежде чем приступить к доказательству, обсудим мотивировку.

Решим такую задачу. Пусть в некоторой стране, валюту которой для определённости мы назовём рублями, в обращении имеются монеты двух номиналов: a рублей и b рублей. Допустим, некоторый товар стоит n рублей. Предположим также, что и у покупателя, и у продавца монет очень много — нет ограничений по количеству монет на сдачу. Всегда ли покупателю удастся расплатиться? А если нет, то каковы условия на стоимость товара n, чтобы расплатиться было возможно?

Наш будущий результат о равенстве множеств $\mathbb{Z}(a,b)$ и $\mathbb{Z}(d)$ как раз отвечает на этот вопрос — это возможно тогда и только тогда, когда $n \vdots d$. Действительно, если покупателю удастся расплатиться, то $n \in \mathbb{Z}(a,b)$, поскольку покупатель отдаст продавцу $(x_1a + y_1b)$ рублей, получив при этом сдачу $(x_2a + y_2b)$ рублей, то есть

$$n = (x_1a + y_1b) - (x_2a + y_2b) = (x_1 - x_2)a + (y_1 - y_2)b \in \mathbb{Z}(a,b).$$

Если же мы докажем, что $\mathbb{Z}(a,b) = \mathbb{Z}(d)$, то это будет означать, что все числа, представимые в виде суммы чисел a и b с целыми коэффициентами, обязательно делятся на их наибольший общий делитель. Таким образом, товар можно будет купить, если и только если его стоимость кратна d. В частности, если a и b взаимно просты, то есть если выполнено равенство $d = (a,b) = 1$, то можно купить товар любой стоимости.

Перейдем теперь к теореме.

Теорема 4.8. [Линейное представление НОД] *Для любых двух целых чисел a и b, не равных нулю одновременно, $\mathbb{Z}(a,b) = \mathbb{Z}(d)$, где $d = (a,b)$.*

Доказательство. Согласно критерию равенства множеств, сформулированному в разделе 2.2, нам нужно доказать два включения:

$$\mathbb{Z}(a,b) \subset \mathbb{Z}(d) \qquad \text{и} \qquad \mathbb{Z}(d) \subset \mathbb{Z}(a,b).$$

Первое включение очевидно. Действительно, пусть k — произвольных общий делитель чисел a и b. Тогда любое число вида $(ax + by)$ делится на k, поскольку

$$ax + by = ka_1x + kb_1y = k(a_1x + b_1y).$$

В частности d делит любое число такого вида.

Обратное включение доказывается более хитро. Нам потребуется несколько свойств множеств $\mathbb{Z}(a,b)$ и $\mathbb{Z}(d)$, которые мы оставим читателю в качестве упражнений.

Упражнение 4.13. *Проверьте, что выполнены следующие включения:*

а) $0, a, b \in \mathbb{Z}(a,b)$;

б) $0, d, a, b \in \mathbb{Z}(d)$.

Упражнение 4.14. *Проверьте, что для любых целых чисел k и l:*
а) если $k, l \in \mathbb{Z}(a, b)$, то $k \pm l \in \mathbb{Z}(a, b)$;
б) если $k, l \in \mathbb{Z}(d)$, то $k \pm l \in \mathbb{Z}(d)$.

Упражнение 4.15. *Проверьте, что для любых целых чисел k и n:*
а) если $k \in \mathbb{Z}(a, b)$, то $nk \in \mathbb{Z}(a, b)$;
б) если $k \in \mathbb{Z}(d)$, то $nk \in \mathbb{Z}(d)$.

Упражнение 4.16. *Докажите, что в множестве $\mathbb{Z}(a, b)$ есть минимальный по модулю ненулевой элемент.*

Обозначим минимальный элемент множества $\mathbb{Z}(a, b)$, который существует согласно упражнению 4.16, буквой t. Можно считать, что $t > 0$; в противном случае, возьмём число $(-t)$ — оно тоже лежит в нашем множестве. Пусть $n = ax + by$ — произвольный элемент из $\mathbb{Z}(a, b)$. Поделим n на t с остатком:

$$n = qt + r, \qquad \text{где } 0 \leqslant r < t.$$

Преобразовывая это выражение, получаем $r = ax + by - qt$. При этом $qt \in \mathbb{Z}(a, b)$ по упражнению 4.15, а значит, $r \in \mathbb{Z}(a, b)$ по упражнению 4.14. Ключевой момент доказательства заключается в наблюдении, что $0 \leqslant r < t$, однако t — наименьший ненулевой элемент! Поэтому мы заключаем, что $r = 0$.

Покажем теперь, что $t = d$. Мы уже знаем, что $\mathbb{Z}(a, b) \subset \mathbb{Z}(d)$, то есть d делит любой элемент из $\mathbb{Z}(a, b)$. В частности, $d \mid t$, а потому $d \leqslant t$ согласно упражнению 4.11. С другой стороны, t — общий делитель a и b, поскольку $a, b \in \mathbb{Z}(a, b)$ и t делит любой элемент этого множества. Но всякий общий делитель не превосходит НОД, поэтому $t \leqslant d$. Таким образом, $d = t$, откуда $d \in \mathbb{Z}(a, b)$ и $\mathbb{Z}(d) \subset \mathbb{Z}(a, b)$ по упражнению 4.15. □

Замечание. Доказанная теорема позволяет дать ещё одно определение наибольшего общего делителя, а именно

$$(a, b) = \min\{|ax + by| \mid x, y \in \mathbb{Z}\}.$$

4.5. Линейные диофантовы уравнения

При изучении свойств целых чисел особую роль играют уравнения, в которые входят переменные, принимающие значения во множестве $\mathbb{Z}$. Такие уравнения называются *диофантовыми*. В простейших случаях для их решения бывает достаточно изучить поведение остатков составных частей уравнения при делении на некоторое число.

Пример 4.5. Рассмотрим диофантово уравнение $x^2 + y^2 = 2019$ от двух переменных x и y. Заметим, что $2019 = 504 \cdot 4 + 3$, то есть остаток при делении 2019 на 4 равен 3. С другой стороны, остаток квадрата целого числа при делении на 4 всегда равен 0 или 1. Таким образом, остаток суммы квадратов $x^2 + y^2$ может принимать лишь значения 0, 1 или 2, а значит, искомое уравнение решений в целых числах не имеет.

Данный раздел посвящён изучению целочисленных решений уравнений вида

$$ax + by = c, \tag{1}$$

где $a, b, c \in \mathbb{Z}$, причём $a, b \neq 0$. Уравнения вида (1) представляют собой наиболее простой частный случай диофантовых уравнений — *линейный*. Благодаря этому их решения можно описать в общем виде в зависимости от параметров a, b и c.

Первое, довольно очевидное, наблюдение состоит в том, что если число c не делится на (a, b), то решений уравнение (1) не имеет. В самом деле, в этом случае при любых $x, y \in \mathbb{Z}$ левая часть делится на НОД, а правая часть — нет. Менее очевидное соображение утверждает, что если $c \vdots (a, b)$, то хоть одно решение найдётся. В самом деле, пусть $c = (a, b) \cdot k$. Благодаря алгоритму Евклида мы знаем, как искать целые числа x_0 и y_0 такие, что

$$ax_0 + by_0 = (a, b).$$

Домножая это равенство на k, мы получим $ax_0k + by_0k = (a, b) \cdot k = c$, что означает, что $x = x_0k$ и $y = y_0k$ суть решение исходного уравнения.

Теперь, зная одно решение уравнения (1), нам бы хотелось обладать методом для поиска всех остальных решений. Главным инструментом тут будет следующая лемма.

Лемма 4.9. *Если целые числа a и c взаимно просты и $ab \vdots c$, то $b \vdots c$.*

Доказательство. Если $(a, c) = 1$, то по теореме 4.8 мы имеем

$$ma + nc = 1$$

для некоторых $m, n \in \mathbb{Z}$. Домножая это равенство на b, получаем

$$mab + nbc = b.$$

Таким образом, c делит левую часть, а значит, $b \vdots c$. □

Упражнение 4.17. *Докажите, что если $a \vdots b$, $a \vdots c$ и $(b, c) = 1$, то $a \vdots bc$.*

Опишем теперь, как построить все решения уравнения (1), угадав или вычислив одно частное решение.

Теорема 4.10. *Пусть $x_0, y_0 \in \mathbb{Z}$ – некоторое решение уравнения (1), то есть*

$$ax_0 + by_0 = c.$$

Тогда множество всех его решений имеет вид

$$x = x_0 + m\frac{b}{(a, b)}, \qquad y = y_0 - m\frac{a}{(a, b)},$$

где m пробегает все целые числа.

Доказательство. Без ограничения общности будем считать, что числа a и b являются взаимно простыми. Действительно, как мы видели выше, если $(a, b) = d$ и уравнение (1)

имеет решение, то $c \vdots d$, так что всё уравнение можно сократить на d. Предположим теперь, что x, y — произвольное решение нашего уравнения. Тогда по условию

$$ax + by = c \qquad \text{и} \qquad ax_0 + by_0 = c.$$

Вычитая из первого уравнения второе, мы получим равенство $a(x - x_0) = b(y_0 - y)$. В силу того, что числа a и b взаимно просты, из леммы 4.9 следует, что $(x - x_0) \vdots b$ и $(y_0 - y) \vdots a$. Иными словами, существуют такие целые числа m и n, что

$$\begin{cases} x - x_0 = mb \\ y_0 - y = na \end{cases} \qquad \Longrightarrow \qquad \begin{cases} x = x_0 + mb \\ y = y_0 - na. \end{cases}$$

Остаётся заметить, что из цепочки равенств

$$ax + by = a(x_0 + mb) + b(y_0 - na) = (ax_0 + by_0) + mab - nab = c + ab(m - n)$$

вытекает, что найденные выражения удовлетворяют уравнению при любых $m = n$. Таким образом, теорема доказана. □

Подведём итог. Для того, чтобы решить произвольное уравнение вида (1), достаточно выполнить следующие действия.

• Проверить, верно ли, что $c \vdots (a, b)$ — в противном случае решений нет. Для этого обычно бывает достаточно применить алгоритм Евклида и найти (a, b).

• Найти какое-нибудь частное решение: либо с помощью обратного хода алгоритма Евклида, либо «методом пристального вглядывания», то есть попросту угадав его.

• Примененить теорему 4.10.

Пример 4.6. Рассмотрим уравнение $5x + 2y = 17$. Легко убедиться, что $x_0 = 3, y_0 = 1$ является его частным решением. Значит, по теореме 4.10 общее решение имеет вид

$$\begin{cases} x = 3 + 2m, \\ y = 1 - 5m, \end{cases} \qquad m \in \mathbb{Z}.$$

С другой стороны, если бы мы не увидели указанного частного решения, можно было бы сначала воспользоваться алгоритмом Евклида для того, чтобы найти $(5, 2)$, а затем, убедившись, что $17 \vdots (5, 2)$, развернуть его и найти решение уравнения $5x + 2y = (5, 2)$:

$$\begin{array}{c} 5 = 2 \cdot 2 + 1 \\ 2 = 2 \cdot 1, \end{array} \qquad \Longrightarrow \qquad (5, 2) = 1 \qquad \Longrightarrow \qquad 1 = 1 \cdot 5 - 2 \cdot 2.$$

Домножая это частное решение на 17, мы найдём частное решение исходного уравнения: $x_0 = 17$, $y_0 = -34$. Остаётся применить теорему 4.10:

$$\begin{cases} x = 17 + 2n, \\ y = -34 - 5n, \end{cases} \qquad n \in \mathbb{Z}.$$

На первый взгляд может показаться, что мы получили разные решения. Но это не так: второе получается из первого подстановкой $m = n + 7$.

4.6. Основная теорема арифметики

Напомним, что число $p \in \mathbb{N}$ называется *простым*, если у него нет делителей, отличных от 1 и p. В противном случае оно называется *составным*. Исключение составляет число 1: оно не считается ни простым числом, ни составным.

Мы начнём с интуитивно понятного, но не вполне тривиального факта.

Утверждение 4.11. *Различных простых чисел бесконечно много.*

Доказательство. В качестве первого шага докажем вспомогательный факт: для любого числа $n > 1$ найдётся простое число p (возможно, равное n) такое, что n делится на p. Для этого используем индукцию. База индукции $n = 2$ очевидна. Индукционный шаг: допустим, что мы умеем доказывать искомое утверждение для всех чисел, меньших n. Само n может быть простым — тогда доказывать нечего — или составным. В последнем случае $n = km$ для некоторых натуральных чисел k и m, меньших n. Для них уже выполняется предположение индукции, например, найдётся простое p, на которое делится число k. Следовательно, и n делится на p.

Вернёмся к основному утверждению. Предположим, что множество простых чисел конечно, и у нас есть их полный список: $p_1, \ldots, p_k$. Тогда рассмотрим число

$$n = p_1 \cdot \ldots \cdot p_k + 1.$$

Как было показано выше, число n имеет простой делитель. С другой стороны, ни одно из перечисленных выше чисел $p_1, \ldots, p_k$ его делителем не является. Противоречие. □

Упражнение 4.18. *Докажите, что любое натуральное число $n > 1$ представляется в виде произведения простых чисел $n = p_1 \cdot p_2 \ldots p_k$ (не обязательно различных).*

Лемма 4.12. *Следующие два условия эквивалентны:*

1) p простое;

2) для любых $a, b \in \mathbb{Z}$, если $p \mid ab$, то $p \mid a$ или $p \mid b$.

Доказательство.

(1) $\Rightarrow$ (2): Пусть p простое и $p \nmid a$, тогда $(p, a) = 1$. Если $p \mid ab$, то по лемме 4.9 получаем $p \mid b$. Аналогично, предположив $p \nmid b$, из $p \mid ab$ получаем $p \mid a$.

(2) $\Rightarrow$ (1): Если p не простое, то $p = n_1 \cdot n_2$ для некоторых $n_1 > 1$ и $n_2 > 1$. Но тогда для $a = n_1$ и $b = n_2$ мы имеем $p \mid ab$, в то время как $p \nmid n_1$ и $p \nmid n_2$ — противоречие. □

Упражнение 4.19. *Пусть p простое число, $n_1, \ldots, n_m \in \mathbb{N}$. Докажите, что если $(n_1 n_2 \ldots n_m) \vdots p$, то существует k, для которого $n_k \vdots p$.*

Теорема 4.13. [Основная теорема арифметики] *Любое целое число $n > 1$ единственным образом представляется в виде*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k,$$

где $p_1, \ldots, p_k$ не обязательно различные простые числа.

Замечание. В такой записи единственность понимается с точностью до изменения порядка сомножителей. Группируя одинаковые сомножители вместе и упорядочивая их от большего к меньшему, мы получим запись вида

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_l^{\alpha_l},$$

где $p_1 < p_2 < \ldots < p_l$ — простые, а $\alpha_1, \alpha_2, \ldots, \alpha_l \in \mathbb{N}$ — натуральные. Такая запись уже единственна для каждого натурального числа n.

Доказательство. Представимость в требуемом виде следует из упражнения 4.18. Для доказательства единственности предположим, что существует другое представление

$$n = q_1 \cdot q_2 \cdot \ldots \cdot q_r$$

числа n в виде произведения простых. Тогда имеет место равенство

$$q_1 \cdot q_2 \cdot \ldots \cdot q_r = p_1 \cdot p_2 \cdot \ldots \cdot p_k.$$

Сократив в нём все совпадающие q_i и p_j, получим новое равенство

$$q'_1 \cdot q'_2 \cdot \ldots \cdot q'_{r'} = p'_1 \cdot p'_2 \cdot \ldots \cdot p'_{k'},$$

где ни одно число q'_i в левой части не равняется никакому числу p'_j в правой. Левая часть, однако, делится, скажем, на p'_1, поэтому по упражнению 4.19 одно из простых чисел q'_m делится на p'_1. Однако последнее бы означало, что $q'_m = p'_1$, а мы сократили все общие множители. Полученное противоречие завершает доказательство. □

Пример 4.7. Число 12 разлагается в виде $12 = 2 \cdot 2 \cdot 3$, но допускаются и разложения $12 = 2 \cdot 3 \cdot 3$ или $12 = 3 \cdot 2 \cdot 2$. Или же можно написать $12 = 2^2 \cdot 3$.

Упражнение 4.20. *Существуют ли такие $x, y, z \in \mathbb{N}$, отличные от единицы, для которых были бы справедливы равенства $xy = 64$ и $yz = 405$?*

Упражнение 4.21. *Пусть p — простое число. Докажите, что для любого $n \in \mathbb{Z}$ свойство $n^2 \vdots p$ влечёт за собой $n^2 \vdots p^2$.*

В качестве приятного приложения докажем классический результат об иррациональности корня из двух. Пусть число $\sqrt{2}$ рационально, то есть $\sqrt{2} = \frac{m}{n}$, $m, n \in \mathbb{Z}$, тогда $2n^2 = m^2$. Без ограничения общности можно считать эту дробь нескоратимой: $(m, n) = 1$. Следовательно, $m^2 \vdots 2$, откуда согласно упражнению 4.21 имеем $m^2 \vdots 4$, то есть $m_2 = 4s$ для некоторого s. Значит,

$$2n^2 = 4s \qquad \Longrightarrow \qquad n^2 = 2s \qquad \Longrightarrow \qquad n^2 \vdots 2 \qquad \Longrightarrow \qquad n \vdots 2.$$

но последнее противоречит предположению о несократимости дроби.

4.7. Литература для дальнейшего изучения

• *Заславский А.А., Пермяков Д.А., Скопенков А.Б., Скопенков М.Б., Шаповалов А.В.*, Математика в задачах. — Москва, МЦНМО, 2009.

• *Калужин Л.А.*, Основная теорема арифметики (Выпуск 47 из серии «Популярные лекции по математике») — Москва, Наука, 1969.

• *Курант Р., Робинс Г.*, Что такое математика? (3-е издание) — Москва, МЦНМО, 2001.

Делимость целых чисел

Задачи семинаров

4.1. Свойства делимости

Задача 4.1. Верно ли, что если ab делится на c^2, то a делится на c или b делится на c?

Задача 4.2. а) Докажите, что число $\overline{a_n a_{n-1} \dots a_1 a_0}$ делится на 11 если и только если знакопеременная сумма $\big(a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n\big)$ делится на 11.

б) Сформулируйте и докажите признак делимости на 111.

Задача 4.3. Докажите, что при любом натуральном n

а) $(5^{2n+1} + 3^{n+2} \cdot 2^{n-1})$ делится на 19;

б) $(7^{2n} - 4^{2n})$ делится на 33.

4.2. Деление с остатком

Задача 4.4. (Т) Найдите остатки от деления:

а) $(12^{14} + 14^{12})$ на 13;

б) $(2222^{5555} + 5555^{2222})$ на 7.

Задача 4.5. (Т) Какой цифрой оканчивается число

а) 14^{14};

б) $14^{14^{14}}$;

в) 7^{7^7}?

Задача 4.6. На клетчатой бумаге нарисован прямоугольник размерами $m \times n$ клеток, стороны которого лежат на линиях сетки. На сколько частей делят его диагональ

а) узлы сетки;

б) линии сетки?

4.3. НОД, алгоритм Евклида и диофантовы уравнения

Задача 4.7. (Т) Вычислите:

а) $(7\,777\,777,\ 7\,777)$;

б) $(3289, 969)$;

в) $(11391, 5673)$;

г) $(17711, 10946)$;

д) $(507885, 60808)$.

Задача 4.8. Пусть $a, b \in \mathbb{Z}$ и $d = (a, b)$. Докажите, что $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

Задача 4.9. Докажите, что для всех натуральных n

а) $(n^3 - n) \vdots 6$;

б) $(n^5 - n) \vdots 30$;

в) $(7^{2n} - 4^{2n}) \vdots 33$.

Задача 4.10. (Т) Решите линейные диофантовы уравнения:

а) $2x + 4y = 5$;

б) $17x + 29y = 31$;

в) $85x + 145y = 505$;

г) $123x + 819y = 505$

Задача 4.11. При каких a и b можно заплатить в кассу 1 рубль, имея на руках неограниченное количество a-рублёвых купюр, если в кассе есть неограниченный запас b-рублёвых купюр?

4.4. Основная теорема арифметики

Задача 4.12. Докажите, что натуральное число n является полным квадратом (то есть $n = k^2$ для некоторого натурального k) тогда и только тогда, когда n имеет нечётное число натуральных делителей (включая 1 и n).

Задача 4.13. Докажите, что число n не является квадратом натурального числа, если

а) $n = 25324851$;

б) $n = 39!$.

Задача 4.14. Существует ли 100 подряд идущих составных чисел?

Задача 4.15. Является ли рациональным число

а) $\sqrt{2}$;

б) $\sqrt{2} + \sqrt{3}$;

в) $\sqrt{2} + \sqrt{3} + \sqrt{6}$?

4.5. Дополнительные задачи

Задача 4.16. Сформулируйте и докажите признак делимости на 7.

Задача 4.17. Для всех пар целых чисел m и n вычислите:

а) $(2^m - 1,\ 2^n - 1)$;

б) $(2^{2^m} + 1,\ 2^{2^n} + 1)$.

Задача 4.18. а) Для двух натуральных чисел, меньших миллиона, провели алгоритм Евклида. Докажите, что он состоял не более чем из 40 шагов.

б) Для каких пар чисел от 1 до 1000 алгоритм Евклида работает дольше всего?

Задача 4.19. У Пети и Васи есть шоколадка в форме равностороннего треугольника со стороной n, разделённая бороздками на дольки— равносторонние треугольники со стороной 1. За один ход можно отломать от шоколадки треугольный кусок вдоль бороздки и съесть его, а остаток передать противнику. Выигрывает тот, кто получает последний кусок — треугольник со стороной 1. Если же игрок не может сделать ход, то он проигрывает. Кто выиграет при правильной игре, если Петя ходит первым?

Задача 4.20. Докажите, что из чисел, обратных к натуральным, можно составить арифметическую прогрессию произвольной длины.

Комбинаторика

Теоретический материал

5.1. Правила суммы и произведения

Пусть A и B — конечные непересекающиеся множества.

Правило суммы: Если элемент из множества A можно выбрать a способами, а элемент из множества B — b способами, то выбрать элемент из множества A **или** элемент из множества B можно $a + b$ способами.

Пример 5.1. Если на столе лежат 5 яблок и 7 апельсинов, то выбрать одно яблоко можно 5 способами, выбрать один апельсин — 7 способами, а значит, выбрать один фрукт можно $5 + 7 = 12$ способами.

Правило произведения: Если элемент из множества A можно выбрать a способами, а элемент из множества B — b способами, то выбрать **пару** элементов из множества A **и** из множества B можно $a \cdot b$ способами.

Пример 5.2. Пусть яблоко можно выбрать 5 способами, апельсин — 7 способами. Тогда выбрать пару "яблоко + апельсин" можно $5 \cdot 7 = 35$ способами.

С помощью правил суммы и произведения решается большинство стандартных комбинаторных задач.

Пример 5.3. Сколько существует автомобильных номеров вида А123БВ, использующих только гласные (без Ы) или только согласные буквы?

► В русском алфавите 9 гласных (без Ы) и 21 согласных. Вычислим количество номеров только с гласными буквами. На первом месте может стоять 9 букв. На втором, третьем и четвёртом — цифры от 0 до 9 (по 10 вариантов). На пятом и шестом — по одной из 9 букв. По правилу произведения получаем $9 \cdot 10 \cdot 10 \cdot 10 \cdot 9 \cdot 9 = 9^3 10^3$ вариантов. Для случая согласных букв получаем $21 \cdot 10 \cdot 10 \cdot 10 \cdot 21 \cdot 21 = 21^3 10^3$ вариантов. Итого по правилу суммы число номеров требуемого вида: $9^3 10^3 + 21^3 10^3$. ◄

Упражнение 5.1. *В классе 20 юношей и 15 девушек. Сколько существует способов составить одну пару для выпускного бала?*

Упражнение 5.2. *а) На шахматную доску поставили короля и ферзя, причём короля на чёрное поле, а ферзя — на белое. Сколькими способами это можно сделать?*

б) А если и короля, и ферзя требуется поставить на белые поля?

в) А если вместо короля и ферзя ставим двух коней?

г) А если мы ставим и короля, и ферзя, и двух коней, причём всех — только на белые поля?

В терминах теории множеств правила суммы и произведения формулируются так:

$$|A \cup B| = |A| + |B| \quad (\text{если } A \cap B = \varnothing); \qquad |A \times B| = |A| \cdot |B|.$$

5.2. Формула включений-исключений

Пример 5.4. Из 80 студентов на курсе 50 знают английский язык, 30 знают немецкий язык, 20 — оба языка. Сколько студентов на курсе не знают ни одного языка?
► Пусть A — множество студентов, знающих английский язык, B — знающих немецкий язык. Тогда $A \cap B$ знают оба языка, $A \cup B$ знают хотя бы один язык. По условию $|A| = 50, |B| = 30, |A \cap B| = 20$. Заметим, что $|A \cup B| = |A| + |B| - |A \cap B|$. В самом деле, в сумме $|A|+|B|$ мы посчитали два раза студентов, знающих оба языка (входящих и в множество A, и в множество B). Вычитая $|A \cap B|$ из суммы $|A| + |B|$, мы получим в точности число студентов, знающих хотя бы один язык.

Таким образом, $|A \cup B| = 50 + 30 - 20 = 60$ студентов знают хотя бы один язык. Значит, $80 - 60 = 20$ студентов не знают ни одного языка. ◄

В аналогичной задаче с тремя языками (английский, немецкий, французский) может быть использована формула для трёх множеств:

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

В общем случае для n множеств имеет место следующая теорема.

Теорема 5.1. [Формула включений-исключений]

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{\substack{i,j=1 \\ i<j}}^{n} |A_i \cap A_j| + \sum_{\substack{i,j,k=1 \\ i<j<k}}^{n} |A_i \cap A_j \cap A_k| - \ldots \pm |A_1 \cap \ldots \cap A_n|.$$

Доказательство. Докажем индукцией по n.
База индукции: Для $n = 1$ утверждение тривиально, для $n = 2$ формула проверяется непосредственно.
Шаг индукции. Пусть для n множеств формула верна. Рассмотрим $(n+1)$ множество и выделим множество A_{n+1}. Тогда:

$$|(A_1 \cup \ldots \cup A_n) \cup A_{n+1}| = |(A_1 \cup \ldots \cup A_n)| + |A_{n+1}| - |(A_1 \cup \ldots \cup A_n) \cap A_{n+1}|,$$

что следует из базы при $n = 2$. Вычитаемое раскладывается как:

$$(A_1 \cup \ldots \cup A_n) \cap A_{n+1} = (A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \ldots \cup (A_n \cap A_{n+1}). \qquad (2)$$

Обозначим $A_i \cap A_{n+1} = B_i$. Получим:

$$|(A_1 \cup \ldots \cup A_n) \cup A_{n+1}| = |A_1 \cup \ldots \cup A_n| + |A_{n+1}| - |B_1 \cup \ldots \cup B_n|.$$

Применив к этим объединениям предположение индукции получим искомые суммы. □

Упражнение 5.3. *Докажите формулу* (2).

Упражнение 5.4. *Сколько чисел в промежутке между 1 и 33000 включительно не делятся ни на 3, ни на 5?*

5.3. Сочетания и размещения

Определение 5.2. *Числом размещений из n по k* называется количество упорядоченных наборов из k различных элементов множества, состоящего из n элементов.

Обозначение. A_n^k.

Пример 5.5. В автопарке 10 различных автобусов. Сколькими способами можно составить колонну из 5 автобусов?

▶ На первое место можно поставить один из 10 автобусов, на второе — один из 9, далее — один из 8, 7, 6 соответственно. Итого по правилу произведения число способов составить колонну равно $A_{10}^5 = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 30240$. ◀

Утверждение 5.3. *Для всех $k, n \in \mathbb{N}$ при $n \geqslant k$ выполняется* $A_n^k = \dfrac{n!}{(n-k)!}$.

Доказательство. В качестве первого элемента можно выбрать один из n, в качестве второго — один из $(n-1)$, и так далее. В итоге по правилу произведения имеем

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

Требуемое доказано. □

Упражнение 5.5. *В клубе 20 спортсменов. Сколько существует способов построить 4 из них в одну шеренгу?*

Определение 5.4. *Числом сочетаний из n по k* называется количество k-элементных подмножеств множества, состоящего из n элементов.

Обозначение. C_n^k или $\binom{n}{k}$.

Пример 5.6. На курсе 15 человек умеют играть в футбол. Сколькими способами можно составить футбольную команду из 7 человек?

▶ Первого футболиста можно выбрать 15 способами, второго — 14, далее 13, 12, 11, 10, 9. Каждую комбинацию из 7 футболистов таким способом мы посчитали 7! раз (нет разницы, в каком порядке выбирать футболистов). Стало быть, число способов составить команду составляет $C_{15}^7 = (15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9)/7! = 585$.

Утверждение 5.5. *Для всех $k, n \in \mathbb{N}$ при $n \geqslant k$ выполняется* $C_n^k = \dfrac{n!}{k!(n-k)!}$.

Доказательство. Набор из k выбранных элементов можно упорядочить $k!$ способами. Поэтому $C_n^k \cdot k! = A_n^k$, то есть $C_n^k = \dfrac{n!}{k!(n-k)!}$. □

Упражнение 5.6. *В наборе 25 цветных карандашей. Сколькими способами можно выбрать 5 из них?*

Утверждение 5.6. *Для всех $k, n \in \mathbb{N}$ если $n \geqslant k$, то $C_n^k = C_n^{n-k}$.*

Доказательство. Неформально, выбрать k элементов из заданных n — это то же самое, что «не выбрать» оставшиеся $(n-k)$ элементов. С формальной точки зрения указанное равенство означает, что между k-элементными подмножествами и $(n-k)$-элементными подмножествами существует биекция. В самом деле, пусть множество X

из n элементов. Тогда множество $\Omega_k = \{Y \subset X \mid |Y| = k\}$ состоит из C_n^k элементов, а множество $\Omega_{n-k} = \{Z \subset X \mid |Z| = n-k\}$ состоит из C_n^{n-k} элементов. Установим биекцию $\Omega_k \to \Omega_{n-k}$, положив $Y \mapsto (X \setminus Y)$. □

Утверждение 5.7. *Для всех $k, n \in \mathbb{N}$ если $n \geqslant k$, то $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.*

Доказательство. Рассмотрим множество из $(n+1)$ элемента, один из которых является «особенным». По определению у этого множества C_{n+1}^{k+1} подмножеств, состоящих из $(k+1)$ элемента. Среди этих подмножеств C_n^{k+1} таких, в которых «особенного» элемента нет, и C_n^k таких, которые его содержат. Отсюда по правилу суммы $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$. □

Утверждение 5.8. *Для всех $k, m, n \in \mathbb{N}$ если $n \geqslant m \geqslant k$, то $C_n^m \cdot C_m^k = C_n^k \cdot C_{n-k}^{m-k}$.*

Доказательство. Оба произведения равны числу способов разбить n-элементное множество A на три подмножества A_1, A_2 и A_3 таких, что в первом $(n-m)$ элементов, во втором $(m-k)$ элементов, а в третьем k элементов. Разница лишь в том, что согласно левой части равенства мы сначала выделяем подмножество $A_2 \cup A_3$, а потом делим его на две части. Если же действовать в соответствии с правой частью равенства, нужно сначала выбрать A_3, а потом из оставшегося подмножества выделить A_2. □

Замечание. Утверждения 5.6, 5.7 и 5.8 можно было бы доказать непосредственным вычислением, используя явные формулы для чисел сочетаний, однако тогда от нас остался бы скрытым их комбинаторный смысл.

Утверждение 5.9. [Бином Ньютона] *Для любых $x, y \in \mathbb{R}$ и $n \in \mathbb{N}$ выполнено*

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k} = C_n^0 x^0 y^n + C_n^1 x^1 y^{n-1} + \ldots + C_n^{n-1} x^{n-1} y^1 + C_n^n x^n y^0.$$

Доказательство. Приведём два различных доказательства.

Комбинаторное. В разложении $(x+y)\cdot(x+y)\cdot\ldots\cdot(x+y)$ из каждой скобки выбирается x либо y. По определению моном, содержащий k иксов и $(n-k)$ игреков можно выбрать C_n^k способами, что и завершает доказательство.

По индукции. База $n = 1$ тривиальна. Индукционный переход: рассмотрим разложение $(x+y)^{n+1} = (x+y)^n(x+y)$ и применим к первому сомножителю предположение индукции:

$$(x+y)^{n+1} = \big(C_n^0 x^0 y^n + C_n^1 x^1 y^{n-1} + \ldots + C_n^{n-1} x^{n-1} y^1 + C_n^n x^n y^0\big)(x+y).$$

Заметим, что моном $x^{k+1}y^{n-k}$ можно получить двумя способами: как произведение $(x^k y^{n-k})x$ и как произведение $(x^{k+1}y^{n-k-1})y$. Поэтому коэффициент при этом мономе будет равен $C_n^k + C_n^{k+1}$. А согласно утверждению 5.7 это в точности C_{n+1}^{k+1}. □

Замечание. При $n = 2$ и $n = 3$ бином Ньютона превращается в хорошо известные из школьной алгебры формулы:

$$(x+y)^2 = x^2 + 2xy + y^2 \qquad \text{и} \qquad (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

5.4. Треугольник Паскаля и его свойства

Выпишем числа сочетаний в строчки следующим образом:

$$
\begin{array}{ccccccccccc}
 & & & & C_0^0 & & & & & & \\
 & & & C_1^0 & & C_1^1 & & & & & \\
 & & C_2^0 & & C_2^1 & & C_2^2 & & & & \\
 & C_3^0 & & C_3^1 & & C_3^2 & & C_3^3 & & & \\
C_4^0 & & C_4^1 & & C_4^2 & & C_4^3 & & C_4^4 & & \\
C_5^0 & & C_5^1 & & C_5^2 & & C_5^3 & & C_5^4 & & C_5^5
\end{array}
$$

$$
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Полученная таблица называется *треугольником Паскаля*. На её краях находятся единицы, а внутри таблицы каждое число равно сумме двух чисел, стоящих слева и справа над ним. Последнее следует из равенства $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

Замечание. Можно, наоборот, определить треугольник Паскаля как числовую таблицу треугольного вида, по бокам которой стоят единицы, а каждое из остальных чисел равно сумме двух чисел, расположенных над ним. В таком случае тот факт, что k-е число в n-й строке равно C_n^k, будет уже свойством, доказываемым по индукции. При этом мы подразумеваем, что нумерация строк начинается с нуля.

Утверждение 5.10. *Сумма чисел n-й строки треугольника Паскаля равна 2^n. Иными словами, для каждого $n \in \mathbb{N}$ выполнено $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n$.*

Доказательство. Приведём два различных доказательства.

Комбинаторное. Пусть X — множество, состоящее из n элементов. Так как C_n^k есть число его подмножеств, состоящих из k элементов, то сумма $C_n^0+C_n^1+C_n^2+\ldots+C_n^n$ равна общему количеству подмножеств множества X. С другой стороны, выбор подмножества определяется тем, включаем ли мы в него каждый конкретный элемент. Поскольку возможностей всего две (либо включаем, либо не включаем), а элементов n, по правилу произведения всего вариантов 2^n.

С помощью бинома Ньютона. Подставляя в бином $x = y = 1$, имеем

$$2^n = (1+1)^n = C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n,$$

что и требовалось доказать. □

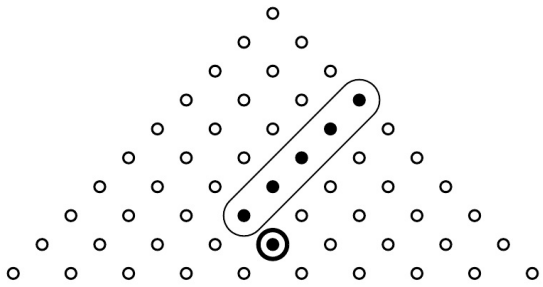
Упражнение 5.7. *Убедитесь, что утверждение 5.10 справедливо, воспользовавшись математической индукцией.*

Упражнение 5.8. *Докажите, что* $C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n = 0$ *для любого* $n \in \mathbb{N}$,

а) при помощи бинома Ньютона;

б) воспользовавшись математической индукцией.

Утверждение 5.11. *Для любых* $k, m \in \mathbb{N}$ *выполнено* $C_k^k + C_{k+1}^k + \ldots + C_{k+m}^k = C_{k+m+1}^{k+1}$.



Доказательство. Заметим, что сумма, стоящая в левой части равенства, представляет собой сумму чисел на диагонали треугольника Паскаля (см. рисунок). Поскольку имеет место равенство $C_k^k = C_{k+1}^{k+1} = 1$, верхнее число в диагонали можно заменить на число, стоящее под ним справа. После такой замены в строчке ниже возникнет два соседних числа, сумма которых по свойству треугольника Паскаля равна числу, стоящему под ними. Продолжая этот процесс и далее, после m операций получим в точности C_{k+m+1}^{k+1} (число, отмеченное на рисунке кружочком). □

Упражнение 5.9. *а) Проведите формальное доказательство утверждения 5.11 с помощью математической индукции.*

б) Какому равенству будет соответствовать картинка, полученная из рисунка выше отражением относительно его оси симметрии?

5.5. Метод перегородок

Утверждение 5.12. *Пусть* $k, m \in \mathbb{N}$, *причём* $m \geqslant k$. *Число способов разложить* m *одинаковых предметов по* k *упорядоченным* **непустым** *кучкам равно* C_{m-1}^{k-1}.

Доказательство. Если мы выложим предметы в ряд, между ними будет $(m-1)$ промежуток:

∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘

Идея заключается в том, чтобы поставить в эти промежутки $(k-1)$ **перегородку** (не более одной перегородки на промежуток). Тогда предметы, лежащие в начале ряда (до первой перегородки) образуют первую кучку, предметы между первой и второй перегородки составляют вторую кучку и так далее. Словом, из $(m-1)$ слота необходимо выбрать $(k-1)$, куда мы поставим перегородки, а это можно сделать C_{m-1}^{k-1} способами. □

Утверждение 5.13. *Пусть $k, m \in \mathbb{N}$. Число способов разложить m одинаковых предметов по k упорядоченным,* **возможно, пустым,** *кучкам равно C_{m+k-1}^{k-1}.*

Доказательство. Приведём два слегка различных доказательства.

Первое. Сведём решение к утверждению 5.12. Для этого в каждую из рассматриваемых кучек добавим по предмету. Таким образом, исходная задача (распределить m предметов по k кучкам, некоторые из которых, возможно, пустые) равносильна распределению $(m+k)$ предметов по k непустым кучкам. А для последней задачи ответ мы уже знаем.

Второе. Как и при доказательстве утверждения 5.12 выложим предметы в ряд и расставим между ними $(k-1)$ перегородку. Однако теперь в один промежуток допустимо поставить две и более перегородок: это будет означать, что соответствующие кучки пусты. Кроме того, можно поставить перегородку в начало или в конец ряда, чтобы с одного краю от неё предметов вообще не было — это будет означать, что первая или последняя кучка пуста. Таким образом, исходная задача сводится к тому, чтобы разложить m предметов и $(k-1)$ перегородку в ряд (и предметы, и перегородки неразличимы между собой). Иными словами, из $(m+k-1)$ мест в ряду нужно выбрать $(k-1)$ место, куда мы положим перегородки, а остальные места заполнить предметами. Ясно, что число способов сделать это равно C_{m+k-1}^{k-1}. □

Пример 5.7. Сколько решений имеет уравнение $x_1 + x_2 + x_3 + ... + x_{10} = 5$ в неотрицательных целых числах?

▶ Каждая переменная x_k может принимать значения от 0 до 5. Возьмём 5 шаров и посчитаем число способов расставить 9 перегородок. Ясно, что таким образом мы получим количество решений искомого уравнения. Имеем 14 позиций, в каждой из которых стоит либо шар, либо перегородка. Число способов разложить 5 шаров по 14 позициям равно $C_{14}^5 = 2002$ (перегородки встанут на оставшиеся позиции). ◀

Упражнение 5.10. *В школьной столовой есть 4 вида пирожков. Сколькими способами можно купить 10 пирожков?*

Упражнение 5.11. [Сочетания с повторениями] *Пусть $k, n \in \mathbb{N}$. Докажите, что*

а) количество упорядоченных наборов из k (возможно, совпадающих) элементов, выбранных из n-элементного множества, равно n^k;

б) количество неупорядоченных наборов из k (возможно, совпадающих) элементов, выбранных из n-элементного множества, равно C_{n+k-1}^k.

5.6. Литература для дальнейшего изучения

• *Виленкин Н.Я.*, Комбинаторика — Москва, Наука, 1969.

• *Заславский А.А., Пермяков Д.А., Скопенков А.Б., Скопенков М.Б., Шаповалов А.В.*, Математика в задачах. — Москва, МЦНМО, 2009.

Комбинаторика

Задачи семинаров

5.1. Основные задачи

Задача 5.1. Пусть $n = p_1^{\alpha_1} \cdot \ldots \cdot p_l^{\alpha_l}$ — разложение числа n на простые множители. Докажите, что n имеет ровно $(\alpha_1 + 1) \cdot \ldots \cdot (\alpha_l + 1)$ различных натуральных делителей (считая тривиальные 1 и n).

Задача 5.2. а) В заборе 20 досок, каждую из которых Том Сойер собирается покрасить в синий, зелёный или жёлтый цвет, причём соседние доски красятся в разные цвета. Сколькими способами это можно сделать?

б) А если требуется ещё, чтобы хоть одна из досок обязательно была синей?

Задача 5.3. Сколькими способами можно разложить 17 одинаковых шариков по 9 пронумерованным ящикам, если

а) в каждом ящике должно быть хотя бы по одному шарику;

б) некоторые ящики могут быть пустыми?

Задача 5.4. Из 12 девушек и 10 юношей выбирают команду в составе 5 человек. Сколькими способами можно выбрать эту команду так, чтобы в неё вошло не более 3 юношей?

Задача 5.5. Пусть $A = \{1, 2, \ldots, m\}$, а $B = \{1, 2, \ldots, n\}$.

а) Сколько существует отображений из A в B?

б) Сколько среди них инъекций?

в) Сколько среди них сюрьекций?

г) Сколько среди них биекций?

д) Сколько среди них возрастающих отображений?

е) Сколько среди них неубывающих отображений?

Задача 5.6. В выражении $(x + y + z)^n$ раскрытили скобки и привели подобные.

а) Сколько получилось различных слагаемых?

б) Чему равен коэффициент при $x^k y^l z^m$?

Задача 5.7. На столе площади 1 лежит три журнала, площадь каждого из которых не меньше $1/2$. Среди их попарных пересечений рассмотрим наибольшее по площади. Какую наименьшую площадь оно может иметь?

Задача 5.8. а) В каких строках треугольника Паскаля все числа будут нечётными?

б) В каких строках все числа, кроме единиц по бокам, будут чётными?

Задача 5.9. Каждая сторона квадрата разбита на n частей. Сколько можно построить треугольников с вершинами в точках деления (не включая вершины квадрата)?

Задача 5.10. Имеется 6 красок. Сколькими способами можно раскрасить ими грани кубика так, чтобы все цвета присутствовали? Способы, отличающиеся вращениями кубика, считаются одинаковыми.

Задача 5.11. Пусть есть n шариков разных цветов. Сколько можно собрать наборов из нечётного числа шариков?

5.2. Дополнительные задачи

Задача 5.12. Меню в школьной столовой постоянно и состоит из n различных блюд. Петя хочет каждый день выбирать себе завтрак по-новому (за один раз он может съесть от 0 до n разных блюд).

а) Сколько дней ему удастся это делать?

б) Сколько блюд он съест за это время?

Вася решил последовать примеру Пети, но съедать каждый день нечётное число блюд.

в) Сколько дней ему удастся это делать?

г) Сколько блюд Вася съест за это время?

Задача 5.13. Пусть $m, n, s \in \mathbb{N}$, причём $s \leqslant m + n$. Докажите, что:

а) $C_m^0 C_n^s + C_m^1 C_n^{s-1} + C_m^2 C_n^{s-2} + \ldots + C_m^s C_n^0 = C_{n+m}^s$.

б) $(C_n^0)^2 + (C_n^1)^2 + (C_n^2)^2 + \ldots + (C_n^n)^2 = C_{2n}^n$.

в) $C_n^1 + 2C_n^2 + \ldots + nC_n^n = n \cdot 2^{n-1}$.

Каков комбинаторный смысл каждого из указанных равенств?

Задача 5.14. Имеется 4 чашки с разными рисунками, 4 одинаковых стакана, 10 одинаковых кусков сахара и 10 соломинок разного цвета. Сколькими способами можно разложить

а) сахар по чашкам;

б) сахар по чашкам;

в) соломинки по чашкам;

г) соломинки по стаканам?

Задача 5.15. а) Докажите, что любое число, кроме единицы, встречается в треугольнике Паскаля конечное число раз.

б) Пусть $n < 2^k$. Докажите, что число n встречается в треугольнике Паскаля не более, чем $2k - 2$ раз.

Задача 5.16. В каких строках треугольника Паскаля все числа, кроме единиц, будут кратны данному простому числу p?

Задача 5.17. По пустыне шёл караван из 9 верблюдов. В какой-то момент каждому из них надоело видеть перед собой одного и того же верблюда. Сколькими способами можно переставить верблюдов так, чтобы теперь перед каждым верблюдом шёл не тот, что раньше?

Задача 5.18. Сколько существует десятизначных чисел, все цифры которых различны и которые делятся на 11111?

Многочлены

Теоретический материал

6.1. Основные определения и свойства

Многочлены в том или ином виде, скорее всего, знакомы читателю со школы. Мы, однако, определим их немного непривычным образом.

• *Многочленом* от переменной x с коэффициентами в множестве $\mathbb{K}$ называется *формальное выражение* вида

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \qquad \text{где } a_k \in \mathbb{K}.$$

В качестве $\mathbb{K}$ мы будем рассматривать $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$ — множества рациональных, действительных и комплексных чисел. Если читатель ещё не знаком с комплексными числами, он может смело игнорировать результаты, которые их используют, и вернуться к ним после освоения главы Комплексные числа.

• Множество многочленов с коэффициентами в множестве $\mathbb{K}$ обозначается $\mathbb{K}[x]$.

• Каждый многочлен $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{K}$ задаёт функцию $f : \mathbb{K} \to \mathbb{K}$, определенную правилом

$$\lambda \mapsto f(\lambda) = a_n \lambda^n + a_{n-1} \lambda^{n-1} + \ldots + a_1 \lambda + a_0.$$

Это дает ещё один, более привычный, способ думать о многочленах. Мы будем смотреть на многочлены как на формальные выражения или как на функции в зависимости от того, какой взгляд удобнее в конкретной ситуации.

• *Нулевой многочлен* на языке формальных выражений — это многочлен, все коэффициенты которого равны нулю. На языке функций — это тождественно равная нулю фунция, то есть такая функция $f(x) \in \mathbb{K}[x]$, что $f(\lambda) = 0$ для любого $\lambda \in \mathbb{K}$. Позже, в разделе 6.5, мы убедимся, что тождественно равная нулю функция может быть реализована только многочленом, все коэффициенты которого равны нулю.

• Каждое слагаемое вида $a_k x^k$, входящее в многочлен, при ненулевом a_k называется *одночленом* или *мономом*. Число k называется *степенью* монома.

• *Степенью многочлена* $f(x) \in \mathbb{K}[x]$ называется максимальная из степеней входящих в него одночленов. Степень нулевого многочлена *не определена*.

• Степень многочлена $f(x)$ обозначается $\deg f(x)$.

Пример 6.1. Многочлен $3x^5 + 8x + 1$ имеет степень 5, а многочлен $x^2 - 2x + 1$ имеет степень 2.

Упражнение 6.1. *Докажите, что* $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$ *для любых ненулевых* $f(x), g(x) \in \mathbb{K}[x]$.

Упражнение 6.2. *Докажите, что* $\deg(f(x) + g(x)) \leqslant \max(\deg f(x), \deg g(x))$ *для любых ненулевых* $f(x), g(x) \in \mathbb{K}[x]$ *(сумму тоже считаем ненулевой).*

Упражнение 6.3. *Докажите, что если $f(x)\cdot g(x)=0$, то либо $f(x)=0$, либо $g(x)=0$. Под равенством нулю здесь понимается равенство нулевому многочлену!*

Следует отметить, что $\mathbb{K}\subset\mathbb{K}[x]$, а именно, подмножество многочленов нулевой степени — это как раз и есть $\mathbb{K}$ (с естественной оговоркой, что нулевой многочлен соответствует нулю). Действительно, любой многочлен нулевой степени $f(x)\in\mathbb{K}$ имеет вид $f(x)=a$, где $a\in\mathbb{K}$, все остальные его коэффициенты равны нулю.

• Число λ называется *корнем* многочлена $f(x)\in\mathbb{K}[x]$, если $f(\lambda)=0$. Вообще говоря, λ может не лежать в $\mathbb{K}$.

Пример 6.2. Корень многочлена $(x^2-2)\in\mathbb{Q}[x]$ не лежит в $\mathbb{Q}$.

• Говорят, что многочлен $f(x)\in\mathbb{K}[x]$ *делится* на многочлен $g(x)\in\mathbb{K}[x]$, и пишут $f(x)\vdots g(x)$, если существует многочлен $h(x)\in\mathbb{K}[x]$ такой, что $f(x)=g(x)\cdot h(x)$. Про многочлен $g(x)$ в таком случае говорят, что он *делит* $f(x)$, и пишут $g(x)\mid f(x)$.

Пример 6.3. $(x^3-1)\in\mathbb{Q}[x]$ делится на $(x-1)$. И правда, $x^3-1=(x-1)(x^2+x+1)$.

• Многочлен $f(x)$ степени $n>0$ называется *приводимым*, если он имеет делитель степени k, где $0<k<n$. В противном случае $f(x)$ называется *неприводимым*.

6.2. Деление с остатком

Говорят, что многочлен $f(x)\in\mathbb{K}[x]$ *делится с остатком* на многочлен $g(x)\in\mathbb{K}[x]$, если существуют многочлены $q(x),r(x)\in\mathbb{K}[x]$ такие, что

$$f(x)=q(x)\cdot g(x)+r(x)\qquad\text{причём}\qquad r(x)=0\ \text{ или }\ \deg r(x)<\deg g(x).$$

Многочлен $q(x)$ называется *неполным частным*, а многочлен $r(x)$ — *остатком* при делении $f(x)$ на $g(x)$.

Пример 6.4. Многочлен x^3+x+1 делится на одночлен x^2 с остатком $x+1$. Действительно, $x^3+x+1=x\cdot x^2+(x+1)$ и $\deg(x+1)=1<2=\deg(x^2)$.

Теорема 6.1. *Пусть $f(x)$ и $g(x)\neq 0$ — многочлены с коэффициентами в $\mathbb{K}$. Тогда существует единственная пара многочленов $q(x),r(x)\in\mathbb{K}[x]$ такая, что*

$$f(x)=q(x)\cdot g(x)+r(x),\qquad\textit{где}\qquad r(x)=0\ \textit{ или }\ \deg r(x)<\deg g(x).$$

Доказательство. Начнем с проверки единственности. Допустим, существует две пары многочленов $(q_1(x),r_1(x))$ и $(q_2(x),r_2(x))$ с коэффициентами в $\mathbb{K}$, удовлетворяющих условиям теоремы, то есть

$$f(x)=q_1(x)\cdot g(x)+r_1(x),\qquad r_1(x)=0\ \text{ или }\ \deg r_1(x)<\deg g(x).$$

$$f(x)=q_2(x)\cdot g(x)+r_2(x),\qquad r_2(x)=0\ \text{ или }\ \deg r_2(x)<\deg g(x).$$

Тогда

$$q_1(x)g(x)+r_1(x)=q_2(x)g(x)+r_2(x)\qquad\Longrightarrow\qquad(q_1(x)-q_2(x))g(x)=r_2(x)-r_1(x).$$

Заметим, что, с одной стороны

$$\big(r_2(x) - r_1(x)\big) \vdots g(x),$$

а с другой стороны,

$$r_2(x) - r_1(x) = 0 \qquad \text{или} \qquad \deg(r_2(x) - r_1(x)) < \deg g(x).$$

Согласно упражнениям 6.1 и 6.2 вторая возможность не реализуется. Таким образом, $r_2(x) - r_1(x) = 0$, а значит, и $g(x)(q_1(x) - q_2(x)) = 0$. Поскольку $g(x) \neq 0$, согласно упражнению 6.3 имеем $q_1(x) = q_2(x)$, что и хотелось доказать.

Перейдём к существованию неполного частного и остатка. Докажем его индукцией по степени многочлена $f(x)$. Введём обозначения:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots a_0 \qquad \text{и} \qquad g(x) = b_m x^m + b_{m-1}x^{m-1} + \dots + b_0 \neq 0.$$

Можно считать, что $\deg g(x) > 0$, поскольку на любые многочлены степени 0 можно делить с нулевым остатком. База индукции тогда очевидна: для любого многочлена $f(x)$ степени 0, то есть для $f(x) = a$, где $a \in \mathbb{K}$, имеет место равенство

$$f(x) = 0 \cdot g(x) + f(x), \qquad \deg f(x) = 0 < \deg g(x).$$

Это же равенство справедливо и в более общем случае $\deg g(x) = m > n = \deg f(x)$, поэтому в дальнейшем будем считать, что $m \leqslant n$. Шаг индукции: предположим, что любой многочлен степени меньше n можно разделить на произвольный ненулевой многочлен $g(x)$ с остатком. Рассмотрим многочлен

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x).$$

Он имеет степень, строго меньшую n, так что по предположению индукции

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = q_1(x)g(x) + r_1(x), \qquad \text{где} \qquad r_1(x) = 0 \ \text{ или } \ \deg r_1(x) < \deg g(x).$$

Отсюда получаем разложение

$$f(x) = \left(\frac{a_n}{b_m} x^{n-m} + q_1(x)\right) g(x) + r_1(x) \qquad \text{где} \qquad r_1(x) = 0 \ \text{ или } \ \deg r_1(x) < \deg g(x),$$

что и требовалось. □

Замечание. Для поиска неполного частного и остатка используется классический метод деления многочленов «столбиком».

Упражнение 6.4. *Поделите с остатком*

а) $x^2 - 4x + 3$ *на* $x - 3$*;*

б) $x^2 - 4$ *на* $x - 5$*;*

в) $x^4 - 2x + 5$ *на* $x^2 + 1$*,*

рассматривая все многочлены как элементы $\mathbb{Q}[x]$*.*

6.3. НОД и его линейное представление

• Многочлен $h(x) \in \mathbb{K}[x]$ называется *общим делителем* двух данных многочленов $f(x),\ g(x) \in \mathbb{K}[x]$, если $h(x) \mid f(x)$ и $h(x) \mid g(x)$. Ясно, что любые два многочлена имеют хотя бы один общий делитель — постоянный многочлен 1.

• *Наибольшим общим делителем* (НОД) многочленов $f(x),\ g(x) \in \mathbb{K}[x]$ называется их общий делитель, имеющий наибольшую степень. Для НОД многочленов применяют те же обозначения, что и для целых чисел:

$$d(x) = \text{НОД}(f(x), g(x)) \qquad \text{или просто} \qquad d(x) = (f(x), g(x)).$$

• Если $(f(x), g(x)) = 1$, то $f(x)$ и $g(x)$ называются *взаимно простыми.*

Замечание. В отличие от целых чисел, НОД многочленов определён неоднозначно. Действительно, пусть $d(x) = (f(x), g(x))$. Тогда для любого ненулевого $\lambda \in \mathbb{K} \setminus \{0\}$ многочлен $\lambda d(x)$ — тоже наибольший общий делитель многочленов $f(x)$ и $g(x)$, поскольку домножение на константу (многочлен нулевой степени) не меняет степень.

Упражнение 6.5. *Докажите, что если $f(x), g(x) \in \mathbb{K}$ — два многочлена, не равных нулю одновременно, то их наибольший общий делитель определён корректно (хотя и не однозначно).*

• Многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ называется *приведённым*, если $a_n = 1$.

Пример 6.5. $x^3 + 6x + 1$ — приведённый многочлен, а $5x^3 + 6x - 1$ — нет.

Пусть $d(x) = (f(x), g(x))$, где $f(x), g(x) \in \mathbb{K}[x]$. Тогда существует такое число α, что $\alpha d(x)$ — приведённый многочлен. В дальнейшем, если не оговорено противное, мы для определённости будем считать НОД приведённым.

Оказывается, что, как и в случае целых чисел, наибольший общий делитель $d(x)$ многочленов ($f(x)$ и $g(x)$) представляется в виде

$$d(x) = a(x)f(x) + b(x)g(x)$$

для некоторых $a(x), b(x) \in \mathbb{K}[x]$. Объяснение этого факта будет проведено в духе раздела 4.4. Для начала, введём следующие обозначения:

$$\mathbb{K}(d(x)) = \{a(x)d(x) \mid a(x) \in \mathbb{K}[x]\}$$

$$\mathbb{K}(f(x), g(x)) = \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in \mathbb{K}[x]\}.$$

Иными словами, $\mathbb{K}(d(x))$ — это множество всех многочленов, которые делятся на $d(x)$, а $\mathbb{K}(f(x), g(x))$ — множество многочленов, представимых в виде *линейной комбинации* многочленов $f(x)$ и $g(x)$.

Упражнение 6.6. *Пусть $f(x), g(x) \in \mathbb{K}[x]$. Докажите, что*

а) $0, f(x), g(x) \in \mathbb{K}(f(x), g(x))$;

б) если, $u(x), v(x) \in \mathbb{K}(f(x), g(x))$, то $\big(u(x) \pm g(x)\big) \in \mathbb{K}(f(x), g(x))$;

в) если $h(x) \in \mathbb{K}(f(x), g(x))$, то $s(x)h(x) \in \mathbb{K}(f(x), g(x))$ для любого $s(x) \in \mathbb{K}[x]$.

Теорема 6.2. *Пусть $f(x), g(x) \in \mathbb{K}$ — два многочлена, не равных нулю одновременно, а $d(x)$ их наибольший общий делитель. Тогда $\mathbb{K}(f(x), g(x)) = \mathbb{K}(d(x))$.*

Доказательство. Как и для целых чисел, очевидно, что $\mathbb{K}(f(x), g(x)) \subset \mathbb{K}(d(x))$, поэтому нужно доказать лишь обратное включение. Для этого в множестве $\mathbb{K}(f(x), g(x))$ рассмотрим приведённый многочлен $t(x)$ минимальной степени. Покажем, что любой многочлен $h(x) \in \mathbb{K}(f(x), g(x))$ делится на $t(x)$. Действительно, в противном случае при делении $h(x)$ на $t(x)$ возникнет ненулевой остаток:

$$h(x) = q(x)t(x) + r(x), \qquad \deg r(x) < \deg t(x).$$

Но тогда $r(x) = h(x) - q(x)t(x)$, а значит, согласно упражнению 6.6, $r(x)$ является элементом множества $\mathbb{K}(f(x), g(x))$. Поскольку $t(x)$ — многочлен минимальной степени в $\mathbb{K}(f(x), g(x))$, отсюда мы заключаем, что $r(x) = 0$. В частности, подставив вместо $h(x)$ многочлены $f(x)$ и $g(x)$, можно сделать вывод, что $t(x)$ является их общим делителем.

Из включения $\mathbb{K}(f(x), g(x)) \subset \mathbb{K}(d(x))$ следует, что $t(x) \vdots d(x)$, откуда вытекает неравенство $\deg t(x) \geqslant \deg d(x)$. С другой стороны, $t(x)$ — общий делитель многочленов $f(x)$ и $g(x)$, а $d(x)$ — их наибольший общий делитель, поэтому $\deg d(x) \geqslant \deg t(x)$. Как следствие, имеем $\deg d(x) = \deg t(x)$. Значит, многочлены $d(x)$ и $t(x)$ совпадают с точностью до коэффициента (они одинаковой степени и один делит другой). Но оба многочлена выбирались приведёнными, поэтому они совпадают. □

Следствие 6.3. *Любой общий делитель многочленов $f(x)$ и $g(x)$ с коэффициентами в $\mathbb{K}$ делит их наибольший общий делитель $d(x) = (f(x), g(x))$.*

Доказательство. Очевидно из существования представления $d(x)$ в виде линейной комбинации многочленов $f(x)$ и $g(x)$. □

Следствие 6.3 позволяет дать альтернативную характеризацию НОДа: это тот из общих делителей данных многочленов, который делится на любой их общий делитель.

6.4. Алгоритм Евклида

Алгоритм Евклида переносится с целых чисел на многочлены с коэффициентами в $\mathbb{K}$ почти без изменений.

Лемма 6.4. *Пусть $f(x), g(x) \in \mathbb{K}[x]$, причём $g(x) \neq 0$. Тогда $(f(x), g(x)) = (g(x), r(x))$, где $r(x)$ — остаток от деления $f(x)$ на $g(x)$.*

Доказательство. Положим $d(x) = (f(x), g(x))$ и $d_1(x) = (g(x), r(x))$. С одной стороны,

$$d(x) \mid (f(x) - q(x)g(x)) = r(x),$$

поэтому $d(x)$ — общий делитель $g(x)$ и $r(x)$. Значит, $d(x) \mid d_1(x)$ согласно следствию 6.3. С другой стороны,

$$d_1(x) \mid f(x) = q(x)g(x) + r(x),$$

поэтому $d_1(x)$ — общий делитель $f(x)$ и $g(x)$, так что $d_1(x) \mid d(x)$ по тем же соображениям. Таким образом, $d_1(x) = d(x)$. □

Благодаря лемме 6.4 можно утверждать, что наибольший общий делитель многочленов $f(x)$ и $g(x)$ может быть найден при помощи *алгоритма Евклида*, заключающегося в выполнении следующей последовательности шагов:

$$\begin{aligned} f(x) &= q_0(x)g(x) + r_0(x) && \text{нулевой шаг} \\ g(x) &= q_1(x)r_0(x) + r_1(x) && \text{первый шаг} \\ &\dots \\ r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x) && n\text{-й шаг} \\ r_{n-1}(x) &= q_{n+1}(x)r_n(x) && (n+1)\text{-й шаг} \end{aligned}$$

Здесь $r_n(x)$ — последний ненулевой остаток, существование которого гарантируется тем фактом, что степень остатка на каждом шаге понижается.

Упражнение 6.7. *Убедитесь в том, что* $(f(x), g(x)) = r_n(x)$.

Утверждение 6.5. *Пусть* $f(x), g(x), h(x) \in \mathbb{K}[x]$ *— многочлены, для которых выполнено* $(f(x), h(x)) = 1$ *и* $f(x)g(x) \vdots h(x)$. *Тогда* $g(x) \vdots h(x)$.

Упражнение 6.8. *Докажите предложение 6.5.*

Утверждение 6.6. *Пусть* $f(x), g(x), h(x) \in \mathbb{K}$, *причём* $h(x)$ *неприводим. Тогда из условия* $f(x)g(x) \vdots h(x)$ *следует, что* $f(x) \vdots h(x)$ *или* $g(x) \vdots h(x)$.

Доказательство. Так как $h(x)$ неприводим, то либо $f(x) \vdots h(x)$, либо $(f(x), h(x)) = 1$. В первом случае всё доказано, а во втором по утверждению 6.5 имеем $g(x) \vdots h(x)$. □

Упражнение 6.9. *Пусть* $f_1(x), \dots, f_n(x), h(x) \in \mathbb{K}[x]$, *причём* $h(x)$ *неприводим. Тогда из* $\big(f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_n(x)\big) \vdots h(x)$ *следует, что* $f_k(x) \vdots h(x)$ *для некоторого* k.

6.5. Корни многочленов и основная теорема алгебры

Этот раздел посвящен доказательству нескольких фундаментальных результатов. Кроме того, мы без доказательства дадим описание неприводимых многочленов с коэффициентами в $\mathbb{R}$ и $\mathbb{C}$.

Теорема 6.7. [Теорема Безу] *Число* $\lambda \in \mathbb{K}$ *является корнем многочлена* $f(x) \in \mathbb{K}[x]$, *если и только если* $f(x) \vdots (x - \lambda)$.

Доказательство. Если $f(x) \vdots (x - \lambda)$, то $f(x) = q(x)(x - \lambda)$ для некоторого $q(x) \in \mathbb{K}$, откуда $f(\lambda) = 0$.

Обратно, пусть $f(\lambda) = 0$. Поделив $f(x)$ с остатком на $(x - \lambda)$, получим

$$f(x) = q(x)(x - \lambda) + r(x), \qquad \text{где} \qquad r(x) = 0 \ \text{ или } \ \deg r(x) < \deg(x - \lambda).$$

Поскольку $\deg(x-\lambda) = 1$, степень остатка должна равняться нулю, то есть $r(x) = a \in \mathbb{K}$. Поэтому $0 = f(\lambda) = q(\lambda) \cdot 0 + r(\lambda) = a$, откуда $r(x) = 0$, что и требовалось. □

Утверждение 6.8. [Формулы Виета] *Пусть многочлен* $x^2 + bx + c \in \mathbb{K}[x]$ *имеет корень* $\lambda \in \mathbb{K}$. *Тогда существует такое число* $\mu \in \mathbb{K}$, *для которого*

$$x^2 + bx + c = (x - \lambda)(x - \mu),$$

причём, $\lambda + \mu = -b$ и $\lambda\mu = c$.

Упражнение 6.10. *Докажите утверждение 6.8.*

Утверждение 6.9. *Количество корней многочлена не превосходит его степени.*

Упражнение 6.11. *а) Докажите, утверждение 6.9.*

б) Убедитесь, что если многочлен тождественно равен нулю как функция, то все его коэффициенты равны нулю.

Теорема 6.10. *Многочлен с коэффициентами в $\mathbb{K}$ единственным образом (с точностью до перестановки и домножения на элементы из $\mathbb{K}$) представляется в виде произведения неприводимых сомножителей.*

Доказательство. Сначала убедимся в существовании разложения. Будем вести индукцию по степени многочлена $n = \deg f(x)$. База индукции справедлива: любой многочлен степени 0 или 1 неприводим. Шаг индукции: если многочлен $f(x) \in \mathbb{K}[x]$ неприводим, то доказывать нечего. В противном случае $f(x) = u(x)v(x)$, причём степени многочленов $u(x)$ и $v(x)$ строго меньше степени $f(x)$, а значит, $u(x)$ и $v(x)$ раскладываются на неприводимые.

Для доказательства единственности предположим, что существует два разложения

$$p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_l(x),$$

где все $p_i(x), q_j(x)$ неприводимы. Без ограничения общности можно считать, что никакие $p_i(x)$ не совпадают с $q_j(x)$ (в противном случае просто сократим на них). Тогда согласно упражнению 6.9 каждый $p_i(x)$ делит некоторый $q_j(x)$, откуда в силу неприводимости последних следует, что они отличаются друг от друга умножением на константу. Теорема доказана. □

Конкретный вид неприводимых многочленов в $\mathbb{K}[x]$ существенно зависит от $\mathbb{K}$.

Пример 6.6. Многочлен $(x^2 - 2)$ неприводим, если рассматривать его как элемент множества $\mathbb{Q}[x]$. Действительно, если бы он был приводим, то раскладывался бы в произведение двух многочленов первой степени (возможно, одинаковых), то есть согласно теореме Безу имел бы корень. Однако, уравнение $x^2 = 2$ не имеет рациональных решений, поскольку $\sqrt{2}$ — иррациональное число.

Тот же самый многочлен, рассматриваемый как элемент множества $\mathbb{R}[x]$, приводим: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Пример 6.7. Многочлен $(x^2 + 1) \in \mathbb{R}[x]$ неприводим, но он становится приводимым, если рассматривать его как элемент $\mathbb{C}[x]$: именно, $x^2 + 1 = (x - i)(x + i)$.

Упражнение 6.12. *Найдите разложение многочлена $f(x) = (x^4 - 4)$ на неприводимые сомножители, рассматривая $f(x)$*

а) как элемент множества $\mathbb{Q}[x]$;

б) как элемент множества $\mathbb{R}[x]$;

в) как элемент множества $\mathbb{C}[x]$.

Приведём формулировку важнейшей теоремы, набросок доказательства которой будет приведён в разделе 10.6.

Теорема 6.11. [Основная теорема алгебры]
Любой многочлен $f(x) \in \mathbb{C}[x]$ представляется в виде

$$f(x) = a(x - \lambda_1) \cdot \ldots \cdot (x - \lambda_n),$$

где $n = \deg f(x)$, $a \in \mathbb{C}$, а среди корней $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ могут быть совпадающие. В частности, неприводимые многочлены с коэффициентами в $\mathbb{C}$ имеют степень 1.

Приведём также без доказательства теорему о классификации неприводимых многочленов с действительными коэффициентами.

Теорема 6.12. *Любой многочлен $f(x) \in \mathbb{R}[x]$ представляется в виде*

$$f(x) = a(x^2 + b_1 x + c_1) \cdot \ldots \cdot (x^2 + b_k x + c_k) \cdot (x - \lambda_1) \cdot \ldots \cdot (x - \lambda_m),$$

где $a, b_i, c_i, \lambda_j \in \mathbb{R}$, а дискриминанты всех квадратичных многочленов отрицательны.

Многочлены

Задачи семинаров

Задача 6.1. Пусть $f(x) \in \mathbb{R}[x]$, $\deg f(x) = 3$.

а) Может ли $f(x)$ не иметь корней в $\mathbb{R}$?

б) Может ли $f(x)$ иметь ровно один корень в $\mathbb{R}$?

в) Может ли $f(x)$ иметь ровно два корня в $\mathbb{R}$?

Задача 6.2. Обобщите формулы Виета на случай многочленов $f(x) \in \mathbb{K}[x]$, обладающих корнями $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$ и удовлетворяющих условию $\deg f(x) = 3$.

Задача 6.3. Докажите, что корни квадратного трёхчлена $(ax^2 + bx + c) \in \mathbb{R}[x]$ при $a \neq 0$ и $b^2 \geqslant 4ac$ могут быть найдены по хорошо известным из школы формулам

$$\lambda_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \qquad \lambda_2 \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Указание: Выделите полный квадрат.

Задача 6.4. Пусть λ_1 и λ_2 — корни квадратного трёхчлена $x^2 + bx + c \in \mathbb{K}[x]$. Докажите, что его дискриминант равен $(\lambda_1 - \lambda_2)^2$.

Задача 6.5. Найдите значение параметра q, если известно, что

а) корни λ_1, λ_2 многочлена $x^2 - 6x + q$ удовлетворяют соотношению $3\lambda_1 + 2\lambda_2 = 4$;

б) многочлен $x^2 + qx + 25$ имеет кратный корень.

Задача 6.6. а) Число $(1 + \sqrt{2})$ — корень некоторого приведенного многочлена второй степени с целыми коэффициентами. Найдите этот многочлен и его второй корень.

б) Число $(3 + \sqrt{5})$ — корень некоторого приведенного многочлена второй степени с целыми коэффициентами. Найдите этот многочлен и его второй корень.

в) Число $(2 - \sqrt{3})$ — корень некоторого приведенного многочлена второй степени с целыми коэффициентами. Найдите этот многочлен и его второй корень.

г) Число $(1 + \sqrt{7})$ — корень некоторого приведенного многочлена второй степени с целыми коэффициентами. Найдите этот многочлен и его второй корень.

д) Число $(4 - \sqrt{3})$ — корень некоторого приведенного многочлена второй степени с целыми коэффициентами. Найдите этот многочлен и его второй корень.

Задача 6.7. Пусть $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ — приведённый многочлен. Докажите, что если $\lambda \in \mathbb{Q}$ является корнем $f(x)$ как многочлена из $\mathbb{Q}[x]$, то $\lambda \in \mathbb{Z}$.

Задача 6.8. При каком значении a многочлен $x^{1000} + ax^2 + 9$ делится на $x + 1$?

Задача 6.9. Докажите, что многочлен $(x^3 - 2) \in \mathbb{Q}[x]$ неприводим.

Задача 6.10. Пусть $a(x) = x^5 + 2x^3 + x^2 + x + 1$ и $b(x) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$. Найдите НОД $a(x)$ и $b(x)$ как элементов $\mathbb{Q}[x]$ и его линейное представление.

Задача 6.11. Докажите, что многочлен $(x + 1)^6 - x^6 - 2x - 1$ делится на многочлен $x(x + 1)(2x + 1)$.

Сравнения

Теоретический материал

7.1. Язык сравнений

Пусть n натуральное число. Введём отношение эквивалентности $\equiv$ на множестве натуральных чисел $\mathbb{N}$ согласно следующему правилу:

$$a \equiv b \pmod{n} \qquad \Leftrightarrow \qquad (a-b) \vdots n$$

В том случае, когда элементы a и b эквивалентны друг другу, говорят, что a *сравнимо с* b *по модулю* n.

Замечание. Корректность этого определения, то есть тот факт, что отношение $\equiv$ на множестве целых чисел в самом деле является отношением эквивалентности, была проверена в упражнении 2.9.

Обозначение. Множество классов эквивалентности обозначается как $\mathbb{Z}/n\mathbb{Z}$.

Замечание. Чтобы определить класс эквивалентности числа a нам достаточно знать его остаток $r_n(a)$ при делении на n. Поэтому множество $\mathbb{Z}/n\mathbb{Z}$ можно представить в виде $\{0, 1, 2, ..., n-1\}$.

Пример 7.1. При $n = 2$ в $\mathbb{Z}/n\mathbb{Z}$ существует всего два класса эквивалентности: чётные и нечётные числа.

На множестве $\mathbb{Z}/n\mathbb{Z}$ сравнений по модулю n естественным образом вводятся операции сложения, вычитания и умножения. Это следует из того факта, что результат не зависит от выбора представителя в классе эквивалентности.

Упражнение 7.1. *Пусть* $a \equiv b \pmod{n}$ *и* $c \equiv d \pmod{n}$. *Докажите, что:*

а) $a + c \equiv b + d \pmod{n}$;

б) $a - c \equiv b - d \pmod{n}$;

в) $a \cdot c \equiv b \cdot d \pmod{n}$;

г) для любого натурального $m \in \mathbb{N}$ *выполнено* $a^m \equiv b^m \pmod{n}$.

Рассматривая в качестве естественных представителей целых чисел a и b их остатки, мы можем задать операции сложения и умножения следующим образом:

$$r(a+b) = r(r(a) + r(b)) \qquad \text{и} \qquad r(a \cdot b) = r(r(a) \cdot r(b)).$$

Пример 7.2. $726 = 11 \cdot 11 \cdot 6 \equiv (-2) \cdot (-2) \cdot 6 \equiv 2 \cdot 12 \equiv 2 \cdot (-1) \equiv 11 \pmod{13}$.

Замечание. Чтобы сложить или перемножить два числа по модулю десяти, достаточно просто сложить или перемножить последние цифры исходных чисел и взять последнюю цифру результата:

$$146 + 8677 \equiv 6 + 7 \equiv 13 \equiv 3 \pmod{10} \qquad \text{и} \qquad 476 \times 335 \equiv 6 \times 5 \equiv 30 \equiv 0 \pmod{10}.$$

Упражнение 7.2. *Как описать сложение и умножение по модулю 2, 3, 5 или 9?*

Замечание. На вычитание можно смотреть как на частный случай сложения. Это означает, что вычитание остатка a, это то же самое, что прибавление остатка $(n-a)$. Поскольку числа $(n-a)$ и $(-a)$ лежит в одном классе эквивалентности, этот остаток часто обозначают как $(-a)$ и называют *противоположным* к a. Резюмируя, противоположный к a остаток характеризуется тем, что $a+(-a) \equiv 0 \pmod{n}$.

Пример 7.3. В множестве $\mathbb{Z}/5\mathbb{Z}$ противоположным к остатку 2 является остаток 3.

С делением всё обстоит сложнее. Рассмотрение несложных примеров показывает, что бездумное сокращение сравнений может приводить к печальным результатам.

Пример 7.4. Имеет место сравнение $6 \equiv 36 \pmod{10}$, однако $1 \not\equiv 6 \pmod{10}$.

С учётом указанного выше замечания, было бы логично заменить деление на a умножением на остаток a^{-1}, *обратный* к a. То есть такой, что $a \cdot a^{-1} \equiv 1 \pmod{n}$. К сожалению, это возможно не всегда.

Упражнение 7.3. *Докажите, что если $n=4$, то не существует такого числа a, что $2a \equiv 1 \pmod{4}$. Таким образом, нельзя делить на 2 по модулю 4.*

Лемма 7.1. *Пусть натуральные числа n и a взаимно просты. Тогда существует остаток x такой, что $ax \equiv b \pmod{n}$.*

Доказательство. Заметим, что так как $(n,a)=1$, то согласно теореме 4.10 Диофантово уравнение $ax+ny=b$ имеет решение x_0, y_0. А согласно упражнению 7.1 можно заменить целое число x_0 на его остаток $x=r(x_0)$. □

Следствие 7.2. *Пусть натуральные числа n и a взаимно просты. Тогда существует остаток a^{-1}, обратный к a по модулю n. Иными словами, на a по модулю n можно делить. В частности, можно делить на любой ненулевой остаток по модулю простого числа.*

Замечание. Теорема 4.10 помогает нам понять также и то, что происходит, если числа n и a не являются взаимно простыми. В этом случае сравнение $ax \equiv b \pmod{n}$ имеет решение тогда и только тогда, когда $b \vdots (n,a)$. В частности, если $b=1$, решений это сравнение не имеет, то есть обратного остатка к a по модулю n не существует.

Пример 7.5. Если $n=10$, то среди остатков взаимно простыми с n являются только 1, 3, 7 и 9. Остатки 3 и 7 обратны друг другу, а остатки 1 и 9 обратны сами себе.

Упражнение 7.4. *Какие остатки может дать квадрат по модулю 3, 8, 24?*

Упражнение 7.5. *Чему равен остаток 3^{2020} по модулю 5?*

7.2. Остатки по простому модулю

Из леммы 7.1 можно увидеть, что остатки по модулю простых чисел похожи на рациональные или вещественные числа в том смысле, что их можно не только складывать, вычитать и умножать, но и делить друг на друга. Эту аналогию можно развивать

и дальше. Так, имеет смысл говорить о решении квадратных уравнений или операции извлечения квадратного корня.

Определение 7.3. Пусть p — простое число. Назовём остаток a *квадратичным вычетом* по модулю p, если существует число q такое, что $q^2 \equiv a \pmod{p}$. Иными словами квадратичный вычет — это остаток, из которого можно извлечь корень.

Утверждение 7.4. *Пусть p — нечётное простое число. Тогда ровно половина ненулевых остатков является квадратичными вычетами по модулю p.*

Доказательство. Выпишем квадраты всех остатков $1^2, 2^2, \ldots, (p-1)^2$. Заметим, что два различных остатка a и b дают один и тот же квадрат, если и только если их сумма равно нулю. Действительно,

$$a^2 \equiv b^2 \pmod{p} \qquad \Leftrightarrow \qquad (a-b)(a+b) \equiv 0 \pmod{p}.$$

Так как $(a-b) \neq 0$, то согласно лемме 7.1 на этот сомножитель можно сократить (отметим, что тут важно, что мы работаем по модулю простого числа). Следовательно, в строке $1^2, 2^2, \ldots, (p-1)^2$ каждый остаток выписан ровно два раза. □

Следствие 7.5. *Пусть p — нечётное простое число. В зависимости от параметра $a \neq 0$ сравнение $x^2 \equiv a \pmod{p}$ либо имеет два решения, либо не имеет решений вовсе.*

Упражнение 7.6. *Какие остатки являются квадратичными вычетами по модулю 7? По модулю 13?*

7.3. Малая теорема Ферма

Теорема 7.6. [Малая теорема Ферма] *Пусть p — простое число. Тогда для любого целого числа a выполнено сравнение $a^p \equiv a \pmod{p}$.*

Доказательство. Для $a = 0$ утверждение очевидно, поэтому ниже мы будем считать, что $a \neq 0$. Мы приведём два различных доказательства этой замечательной теоремы.

Элементарное. Рассмотрим конечный набор чисел $a, 2a, 3a, \ldots, (p-1)a$. Заметим, что остатки этих чисел при делении на p попарно различны. В самом деле, в противном случае для некоторых $k, l \in \{1, 2, \ldots, p-1\}$ выполняется $(k-l)a \vdots p$. В силу взаимной простоты a и p по лемме 7.1 на a можно сократить, что влечёт за собой равенство $k = l$. Таким образом, наша последовательность содержит всё те же остатки $1, 2, \ldots, (p-1)$, но записанные в другом порядке. Перемножая их, получаем

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

Для завершения доказательства осталось разделить обе части равенства на $(p-1)!$, что допустимо, поскольку числа p и $(p-1)!$ взаимно просты.

Комбинаторное. Зададимся следующим вопросом: сколькими способами можно раскрасить круг, разбитый на p одинаковых секторов, a различными красками? Поскольку каждый сектор можно покрасить a способами, по правилу произведения всего способов

раскраски круга a^p. При этом если отождествлять раскраски, получающиеся друг из друга поворотом, то каждая раскраска, кроме a одноцветных, будет посчитана p раз. Это значит, что неодноцветных раскрасок в точности $(a^p-a)/p$. Однако это целое число, откуда $(a^p - a) \vdots p$. $\square$

Упражнение 7.7. *Где в комбинаторном доказательстве малой теоремы Ферма был использован тот факт, что p — простое число? Почему для составных p доказательство не работает?*

Теорема 7.7. [Теорема Вильсона] *Число p является простым тогда и только тогда, когда $\big((p-1)!+1\big)$ делится на p.*

Доказательство. Пусть p — простое. Разобьём остатки на пары a, a^{-1}. Посмотрим на остатки, которые остались без пары — это те остатки, которые обратны сами себе. Остаток a сам себе обратен в том случае, когда

$$a^2 \equiv 1 \pmod p \qquad \Longrightarrow \qquad (a-1)(a+1) \vdots p.$$

Следовательно, лишь остатки 1 и $(p-1)$ обратны самим себе. Значит,

$$(p-1)! \equiv 1 \cdot (2 \cdot 2^{-1}) \cdot \ldots \cdot (p-1) \pmod p$$

и произведение всех остатков сравнимо с $(p-1)$.

Обратно, допустим, p — составное. Тогда существует $d < p$, делящее p. Поэтому $(p-1)!$ делится на d, а $(p-1)!+1$ — не делится. А значит, не делится и на p. $\square$

Пример 7.6. Если $n = 17$, то остатки в числе 16! разбиваются на пары обратных друг к другу следующим образом:

$$17! = 1 \cdot (2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14) \cdot 16 \equiv 16 \pmod{17}.$$

Упражнение 7.8. *Пусть p простое число.*

а) Покажите, что если $1 < k < p$, то C_p^k делится на p.

б) Докажите, что для любых $a, b \in \mathbb{Z}$ справедливо $(a+b)^p \equiv a^p + b^p \pmod p$.

в) Используя метод математической индукции и предыдущие пункты, придумайте ещё одно доказательство малой теоремы Ферма.

7.4. Китайская теорема об остатках

Пример 7.7. Рассмотрим систему сравнений:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Нетрудно проверить, что $x = 23$ является решением. Более того, оказывается, что общее решение имеет вид $x = 23 + 105t$, где $t \in \mathbb{Z}$.

Рассмотренный выше пример является частным случаем более общей ситуации.

Теорема 7.8. [Китайская теорема об остатках]
Пусть $n_1, n_2, \ldots, n_m$ — попарно взаимно простые натуральные числа. Тогда для любых целых чисел $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ существует $x \in \mathbb{Z}$ такое, что

$$\begin{cases} x & \equiv & a_1 \pmod{n_1} \\ & \ldots & \\ x & \equiv & a_m \pmod{n_m} \end{cases}$$

Более того, оно единственно по модулю $N = n_1 \cdot n_2 \cdot \ldots \cdot n_m$.

Доказательство. Сначала проверим существование решения. Для каждого индекса $k \in \{1, 2, \ldots, m\}$ положим $N_k = N/n_k$ и $b_k \equiv N_k^{-1} \pmod{n_k}$. Тогда оказывается, что решение можно записать в виде

$$x = a_1 N_1 b_1 + a_2 N_2 b_2 + \ldots + a_m N_m b_m.$$

Убедимся, что x, заданный такой формулой, является решением. В самом деле, Если $k \neq 1$, то $N_k \vdots n_1$. При этом $a_1 N_1 b_1 \equiv a_1 \pmod{a_1}$. Таким образом, $x \equiv a_1 \pmod{a_1}$ и первое сравнение справедливо. Аналогично проверяются и остальные сравнения.

Теперь удостоверимся в единственности. От противного, пусть имеется два решения: x и x'. Тогда для любого k справедливо $(x - x') \vdots n_k$. Последнее в силу попарной взаимной простоты чисел $n_1, n_2, \ldots, n_m$ влечёт за собой $(x - x') \vdots N$. Требуемое доказано. □

Замечание. 1) Доказать единственность можно было бы и из количественных соображений. В самом деле, число различных неэквивалентных наборов вида $a_1, a_2, \ldots, a_m$ равно $n_1 \cdot n_2 \cdot \ldots \cdot n_m = N$, и каждому такому набору соответствует какое-то решение. С другой стороны, различных остатков по модулю N ровно N. Значит, каждому набору соответствует ровно одно решение.

2) Китайскую теорему об остатках можно переформулировать в терминах теории множеств. Именно, если числа $n_1, n_2, \ldots n_m$ — попарно взаимно простые числа, N — их произведение, а $r_{n_k}(a)$ обозначает остаток при делении a на n_k, то отображение

$$f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_m\mathbb{Z}$$

$$a \mapsto (r_{n_1}(a), r_{n_2}(a) \ldots, r_{n_m}(a))$$

является биекцией. На самом деле утверждается даже большее: эта биекция сохраняет структуру, то есть операции сложения и умножения (понимаемые в правом множестве как покомпонентные). Эта конструкция имеет глубокие обобщения в «большой науке».

Пример 7.8. Условие попарной взаимной простоты является необходимым. В самом деле, рассмотрим следующую систему:

$$\begin{cases} x & \equiv & 1 \pmod 3 \\ x & \equiv & 3 \pmod 6 \end{cases}$$

Из второго сравнения видно, что $(x - 3) \vdots 6$, то есть x делится на 3. Но из первого сравнения $(x - 1) \vdots 3$. Следовательно, искомая система сравнений решений не имеет.

Сравнения

Задачи семинаров

Задача 7.1. (Т) Какие остатки от деления на 7 и на 9 может давать

а) полный квадрат;

б) полный куб?

Задача 7.2. (Т) Решите в целых числах уравнение

а) $7x^3 + 2 = y^3$;

б) $x^2 + y^2 = 3z^2$;

в) $8x^3 - 13y^3 = 17$.

Задача 7.3. (Т) Найдите решения следующих сравнений:

а) $7x \equiv 3 \pmod{15}$;

б) $6x \equiv 5 \pmod{9}$;

в) $4x \equiv 2 \pmod{18}$.

Задача 7.4. Сколько решений имеет сравнение $21x \equiv 14 \pmod{91}$?

Задача 7.5. (Т) Используя свойства сравнений, найдите остаток от деления

а) 12^{100} на 13;

б) 2^{1001} на 11;

в) 45^{10000} на 101;

г) $14^{14^{14}}$ на 17.

Задача 7.6. Пусть n — нечётное число. Найдите остаток от деления на n следующей суммы: $1^3 + 2^3 + \ldots + (n-1)^3$.

Задача 7.7. Докажите, что число $\dfrac{n^7}{7} + \dfrac{n^{11}}{11} + \dfrac{59n}{77}$ является целым.

Задача 7.8. (С) Пусть m и n — взаимно простые натуральные числа, a и b — произвольные целые числа.

а) Докажите, что числа a, $a+m$, $a+2m$, …, $a+(n-1)m$ дают разные остатки при делении на n.

б) Докажите, что пересечение арифметической прогрессии $a, a+m, a+2m, a+3m, \ldots$ с арифметической прогрессией $b, b+n, b+2n, b+3n, \ldots$ является арифметической прогрессией с разностью mn.

Задача 7.9. (Т) Решите следующие системы сравнений:

а) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$;

б) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 6 \pmod{7} \\ x \equiv 4 \pmod{9} \end{cases}$;

в) $\begin{cases} x \equiv a \pmod{4} \\ x \equiv b \pmod{5} \\ x \equiv c \pmod{7} \end{cases}$, где a, b, c — произвольные натуральные числа.

Задача 7.10. (Т) Найдите наименьшее натуральное число, дающее при делении на 2, 3, 5, 7 остатки 1, 2, 4, 6 соответственно.

Задача 7.11. При каких целых n число $n^2 + 3n + 1$ делится на 55?

7.1. Дополнительные задачи

Задача 7.12. По аналогии с признаками делимости на 3 и на 9 можно предложить признак делимости на 27: «если сумма цифр числа делится на 27, то и число делится на 27». Верен ли этот признак?

Задача 7.13. Докажите, что существует бесконечно много натуральных чисел, которые не представимы в виде суммы двух квадратов.

Задача 7.14. Найдите остаток от деления числа, состоящего из 19 девяток, на 19.

Определение 7.9. Пусть $n \in \mathbb{N}$. *Функция Эйлера* $\phi(n)$ — это количество чисел от 1 до n включительно, взаимно простых с n.

Задача 7.15. Докажите следующие свойства функции Эйлера.

а) $\phi(p^k) = p^{k-1}(p-1)$, где p — простое, k — натуральное;

б) Пусть a и b взаимно просты. Покажите, что $\phi(ab) = \phi(a)\phi(b)$;

в) Разложим число n как произведение степеней простых чисел: $n = p^{\alpha_1} \cdot \ldots \cdot p^{\alpha_l}$. Выразите $\phi(n)$ через $p_1, \ldots, p_l$ и $\alpha_1, \ldots, \alpha_l$.

Задача 7.16. [Теорема Эйлера] Пусть натуральные числа a и n взаимно просты. Докажите, что $a^{\phi(n)} \equiv 1 \pmod{n}$.

Определение 7.10. Будем говорить, что остаток a по модулю n является *обратимым вычетом*, если для него найдется такой остаток b, что $ab \equiv 1 \pmod{n}$.

Задача 7.17. Сколько существует обратимых вычетов

а) по модулю p^α, где p — простое, α —натуральное;

б) по модулю $p_1^{\alpha_1} p_2^{\alpha_2}$, где p_k — различные простые, α_k — натуральные;

в) по модулю $p_1^{\alpha_1} \ldots p_2^{\alpha_l}$, где p_k — различные простые, α_k — натуральные?

г) По каким модулям нет обратимых вычетов кроме ± 1?

Задача 7.18. Пусть p — простое число, $a, b, c \in \mathbb{Z}$. Сколько решений может иметь

а) сравнение $x^2 \equiv 1 \pmod{p}$;

б) сравнение $x^2 \equiv a \pmod{p}$;

в) сравнение $ax^2 + bx + c \equiv 0 \pmod{p}$?

Задача 7.19. Пусть p — простое число. Докажите, что сравнение

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p}$$

имеет нетривиальное решение в целых числах (*тривиальное решение* — это решение $x \equiv y \equiv z \equiv 0 \pmod{p}$).

Действительные числа

Теоретический материал

8.1. Введение

Этот раздел посвящён действительным (вещественным) числам. Из школьной программы хорошо известны понятия натуральных, целых и рациональных чисел. Действительные числа $\mathbb{R}$ — следующий, ещё более широкий класс чисел.

Предыдущие расширения были нужны для того, чтобы какие-то операции были возможны для большего множества аргументов. Например: в целых числах, в отличие от натуральных, всегда можно вычитать из одного числа другое (иначе говоря, решать уравнение $x + a = b$ при любых a и b), а в рациональных — делить одно на другое ненулевое (решать уравнение $ax = b$ при $a \neq 0$).

При этом мы хотим, чтобы при расширении «старые» свойства по возможности сохранялись и в новом множестве чисел. Перечислим некоторые из этих свойств.

$$\begin{gathered} a+b=b+a, \qquad ab=ba \qquad \text{(коммутативность)},\\ (a+b)+c=a+(b+c), \quad (ab)c=a(bc) \qquad \text{(ассоциативность)},\\ a(b+c)=ab+ac \qquad \text{(дистрибутивность)}, \end{gathered}$$

$$\begin{aligned} (a \leqslant b) \wedge (b \leqslant c) \quad &\Rightarrow \quad a \leqslant c,\\ (a \leqslant b) \wedge (c \leqslant d) \quad &\Rightarrow \quad a+c \leqslant b+d,\\ (0 \leqslant a \leqslant b) \wedge (0 \leqslant c \leqslant d) \quad &\Rightarrow \quad 0 \leqslant ac \leqslant bd. \end{aligned}$$

Вообще говоря, при расширении множества чисел эти свойства для нового множества ($\mathbb{Z}$ или $\mathbb{Q}$) являются теоремами, которые можно доказать, используя свойства исходного множества чисел ($\mathbb{N}$ и $\mathbb{Z}$ соответственно). Мы, однако, будем их использовать без доказательства.

Сложность с действительными числами возникает в двух вещах. Во-первых, есть несколько возможных конструкций; каждая из них достаточно сложная, и априори изначально непонятно,

(а) почему они задают какой-то интересный объект,

(б) будет ли этот объект один и тот же.

В последнем явно проявляется отличие от целых или рациональных чисел, где есть единственная простая конструкция. Во-вторых, трудно задать то свойство, ради которого нужно расширять множество рациональных чисел. Чтобы подойти к описанию этого свойства, приведём два примера чисел, которых нет в множестве $\mathbb{Q}$.

Первый пример проистекает из того факта, что в $\mathbb{Q}$ далеко не всегда можно извлекать корень. Например, как было доказано в разделе 4.6, уравнение $x^2 = 2$ (а именно его положительный корень и обозначается $\sqrt{2}$) не имеет решений в рациональных числах. То есть нам нужно добавить к исходному множеству числа $\sqrt{2}$, $\sqrt{3}$ и так далее, а также

более сложные выражения типа $\sqrt[3]{\sqrt{2}+\sqrt{3}}$. Здесь, правда, возникает одна сложность: непонятно, как определить равенство чисел. Например, оказывается, что

$$\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}=1,$$

хотя это и неочевидно. В данном случае легко проверить, что

$$\Big(\frac{1\pm\sqrt{5}}{2}\Big)^3=2\pm\sqrt{5},$$

поэтому левая часть предыдущего равенства равна

$$\frac{1+\sqrt{5}}{2}+\frac{1-\sqrt{5}}{2}=1$$

Кроме корней из положительных чисел можно пытаться добавить и корни из отрицательных чисел, например, решение уравнения $x^2=-1$ (его традиционно обозначают i). К сожалению, если допустить существование корня у этого уравнения, нам придётся кое от чего отказаться. Действительно, попробуем понять, является число i положительным или отрицательным. Если $i>0$, то $-1=i\cdot i>0$. Если же $i<0$, то $-i>0$, а тогда $-1=(-i)\cdot(-i)>0$. Так что за существование корня из -1 приходится платить невозможностью сравнения чисел.

Тем не менее, такое множество чисел часто полезно; оно называется *множеством комплексных чисел*, и к нему мы ещё вернёмся в главе Комплексные числа. Пока же мы хотим сохранить возможность сравнения чисел, поэтому корни чётной степени из отрицательных чисел рассматривать не будем.

Как известно, если мы имеем возможность извлекать квадратный корень, то и любое квадратное уравнение мы можем решить по хорошо известной со школы формуле (см. задачу 6.3). Более того, имеются подобные формулы и для уравнений третьей и четвёртой степени.

Однако бывают уравнения пятой степени, которые нельзя решить с помощью формул, содержащих арифметические операции и взятие корня любой степени. Например, таково уравнение $x^5+x+1=0$. В то же время ясно, что оно должно иметь корень: достаточно заметить, что при $x=-1$ левая часть отрицательна, а при $x=0$ положительна. Естественно считать, что в какой-то промежуточной точке она обратится в ноль.

Упражнение 8.1. *Покажите, что корень у этого уравнения $x^5+x+1=0$ всего один.*

По той же причине мы можем считать, что всякое уравнение $P(x)=0$, в котором многочлен P принимает значения разных знаков, должен иметь корень. Соответственно, к числу рассматриваемых операций, наряду с арифметическими и $\sqrt[k]{\ }$, мы можем добавить такую: если дан многочлен P, принимающий значения разных знаков, то можно получить его корни. Числа, получающиеся из целых чисел с помощью этого набора

операций, называются *алгебраическими*.[1]

Другое число, которого нам не хватает среди рациональных, — это π, отношение длины окружности к её диаметру. Можно доказать, что π не является рациональным числом, и даже алгебраическим числом, но соответствующие доказательства сложны, и мы их обсуждать здесь не будем.

Напомним определение числа π. Рассмотрим вписанные в единичную окружность правильные n-угольники для всё больших значений натурального числа n. Тогда оказывается, что их периметры стремятся к числу, которое и называется длиной этой окружности и обозначается 2π.

Нам будет удобнее рассмотреть не все n-угольники, а только те, число сторон которых является степенью двойки. Итак, пусть P_n — периметр правильного 2^n-угольника, вписанного в единичную окружность. Тогда $P_{n+1} \geqslant P_n$. Действительно, если к вершинам 2^n-угольника добавить середины дуг, на которые опираются его стороны, получатся вершины правильного 2^{n+1}-угольника. Пусть для какой-нибудь стороны AB исходного 2^n-угольника точка C — это середина соответствующей дуги. Тогда сумма $AC + CB$ длин двух сторон 2^{n+1}-угольника по неравенству треугольника больше длины AB. Сложив такие неравенства для всех сторон 2^n-угольника, мы и получим $P_{n+1} \geqslant P_n$.

Как может себя вести возрастающая последовательность чисел (x_n)? Во-первых, она может «уходить в бесконечность»: для любого числа C все члены последовательности, начиная с некоторого k-го, становятся больше C. Для нашей последовательности (P_n) это не так: покажем, что $P_n \leqslant 8$ при всех n. Рассмотрим часть 2^n-угольника, попадающую в первый квадрант: это ломаная $A_0A_1 \dots A_{2^{n-2}}$, где $A_0 = (1, 0)$, $A_{2^{n-2}} = (0, 1)$. Длина этой ломаной равна $L_n = P_n/4$. Если обозначить $A_s = (x_s, y_s)$, то последовательности $(x_s)_{s=0}^{2^{n-2}}$ и $(y_s)_{s=0}^{2^{n-2}}$ — убывающая и возрастающая соответственно. Следовательно,

$$A_sA_{s+1} = \sqrt{(x_s - x_{s+1})^2 + (y_s - y_{s+1})^2} \leqslant \\ \leqslant |x_s - x_{s+1}| + |y_s - y_{s+1}| = (x_s - x_{s+1}) + (y_{s+1} - y_s)$$

(неравенство на втором шаге вытекает из того, что длина гипотенузы короче суммы длин катетов). Суммируя полученные неравенства при всех $s = 0, \dots, (2^{n-2} - 1)$, получим $L_n \leqslant (x_0 - x_{2^{n-2}}) + (y_{2^{n-2}} - y_0) = 2$, что и требовалось.

Таким образом, последовательность $P_n = 4L_n$ не может уходить на бесконечность. Поэтому естественно считать, что она постепенно приближается к некоторому числу, которое и называется длиной окружности.

Ключевое свойство действительных чисел, *полнота*, как раз и состоит в том, что возрастающие последовательности, которые не уходят на бесконечность, действительно

[1] Точнее, *вещественно-алгебраическими*. Отметим, что на самом деле вместо многократного применения операции нахождения корней уравнений можно обойтись однократным. Например, если y является одним из корней уравнения $y^2 = 2$, а x — корень уравнения $x^2 + 2yx + 1 = 0$, то x является корнем уравнения $x^4 - 6x^2 + 1 = 0$. Действительно, x — корень одного из уравнений $x^2 \pm 2\sqrt{2}x + 1 = 0$, то есть это корень уравнения $(x^2 + 2\sqrt{2}x + 1)(x^2 - 2\sqrt{2}x + 1) = 0$, и остаётся только раскрыть здесь скобки. В общем случае доказательство основано на той же идее, но более сложно.

приближаются к некоторому числу. Точной формулировке этого свойства посвящена следующая часть.

8.2. Полнота

Этот подраздел посвящён *аксиоме полноты* — тому свойству, которое и выделяет множество действительных чисел.

Прежде чем переходить к аксиоме полноты, обсудим ещё одно утверждение, на первый взгляд настолько очевидное, что не требует особой формулировки. Речь идёт об *аксиома Архимеда*. Сам Архимед формулировал её (в переводе на современный математический язык) так: если есть два отрезка, то первый можно отложить столько раз, что полученный отрезок станет длинее второго. Если перейти от отрезков к их длинам a и b, то это означает, что существует такое натуральное n, что

$$\underbrace{a + a + \cdots + a}_{n \text{ раз}} = na > b.$$

Поделив это неравенство на a и обозначив $c = b/a$, получим современную формулировку: для любого числа c существует натуральное число n такое, что $n > c$.

Для множества рациональных чисел это свойство очевидно: например, можно при $c \leqslant 0$ взять $n = 1$, а при $c = p/q > 0$ взять $n = p + 1$. Но, вообще говоря, бывают множества с операциями сложения и умножения, в которых аксиома Архимеда неверна. Поэтому для множества действительных чисел мы потребуем её выполнения.

Перейдём теперь к полноте. Есть несколько эквивалентных формулировок этого понятия, о которых вам расскажут в курсе математического анализа (точнее говоря, они эквивалентны, если предполагать верной аксиому Архимеда; иначе к некоторым из этих формулировок нужно её добавить, а к другим её добавлять не нужно, поскольку она из них выводится). Мы ограничимся лишь одной формулировкой — той, которая уже обсуждалась выше, когда речь шла о длине окружности. Мы рассматриваем последовательность (x_n), *неубывающую* ($x_n \leqslant x_{n+1}$ при всех n) и *ограниченную сверху* (существует C, для которого $x_n \leqslant C$ при всех n). Нам нужно определить, что означает, что такая последовательность приближается сколь угодно близко (обычно говорят «стремится») к некоторому числу A (его называют *пределом* последовательности (x_n)).

Во-первых, A должно быть не меньше любого члена последовательности, иначе какой-то член x_k последовательности станет больше A, а тогда все последующие члены последовательности будут удалены от A на расстояние не меньше $(x_k - A)$.

Но чисел, не меньших всех членов последовательности много: если мы нашли одно такое число a, то и любое число $a' > a$ тоже таково. Поэтому естественно рассмотреть наименьшее число с таким свойством: $A = \min\{a \mid x_n \leqslant a \ \ \forall n \in \mathbb{N}\}$.

Вообще говоря, не во всяком множестве есть наименьший элемент. Например, множество $Z = \{x \mid x > 1\}$ такого элемента не имеет. Действительно, если взять произвольный элемент $a \in Z$, то для $b = (a + 1)/2$ верно, что $b \in Z$ и $b < a$, а потому a не может быть минимальным элементом множества Z.

Упражнение 8.2. *Проверьте, что множество* $\{x > 0 \mid x^2 > 2\}$ *не имеет наименьшего элемента, не используя существования* $\sqrt{2}$.

Формулировка аксиомы полноты утверждает, что в нашем случае наименьший элемент есть.

Аксиома 8.1. [Аксиома полноты] *Пусть последовательность* (x_n)

- *неубывающая, то есть* $x_{n+1} \geqslant x_n$ *при всех* $n \in \mathbb{N}$;
- *ограничена сверху, то есть существует такое* C, *что* $x_n \leqslant C$ *при всех* $n \in \mathbb{N}$.

Тогда множество чисел $S = \{a \mid x_n \leqslant a \ \ \forall n\}$ *имеет наименьший элемент* $A = \min S$. *Этот элемент называют* предел *последовательности* (x_n).

Обозначение. Обозначение: $A = \lim\limits_{n\to\infty} x_n$.

Предупреждение. В курсе матанализа вам будет дано другое определение предела последовательности, которое работает не только для монотонных последовательностей. Однако для монотонных последовательностей наше определение будет эквивалентно этому более общему.

Замечание. Заметим, кстати, что множество S непусто тогда и только тогда, когда (x_n) ограничена сверху, так что это условие отбросить нельзя.

Из аксиомы полноты прямо следует, что существует длина окружности. Действительно, последовательность (P_n) периметров 2^n-угольников, вписанных в единичную окружность, возрастает и ограничена сверху числом 8. Значит, по аксиоме полноты она имеет предел, который можно обозначить 2π. В частности, отсюда вытекает, что $\pi \leqslant 4$. Действительно, число 8 лежит в множестве $\{c \mid \forall n : \ P_n \leqslant c\}$, а число 2π — это минимальный элемент в этом множестве, поэтому $2\pi \leqslant 8$.

Чтобы доказать существование корня из двух, нам будет удобно рассмотреть убывающую, а не возрастающую последовательность. Аналог аксиомы полноты для невозрастающих последовательностей звучит так: если последовательность (x_n)

- невозрастающая, то есть $x_{n+1} \leqslant x_n$ при всех $n \in \mathbb{N}$;
- ограничена снизу, то есть существует такое C, что $x_n \geqslant C$ при всех $n \in \mathbb{N}$,

то существует $A = \max\{c \mid x_n \geqslant c \ \ \forall n\}$.

Упражнение 8.3. *Выведите это утверждение из аксиомы полноты.*

Рассмотрим теперь последовательность, строящуюся по правилу

$$x_1 = 2, \qquad x_{n+1} = \frac{1}{2}\left(x_n + \frac{2}{x_n}\right) \quad \text{при } n \in \mathbb{N}.$$

Доказательство того, что она стремится к $\sqrt{2}$, получается из следующей серии задач.

Упражнение 8.4. *Проверьте, что*

а) $x_n^2 \geqslant 2$;

б) (x_n) — *невозрастающая последовательность.*

Поскольку $x_n \geqslant 0$, последовательность (x_n) ограничена снизу, а потому имеет некоторый предел, который мы обозначим за x.

Упражнение 8.5. *Докажите, что*

$$x_n^2 - x^2 \leqslant 4(x_n - x).$$

Выведите отсюда, что $x^2 \geqslant 2$.

Упражнение 8.6. *Докажите, что*

$$x_{n+1}^2 - 2 \leqslant \frac{x_n^2 - 2}{4}.$$

Выведите отсюда, что $x^2 = 2$.

Если эти задачи вызывают у вас затруднения, прочитайте следующие главы — там есть приёмы, которые помогут и здесь.

8.3. Десятичная запись (напоминание)

В разделе 4.1 мы уже обсуждали, что такое десятичная запись натурального числа. Здесь мы дадим формальное изложение этого вопроса в более широком ключе, затронув не только десятичную, но и d-ичную запись для произвольного $d \in \mathbb{N}$. Оно нам понадобится далее, когда мы будем говорить о бесконечных десятичных дробях.

Зафиксируем натуральное $d \geqslant 2$ — *основание системы счисления*. Тогда для чисел $a_j \in \{0, 1, \ldots, d-1\}$ (которые можно было бы назвать *цифрами*), где $a_n \neq 0$, положим

$$\overline{a_n \ldots a_1 a_0}_d = \sum_{j=0}^{n} a_j d^j = a_n d^n + a_{n-1} d^{n-1} + \ldots + a_1 d + a_0.$$

Далее мы будем считать d фиксированным и опускать его в этом обозначении: $\overline{a_n \ldots a_1 a_0}$.

Данное выше определение позволяет нам сказать, к примеру, что $\overline{752}_8 = 7{\cdot}8^2 + 5{\cdot}8 + 2$, но из него неясно, любое ли натуральное число обладает d-ичной записью и единственна ли она.

Теорема 8.2. *Пусть* $d \geqslant 2$. *Тогда для любого натурального* N *существуют и единственны* $n \geqslant 0$ *и* $a_j \in \{0, 1, \ldots, d-1\}$, $j = 0, \ldots, n$, *где* $a_n \neq 0$, *для которых выполнено равенство* $N = \overline{a_n \ldots a_1 a_0}_d = N$.

Это утверждение может показаться тавтологией, но это не так. Дело в том, что натуральное число обозначает количество элементов в непустом конечном множестве, а десятичная запись уже вторична. Представьте себе, что вы объяснили эту теорему древнему римлянину, который ни о какой десятичной записи не знает. Тогда он может записать, например, что[2]

$$\text{число дней в невисокосном году} = \overline{(\text{III})(\text{VI})(\text{V})}_{\text{X}} = \overline{(\text{I})(\text{IV})(0)(\text{V})}_{\text{VI}}.$$

[2]Общеупотребительного символа для нуля в античности не было. Известны отдельные применения нескольких знаков, например, «$\overline{\circ}$» или «N».

И для него совсем неочевидно, что такое представление у любого числа есть и оно единственно.

Мы дадим два доказательства этой теоремы.

Доказательство. [Первое.] Начнём с единственности. Заметим, что

$$N = \sum_{j=0}^{n} a_j d^j = a_0 + d\sum_{j=1}^{n} a_j d^{j-1}.$$

Поэтому последняя цифра a_0 определена однозначно — это остаток от деления N на d, а неполное частное равно $N_1 = a_n d^{n-1} + a_{n-1} d^{n-2} + \ldots + a_1$. Поделив N_1 с остатком на d, мы получим, что остаток равен a_1, а неполное частное $N_2 = a_n d^{n-2} + a_{n-1} d^{n-3} + \ldots + a_2$, и так далее.

Таким образом, если у числа есть d-ичная запись, то все её цифры находятся однозначно: они получаются как последовательные остатки при многократном делении N на d. Число n при этом тоже находится однозначно: это первое такое k, что неполное частное N_{k+1} равно нулю. Действительно, при $k < n$

$$N_{k+1} = a_n d^{n-k-1} + a_{n-1} d^{n-k-2} + \ldots + a_{k+1} \geqslant a_n d^{n-k-1} \geqslant d^{n-k-1} > 0,$$

так как $a_n \geqslant 1$. Единственность доказана.

Эти же вычисления подсказывают алгоритм для поиска d-ичной записи: нужно последовательно делить N на d с остатком, пока неполное частное не станет равно нулю:

$$N = dN_1 + a_0, \qquad N_1 = dN_2 + a_1, \qquad \ldots, \qquad N_n = d \cdot 0 + a_n.$$

Тогда $a_j \in \{0, 1, \ldots, d-1\}$, поскольку это остатки от деления на d, а $a_n = N_n > 0$. Последовательно подставляя эти формулы друг в друга, получаем

$$N = a_0 + d(a_1 + d(a_2 + d(\cdots + (a_{n-1} + d(a_n + d \cdot 0)) \ldots))) = \sum_{j=0}^{n} a_j d^j,$$

что и требовалось.

Однако, пока в этом доказательстве есть пробел: почему обязательно наступит такой момент n, что $N_{n+1} = 0$? Это следует из такого соображения: если $N_{k+1} > 0$, то

$$N_k = dN_{k+1} + a_k \geqslant dN_{k+1} > N_{k+1}$$

(на последнем шаге мы воспользовались тем, что $d > 1$). Поэтому $N_k \geqslant N_{k+1} + 1$ (это ведь целые числа), а тогда если $N_N > 0$, то $N = N_0 \geqslant N_N + N > N$. Таким образом, N_N заведомо равно нулю. $\square$

Доказательство. [Второе.] Начнём с того, что оценим, на каком интервале может лежать d-ичная запись $\overline{a_n \ldots a_0}$. С одной стороны,

$$\sum_{j=0}^{n} a_j d^j \geqslant a_n d^n \geqslant d^n,$$

а с другой,

$$\sum_{j=0}^{n} a_j d^j \leqslant \sum_{j=0}^{n} (d-1)d^j = \sum_{j=0}^{n} (d^{j+1} - d^j) = d^{n+1} - 1. \tag{3}$$

Последнее равенство проще увидеть, если расписать знак $\sum$ с помощью многоточия: каждый член d^k встретится в сумме два раза, один раз с плюсом, один раз с минусом.

Это значит, что число разрядов в d-ичной записи находится однозначно: нужно рассмотреть строго возрастающую последовательность $d^0, d^1, \ldots, d^k, \ldots$ и выяснить, между какими её членами лежит N: если $d^n \leqslant N < d^{n+1}$, то d-ичная запись должна иметь вид $\overline{a_n \ldots a_0}$. Здесь, кстати, опять нужно обосновать почему не может быть так, что $d^n < N$ при любом n. Действительно, $d^k \geqslant d^{k-1} + 1$, поэтому $d^k \geqslant k + 1$, так что $d^N > N$.

Итак, пусть $d^n \leqslant N < d^{n+1}$. Покажем, что запись $N = \overline{a_n \ldots a_0}$ единственна. Для этого заметим, что $N = a_n d^n + K_1$, где $K_1 = a_{n-1}d^{n-1} + \ldots + a_1 d + a_0 \leqslant d^n - 1$. Следовательно, K_1 — остаток, а a_n — неполное частное от деления N на d^n. Далее, $K_1 = a_{n-1}d^{n-1} + K_2$, где $K_2 = a_{n-2}d^{n-2} + \ldots + a_1 d + a_0 \leqslant d^{n-1} - 1$, так что a_{n-1} и K_2 — остаток и неполное частное от деления на d^{n-1}. Продолжая, дойдём до $K_n = a_0 \cdot 1$, где деление на единицу даёт нулевой остаток. Значит, и длина записи, и все цифры находятся однозначно.

Покажем теперь, что запись $\overline{a_n \ldots a_0}$ числа N, где $d^n \leqslant N < d^{n+1}$, существует. Для этого будем делить исходное число на d^n, потом остаток на d^{n-1} и так далее:

$$N = a_n d^n + K_1, \quad K_1 = a_{n-1}d^{n-1} + K_2, \quad \ldots, \quad K_{n-1} = a_1 d + K_n, \quad K_n = a_0 \cdot 1 + 0.$$

Тогда $N < d^{n+1}$, $K_j < d^{n+1-j}$ (поскольку K_j — остаток от деления на d^{n+1-j}). Поэтому при делении K_j на d^{n-j} неполное частное a_{n-j} меньше d, то есть $a_j \in \{0, 1, \ldots, d-1\}$. Кроме того, $N \geqslant d^n$, поэтому при первом делении неполное частное a_n положительно. Значит, все условия для a_j выполнены, а последовательная подстановка формул для K_j даёт нам

$$N = a_n d^n + (a_{n-1}d^{n-1} + (\cdots + (a_1 d + a_0 \cdot 1)) \ldots).$$

Что и требовалось доказать. □

Теперь то, что известные из начальной школы алгоритмы для сложения, умножения и прочих операций дают верный ответ — это теоремы. Строго они формулируются так: если $a = \overline{a_k \ldots a_0}$, $b = \overline{b_l \ldots b_0}$ и применение алгоритма сложения в столбик (или другого алгоритма) к $(a_k \ldots a_0)$ и $(b_l \ldots b_0)$ даёт $(c_m \ldots c_0)$, то $\overline{c_m \ldots c_0} = a + b$. Мы эти теоремы доказывать не будем.

Напомним ещё, как определяются десятичные записи целых чисел и некоторых рациональных. Для целых чисел d-ичная запись определяется просто: для натуральных мы её уже определили, для нуля это 0, а для целого отрицательного числа $-N$ нужно перед записью натурального числа N поставить знак «−».

В множестве рациональных чисел определяются *конечные d-ичные дроби* — записи вида $\pm\overline{a_n \ldots a_0, a_{-1} \ldots a_{-m}}$. Единственность здесь имеет место, если отождествить записи с добавлением нулей в конец числа: например, 0,47 = 0,470 = 0,4700. Однако

не каждое число можно представить в таком виде: нужно, чтобы оно было представимо в виде p/d^m ($p, m \in \mathbb{Z}$). Такие числа называют *d-ично-рациональными* (двоично-рациональными, троично-рациональными и так далее).

Нам будет далее удобно, однако, использовать немного непривычный вариант такой записи: для отрицательных чисел мы будем считать, что «минус» относится только к целой части, так что число $-273,15$ мы будем записывать как $(-274),85$.[3]

Итак, дадим формальное определение. Пусть $A \in \mathbb{Z}$, $a_j \in \{0, \ldots, d-1\}$. Тогда

$$\overline{A{,}a_1 \ldots a_m} = A + \sum_{j=1}^{m} a_j d^{-j} = A + \frac{a_1}{d} + \frac{a_2}{d^2} + \ldots + \frac{a_m}{d^m}.$$

Соответствующая теорема звучит так: если $x = p/d^m$, то существует единственное представление x в виде d-ичной дроби с m разрядами после запятой. Доказательство этих существования и единственности можно провести, повторяя рассуждения из доказательств теоремы для натуральных чисел. Другой вариант — показать, что по d-ичной записи натурального числа p строится d-ичная запись числа x (как?) и наоборот, и воспользоваться теоремой существования и единственности для натуральных чисел.

Упражнение 8.7. *Проведите описанное в последнем предложении рассуждение для*

а) положительных x;

б) отрицательных x.

Неединственность, связанная с добавлением нулей в конец записи, в такой формулировке спрятана в неединственность представления числа в виде p/d^m:

$$x = \frac{p}{d^m} = \frac{pd}{d^{m+1}} = \frac{pd^2}{d^{m+2}} = \ldots$$

На самом деле любое рациональное число обладает бесконечной десятичной записью: например, $1/6 = 0{,}166666666\ldots$. Эта запись состоит из некоторой начальной части (предпериода) и затем повторяющего бесконечно много раз периода. Однако определение того, что означает такая запись, должно использовать сумму бесконечного числа слагаемых, а эта операция требует рассмотрения предела последовательности сумм первых n слагаемых. Мы обсудим этот вопрос далее.

[3] Такой вариант записи прежде использовался при вычислениях с логарифмическими таблицами. Например, чтобы умножить $x = 0{,}02021 \times 1147 \times 1{,}520$, можно найти в таблице логарифмов, что $\log_{10} 0{,}02021 = (-2) + \log_{10} 2{,}021 = (-2){,}3056$, $\log_{10} 1147 = 3 + \log_{10} 1{,}147 = 3{,}0596$, $\log_{10} 1{,}520 = 0{,}1818$. Теперь логарифмы нужно сложить: целые части складываются в уме, а все три дробные части складываются в столбик вместе за одну операцию: $\log_{10} x = 1{,}5470$, и из таблицы антилогарифмов получаем $x = 35{,}23$. Если бы мы использовали «обычное» представление $\log_{10} 0{,}02021 = -1{,}6944$, то нам бы понадобилось две дополнительных операции: вычитание при получении из табличного логарифма $\log_{10} 2{,}021$ требуемого $\log_{10} 0{,}02021$, а затем вместо одного сложения в столбик понадобились бы сложение и вычитание. Сейчас, конечно, эти приёмы ручных вычислений никакого практического значения не имеют.

8.4. Бесконечная d-ичная запись и действительные числа

Определения натуральных, целых и рациональных чисел никак не опирались на понятие d-ичных записей. Для действительных чисел ситуация двоякая. Если это множество *уже* построено, то мы можем сказать, что какое-то число обладает такой-то d-ичной записью (как мы, например, говорим, что число полей на шахматной доске обладает десятичной записью 64 или троичной записью 2101). С другой стороны, можно использовать сами бесконечные d-ичные записи как способ построения действительных чисел.

В этой части мы обсудим первую ситуацию, когда множество действительных чисел уже есть. Бесконечная d-ичная запись $\overline{A,a_1a_2\ldots}$, где $A\in\mathbb{Z}$ и $a_j\in\{0,\ldots,d-1\}$, обозначает бесконечную сумму

$$\overline{A,a_1a_2\ldots}=A+\sum_{j=1}^{\infty}a_jd^{-j}=A+\frac{a_1}{d}+\frac{a_2}{d^2}+\ldots.$$

Чтобы определить, что означает бесконечная сумма в правой части этого равенства, рассмотрим частичные суммы

$$x_n=A+\sum_{j=1}^{n}a_jd^{-j}=\overline{A,a_1a_2\ldots a_n}.$$

Это неубывающая последовательность, которая ограничена сверху.

Упражнение 8.8. *Проверьте по аналогии с выкладкой* (3)*, что* $x_n\leqslant A+1$.

Значит, по аксиоме полноты эта последовательность имеет некоторый предел x, и по определению имеет место равенство

$$x=\sum_{j=1}^{\infty}a_jd^{-j}.$$

Как и в случае записей натуральных чисел, возникает вопрос существования и единственности d-ичной записи. Выясняется, что единственность имеет место не всегда:

$$\overline{A,a_1\ldots a_k(d-1)(d-1)\ldots}=\overline{A,a_1\ldots a_{k-1}(a_k+1)00\ldots}. \tag{4}$$

Например, для десятичных записей $2{,}49999\ldots=2{,}50000\ldots$ или $0{,}99999\cdots=1{,}00000\ldots$ (в последнем случае $k=0$, так что «+1» уходит к целой части).

Проверим равенство (4). Для этого определим частичные суммы (конечные дроби) для обеих частей этого равенства. При $n\geqslant k$ получаем

$$x_n=\overline{A,a_1\ldots a_k(d-1)\ldots(d-1)},\qquad y_n=\overline{A,a_1\ldots a_{k-1}(a_k+1)0\ldots0}$$

(здесь в каждой дроби n знаков после запятой). Следовательно, при $n\geqslant k$ выполнено равенство $y_n=x_n+d^{-n}$. При этом все y_n при $n\geqslant k$ равны между собой:

$$y_n=y=\overline{A,a_1\ldots a_{k-1}(a_k+1)}.$$

Поэтому $\lim\limits_{n\to\infty} y_n = y$.

Вычислим предел

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \left(y - \frac{1}{d^n} \right).$$

Во-первых, $x_n \leqslant y$, то есть (x_n) ограничена сверху, а значит, имеет предел. Более того, если $x = \lim\limits_{n\to\infty} x_n$, то $x \leqslant y$. Предположив, что $x < y$, мы бы получили $x = y - \delta$ для некоторого $\delta > 0$, и чтобы прийти к противоречию, нам нужно доказать, что существует такое $n \in \mathbb{N}$, для которого $x_n > x$, то есть для которого $1/d^n < \delta$. Это эквивалентно неравенству $d^n > (1/\delta)$, для проверки которого мы воспользуемся доказанной выше оценкой $d^n \geqslant n + 1$. Теперь достаточно убедиться, что существует $n \geqslant (1/\delta) - 1$, а это верно по аксиоме Архимеда.

Перейдём к доказательству существования и единственности d-ичной записи (с точностью до замены «хвоста девяток» на «хвост нулей»). Прежде чем читать дальше, на минуту остановитесь здесь и попробуйте понять, какое из двух доказательств существования и единственности для натуральных чисел (теорема 8.2) можно пытаться обобщить на этот случай.

Ответ на этот вопрос таков. Нужно воспользоваться тем, которое находит значения разрядов слева направо: «наименьшего» разряда у нас теперь нет.

Лемма 8.3. *Пусть $m > n$ — натуральные числа. Тогда*

$$\overline{A,a_1\dots a_n} \leqslant \overline{A,a_1\dots a_m} \leqslant \overline{A,a_1\dots a_n} + d^{-n}.$$

Доказательство. Искомое неравенство эквивалентно следующему:

$$A + \sum_{j=1}^{n} a_j d^{-j} \leqslant A + \sum_{j=1}^{m} a_j d^{-j} \leqslant A + \sum_{j=1}^{n} a_j d^{-j} + d^{-n},$$

или, после сокращения одинаковых слагаемых,

$$0 \leqslant \sum_{j=n+1}^{m} a_j d^{-j} \leqslant d^{-n}.$$

Левое неравенство очевидно, а в правом $a_j < d - 1$:

$$\sum_{j=n+1}^{m} a_j d^{-j} \leqslant \sum_{j=n+1}^{m} (d-1) d^{-j} = d^{-n} - d^{-m} \leqslant d^{-n}.$$

Требуемое доказано. □

Из леммы следует, что предел $x = \overline{A,a_1a_2\dots}$ попадает на тот же отрезок. Геометрически это означает, что если разбить ось на отрезки длины d^{-n} точками вида p/d^n, то все записи с одинаковым началом $\overline{A, a_1\dots a_n}$ попадут в один такой отрезок.

Предположим теперь, что $x = \overline{A,a_1a_2\ldots} = \overline{B,b_1b_2\ldots}$. Пусть эти записи совпадают до $(k-1)$-го разряда, а $a_k \neq b_k$. Тогда число x должно лежать одновременно в двух отрезках: $[z + a_k d^{-k}, z + (a_k+1)d^{-k}]$ и $[z + b_k d^{-k}, z + (b_k+1)d^{-k}]$, где $z = \overline{A,a_1\ldots a_{k-1}}$. Эти два отрезка могут пересекаться только если $a_k = b_k \pm 1$, и в этом случае они имеют общий конец.

Пусть $b_k = a_k + 1$ (иначе можно поменять местами $a_j \leftrightarrow b_j$). Тогда эти отрезки пересекаются по одной точке: $x = z + (a_k+1)d^{-k}$. Остаётся проверить, что $a_j = d-1$, $b_j = 0$ при $j > k$. Действительно, если есть $b_s > 0$, то

$$x = \overline{B,b_1b_2\ldots} \geqslant \overline{B,b_1b_2\ldots b_s} \geqslant \overline{B,b_1b_2\ldots b_k} + d^{-s} = x + d^{-s} > x.$$

Аналогичным образом, если $a_s < d-1$, то

$$x = \overline{A,a_1a_2\ldots} \leqslant \overline{A,a_1a_2\ldots a_s} + d^{-s} <$$
$$< \overline{A,a_1a_2\ldots a_k} + \sum_{j=k+1}^{s} (d-1)d^{-s} + d^{-s} = \overline{A,a_1a_2\ldots a_k} + d^{-k} = x.$$

Таким образом, мы доказали, что неединственность d-ичной записи возможна только в случае, указанном в формуле (4).

Перейдём к доказательству существования. Будем последовательно определять цифры a_j так, чтобы отрезок в лемме 8.3 содержал точку x.

Во-первых, выберем A так, чтобы $A \leqslant x \leqslant A+1$. Действительно, по аксиоме Архимеда существуют натуральные числа $C > x$ и $D \geqslant -x$. Покажем, что такое A есть среди чисел $-D, -D+1, \ldots, C-1, C$. Пусть это не так. Раз $A = -D$ не удовлетворяет неравенству $A \leqslant x \leqslant A+1$, но при этом $-D \leqslant x$, мы получаем, что $-D+1 < x$. Рассматривая $A = -D+1$, аналогично заключаем, что $-D+2 < x$. Продолжая по индукции, мы придём к тому, что $C < x$, что противоречит выбору C.

На каждом следующем шаге будем поступать так: пусть число $y_k = \overline{A, a_1\ldots a_k}$ уже построено. Тогда отрезок из леммы 8.3 для этой записи имеет вид $[y_k, y_k + d^{-k}]$. С другой стороны, рассмотрим d записей $\overline{A, a_1\ldots a_k r}$, где $r = 0, 1, \ldots, d-1$: для них аналогичные отрезки имеют вид $[y_k + rd^{-k-1}, y_k + (r+1)d^{-k-1}]$. Эти отрезки образуют покрытие отрезка $[y_k, y_k + d^{-k}]$, а значит, можно выбрать цифру r таким образом, что справедливо $x \in [y_k + rd^{-k-1}, y_k + (r+1)d^{-k-1}]$. Соответствующее r мы и обозначим a_{k+1}.

Остаётся проверить, что так построенная d-ичная запись $\overline{A, a_1a_2\ldots}$ действительно равна x. Для этого достаточно заметить, что y_k — её частичные суммы, и по построению $x - d^{-k} \leqslant y_k \leqslant x$. Рассуждая так же, как при доказательстве равенства (4), заключаем, что $\lim\limits_{n\to\infty} y_k = x$.

8.5. Построение действительных чисел как d-ичных записей

В этой, заключительной, части мы попробуем разобрать конструкцию множества действительных чисел, основанную на d-ичных дробях. Это не самый естественный способ: представьте себе, что множество натуральных чисел определяется как множество конечных последовательностей из элементов $\{0, 1, \dots, d-1\}$ при каком-нибудь фиксированном d, причём две последовательности складываются или умножаются по известным алгоритмам «в столбик». Тогда сразу возникают вопросы:

(1) почему такое странное определение даёт интересный объект;

(2) почему определения при разных d дают в каком-то смысле «одно и то же».

Те же проблемы возникают и для такого определения действительных чисел. Мы здесь на этих вопросах не останавливаемся, они будут изучаться в курсах математического анализа и топологии.

Итак, рассмотрим множество записей вида $\overline{A,a_1a_2\dots}$, где $A \in \mathbb{Z}$, $a_j \in \{0, 1, \dots, d-1\}$. При этом можно запретить хвосты девяток, но для дальнейшего будет удобнее объявить, что пары записей из формулы (4) эквивалентны друг другу. Множество классов эквивалентности и будет нашим множеством $\mathbb{R}$.

Следующий шаг — надо объяснить, как определяются операции сложения и умножения, а также отношение «меньше». С последним проще всего: чтобы установить, что $x < y$, надо, во-первых, проверить, что $x \neq y$, а во-вторых, взять записи $x = \overline{A,a_1\dots}$ и $y = \overline{B,b_1\dots}$ и сравнивать их слева направо (сначала A и B, потом a_1 и b_1 и т.д.), пока не найдём первый различающийся разряд: в нём должно быть $a_j < b_j$.

Нужно только проверить, что результат не зависит от того, какие именно записи мы выбираем из класса x или y. Пусть мы сравниваем одну и ту же запись $x = \overline{A,a_1\dots}$ с записями $y = \overline{B,b_1\dots b_k99\dots} = \overline{B,b_1\dots b_{k-1}(b_k+1)00\dots}$. Если первое различие наблюдается при $j < k$, то разницы нет. Посмотрим теперь на k-й разряд. Здесь есть два случая, требующих рассмотрения: $a_k = b_k$ и $a_k = b_k+1$. Пусть $a_k = b_k$. Тогда для второй записи (а мы предполагаем, что $x \neq y$) вердикт однозначен: $x < y$, а для первой надо продолжать сравнивать a_{k+1} с 9, a_{k+2} с 9 и так далее. Рано или поздно нам встретится $a_{k+s} < 9$ (иначе $x = y$), а тогда $x < y$ и для этой записи. Второй случай $a_k = b_k + 1$ полностью аналогичен.

Определим теперь операцию сложения. Это делается с помощью сложения конечных приближений. А именно, для

$$x = \overline{A,a_1a_2\dots} \text{ и } y = \overline{B,b_1b_2\dots}$$

определим конечные приближения

$$x_n = \overline{A,a_1\dots a_n} \text{ и } y_n = \overline{B,b_1\dots b_n}.$$

Это d-ично-рациональные числа, поэтому их сумма снова будет d-ично рациональным числом: $z_n = x_n + y_n = \overline{C^{(n)},c_1^{(n)}c_2^{(n)}\dots c_n^{(n)}}$. Покажем, что с ростом n цифры в записях z_n стабилизируются, то есть что существует такое N_i, что при всех $n \geqslant N_i$ цифра $c_i^{(n)}$ одна и та же: $c_i^{(n)} = c_i$; тогда мы сможем по определению положить $x + y = \overline{C,c_1c_2\dots}$.

Заметим, что последовательность z_n неубывающая и ограниченная сверху (например, числом $A+B+2$). Тогда целочисленная последовательность $C^{(n)} = [z_n]$ тоже неубывающая и ограниченная сверху, а потому она стабилизируется: $C^{(n)} = C$ при всех $n \geqslant N_0$. Рассмотрим теперь последовательность $c_1^{(n)}$ при $n \geqslant N_0$. Нетрудно заметить, что $c_1^{(n)} = [d(z_n - C)]$, поэтому при $n \geqslant N_0$ эта последовательность также неубывает и ограничена сверху числом $d-1$. Значит, она стабилизируется: $c_1^{(n)} = c_1$ при $n \geqslant N_1$ (мы считаем $N_1 \geqslant N_0$). Тогда при $n \geqslant N_1$ имеем $c_2^{(n)} = [d^2(z_n - \overline{C,c_1})]$, это снова невозрастающая последовательность цифр, которая также стабилизируется при $n \geqslant N_2$ и так далее.

На самом деле в этом определении есть ещё один неясный момент: некоторые записи мы считаем эквивалентными, поэтому если бы выбор разных записей приводил к разным результатам, сложение не было бы корректно определено.

Итак, рассмотрим два сложения:

$$\overline{A,a_1\ldots a_{k-1}(a_k+1)00\ldots} + \overline{B,b_1b_2\ldots} = \overline{C,c_1c_2\ldots},$$
$$\overline{A,a_1\ldots a_{k-1}a_k(d-1)(d-1)\ldots} + \overline{B,b_1b_2\ldots} = \overline{C',c'_1c'_2\ldots},$$

и докажем, что результаты будут эквивалентными записями.

Обозначим конечные дроби для слагаемых в первой формуле x_n и y_n, а для слагаемых во второй формуле — x'_n и y_n. Тогда $x_n = x'_n + d^{-n}$ и потому $z_n = z'_n + d^{-n}$. Зафиксируем $k \in \mathbb{N}$ и будем смотреть на первые k цифр после запятой. Как мы обсуждали выше, их значения определяются тем, в какой полуинтервал[4] вида $[p/d^k, (p+1)/d^k)$ попадут z_n и z'_n. Поскольку первые k разрядов в записях z_n и z'_n стабилизируются, мы можем взять $n > k$ настолько большое, что первые k разрядов z_n — это $\overline{C,c_1\ldots c_k}$, а для z'_n это $\overline{C',c'_1\ldots c'_k}$. Так как $|z_n - z'_n|$ меньше длины полуинтервала, числа z_n и z'_n попадают либо в один и тот же интервал, либо в соседние. Итак, либо $\overline{C,c_1\ldots c_k} = \overline{C',c'_1\ldots c'_k}$, либо $\overline{C,c_1\ldots c_k} = \overline{C',c'_1\ldots c'_k} + d^{-k}$.

Посмотрим теперь, какой из этих двух случаев имеет место для различных k. Ясно, что если для какого-то $k = k_0$ имеет место первый случай, то он же имеет место и при всех $k < k_0$. Значит, есть две возможности: либо первый случай имеет место при всех k (и тогда записи результатов совпадают), либо для некоторого n первый случай имеет место при $k < n$, а второй при $k \geqslant n$. Итак, $C = C'$, $c_1 = c'_1, \ldots, c_{n-1} = c'_{n-1}$, $c_n = c'_n + 1$. Чему могут равняться c_{n+1} и c'_{n+1}? Заметим, что

$$\begin{aligned} d^{-(n+1)} = \overline{C,c_1\ldots c_{n+1}} - \overline{C',c'_1\ldots c'_{n+1}} = \\ = \overline{C,c_1\ldots c_n} - \overline{C',c'_1\ldots c'_n} + d^{-(n+1)}(c_{n+1} - c'_{n+1}) = \\ = d^{-(n+1)}(d + c_{n+1} - c'_{n+1}), \end{aligned}$$

поэтому $c'_{n+1} - c_{n+1} = d-1$, а поскольку это цифры, $c'_{n+1} = d-1$, $c_{n+1} = 0$. Продолжая те же рассуждения, получим, что $c'_j = d-1$, $c_j = 0$ при всех $j > n$, то есть записи $\overline{C,c_1c_2\ldots}$ и $\overline{C',c'_1c'_2\ldots}$ эквивалентны друг другу.

[4] Как видно из доказательства леммы 8.3, правое неравенство в формулировке на самом деле строгое.

Отметим, что при сложении дробей сложения может получиться как результат с хвостом нулей, так и с хвостом девяток. Запрет одной из этих дробей заставил бы нас усложнить определение сложения: нужно было бы добавить, что при получении «запрещённой» дроби в сумме она заменяется на эквивалентную «правильную». Соответственно, при доказательстве свойств сложения пришлось бы особо рассматривать случаи, когда делается такая корректировка.

Определение умножения даётся аналогично, если сомножители неотрицательны: рассматривается последовательность $z_n = x_n y_n$, которая неубывает, а потому разряды в записях z_n стабилизируются. Корректность определения также доказывается похожим образом.

Если же один или оба сомножителя отрицательны, умножение определяется более сложным образом: нужно найти записи абсолютных величин, их перемножить, дописать к результату правильный знак, после чего при необходимости обратно занести этот знак в целую часть, например:

$$(-3),4336\ldots \cdot 2,1083\ldots = (-2,5663\ldots)\cdot 2,1083\ldots = \\ = -(2,5663\ldots \cdot 2,1083\ldots) = -(5,410\ldots) = (-6),589\ldots .$$

Упражнение 8.9. *Пусть $\alpha = \overline{A,a_1a_2\ldots}$. Решите уравнение $x+\alpha = 0$ (то есть найдите запись для $-\alpha$).*

Итак, мы построили множество действительных чисел: само множество (множество классов эквивалентности бесконечных d-ичных дробей), операции сложения и умножения и отношение сравнения на этом множестве.

Дальше при полноценном построении нам пришлось бы доказывать разные свойства этих операций: коммутативность (очевидно), ассоциативность (требует работы) и другие. Или, например, существование числа $1/x$ (ещё сложнее). Мы остановимся лишь на аксиоме Архимеда и аксиоме полноты.

Аксиома Архимеда здесь очевидна:

$$\overline{A,a_1\ldots} \leqslant A+1 = \overline{(A+1),000\ldots}.$$

Проверим аксиому полноты. Пусть $x_n = \overline{A^{(n)},a_1^{(n)}a_2^{(n)}\ldots}$ — неубывающая последовательность, ограниченная сверху каким-то числом. По аксиоме Архимеда можно вместо него взять натуральное M. Будем также считать, что x_n записаны без хвостов девяток. Тогда $A^{(n)}$ — неубывающая последовательность целых чисел, ограниченная сверху целым числом M. Но такая последовательность должна стабилизироваться (возможно не более $M - A^{(1)}$ мест, где она меняется). Пусть $A^{(n_0)} = B$ — стабилизировавшееся значение. Посмотрим теперь на следующий разряд $a_1^{(n)}$ при $n \geqslant n_0$. Это снова неубывающая последовательность, не превосходящая $d-1$, а потому она стабилизируется на $a_1^{(n_1)} = b_1$. Теперь смотрим на $a_2^{(n)}$ при $n \geqslant n_1$ и т. д. Остаётся показать, что число $x = \overline{B,b_1\ldots}$ представляет собой предел последовательности (x_n).

Во-первых, $x \geqslant x_n$. Действительно, у всех x_n с $n < n_0$ целая часть меньше B (и про них всё доказано), а у всех с $n \geqslant n_0$ она равна B. Теперь при $n_0 \leqslant n < n_1$ имеем $a_1^{(n)} < b_1$

(и всё доказано), а дальше они равны и мы смотрим на b_2 и т.д. Таким образом, при сравнении x и x_n никакой разряд не может быть первым, где сравнение цифр дало бы «не тот» результат.

Теперь нужно доказать, что любое $y < x$ будет меньше какого-то x_n. Но действительно, рассмотрим тот разряд, где запись $y = \overline{C, c_1 \dots}$ отличается от $\overline{B, b_1 \dots}$: $c_k < b_k$. Тогда при $n \geqslant n_k$ верно, что $x_n = \overline{B, b_1 \dots b_k *}$, а тогда $x_k \geqslant y$. Остаётся рассмотреть случай $x_n = y$ (в этом случае для y взята запись с хвостом девяток, а для x_n с хвостом нулей), причём это так при всех $n \geqslant n_k$. Значит, все члены последовательности x_n одинаковы, начиная с x_{n_k}, а тогда и x имеет ту же самую запись, то есть $y = x$. Аксиома полноты доказана.

8.6. Литература для дальнейшего изучения

• *Курант Р., Робинс Г.*, Что такое математика? (3-е издание) — Москва, МЦНМО, 2001.

• *Фомин С.В.*, Системы счисления (Выпуск 40 из серии «Популярные лекции по математике») — Москва, Физматгиз, 1987.

Действительные числа

Задачи семинаров

8.1. Основные задачи

Задача 8.1. (Т) Найдите d-ичные записи чисел 15, 125 и 2749, если

а) $d = 2$;

б) $d = 3$;

в) $d = 5$;

г) $d = 7$;

д) $d = 11$.

Задача 8.2. (Т) Найдите 99-ю цифру после запятой в десятичной записи числа $5/7$.

Определение 8.4. Бесконечная d-ичная дробь называется *периодической*, если существуют такие $k, l \in \mathbb{N}$, что при всех натуральных $m > k$ выполняется условие $a_{m+l} = a_m$. Если k — минимальный такой индекс, то последовательность цифр $\alpha_1 \dots \alpha_k$ называется *предпериодом дроби*, а $\alpha_{k+1} \dots \alpha_{k+l}$ — *периодом дроби*.

Обозначение. $\pm A{,}\alpha_1\alpha_2 \dots \alpha_k(\alpha_{k+1} \dots \alpha_{k+l})$.

Задача 8.3. а) Докажите, что d-ичной дроби $0,(\beta_1 \dots \beta_m)$ соответствует число $\dfrac{\overline{\beta_1 \dots \beta_m}}{d^m - 1}$.

б) Найдите число, соответствующее d-ичной дроби $A, \alpha_1 \dots \alpha_{k-1}(\beta_1 \dots \beta_m)$.

Задача 8.4. (С) Докажите, что:

а) всякая периодическая d-ичная дробь задаёт рациональное число;

б) всякое рациональное число задаётся периодической d-ичной дробью.

Задача 8.5. (Т) Найдите d-ичные записи чисел $1/7$ и $1/17$, если

а) $d = 2$;

б) $d = 3$;

в) $d = 5$;

г) $d = 7$;

д) $d = 11$.

Задача 8.6. Пусть $k, n \in \mathbb{N}$. Докажите, что сумма длин предпериода и минимального периода дроби k/n не больше n.

Задача 8.7. Минимальный период дроби $1/n$ начинается «сразу после запятой» и имеет длину t. Докажите, что t — минимальное целое число, для которого $10^t - 1$ делится на n.

Задача 8.8. При каких натуральных n десятичная дробь $1/n$

а) является конечной;

б) не имеет предпериода?

Задача 8.9. Пусть натуральные числа k и n взаимно просты. Докажите, что минимальные периоды у k/n и $1/n$ имеют одинаковую длину.

Задача 8.10. Докажите, что множество всех точек отрезка $[0, 1]$ равномощно множеству всех бесконечных последовательностей нулей и единиц (а значит, несчётно).

Движения плоскости и векторы

Теоретический материал

9.1. Векторы как класс эквивалентности

Разговор о векторах мы начнём с напоминания «школьного» определения.

• *Вектор* (а точнее, *закреплённый вектор*) — это направленный отрезок. Каждый вектор определяется упорядоченной парой точек A и B — его *началом* и *концом* соответственно.

Обозначения. Вектор с началом в точке A и концом в точке B обозначается как $\overrightarrow{AB}$. С данным определением также ассоциированны понятия *направления* и *длины (модуля)* вектора, обозначаемой как $|AB|$.

• Векторы, имеющие одинаковые направление, называются *сонаправленными*, а имеющие противоположное – *противоположно направленными*.

• Два отличных от нуля вектора, которые находятся на одной прямой или параллельных прямых, называются *коллинеарными* векторами. Таким образом, коллинеарные векторы либо сонаправлены, либо противоположно направлены.

Как известно из школьного курса математики, векторы, начинающиеся в разных точках, но имеющие одинаковые направление и длину, считаются равными. Для того, чтобы это формализовать, удобно воспользоваться понятием *отношения эквивалентности* (см. раздел 2.4). В упражнении 2.8 мы видели, что векторы можно задавать как классы эквивалентности направленных отрезков. Приведём это определение здесь.

Определение 9.1. Введём отношение эквивалентности на множестве закреплённых векторов: назовём $\overrightarrow{AB}$ и $\overrightarrow{CD}$ эквивалентными, если они коллинеарны, имеют одинаковые направления и $|AB| = |CD|$. Классы эквивалентности по этому отношению называются *(свободными) векторами*.

Замечание. В разговорной речи большой разницы между закреплёнными и свободными векторами обычно не делается: и те, и другие называют просто векторами. Запись вида $\overrightarrow{AB}$ подразумевает наличие начала и конца, то есть речь идёт о закреплённом векторе. Что же касается свободных векторов, то их чаще всего обозначают строчными латинскими буквами: $\overrightarrow{u}$, $\overrightarrow{v}$, $\overrightarrow{w}$ и так далее.

9.2. Операции над векторами

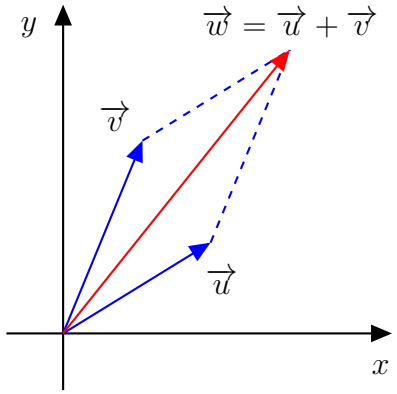
Вспомним базовые операции с векторами: их можно складывать и умножать на числа. Нам потребуется следующее определение:

Определение 9.2. Если точка A является началом какого-либо вектора $\overrightarrow{v}$, то говорят, что вектор $\overrightarrow{v}$ отложен от точки A.

Замечание. Когда мы откладываем вектор $\overrightarrow{v}$ от точки A, с точки зрения введённого в определении 9.1 отношения эквивалентности это означает, что мы выбираем представителя в классе эквивалентности $\overrightarrow{v}$. Если точка A для вектора $\overrightarrow{v}$ явно не задана, то по умолчанию можно считать, что он отложен от начала координат.

Теперь мы можем определить сумму векторов:

• Чтобы прибавить к вектору $\overrightarrow{u}$ вектор $\overrightarrow{v}$, нужно отложить вектор $\overrightarrow{v}$ от концевой точки вектора $\overrightarrow{u}$. Тогда вектором суммы будет вектор $\overrightarrow{w}$, проведённый от начала вектора $\overrightarrow{u}$ к концу вектора $\overrightarrow{v}$.



• Результат умножения вектора $\overrightarrow{v}$ на число $\lambda > 0$ — это вектор $\lambda\overrightarrow{v}$, сонаправленный вектору $\overrightarrow{v}$ и равный по модулю $|\lambda| \cdot |\overrightarrow{v}|$. Если же $\lambda < 0$, то вектор $\lambda\overrightarrow{v}$ является противоположно направленным по отношению к вектору $\overrightarrow{v}$, но всё так же равным по модулю $|\lambda| \cdot |\overrightarrow{v}|$.

• Чтобы вычесть из вектора $\overrightarrow{u}$ вектор $\overrightarrow{v}$, нужно прибавить к $\overrightarrow{u}$ вектор $(-1) \cdot \overrightarrow{v}$.

9.3. Базис на плоскости

Как мы увидели в предыдущем разделе, вектор на плоскости может быть представлен в виде суммы двух других векторов. Оказывается, если мы возьмём любые два неколлинеарных вектора, то каждый вектор можно выразить как их сумму с некоторыми числовыми коэффициентами. Сумма векторов с ненулевыми числовыми коэффициентами называется их *линейной комбинацией*.

Как вы узнаете позднее из курса линейной алгебры, аналог этого утверждения выполняется не только на плоскости, но и в трёхмерном, четырёхмерном и, более общо, n-мерном пространстве с той лишь разницей, что нам необходимо выбрать такое количество векторов, какова размерность рассматриваемого пространства. Но сейчас для простоты мы сосредоточимся на случае двумерного пространства — плоскости.

• *Базисом* называется множество таких векторов, что любой вектор может быть единственным образом представлен в виде линейной комбинации векторов из этого множества.

• Допустим, мы обозначили базисные вектора через $\overrightarrow{u}$ и $\overrightarrow{v}$. Тогда для любого вектора $\overrightarrow{x}$ в его представлении через базис $\overrightarrow{w} = a\overrightarrow{u} + b\overrightarrow{v}$ коэффициенты a и b называются *координатами* вектора $\overrightarrow{w}$ в базисе $\{\overrightarrow{u}, \overrightarrow{v}\}$.

Поймём на примере обычной координатной плоскости, что на самом деле мы уже знакомы с одним примером базиса. Действительно, координаты произвольной точки M в декартовой системе координат есть ни что иное, как координаты вектора с началом в точке $(0, 0)$ и концом в точке M в базисе из единичных векторов на осях Ox и Oy.

Обозначение. Если обозначить единичные векторы на осях Ox и Oy как $\overrightarrow{x}$ и $\overrightarrow{y}$ соотвественно, то для краткости вектор $\overrightarrow{v} = a\overrightarrow{x} + b\overrightarrow{y}$ с координатами a и b мы будем записывать как $\overrightarrow{v} = (a, b)$.

Пример 9.1. Пусть даны векторы $\overrightarrow{u} = (1, 1)$, $\overrightarrow{v} = (1, -1)$. Тогда вектор $\overrightarrow{w} = (5, 7)$ можно выразить в виде их линейной комбинации: $\overrightarrow{w} = 6\overrightarrow{u} - \overrightarrow{v}$. Да и вообще, какими бы ни были числа $a, b \in \mathbb{R}$, вектор (a, b) выражается через $\overrightarrow{u}$ и $\overrightarrow{v}$:

$$(a, b) = \frac{a+b}{2} \cdot \overrightarrow{u} + \frac{a-b}{2} \cdot \overrightarrow{v},$$

причём это представление единственно. Значит, набор $\{\overrightarrow{u}, \overrightarrow{v}\}$ является базисом.

Упражнение 9.1. *Докажите, что любые два неколлинеарных вектора образуют базис на плоскости.*

Упражнение 9.2. *Пусть на плоскости заданы векторы $\overrightarrow{u} = (2, 3)$ и $\overrightarrow{v} = (1, 5)$. Вычислите координаты вектора $\overrightarrow{w}$ в базисе $\{\overrightarrow{u}, \overrightarrow{v}\}$, если:*

а) $\overrightarrow{w} = (2, 10)$;
б) $\overrightarrow{w} = (0, -7)$;
в) $\overrightarrow{w} = (1, 1)$.

9.4. Преобразования плоскости, движения и их свойства

Пусть α — плоскость. Воспользовавшись понятиями *отображения* (раздел 2.5) и *биекции* (раздел 2.6), мы можем определить её *преобразование* следующим образом.

Определение 9.3. Биективное отображение $f : \alpha \to \alpha$ называется преобразованием плоскости.

Мы также можем определить *движения* плоскости.

Определение 9.4. Преобразование плоскости $f : \alpha \to \alpha$ называется движением, если для любых точек A и B расстояние между ними равно расстоянию между их образами $f(A)$ и $f(B)$.

Простейшим примером движения является *тождественное отображение* id, оставляющее каждую точку плоскости на месте. Более содержательные примеры будут освещены в следующем разделе.

Упражнение 9.3. *Докажите, что движение сохраняет углы.*

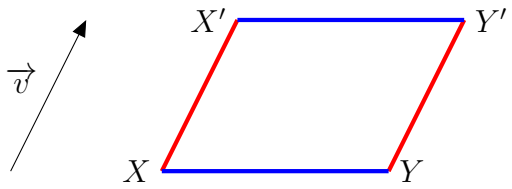
Упражнение 9.4. *Докажите, что прямые при движениях переходят в прямые.*

9.5. Виды движений: параллельный перенос, осевая симметрия, поворот

В данном разделе мы поговорим о разных видах движений.

• *Параллельным переносом* $T_{\overrightarrow{v}}$ на вектор $\overrightarrow{v}$ называется движение, при котором каждая точка X отображается в такую точку X', что вектор $\overrightarrow{XX'}$ равен вектору $\overrightarrow{v}$.

Давайте проверим корректность этого определения и покажем, что параллельный перенос действительно является движением. Рассмотрим две произвольные точки X и Y, образы которых мы обозначим как X' и Y' соответственно. Нужно показать, что $XY = X'Y'$. Действительно, так как $\overrightarrow{XX'} = \overrightarrow{v} = \overrightarrow{YY'}$, то $XX' = YY'$ и $XX' \parallel YY'$. Следовательно, $XYY'X'$ — параллелограмм, а значит, $XY = X'Y'$.



• *Осевая симметрия* S_l с осью l — это движение, переводящее каждую точку X в такую точку X', что прямая l является серединным перпендикуляром к отрезку XX'.

• *Поворотом* $R_{O,\phi}$ около точки O на угол ϕ называется движение, оставляющее точку O на месте и переводящее каждую точку $X \neq O$ в такую точку X', что $OX = OX'$ и $\angle XOX' = \phi$.

• Важным частным случаем поворота является *центральная симметрия* S_O относительно точки O — поворот на угол $\phi = 180°$ около точки O.

Упражнение 9.5. *Покажите, что осевая симметрия и поворот действительно являются движениями.*

9.6. Композиции движений

Как мы видели в разделе 2.7, отображения (а следовательно, и движения) можно применять последовательно. Таким образом, мы рассматриваем их *композицию*.

Пример 9.2. Давайте покажем, что композиция $S_l \circ S_l$ осевой симметрии S_l самой с собой — это тождественное отображение. Действительно, если при единичном применении осевой симметрии точка X перешла в точку X' такую, что прямая l является серединным перпендикуляром к отрезку XX', то при повторном применении S_l для точки X' такой точкой станет точка X. Таким образом, мы показали, что $S_l \circ S_l = \mathrm{id}$.

Пример 9.3. Теперь покажем, что композиция двух параллельных переносов $T_{\overrightarrow{u}}$ и $T_{\overrightarrow{v}}$ есть параллельный перенос $T_{\overrightarrow{u}+\overrightarrow{v}}$ на сумму векторов $\overrightarrow{u} + \overrightarrow{v}$. Пусть точка X под действием $T_{\overrightarrow{u}}$ отобразилась в точку X', а точка X' под действием $T_{\overrightarrow{v}}$ — в точку X''. По определению движения $\overrightarrow{XX'} = \overrightarrow{u}$ и $\overrightarrow{X'X''} = \overrightarrow{v}$, но тогда по определению суммы векторов $\overrightarrow{XX''} = \overrightarrow{u} + \overrightarrow{v}$. Таким образом, мы показали, что $T_{\overrightarrow{v}} \circ T_{\overrightarrow{u}} = T_{\overrightarrow{u}+\overrightarrow{v}}$.

• Важным примером движения плоскости, полученого как композиция других, является *скользящая симметрия*. Скользящей симметрией называют композицию симметрии относительно некоторой прямой l и параллельного переноса на вектор, параллельный l (если этот вектор нулевой, то мы получаем частный случай осевой симметрии).

Упражнение 9.6. *а) Пусть S_O — центральная симметрия, X и Y — произвольные точки плоскости, $X' = S_O(X)$ и $Y' = S_O(Y)$ — их образы при симметрии. Как связаны между собой векторы $\overrightarrow{XY}$ и $\overrightarrow{X'Y'}$?*

б) Убедитесь в том, что композиция двух центральных симметрий представляет собой параллельный перенос. Как найти вектор переноса?

Упражнение 9.7. *Даны повороты R_{φ,O_1} и $R_{-\varphi,O_2}$, для которых $O_1 \neq O_2$. Найдите композицию $R_{-\varphi,O_2} \circ R_{\varphi,O_1}$ этих поворотов.*

Упражнение 9.8. *Даны повороты R_{φ_1,O_1} и R_{φ_2,O_2}, для которых $\varphi_1 + \varphi_2 \neq 0$.*

а) покажите, что композиция $R_{\varphi_2,O_2} \circ R_{\varphi_1,O_1}$ есть поворот $R_{\varphi_1+\varphi_2,O}$ на угол $\varphi_1+\varphi_2$ относительно некоторой точки O;

б) постройте эту точку O с помощью циркуля и линейки по точкам O_1, O_2 и углам φ_1, φ_2.

9.7. Движение как образ трёх точек общего положения

Попытаемся понять, образы скольких точек нам нужно знать для того, чтобы однозначно восстановить по ним исходное движение.

Упражнение 9.9. *Покажите, что существует как минимум два различных движения, для которых совпадают*

а) образы данной точки A;

б) образы двух данных точек A и B.

Упражнение 9.10. *Пусть точки A, B и C не лежат на одной прямой. Докажите, что если образы этих точек при движениях f и g совпадают, то f=g, то есть для любой точки D выполнено равенство $f(D) = g(D)$.*

Следствием этих двух упражнений является следующее утверждение.

Лемма 9.5. *Образы трёх точек, не лежащих на одной прямой, задают движение однозначно.*

9.8. Теорема Шаля

Рассмотрев композиции разных типов движений, мы получили лишь одно новое движение: скользящую симметрию. Возникает естественный вопрос: а какие вообще бывают движения? Ответ даётся следующей теоремой.

Теорема 9.6. [Теорема Шаля.] *Всякое движение плоскости есть либо:*

-тождественное преобразование id*;*
-параллельный перенос $T_{\overrightarrow{v}}$ *на ненулевой вектор* $\overrightarrow{v}$*;*
-поворот на ненулевой угол $R_{\phi,O}$*,* $\phi \neq 0$*;*
-осевая симметрия S_l *с осью* l*;*
-скользящая симметрия $T_{\overrightarrow{v}} \circ S_l$*.*

Идея доказательства. Рассмотрим два равных треугольника ABC и $A'B'C'$, каким-то образом расположенные на плоскости. Как мы знаем из леммы 9.5, они однозначно задают движение, переводящее треугольник ABC в $A'B'C'$. Посмотрим, какой набор движений, композиция которых переведёт вершины одного треугольника в соответствующие вершины другого, мы можем получить. Для этого нам потребуется параллельный перенос на AA' (точка A переходит в A') и поворот с центром A так, чтобы точка B совместилась с B'. Далее возможны два случая: либо точки C и C' совпадут (и тогда мы получили движение), либо для их совпадения необходимо выполнить еще осевую симметрию относительно $A'B'$. В зависимости от того, какие именно движения нам понадобились, мы получаем в результате их композиции те варианты, что были указаны в формулировке теоремы.

Движения плоскости и векторы

Задачи семинаров

Задача 9.1. Докажите, что движение, сохраняющее направления лучей, — это параллельный перенос, либо тождественное преобразование.

Задача 9.2. Дан треугольник ABC.

а) Найдите все точки K на прямой AB такие, что $AK : KB = 2 : 7$.

б) Для каждой такой точки K выразите вектор $\overrightarrow{CK}$ через векторы $\overrightarrow{CA}$ и $\overrightarrow{CB}$.

Задача 9.3. В треугольнике ABC известны стороны: $BC = a$, $CA = b$, $AB = c$; кроме того, точка I — центр вписанной окружности.

а) Докажите, что $a\overrightarrow{IA} + b\overrightarrow{IB} + c\overrightarrow{IC} = 0$.

б) Докажите, что если $a\overrightarrow{JA} + b\overrightarrow{JB} + c\overrightarrow{JC} = 0$, то $J = I$.

в) Докажите, что для произвольной точки X справедливо

$$\overrightarrow{XI} = \frac{a\overrightarrow{XA} + b\overrightarrow{XB} + c\overrightarrow{XC}}{a + b + c}\,.$$

Задача 9.4. Преобразованием какого типа может являться композиция двух скользящих симметрий? Какой из типов реализуется при каких условиях на взаимное расположение осей исходных симметрий?

Задача 9.5. Пусть ABC — равнобедренный прямоугольный треугольник с гипотенузой BC. Дайте точное описание композиции движений $S_{CA} \circ S_{BC} \circ S_{AB}$.

Задача 9.6. На боковых сторонах AB и BC треугольника ABC построены вне его квадраты $ABMN$ и $BCPQ$. Докажите, что отрезки CM и QA перпендикулярны и равны между собой.

Задача 9.7. С помощью циркуля и линейки постройте равносторонний треугольник, одна вершина которого лежит в заданной точке A, а две другие — соответственно на двух данных окружностях.

Задача 9.8. Через две точки A и B, находящиеся по одну сторону от прямой l, при помощи циркуля и линейки проведите окружность, касающуюся этой прямой.

Задача 9.9. К какому из типов движений плоскости, указанных в теореме Шаля, относится композиция осевых симметрий $S_n \circ S_m \circ S_l$ в случае, когда

а) $n \parallel l$, $n \neq l$ и $m \perp l$;

б) $n \parallel l$, $n \neq l$ и m пересекает l.

Комплексные числа

Теоретический материал

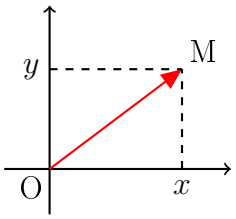
10.1. Алгебраическая форма комплексного числа

В этой главе мы займёмся построением анонсированного ранее множества комплексных чисел и изучением его свойств. Такое построение можно провести как минимум двумя способами: алгебраически, задав операции сложения и умножения на декартовом произведении $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, и геометрически, исходя из наглядных соображений о векторах. Мы пойдём геометрическим путём.

В качестве основного объекта будем рассматривать вещественную плоскость, множество точек которой мы назовём *комплексными числами* и обозначим за $\mathbb{C}$. Если зафиксировать на этой плоскости декартову систему координат Oxy, то каждая точка M будет иметь некоторые координаты (x, y), которые мы обозначим одним символом:

$$z = (x, y).$$

Запись $M(z)$ будет означать, что z — комплексная координата точки M. Её вещественные координаты x и y мы будем называть *действительной* и *мнимой* частями числа z и обозначать $\mathrm{Re}\,(z)$ и $\mathrm{Im}\,(z)$ соответственно.



Поскольку вектор $\overrightarrow{OM}$ имеет такие же координаты, как и точка M, про комплексные числа удобно думать как про векторы с началом в точке O. Введём обозначения для базисных векторов $(1, 0)$ и $(0, 1)$:

$$1 = (1, 0) \qquad \text{и} \qquad i = (0, 1).$$

Тогда комплексное число $z = (x, y)$ представимо в виде их линейной комбинации:

$$z = x \cdot (1, 0) + y \cdot (0, 1) = x \cdot 1 + y \cdot i.$$

Выражение вида $(x + iy)$, где $x, y \in \mathbb{R}$, называют *алгебраической формой* комплексного числа z.

Дадим ещё одно определение, значимость которого прояснится в дальнейшем. Число $\bar{z} = x - iy$ называется *комплексно сопряженным* к числу $z = x + iy$. Соответственно, преобразование комплексной плоскости $z \mapsto \bar{z}$, называется *комплексным сопряжением*.

Упражнение 10.1. *Является ли комплексное сопряжение движением? Если да, то что это за движение?*

10.2. Арифметика комплексных чисел

В этом разделе мы обсудим, каким образом на множестве комплексных чисел $\mathbb{C}$ определяются арифметические операции. Сложение вводится естественным образом, если мыслить комплексные числа как векторы, — по правилу параллелограмма. Именно, чтобы сложить два комплексных числа $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$, нужно соответственно сложить их действительные и мнимые части:

$$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2).$$

Аналогичным образом определяется вычитание:

$$z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2).$$

Упражнение 10.2. *Покажите, что для любого $z \in \mathbb{C}$ справедливо*

$$\operatorname{Re}(z) = \frac{z + \bar{z}}{2} \qquad \text{и} \qquad \operatorname{Im}(z) = \frac{z - \bar{z}}{2i}.$$

Умножение сначала определим для базисных векторов: 1 и i. Поскольку естественно считать, что умножение на единицу числа не изменяет, ключевым становится вводимое нами тождество $i^2 = -1$. В итоге таблица умножения принимает следующий вид:

$\cdot$	1	i
1	1	i
i	i	-1

Для остальных чисел воспользуемся дистрибутивностью умножения относительно сложения. Иначе говоря, определим умножение, пользуясь обычными правилами раскрытия скобок и приведения подобных:

$$z_1 \cdot z_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).$$

Пример 10.1. $(5 + 2i)(3 - i) = 5 \cdot 3 - 5 \cdot i + 2i \cdot 3 - 2i \cdot i = 15 - 5i + 6i + 2 = 17 - i$.

Упражнение 10.3. *Вычислите:* $i + 2i^2 + 3i^3 + \cdots + 10i^{10}$.

Для того, чтобы выяснить, как делить на ненулевое число $z \in \mathbb{C}$, нам понадобится одно нетривиальное наблюдение. Именно, если $z = x + iy$, то

$$z\bar{z} = (x + iy)(x - iy) = x^2 + y^2 \qquad \Longrightarrow \qquad \frac{1}{z} = \frac{1}{x + iy} = \frac{x - iy}{x^2 + y^2}.$$

Таким образом, деление сводится к умножению.

Пример 10.2. $\dfrac{5 + 2i}{3 - i} = \dfrac{(5 + 2i)(3 + i)}{(3 - i)(3 + i)} = \dfrac{15 + 5i + 6i - 2}{9 + 1} = \dfrac{13 + 11i}{10} = 1{,}3 + 1{,}1i.$

Упражнение 10.4. *Запишите комплексное число $w \in \mathbb{C}$ в форме $x + iy$, если*

$$w = \frac{5}{1 - \dfrac{1}{1 + i}}.$$

10.3. Тригонометрическая форма комплексного числа

Наблюдение, которым мы воспользовались в предыдущем разделе для того, чтобы определить деление, мотивирует нас охарактеризовать умножение и деление комплексных чисел с точки зрения векторов. Мы знаем, что каждый (свободный) вектор задаётся двумя параметрами: длиной и направлением. Применительно к комплексной плоскости уместно рассмотреть следующие две величины.

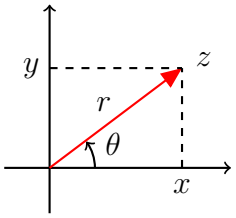
• *Модуль* комплексного числа $z = x + iy$ — это длина вектора z, то есть действительная неотрицательная величина

$$|z| = \sqrt{x^2 + y^2}.$$

• *Аргумент* ненулевого комплексного числа z — это угол θ между положительным направлением оси Ox и вектором z:

$$\arg(z) = \theta.$$

Очевидно, что аргумент комплексного числа определен не однозначно, а с точностью до 2π.[5] Удобно брать значения $\theta \in [0; 2\pi)$.



Пусть r и θ обозначают модуль и аргумент ненулевого комплексного числа $z = x+iy$ соответственно. Тогда число z можно записать, используя *полярные координаты* (r, θ):

$$z = r(\cos\theta + i\sin\theta).$$

Такая форма записи называется *тригонометрической формой* комплексного числа.

Упражнение 10.5. *Пусть $z = x + iy \neq 0$. Выразите модуль r и аргумент θ числа z через x и y.*

Оказывается, тригонометрическая форма комплексного числа гораздо лучше подходит для того, чтобы выполнять операции умножения и деления. В самом деле, пусть даны два комплексных числа

$$z_1 = r_1(\cos\alpha_1 + i\sin\alpha_1) \qquad \text{и} \qquad z_2 = r_2(\cos\alpha_2 + i\sin\alpha_2).$$

[5] С формальной точки зрения нужно ввести на множестве $\mathbb{R}$ отношение эквивалентности: $a \sim b$, если разность $(a - b)$ представима в виде $2\pi k$, для некоторого $k \in \mathbb{Z}$. Тогда аргумент — это класс эквивалентности по такому отношению.

Вычислим их произведение:

$$z_1 \cdot z_2 = \big(r_1(\cos\alpha_1 + i\sin\alpha_1)\big)\big(r_2(\cos\alpha_2 + i\sin\alpha_2)\big) = \\ = r_1 \cdot r_2\big((\cos\alpha_1\cos\alpha_2 - \sin\alpha_1\sin\alpha_2) + i(\cos\alpha_1\sin\alpha_2 + \sin\alpha_1\cos\alpha_2)\big).$$

Тем самым, получаем

$$z_1 \cdot z_2 = r_1 \cdot r_2\big(\cos(\alpha_1+\alpha_2) + i\sin(\alpha_1+\alpha_2)\big).$$

Таким образом, для того, чтобы перемножить два ненулевых комплексных числа, нужно перемножить их модули, а аргументы — сложить.

Пример 10.3. Рассмотрим произведение $w = i(1+i)^2$. С одной стороны, в алгебраической форме имеем $w = i(1+2i-1) = i\cdot 2i = -2$. С другой стороны,

$$w = \left(1\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)\right)\left(\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)\right)^2 = \\ = 1\cdot\left(\sqrt{2}\right)^2\left(\cos\left(\frac{\pi}{2} + 2\cdot\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2} + 2\cdot\frac{\pi}{2}\right)\right) = 2\big(\cos\pi + i\sin\pi\big) = -2.$$

В качестве следствия получается формула для возведения в степень.

Теорема 10.1. [Формула Муавра] *Пусть r и α — модуль и аргумент ненулевого комплексного числа z соответственно. Тогда для любого $n \in \mathbb{Z}$ имеет место формула:*

$$z^n = r^n(\cos n\alpha + i\sin n\alpha).$$

Упражнение 10.6. *Докажите формулу Муавра.*

Упражнение 10.7. *Выразите $\cos 3\alpha$ и $\sin 3\alpha$ через $\cos\alpha$ и $\sin\alpha$ соответственно.*

10.4. Извлечение корня

Как мы выяснили в предыдущем разделе, возведение комплексного числа в степень в тригонометрической форме устроено очень просто. В данном разделе мы займёмся обратной операцией — извлечением корня n-ой степени для произвольного $n \in \mathbb{N}$.

Пусть $z = r(\cos\alpha + i\sin\alpha)$ и $w = \rho(\cos\theta + i\sin\theta)$ — ненулевые комплексные числа. Попробуем решить относительно z уравнение

$$z^n = w. \tag{5}$$

Для начала, воспользуемся формулой Муавра:

$$z^n = r^n(\cos n\alpha + i\sin n\alpha).$$

Следовательно,

$$\begin{cases} r^n &= \rho \\ n\alpha &= \theta + 2\pi k \end{cases} \quad \Longrightarrow \quad \begin{cases} r &= \sqrt[n]{\rho} \\ \alpha &= \dfrac{\theta + 2\pi k}{n} \end{cases}, \qquad k \in \{0, \dots n-1\}.$$

Таким образом, существует ровно n решений уравнения (5) — *корней n-ой степени* из числа w. Поскольку они могут быть вычислены по формуле

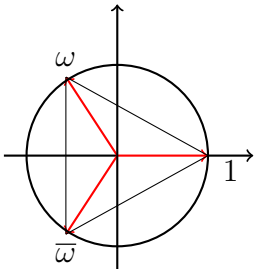
$$z_k = \sqrt[n]{\rho}\left(\cos\frac{\theta + 2\pi k}{n} + i\sin\frac{\theta + 2\pi k}{n}\right), \quad k \in \{0, \dots n-1\},$$

это означает, что корни лежат на окружности радиуса $\sqrt[n]{\rho}$ и являются вершинами правильного n-угольника, вписанного в эту окружность.

Упражнение 10.8. *а) Пусть ω_1 и ω_2 – корни n-ой степени из единицы. Докажите, что числа $\omega_1 \cdot \omega_2$ и $\dfrac{\omega_1}{\omega_2}$ также являются корнями n-ой степени из единицы.*

б) Пусть ω — фиксированный корень n-ой степени из числа $w \in \mathbb{C}$, а ε – корень n-ой степени из единицы. Докажите, что $\varepsilon \cdot \omega$ также является корнем n-ой степени из числа w.

Пример 10.4. Кубические корни из единицы удовлетворяют уравнению $z^3 = 1$. Один них равен 1. Другие два — комплексно сопряженные числа $\omega = \dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ и $\overline{\omega} = \dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$.



Упражнение 10.9. *Докажите тождество*

$$x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y).$$

10.5. Квадратные уравнения

Цель этого раздела — выяснить, как решать квадратные уравнения с комплексными коэффициентами и применима ли к ним известная со школы формула, выражающая корни квадратного уравнения через дискриминант.

Итак, пусть $a, b, c \in \mathbb{C}$, причём $a \neq 0$. Рассмотрим уравнение

$$az^2 + bz + c = 0.$$

Для того, чтобы решить его, выделим полный квадрат:

$$a\left(z+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}.$$

Как мы видим, задача сводится к извлечению квадратного корня из *дискриминанта* $D=b^2-4ac$. Согласно результатам, полученным в предыдущем разделе, при $D\neq 0$ таких корней ровно два, причём они отличаются друг от друга умножением на (-1). В самом деле, если $D=r(\cos\theta+i\sin\theta)$, то квадратные корни из D имеют вид

$$d_1=\sqrt{r}\left(\cos\frac{\theta}{2}+i\sin\frac{\theta}{2}\right)\qquad\text{и}\qquad d_2=\sqrt{r}\left(\cos\left(\frac{\theta}{2}+\pi\right)+i\sin\left(\frac{\theta}{2}+\pi\right)\right)=-d_1.$$

Поэтому, обозначая для определённости первый из них за $\sqrt{D}$, мы можем неформально утверждать, что справедлива классическая формула для корней исходного уравнения:

$$z_{1,2}=\frac{-b\pm\sqrt{D}}{2a}.$$

Таким образом, любое квадратное уравнение с комплексными коэффициентами имеет два корня, совпадающие при $D=0$.

Замечание. В вещественном случае, когда $D\in\mathbb{R}$ и $D>0$, мы обозначаем за $\sqrt{D}$ положительный корень уравнения $x^2=D$. В противоположность ему, в комплексном случае у нас нет канонического способа определить, какой из двух корней уравнения $z^2=D$ «главнее». Поэтому символ $\sqrt{D}$ традиционно обозначает **множество** всех корней из числа D и не используется в арифметических действиях.

Пример 10.5. Рассмотрим уравнение $z^2+2z+2=0$. Вычислим его дискриминант: $D=2^2-4\cdot 2=-4$. Имеется два квадратных корня из числа (-4), а именно $2i$ и $(-2i)$. Следовательно, решение исходного уравнения имеет вид

$$z_{1,2}=\frac{-2\pm 2i}{2}=-1\pm i.$$

Упражнение 10.10. *Решите следующие уравнения:*

а) $z^2+z+1=0$;

б) $z^2+(i-1)z+2-2i=0$;

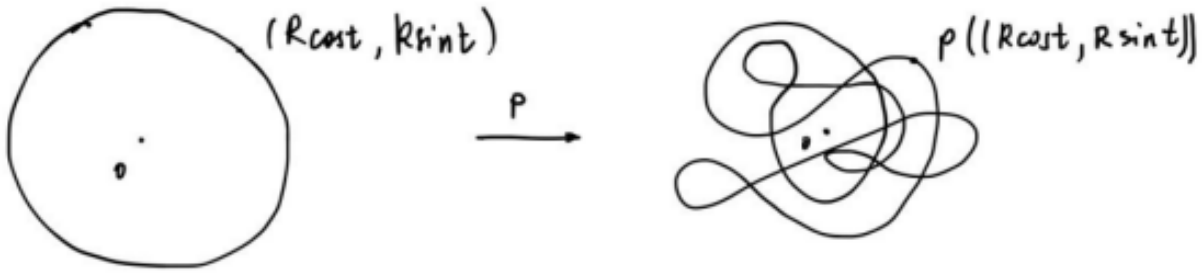
в) $z^4+4=0$.

10.6. Основная теорема алгебры

В предыдущем разделе мы убедились, что любой квадратный трёхчлен с комплексными коэффициентами имеет комплексный корень. То же самое, как было анонсировано в разделе 6.5, справедливо и для произвольного многочлена $p(z)\in\mathbb{C}[z]$.

Теорема 10.2. [Основная теорема алгебры]
Всякий многочлен $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$ с комплексными коэффициентами, степень которого $n \geqslant 1$, имеет комплексный корень.

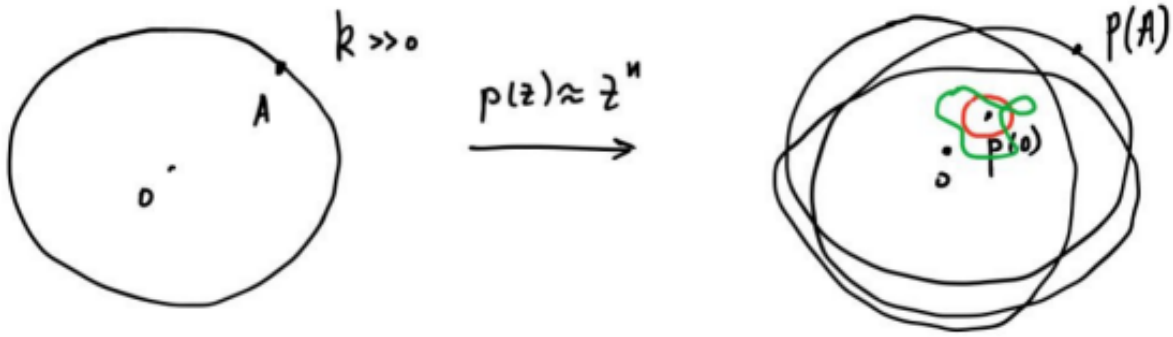
Набросок доказательства. Допустим, не существует такого $\omega \in \mathbb{C}$, что $p(\omega) = 0$. На комплексной плоскости $\mathbb{C}$ рассмотрим окружность с центром нуле радиуса R. Её образ при отображении $p : \mathbb{C} \to \mathbb{C}$ — некоторая кривая, не проходящая через ноль, то есть кривая в $\mathbb{C} \setminus \{0\}$.



Когда $R = 0$, мы получаем постоянную кривую $p(0) \neq 0$ — это точка. А когда R очень большое, $p(z)$ в первом приближении ведёт себя примерно как z^n,

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 = z^n \left(1 + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n}\right),$$

и выражение в скобках стремится к 1 при $R \to \infty$. Поэтому мы, приблизительно, получаем множество точек $\{(R^n \cos nt, R^n \sin nt) \mid t \in \mathbb{R}\}$ — это окружность радиуса R^n, намотанная сама на себя n раз.



Пока мы меняем радиус от нуля до больших значений, у нас появляется промежуточное семейство кривых (красная и зелёная кривые на рисунке). Интуитивно очевидно, что кривые при изменении R меняются непрерывно, а потому для некоторого значения R одна из этих кривых пройдет через ноль, что противоречит предположению.

Упражнение 10.11. *Разложите на линейные множители многочлен $p(z)$, если*
а) $p(z) = z^2 + 1$;
б) $p(z) = z^3 + z - 2$;
в) $p(z) = z^n - 1$.

10.7. Прямые и окружности

В этом разделе мы научимся описывать прямые и окружности, лежащие на комплексной плоскости, единым уравнением.

Рассмотрим сначала произвольную прямую l. Пусть она записывается в вещественных координатах (x, y) следующим образом:

$$\alpha x + \beta y + \gamma = 0, \qquad \alpha, \beta, \gamma \in \mathbb{R}.$$

На комплексной плоскости это множество точек соответствует таким числам z, для которых $x = \mathrm{Re}\,(z)$ и $y = \mathrm{Im}\,(z)$. Используя формулы из упражнения 10.2, выразим x и y через z и $\bar{z}$. Тогда уравнение прямой l приобретёт такой вид:

$$\alpha\frac{z+\bar{z}}{2} + \beta\frac{z-\bar{z}}{2i} + \gamma = 0;$$

или

$$\left(\frac{\alpha}{2} - i\cdot\frac{\beta}{2}\right) z + \left(\frac{\alpha}{2} + i\cdot\frac{\beta}{2}\right)\bar{z} + \gamma = 0.$$

Вводя обозначения $b = \left(\dfrac{\alpha}{2} - i\cdot\dfrac{\beta}{2}\right)$ и $c = \gamma$, получаем:

$$bz + \bar{b}\bar{z} + c = 0, \qquad b \in \mathbb{C},\ c \in \mathbb{R}.$$

Рассмотрим теперь произвольную окружность. Пусть её радиус равен R, а центр находится в точке z_0. Тогда эту окружность можно описать уравнением

$$|z - z_0| = R.$$

Перепишем это уравение в независимом от знака модуля виде, выразив через z и $\bar{z}$. Для этого сначала возведём обе части равенства в квадрат: $|z - z_0|^2 = R^2$. Следовательно, имеет место равенство

$$(z - z_0)(\bar{z} - \bar{z}_0) = R^2,$$

которое после раскрытия скобок превращается в

$$z\bar{z} - \bar{z}_0 z - z_0\bar{z} + z_0\bar{z}_0 - R^2 = 0.$$

Вводя обозначения $b = -\bar{z}_0$ и $c = z_0\bar{z}_0 - R^2$, получаем окончательно:

$$z\bar{z} + bz + \bar{b}\bar{z} + c = 0, \qquad b \in \mathbb{C},\ c \in \mathbb{R}.$$

Обобщенной окружностью на комплексной плоскости $\mathbb{C}$ называется его подмножество, являющееся прямой или окружностью. Как следует из приведённых выше рассуждений, обобщённая окружность задаётся уравнением

$$az\bar{z} + bz + \bar{b}\bar{z} + c = 0, \qquad a, c \in \mathbb{R},\ b \in \mathbb{C}.$$

Упражнение 10.12. *Изобразите на комплексной плоскости множество точек z, задаваемое условием:*

а) $\operatorname{Re} z = 3$*;*

б) $|z - 2 + i| = 3$*;*

в) $|z - i| = |z + 1|$.

Какие из указанных множеств являются обобщёнными окружностями (для них укажите канонический вид)?

10.8. Преобразования комплексной плоскости

В заключительном разделе мы обсудим, каким образом различные преобразования плоскости могут быть записаны в комплексных координатах.

Наиболее естественно начать наш небольшой обзор с движений. Напомним, что движением (комплексной) плоскости называется преобразование, сохраняющее расстояние между точками. Иными словами, если $f : \mathbb{C} \to \mathbb{C}$ — движение, то для любых точек $z, w \in \mathbb{C}$ расстояние между их образами совпадает с первоначальным:

$$|z - w| = |f(z) - f(w)|.$$

Примерами движений комплексной плоскости являются следующие преобразования:

1. *Тождественное преобразование* $\mathrm{id}_{\mathbb{C}}$*:*

$$z \mapsto z.$$

2. *Параллельный перенос* на вектор $b \in \mathbb{C}$:

$$z \mapsto z + b.$$

3. *Поворот* вокруг начала координат на угол θ:

$$z \mapsto az, \qquad a = \cos\theta + i\sin\theta.$$

4. *Симметрия* относительно оси Ox:

$$z \mapsto \bar{z}.$$

5. *Скользящая симметрия* относительно оси Ox со сдвигом на вектор $c \in \mathbb{R}$:

$$z \mapsto \bar{z} + c.$$

Упражнение 10.13. *Пусть* $z = \frac{1}{2} + i\frac{1}{2}$. *Изобразите* $-i\bar{z} - 1 + 3i$.

Другим важным преобразованием плоскости является гомотетия. *Гомотетией* с центром A и коэффициентом $k \in \mathbb{R}\setminus\{0\}$ называют преобразование плоскости, переводящее каждую точку X в точку X' такую, что $\overrightarrow{AX'} = k \cdot \overrightarrow{AX}$.

Обозначение. H_A^k.

Упражнение 10.14. *Докажите, что гомотетия*

а) переводит прямые в прямые, а окружности — в окружности;

б) сохраняет величины углов между лучами;

в) переводит треугольники в треугольники, подобные исходным с коэффициентом подобия k.

При $k = 1$ гомотетия H_A^k представляет собой тождественное преобразование, а при $k = -1$ — центральную симметрию относительно точки A. Если же $A = O$ совпадает с началом координат, то гомотетия H_O^k в комплексных координатах записывается как

$$z \mapsto kz.$$

Упражнение 10.15. *Как в комплексных координатах записывается гомотетия с центром* $A(a)$ *и коэффициентом* $k \in \mathbb{R} \setminus \{0\}$*?*

Наиболее хитрым из преобразований, которые мы бы хотели упомянуть, является инверсия, поэтому мы остановимся на ней подробнее. *Инверсией* относительно окружности с центром в точке A радиуса R называется преобразование плоскости, переводящее точку X в точку X', лежащую на луче AX и удовлетворяющую соотношению

$$|AX| \cdot |AX'| = R^2. \tag{6}$$

Выведем формулу инверсии в комплексных координатах. Пусть точка A имеет координату $a \in \mathbb{C}$, а точки X и X' — координаты z и w соответственно. Тогда мы можем записать равенство (6) следующим образом. Отрезок AX имеет длину $|a - z|$, а отрезок $|AX'|$ — длину $|a - w|$. Поэтому, пользуясь равенством $|z|^2 = z\bar{z}$, мы получим уравнение

$$(a - z)(\bar{a} - \bar{z})(a - w)(\bar{a} - \bar{w}) = R^4.$$

Теперь воспользуемся тем, что точки A, X и X' лежат на одной прямой, то есть вектора $\overrightarrow{AX}$ и $\overrightarrow{AX'}$ коллинеарны:

$$(a - z)(\bar{a} - \bar{w}) = (a - w)(\bar{a} - \bar{z}).$$

Объединяя это условие с полученным выше уравнением, имеем

$$(\bar{a} - \bar{z})(a - w) = R^2.$$

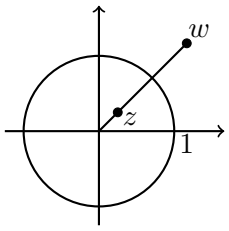
Остаётся выразить отсюда координату точки X':

$$w = \frac{R^2}{\bar{z} - \bar{a}} + a, \qquad \text{где } R \in \mathbb{R},\ a \in \mathbb{C}.$$

Таким образом, мы получили формулу инверсии.

В частности, инверсия относительно единичной окружности с центром в нуле задается совсем просто

$$z \mapsto w = \frac{1}{\bar{z}}.$$



Упражнение 10.16. *Докажите, что инверсия переводит обобщённую окружность в обобщённую окружность.*

10.9. Литература для дальнейшего изучения

• *Курант Р., Робинс Г.*, Что такое математика? (3-е издание) — Москва, МЦНМО, 2001.

• *Понарин Я.П.*, Алгебра комплексных чисел в геометрических задачах — Москва, МЦНМО, 2004.

Комплексные числа

Задачи семинаров

10.1. Тригонометрическая форма записи

Задача 10.1. (Т) Представьте в форме $x + iy$:

а) $\dfrac{1-i}{1+i}$;

б) $(1+i)^8$.

Задача 10.2. (Т) Найдите множество значений:

а) $\sqrt{-1}$;

б) $\sqrt{-i}$;

в) $\sqrt{1-i}$;

г) $\sqrt[3]{i}$.

Задача 10.3. (Т) Решите следующие уравнения:

а) $\bar{z} = z^2$;

б) $z^2 = i$;

в) $z^3 = \dfrac{1-i}{1+i}$.

Задача 10.4. Найдите тригонометрическую форму чисел

а) $\cos\alpha - i\sin\alpha$;

б) $\sin\alpha + i\cos\alpha$;

в) $1 + \cos\alpha + i\sin\alpha$.

Задача 10.5. Для натурального числа $k \in \mathbb{N}$ найдите представления $\cos k\alpha$ и $\sin k\alpha$ в виде многочленов от $\cos\alpha$ и $\sin\alpha$ соответственно.

10.2. Параллельность и перпендикулярность

Задача 10.6. Даны две различные точки $A(a)$ и $B(b)$, отличные от начала координат O. В терминах комплексных чисел a и b напишите

а) условие коллинеарности точек O, A и B;

б) условие перпендикулярности прямых OA и OB.

Задача 10.7. Напишите условие коллинеарности трёх различных точек $A(a)$, $B(b)$ и $C(c)$ в терминах комплексных чисел a, b и c.

Задача 10.8. Даны четыре различные точки $A(a)$, $B(b)$, $C(c)$ и $D(d)$. Напишите условие коллинеарности векторов $\overrightarrow{AB}$ и $\overrightarrow{CD}$.

10.3. Прямые, окружности и преобразования

Задача 10.9. Запишите в комплексных координатах уравнение

а) прямой, проходящей через точки $2i+1$ и $-4+i$;

б) окружности, с центром в точке $3+i$ и радиуса 2.

Куда данные прямая и окружность перейдут при инверсии комплексной плоскости относительно единичной окружности с центром в начале координат?

Задача 10.10. Запишите в виде функции комплексной переменной:

а) ортогональную проекцию на ось Ox;

б) симметрию относительно оси Oy;

в) поворот на угол φ относительно точки $A(a)$;

г) скользящую симметрию относительно прямой $y=3$ со сдвигом на 1 влево;

д) поворот, переводящий ось Ox в прямую $y=2x+1$;

е) симметрию относительно прямой $y=2x+1$.

10.4. Уравнения и основная теорема алгебры

Задача 10.11. (С) Пусть $\omega_0, \omega_1, \ldots, \omega_{n-1}$ — различные корни n-ой степени из единицы.

а) Чему равна сумма $\omega_0+\omega_1+\ldots+\omega_{n-1}$?

б) Чему равно произведение $\omega_0\cdot\omega_1\cdot\ldots\cdot\omega_{n-1}$?

в) Докажите, что если $\omega_0=1$, то $(1-\omega_1)(1-\omega_2)\ldots(1-\omega_{n-1})=n$.

Задача 10.12. (С) Докажите, что

а) если α — корень многочлена с вещественными коэффициентами, то $\bar{\alpha}$ — тоже корень этого многочлена;

б) каждый многочлен с вещественными коэффициентами, отличный от постоянного, можно разложить на множители первой и второй степени.

Задача 10.13. Пусть $f(z)$ — многочлен с вещественными коэффициентами, степень которого не превосходит 4. Пусть, кроме того, многочлен $f(z)$ удовлетворяет равенству $f(1+i)=f(33-i)=0$. Найдите все возможные корни этого многочлена.

Задача 10.14. Пусть $\alpha, \beta, \gamma, \delta$ — такие комлексные числа, что z является корнем уравнений

$$\alpha z^3+\beta z^2+\gamma z+\delta=0 \qquad \text{и} \qquad \beta z^3+\gamma z^2+\delta z+\alpha=0.$$

Найдите возможные значения z.

10.5. Суммирование

Задача 10.15. Вычислите:

а) $\sin x+\sin 2x+\cdots+\sin nx$;

б) $\cos x+2\cos 2x+3\cos 3x+\cdots+n\cos nx$;

в) $\sin x+C_n^1\sin 2x+C_n^2\sin 3x+\ldots+C_n^n\sin(n+1)x$.

Математический практикум

Основные задачи

Задача 11.1. Для каких пар чисел a и b из равенства $ax^2 = x + 1$ следует равенство $x^2 = x + b$?

Задача 11.2. а) Докажите, что формулы $(X \to Y)$ и $(\neg Y \to \neg X)$ эквивалентны.

б) Используя пункт а), докажите, что если квадрат натурального числа n является чётным числом, то и само число n чётно.

Задача 11.3. Высказывание $X \downarrow Y$ означает, что оба утверждения X, Y ложны. Используя только знак «$\downarrow$» и скобки, запишите высказывания, эквивалентные высказываниям $X \vee Y$ и $X \wedge Y$.

Задача 11.4. В комнате находятся 12 человек. Некоторые из них всегда лгут, а остальные всегда говорят правду. Каждый из них сделал одно утверждение.

Первый сказал: «Здесь нет ни одного честного человека».

Второй сказал: «Здесь не более одного честного человека».

Третий сказал: «Здесь не более двух честных людей».

. . . . . .

Двенадцатый сказал: «Здесь не более одиннадцати честных людей».

Сколько в комнате честных людей?

Задача 11.5. а) Сколько элементов в следующих множествах:

$$\{0\},\ \{\text{Петя}\},\ \{0, \{0\}\},\ \{x \mid \text{буква } x \text{ встречается в слове «крокодил»}\}?$$

б) Сколько в них подмножеств?

Задача 11.6. Докажите, что если $A \subset B$ и $B \subset C$, то $A \subset C$.

Задача 11.7. Пусть A, B, C — множества. Определим множество X как множество всех элементов $x \in A$, таких, что

$$(x \in B) \ \to \ (x \in C).$$

Выразите множество X через множества A, B и C при помощи операций объединения, пересечения и разности.

Задача 11.8. Пусть $A = \{b, c, d, e\}$, $B = \{c, e, k\}$, $C = \{a, b, e, k\}$, $D = \{a, c, k, l\}$. Найдите следующие множества:

а) $(D \cup A) \cap (C \cup B)$,

б) $(A \cap (B \cap C)) \cap D$,

в) $(A \cup D) \backslash (B \cup C)$,

г) $D \backslash ((B \cup A) \backslash C)$.

Задача 11.9. Верно ли, что $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$? Докажите или приведите контрпример.

Задача 11.10. Постройте бинарное отношение C на 3-элементном множестве $\{x, y, z\}$
а) такое, что C рефлексивно и симметрично, но не транзитивно;
б) такое, что C рефлексивно и транзитивно, но не симметрично.

Задача 11.11. На всех сторонах и диагоналях многоугольника расставлены стрелки. Докажите, что, поменяв направление не более чем одной стрелки, можно будет добраться по стрелкам из любой вершины до любой другой.

Задача 11.12. Бизнесмен заключил с чёртом сделку: он может любую имеющуюся у него купюру обменять у чёрта на любой набор купюр любого меньшего достоинства (по своему выбору, без ограничения общей суммы). Бизнесмен также может тратить деньги, но не может получать их в другом месте (кроме как у чёрта). При этом каждый день на еду нужен рубль. Сможет ли бизнесмен жить так бесконечно долго?

Задача 11.13. На доске написаны два числа $1, 1$. Вписав между числами их сумму, мы получим числа $1, 2, 1$. Повторив эту операцию ещё раз, получим числа $1, 3, 2, 3, 1$. Какова будет сумма всех чисел на доске после 100 операций?

Задача 11.14. $n > 4$ сплетников разговаривают по телефону. За один разговор два участвующих в нём сплетника успевают рассказать друг другу все известные им сплетни. Докажите, что можно так организовать переговоры, что за $2n-4$ разговора каждый сплетник будет знать все сплетни остальных.

Задача 11.15. Отображение f из множества всех целых чисел в множество всех целых чисел определено следующим образом. Число $f(x)$ равно наименьшему простому числу, которое превосходит x^2. Принадлежит ли 19 множеству значений отображения f? Найдите $f^{-1}(17)$. Строго обоснуйте ответы.

Задача 11.16. Пусть $f : X \to Y$ — отображение, и A, $B \subset X$. Всегда ли верно, что $f(A\backslash B) \subset f(A)\backslash f(B)$? $f(A\backslash B) \supset f(A)\backslash f(B)$? Докажите или приведите контрпримеры.

Задача 11.17. Пусть $f : X \to Y$ — отображение, а $C, D \subset Y$. Всегда ли верно, что если $f^{-1}(C) \subset f^{-1}(D)$, то $C \subset D$? Докажите или приведите контрпример.

Задача 11.18. Докажите, что следующее свойство отображения $f : X \to Y$ эквивалентно инъективности: существует отображение $g : Y \to X$ со свойством $g \circ f = \mathrm{id}_X$. Приведите аналогичное свойство, эквивалентное сюръективности.

Задача 11.19. Дано множество A из 30 элементов и отображение $f : A \to A$. Сколько элементов может быть в образе $f(A)$, если в образе $f(f(A))$ ровно 10 элементов?

Задача 11.20. Постройте биекцию между множеством всех последовательностей натуральных чисел и множеством всех возрастающих последовательностей натуральных чисел.

Задача 11.21. Найдётся ли натуральное число, произведение цифр которого равно 528?

Задача 11.22. Пусть p_n — "энное" по счёту простое число ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$ и так далее). Докажите, что при $n > 12$ выполнено неравенство $p_n > 3n$.

Задача 11.23. Опишите все такие числа n, что
а) $\mathrm{НОД}(n, n + 12) = 6$;

б) НОД$(n, n+12) = 1$.

Задача 11.24. Пусть $d(k)$ обозначает наибольший нечётный делитель числа k. Докажите, что $d(n+1) + d(n+2) + \ldots + d(2n) = n^2$.

Задача 11.25. Докажите, что если $a \mid bc$, то $\frac{a}{(a,b)} \mid c$.

Задача 11.26. На бесконечной шахматной доске стоит слонопотам. За один ход он умеет перемещаться на m клеток в одном направлении и на n клеток в направлении, перпендикулярном первому. При каких m и n слонопотам сможет попасть в клетку, соседнюю с исходной? (Конь — тоже слонопотам при $m = 2$ и $n = 1$.)

Задача 11.27. Квадрат разделён на 16 равных квадратов. Сколькими способами можно раскрасить их в белый, черный, красный и жёлтый цвета так, чтобы в каждом горизонтальном и каждом вертикальном ряду были все четыре цвета?

Задача 11.28. Сколькими способами три человека могут поделить между собой

а) 15 различных конфет;

б) 15 одинаковых конфет?

(Делят не обязательно поровну, человеку может достаться ноль конфет.)

Задача 11.29. Пусть $X = \{1, \ldots, 42\}$ и $Y = \{1, \ldots, 21\}$. Сколько существует отображений из X в Y таких, что у каждого элемента из Y ровно два прообраза?

Задача 11.30. На сколько нулей оканчивается число $11^{100} - 1$?

Задача 11.31. В ожесточенном бою 70 из 100 пиратов потеряли один глаз, 75 — одно ухо, 80 — одну руку и 85 — одну ногу. Каково минимальное число потерявших одновременно глаз, ухо, руку и ногу?

Задача 11.32. Найдите остаток от деления многочлена $(x-1)^{2019}$ на многочлен $(x-2)$.

Задача 11.33. Пусть $m, n \in \mathbb{N}$ — натуральные числа, для которых $n \geqslant m$. Разделите с остатком многочлен $(x^n - 1)$ на многочлен $(x^m - 1)$.

Задача 11.34. Приведите пример многочлена $f(x) \in \mathbb{Z}[x]$ такого, что $f(\sqrt{2} + \sqrt{5}) = 0$.

Задача 11.35. Найдите остаток от деления многочлена $x^{81} + x^{27} + x^9 + x^3 + x$ на $x^2 - 1$.

Задача 11.36. Пусть $f(x) = x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$. Найдите все рациональные корни многочлена $f(x)$.

Задача 11.37. Пусть $n \in \mathbb{N}$ — натуральное число, $a, b \in \mathbb{Z}$ — целые числа, удовлетворяющие сравнению $a \equiv b \pmod{n}$. Можно ли утверждать, что для любого целого числа l справедливо $l^a \equiv l^b \pmod{n}$?

Задача 11.38. Сколько решений, различных по модулю 777, имеет следующее сравнение: $123x \equiv 321 \pmod{777}$?

Задача 11.39. Найдите наимешее нечётное натуральное число n такое, что $(n+1)$ делится на 3, $(n+4)$ делится на 5, а $(n+7)$ делится на 11.

Задача 11.40. Пусть p — нечётное простое число. Введём обозначения:

$$X = 1 \cdot 3 \cdot \ldots \cdot (p-2) \qquad \text{и} \qquad Y = 2 \cdot 4 \cdot \ldots \cdot (p-1).$$

Докажите, что либо $(X - Y)$ делится на p, либо $(X + Y)$ делится на p. Для каких p верно первое утверждение, а для каких второе?

Задача 11.41. Пусть p — простое число, $k \in \mathbb{N}$. Докажите, что $C_{p-1}^{k} \equiv (-1)^{k-1} \pmod{p}$.

Задача 11.42. Укажите такое k-значное число $N \in \mathbb{N}$, что десятичные записи чисел N, $2N$, …, kN отличаются только порядком цифр, если

а) $k = 6$;

б) $k = 16$.

Задача 11.43. Докажите, что число $0{,}123456789101112131415161718\ldots$ иррационально.

Задача 11.44. Докажите, что любое положительное число можно представить в виде суммы девяти чисел, десятичные записи которых содержат только цифры 0 и 7.

Задача 11.45. Длина минимального периода у одной бесконечной десятичной дроби равна 6, а у другой — равна 12. Какой может быть длина минимального периода у суммы этих дробей?

Задача 11.46. Может ли геометрическая фигура иметь ровно два центра симметрии?

Задача 11.47. К какому из типов движений плоскости, указанных в теореме Шаля, относится композиция движений $S_m \circ T_{\vec{v}} \circ S_l$ в случае, когда

а) $m \parallel l$, $m \neq l$ и $\vec{v} \parallel l$;

б) $m = l$ и $\vec{v} \parallel l$?

Задача 11.48. Докажите, что движение, меняющее направления лучей на противоположные — это центральная симметрия.

Задача 11.49. Преобразованием какого типа может являться композиция трех осевых симметрий? Какой из типов реализуется при каких условиях на взаимное расположение осей исходных симметрий?

Задача 11.50. Докажите, что для любых двух комплексных чисел a и b имеют место неравенства: $|a + b| \leqslant |a| + |b|$, $|a - b| \leqslant |a| + |b|$. При каких условиях неравенства обращаются в равенства?

Задача 11.51. Докажите, что четырёхугольник $ABCD$ является параллелограммом тогда и только тогда, когда комплексные координаты a, b, c, d его вершин удовлетворяют условию $a + c = b + d$.

Задача 11.52. Дан положительно ориентированный квадрат $ABCD$ и комплексные координаты a и b его вершин A и B. Найдите комплексные координаты вершин C и D (при произвольном выборе нулевой точки O).

Задача 11.53. Пусть f — многочлен с действительными коэффициентами. Докажите, что если $f(i) = 0$, то f делится на $x^2 + 1$.

Задача 11.54. Можно ли ввести на комплексных числах отношение порядка $>$, согласованное со сложением и умножением? Последнее означает, что для всех $a, b, c \in \mathbb{C}$:

(1) из $a > b$ следует $a + c > b + c$;

(2) из $a > 0$ и $b > 0$ следует, что $ab > 0$.

Задача 11.55. Найдите число упорядоченных пар $(x, y), x, y \in \mathbb{R}$, таких, что

$$(x + iy)^{2020} = x - iy.$$

Дополнительные задачи

Задача 12.1. На химической конференции присутствовало n учёных — химиков и алхимиков, причём химиков было больше, чем алхимиков. Известно, что на любой вопрос химики всегда отвечают правду, а алхимики иногда говорят правду, а иногда лгут. Оказавшийся на конференции математик про каждого учёного хочет установить, химик тот или алхимик. Для этого он любому учёному может задать вопрос: «Кем является X: химиком или алхимиком?» (в частности, он может спросить, кем является сам этот учёный). Докажите, что при $n > 1$ математик может установить это за $2n - 3$ вопроса.

Задача 12.2. Десять пиратов хотят поделить добычу. Любой из них убеждён, что он поделил бы добычу на равные части, однако остальные ему не верят. Каким образом надо действовать пиратам, чтобы после раздела каждый был уверен, что ему досталось не менее десятой части добычи?

Задача 12.3. Пусть $n > 1$. Может ли быть целым число $1 + \dfrac{1}{2} + \dfrac{1}{3} + \ldots + \dfrac{1}{n}$?

Задача 12.4. Выведите формулу для суммы квадратов делителей числа $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$.

Задача 12.5. Найдите все натуральные $n \in \mathbb{N}$, для каждого из которых существует $k \in \{1, 2, \ldots, n-1\}$ такое, что выполняется равенство $2C_n^k = C_n^{k-1} + C_n^{k+1}$.

Задача 12.6. Вычислите значения следующих выражений:

а) $C_n^0 + C_{n-1}^1 + C_{n-2}^2 + C_{n-3}^3 + \ldots$

б) $C_n^0 - C_{n-1}^1 + C_{n-2}^2 - C_{n-3}^3 + \ldots$

Задача 12.7. Для каждого натурального n определите, сколько существует троек натуральных чисел, сумма которых равна $6n$.

Задача 12.8. Докажите, что числитель дроби $1 + \dfrac{1}{2} + \dfrac{1}{3} \ldots + \dfrac{1}{p-1}$ делится на p, если p — простое число, не равное двум.

Задача 12.9. Докажите, что последовательность остатков чисел $1^1, 2^2, 3^3, \ldots$ по модулю простого числа p периодична. Оцените её период.

Задача 12.10. Является ли счётным любое бесконечное множество непересекающихся

а) интервалов на прямой;

б) кругов на плоскости?

Задача 12.11. Может ли длина периода дроби $1/n$ быть равной $(n-1)$, если n является составным числом?

Задача 12.12. При помощи циркуля и линейки восстановите семиугольник по серединам его сторон.

Задача 12.13. Найдите $k \in \mathbb{N}$ такое, что $\operatorname{arctg}\dfrac{1}{3} + \operatorname{arctg}\dfrac{1}{5} + \operatorname{arctg}\dfrac{1}{7} + \operatorname{arctg}\dfrac{1}{k} = \dfrac{\pi}{4}$.

Задача 12.14. а) Докажите, что если целые числа m и n представляются в виде суммы двух полных квадратов, то их произведение mn тоже представляется в виде суммы двух полных квадратов (и даже двумя способами).

б) Докажите, что неотрицательный вещественный многочлен можно представить как сумму двух квадратов вещественных многочленов.

Ответы и указания к упражнениям

12.0. Вступительный тест

0.1. *Ответ:* 1.
0.2. *Ответ:* 16.
0.3. *Ответ:* -1.
0.4. *Ответ:* 60.
0.5. *Ответ:* S.
0.6. *Ответ:* 9.
0.7. *Ответ:* 2.
0.8. *Ответ:* $C_{2020}^2 = 2039190$.
0.9. *Ответ:* $\bar{\omega} - C$, $-\omega - B$, $i\omega - A$.
0.10. *Ответ:* 32.
0.11. *Ответ:* 38.
0.12. *Ответ:* $2^{11} = 2048$.
0.13. *Ответ:* в) «Если B истинно, то A ложно».
0.14. *Ответ:* -1.
0.15. *Ответ:* а) $\dfrac{n^m - 1}{n - 1}$, б) $\dfrac{1000!}{(100!)^{10}}$, в) $\dfrac{n^4 + n^2 + 1}{n^2 + n + 1}$, д) $\dfrac{(1+\sqrt{2})^n}{2} + \dfrac{(1-\sqrt{2})^n}{2}$.
0.16. *Ответ:* 3.
0.17. *Ответ:* в) $(A \cap B) \setminus (A \cap B \cap C)$.
0.18. *Ответ:* C_{n+d-1}^{d-1}.
0.19. *Ответ:* а) Для любого комплексного числа z число $z \cdot \bar{z}$ является вещественным. е) Пусть точки X, Y и Z имеют комплексные координаты $27 - 4i$, $2 - 10i$ и $-4 + 15i$ соответственно. Тогда прямые XY и YZ перпендикулярны.
0.20. *Ответ:* а) Параллельный перенос. б) Поворот. г) Центральная симметрия.
0.21. *Ответ:* 2.
0.22. *Ответ:* в) $(\neg A \vee C) \wedge (\neg B)$.
0.23. *Ответ:* д) Утверждение неверное, ошибка в индукционном переходе.
0.24. *Ответ:* $\{4, 6\}$.
0.25. *Ответ:* $\left\{\dfrac{2\pi}{3}, \dfrac{8\pi}{9}\right\}$.
0.26. *Ответ:* 20101.
0.27. *Ответ:* 7.

12.1. Математическая логика

1.1. *Ответ:* A и C ложны, B истинно.

1.2. *Ответ:* $X \wedge Y$: «n равно 3»; $X \vee Y$: «n — натуральное число».

1.3. *Ответ:* Всего 48 формул.

Решение: Рассмотрим несколько случаев.

- Обе операции — отрицания. В таком случае формула может иметь лишь вид $\neg\neg X$, где X — переменная. Но, по условию, мы рассматриваем формулы от двух переменных. Следовательно, данный случай нас не интересует.

- Одна из операций — отрицание. В таком случае мы получаем следующие формулы: $\neg X \wedge Y, \neg X \vee Y, X \wedge \neg Y, X \vee \neg Y$, а также $\neg(X \wedge Y), \neg(X \vee Y)$. Более того, ещё 6 формул получается из перечисленных с помощью перестановок. Например, из формулы $\neg X \wedge Y$ можно получить формулу $Y \wedge \neg X$.

- Наконец, если среди операций отрицаний нет, то искомые формулы могут быть устроены одним из следующих способов: $\text{var} \wedge \text{var} \wedge \text{var}$, $\text{var} \vee \text{var} \vee \text{var}$, $\text{var} \wedge \text{var} \vee \text{var}$, $\text{var} \vee \text{var} \wedge \text{var}$, $\text{var} \wedge (\text{var} \vee \text{var})$, $(\text{var} \vee \text{var}) \wedge \text{var}$. В нашем алфавите 2 переменных, а «слотов» для переменных в каждой такой формуле 3. Следовательно, какая-то из переменных будет участвовать 2 раза, допустим, X. Таким, образом, получаем по 3 формулы каждого типа: переменные X, X, Y можно подставить в каждую из формул тремя способами. Итого, 18 формул. Другие 18 формул получим, подставляя переменные Y, Y, X.

Суммируя, имеем всего $12 + 18 + 18 = 48$ формул.

1.4. *Решение:* Искомые таблицы истинности имеют следующий вид:

X	Y	$X \to Y$	$X \wedge (X \to Y)$
0	0	1	0
0	1	1	0
1	0	0	0
1	1	1	1

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

1.5. *Решение:* Построим таблицу истинности для искомой формулы:

X	Y	$X \to Y$	$Y \to X$	$(X \to Y) \vee (Y \to X)$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	1
1	1	1	1	1

1.6. *Решение:* Если формула $(\varphi \to \psi) \wedge (\psi \to \varphi)$ — тавтология, значит, при любых значениях входящих в неё переменных обе формулы $(\varphi \to \psi)$ и $(\psi \to \varphi)$ истинны. Последнее означает, что формулы φ и ψ истинны при одних и тех же значениях переменных. Следовательно, по определению 1.7, они эквивалентны.

Пусть формулы φ и ψ эквивалентны, то есть, истинны при одних и тех же значениях входящих в них переменных. Следовательно, при любых значениях переменных, формулы $(\varphi \to \psi)$ и $(\psi \to \varphi)$ истинны. Но тогда и их конъюнкция истинна при любых значениях переменных, следовательно является тавтологией, по определению 1.8.

1.7. *Ответ:* $\neg X \vee Y$.

1.8. *Решение:* Пусть (a_n) — арифметическая прогрессия со знаменателем d. Допустим, $q = (a_1, d)$ — наибольший общий делитель чисел a_1 и d. Тогда любой член прогрессии $a_{j+1} = a_1 + jd$ делится на q. Если среди членов прогрессии есть простое число p, то либо $q = 1$, либо $q = p$. В первом случае, a_1 и d взаимно просты, второй же случай реализуется только при $a_1 = p$.

1.9. *Решение:* Допустим, $a \neq b$. Приведём дроби к общему знаменателю и перенесём слагаемые в левую часть. Получим следующее равенство:

$$\frac{a(1+a) - b(1+b)}{(1+a)(1+b)} = 0,$$

или, что эквивалентно,

$$\frac{(a-b)(1+a+b)}{(1+a)(1+b)} = 0.$$

По предположению, $a - b \neq 0$, следовательно, множитель $(a-b)$ можно сократить. В таком случае, равенство выполняется лишь при $a+b+1 = 0$. Однако это невозможно, так как a и b — строго положительные вещественные числа. Противоречие. Следовательно, $a = b$, что и требовалось доказать.

1.10. *Решение:* Верно первое. Действительно, для любого натурального n, верно неравенство $n + 1 > n$. Второе утверждение с помощью этого неравенства можно опровергнуть. Действительно, если бы существовало указанное во втором утверждении натуральное число N, большее всех натуральных чисел, то, в частности, было бы выполнено очевидно неверное неравенство $N + 1 < N$.

12.2. Множества и отображения

2.1. *Ответ:* а) 1. б) 3. в) 6.

2.2. *Ответ:* $5, 10, 15, 20, 25, 30, 35, 40, 45$.

2.3. *Ответ:* $\varnothing$, $\{\varnothing\}$, $\{\{0\}\}$, $\{1\}$, $\{\varnothing, \{0\}\}$, $\{\varnothing, 1\}$, $\{\{0\}, 1\}$, $\{\varnothing, \{0\}, 1\}$.

2.4. *Ответ:* $2^4 = 16$.

2.5. *Ответ:* Объединением является множество $\mathbb{N}$, а пересечением – $\varnothing$.

2.6. *Решение:* а) Для доказательства равенства $A \cup A = A$ нужно проверить, что если $x \in A \cup A$, то и $x \in A$. В самом деле, любой элемент из $X \cup Y$ принадлежит либо X, либо Y, в нашем случае — только A $(X = Y = A)$. В обратную сторону, любой элемент X и Y принадлежит $X \cup Y$, следовательно, если $x \in A$, то и $x \in A \cup A$.

Для доказательства равенства $A \cap A = A$ проверим, что $A \cap A \subset A$ и $A \subset A \cap A$. Действительно, $X \cap Y \subset X$ и $X \cap Y \subset Y$ по определению пересечения, а $X \subset X \cap Y$ тогда и только тогда, когда $X \subset Y$, что выполнено в нашем случае $X = Y = A$.

Указание: Для остальных пунктов следует аналогичным образом воспользоваться приведёнными выше критериями равенства из раздела 2.2, выбирая более удобный на своё усмотрение.

2.7. *Решение:* Так как $x \in C(y)$, то $x \sim y$. Для каждого $z \in C(x)$ имеем $z \sim x$ по определению класса $C(x)$. Значит, $z \sim y$ в силу транзитивности, откуда $z \in C(y)$. Обратно, если $w \in C(y)$, то $w \sim y$. Снова $w \sim x$ по транзитивности и $w \in C(x)$.

2.8. *Ответ:* Направленные отрезки $\overrightarrow{AB}$ и $\overrightarrow{CD}$ называются эквивалентными, если они коллинеарны, имеют одинаковые направления и $|AB| = |CD|$.

2.9. *Указание:* Проверьте рефлексивность, симметричность и транзитивность.

2.10. *Ответ:* $(x, y) \mapsto (y, x)$.

2.11. *Ответ:* Всего 8 отображений. Среди них 6 сюръекций, инъекций и биекций нет.

Указание: Расставьте стрелки из элементов первого множества в элементы второго всевозможными способами и проверьте для получившихся отображений инъективность и сюръективность по определению.

2.12. *Решение:* Если f не инъективно, то найдутся $x \neq x'$ такие, что $f(x) = f(x')$. Тогда для любого отображения $g : Y \to X$ имеем $g(f(x)) = g(f(x'))$, то есть $g \circ f \neq \mathrm{id}_X$. Если f не сюръективно, то найдётся $y \in Y$ такой, что $f^{-1}(y) = \varnothing$. Тогда для любого отображения $g : Y \to X$ имеем $(f \circ g)^{-1} = g^{-1}(\varnothing) = \varnothing$, то есть $f \circ g \neq \mathrm{id}_Y$. То есть инъективность и сюръективность отображения f являются необходимым условием существования обратного отображения. С другой стороны, если f биективно, то любой $y \in Y$ имеет ровно один прообраз, и именно его достаточно назначить образом элемента y при отображении g.

2.13. *Ответ:* Отображение f не инъективно (в множестве A больше элементов, чем в его образе), поэтому ни обратного, ни левого обратного нет. Однако f сюръективно, поэтому существует правое обратное, например, $g(x) = x + 5$.

2.14. *Ответ:* а) Биекция для целых чисел:

$\mathbb{Z}:$	1	-1	2	-2	3	-3	4	-4	5	-5	6	-6	7	-7	8	-8	9
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$\mathbb{N}:$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

б) Биекцию $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ можно задать формулой $f(a, b) = 2^{a-1}(2b - 1)$.

2.15. *Решение:* Доказательство теоремы 2.4: пусть $A \subset \mathbb{N}$. Если $A = \varnothing$, то A конечно. В противном случае в A существует минимальный элемент a_1. Если $A \setminus \{a_1\} = \varnothing$, то $A = \{a_1\}$ конечно. Иначе в множестве $A \setminus \{a_1\}$ существует минимальный элемент a_2. Опять же, либо $A = \{a_1, a_2\}$ конечно, либо в $A \setminus \{a_1, a_2\}$ существует минимальный элемент a_3 и так далее. В конечном итоге, либо процесс окажется конечным, и тогда $A = \{a_1, \ldots, a_n\}$. Либо процесс никогда не закончится, а значит, $A = \{a_1, \ldots, a_n, \ldots\}$ (в самом деле, если бы нашёлся элемент $a \in A$, не совпадающий ни с каким a_k, то нашлось бы $n < a$ такое, что $a_n < a < a_{n+1}$, что противоречит выбору числа a_{n+1}).

Доказательство теоремы 2.5: пусть $C_k = \{a_{ki} \mid i \in \mathbb{N}\}$ — счётные множества, а множество D является их объединением. Пусть сначала все множества попарно непересекаются. Если $k \in \{1, \ldots, n\}$ то $f : D \to \mathbb{N}$ можно задать формулой $f(a_{ij}) = i + n(j-1)$ (перечисление по столбцам); если же $k \in \mathbb{N}$, то формулой $f(a_{ij}) = \big(1+2+\ldots+(i+j-2)\big)+i$

(перечисление по диагоналям). Если же есть повторяющиеся элементы, то их достаточно исключить из рассмотрения, отобразив оставшиеся в том же порядке.

Вторая часть теоремы 2.5 следует из первой и равенства $A \times B = \bigcup\limits_{k=1}^{\infty} A \times \{b_k\}$.

2.16. *Решение:* Множество $\mathbb{Q}$ представимо в виде счётного объединения множеств вида $Q_n = \{m/n \mid m \in \mathbb{Z}\}$, каждое из которых счётно (пользуемся теоремой 2.5).

2.17. *Ответ:* $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$.

12.3. Математическая индукция

3.1. *Указание:* Решение изложено в разделе 3.3.

3.2. *Решение:* Будем называть город *крайним*, если он соединён дорогой ровно с одним городом. Докажем, что в любой конфигурации, удовлетворяющей условию задачи, найдётся крайний город. Для этого выберем произвольный город и начнём из него обходить другие города, каждый раз выбирая ещё не пройденную ранее дорогу. Заметим, что мы не можем попасть в город, где уже бывали до этого, поскольку это противоречило бы условию — мы ведь не разворачивались. Значит, мы окажемся в городе, откуда нельзя выехать по не пройденным ранее дорогам, что означает, что в него ведёт ровно одна дорога — по которой мы в него попали.

Теперь докажем исходное утверждение. База индукции: если в системе только один город, то дорог там нет (то есть дорог на одну меньше, чем городов). Индукционный переход: допустим, мы умеем доказывать утверждение для системы из n городов. Рассмотрим произвольную систему из $(n+1)$ города и мысленно удалим крайний город с выходящей из него дорогой. Оставшаяся система по-прежнему удовлетворяет условию, поэтому в ней дорог на 1 меньше, чем городов. А значит, и для исходной системы это было верно.

3.3. *Решение:* База индукции $n = 2$ очевидна. Пусть при $n = k$ справедливо

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \ldots + \frac{1}{(k-1)\cdot k} = \frac{k-1}{k}.$$

Тогда при $n = k+1$ имеем

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \ldots + \frac{1}{(k-1)\cdot k} + \frac{1}{k\cdot(k+1)} = \frac{k-1}{k} + \frac{1}{k\cdot(k+1)}.$$

Приводя правую часть к общему знаменателю, получаем

$$\frac{k^2-1}{k\cdot(k+1)} + \frac{1}{k\cdot(k+1)} = \frac{1}{k+1} = \frac{(k+1)-1}{(k+1)},$$

как и требовалось.

3.4. *Решение:* а) База индукции $n = 3$ выполнена: в триангуляции $n - 1 = 1$ треугольник. Индукционный переход: пусть в любую триангуляцию n-угольника входит

ровно $(n-2)$ треугольника при каждом $n<k$. Рассмотрим произвольный k-угольник и какую-нибудь его внутреннюю диагональ, входящую в данную триангуляцию. Эта диагональ делит его на два многоугольника — k_1-угольник и k_2-угольник — имеющие две общие вершины (концы диагонали), поэтому $k_1+k_2=k+2$. С другой стороны, по предположению индукции, числа входящих в их триангуляции треугольников равны (k_1-2) и (k_2-2) соответственно. Следовательно, в триангуляции исходного k-угольника $(k_1-2)+(k_2-2)=(k+2)-4=k-2$ треугольника.

б) Рассмотрим произвольную правильную триангуляцию n-угольника. Сумма углов n-угольника есть сумма углов входящих в него треугольников, а она равна $(n-2)\pi$.

12.4. Делимость целых чисел

4.1. *Ответ:* Отношение порядка рефлексивно и транзитивно, но не симметрично.

4.2. *Решение:* По условию $a=q_1n, b=q_2n$, поэтому

$$a+b=q_1n+q_2n=(q_1-q_2)n, \qquad \text{и} \qquad a-b=q_1n+q_2n=(q_1-q_2)n.$$

4.3. *Решение:* Проведём доказательство от противного. Предположим, что $n\mid a$, $n\nmid b$ и $n\mid(a+b)$. Тогда согласно упражнению 4.2 имеем $n\mid\big((a+b)-a\big)=b$. Противоречие.

4.4. *Решение:* По определению $a=q_1b$ и $b=q_2c$, так что $a=q_1b=q_1q_2c$.

4.5. *Указание:* Используйте определение десятичной записи и упражнения 4.2 и 4.4.

Решение: а) Делимость на 2. $\overline{a_na_{n-1}a_{n-2}\ldots a_0}:=a_n10^n+a_{n-1}10^{n-1}+\ldots+a_0$. Каждое из слагаемых, кроме последнего, заведомо делится на 2. Поэтому согласно упражнениям 4.2 и 4.4 число $\overline{a_na_{n-1}a_{n-2}\ldots a_0}$ делится на 2 если и только если a_0 делится на 2.

Делимость на 4. $\overline{a_na_{n-1}a_{n-2}\ldots a_0}:=a_n10^n+a_{n-1}10^{n-1}+\ldots+a_0$. Каждое из слагаемых, кроме двух последних, заведомо делится на 4. Значит, согласно упражнениям4.2 и 4.4, число $\overline{a_na_{n-1}a_{n-2}\ldots a_0}$ делится на 4 если и только если $10a_1+a_0=\overline{a_1a_0}$ делится на 4.

Делимость на 5. Полностью аналогично делимости на 2.

б) • Число делится на 8 если и только если число, составленное из трёх его последних цифр, делится на 8.

• Число делится на 16 если и только если число, составленное из четырёх его последних цифр, делится на 16.

• Число делится на 25 если и только если число, составленное из двух его последних цифр, делится на 25.

• Число делится на 125 если и только если число, составленное из трёх его последних цифр, делится на 125.

4.6. *Указание:* $10=9+1$, $1000=999+1$, ... В общем случае, $10^n=\underbrace{99\ldots99}_{n\text{ штук}}$.

Решение: Для простоты написания проиллюстрируем идею на трёхзначных числах; с учётом указания, читатель с легкостью её обобщит. Представим искомое число в виде $\overline{a_2a_1a_0}=a_2\cdot100+a_1\cdot10+a_0=a_2\cdot99+a_1\cdot9+(a_2+a_1+a_0)$. Поскольку $99a_2+9a_1$ делится

как на 3, так и на 9, упражнения 4.2 и 4.4 позволяют свести делимость исходного числа к делимости $(a_2 + a_1 + a_0)$. Что и требовалось.

4.7. *Решение:* Если $r' = 0$, то требуемое очевидно. Если же $r' > 0$, имеет место равенство: $a = q'b - r' = q'b + b - b - r' = (q' + 1)b + (-b - r') = qb + r$. Поскольку число b отрицательно, а $0 < r' < |b|$, число $r = (-b - r')$ положительно и меньше $|b|$.

4.8. *Решение:* Если $a > 0$, $b < 0$, то можно использовать рассуждение из упражнения 4.7. Если же $a < 0$, то разделим $-a$ на $-b$ с остатком — получим $-a = q'(-b) + r'$, где $0 \leqslant r' < |b|$. Из равенства $a = q'b - r'$ вытекает дальнейшее. Если $r' = 0$, нужно положить $q = q'$ и $r = 0$. Если $r \neq 0$ и $b > 0$, то надо взять $q = (q' - 1)$ и $r = b - r'$. Если же $r \neq 0$ и $b < 0$, то $q = (q' + 1)$ и $r = -b - r'$. Все доказательства аналогичны решению упражнения 4.7.

4.9. *Ответ:* $0, 1, 4, 5, 6, 9$.

Решение: Заметим, что последняя цифра — это остаток при делении на 10. При этом играет роль только последняя цифра числа $n = \overline{a_n a_{n-1} a_{n-2} \dots a_0}$, поскольку выполнено равенство $(10b + a_0)^2 = 10(10b^2 + 2ba_0) + a_0^2$, где $b = \overline{a_n a_{n-1} a_{n-2} \dots a_1 0}$. Остаётся составить таблицу квадратов всех цифр.

a_0	0	1	2	3	4	5	6	7	8	9
a_0^2	0	1	4	9	16	25	36	49	64	81

4.10. *Ответ:* а) 1. б) 3.

Решение: Заметим, что если $a_1 = q_1 b + r_1$ и $a_2 = q_2 b + r_2$, то справедливо равенство $a_1 a_2 = (q_1 q_2 b + q_1 r_2 + q_2 r_1)b + r_1 r_2$. Значит, остатки чисел $a_1 a_2$ и $r_1 r_2$ при делении на b совпадают. Таким образом, остаток числа a^n при делении на b однозначно определяется остатком числа a^{n-1} при делении на b.

а) Числа $2, 4, 8, 16, \dots, 2^{2019}, 2^{2020}$ последовательно дают остатки $2, 1, 2, 1, 2, 1, \dots, 2, 1$.

б) Числа $3, 9, 27, 81, \dots, 3^{776}, 3^{777}$ последовательно дают остатки $3, 9, 7, 1, 3, 9, \dots, 1, 3$.

Замечание: Используя сравнения (раздел 7.1), то же самое рассуждение можно было бы оформить следующим образом:

а) $2^{2015} = (2^2 \cdot 2^2 \cdot \ldots \cdot 2^2) \cdot 2 \equiv 1 \cdot 1 \ldots \cdot 1 \cdot 2 = 2 \pmod 3$, поскольку $2^2 = 4 \equiv 1 \pmod 3$.

б) $3^{777} = 3^{776} \cdot 3 = (3^4 \cdot \ldots \cdot 3^4) \cdot 3 \equiv 1 \cdot \ldots \cdot 1 \cdot 3 = 3 \pmod 5$, ведь $3^4 = 81 \equiv 1 \pmod 5$.

4.11. *Решение:* Очевидно, если $k, m \in \mathbb{N}$, то $k \cdot m \geqslant k$. Теперь, если $l, n \in \mathbb{Z}$, то $|l \cdot n| = |l| \cdot |n|$, откуда и вытекает требуемое утверждение.

4.12. *Ответ:* $(372, 69) = 3$.

Решение: Проведём выкладки:

$$372 = 5 \cdot 69 + 27,$$
$$69 = 2 \cdot 27 + 15,$$
$$27 = 1 \cdot 15 + 12,$$
$$15 = 1 \cdot 12 + 3,$$
$$12 = 4 \cdot 3.$$

4.13. *Решение:* а) $0 = 0 \cdot a + 0 \cdot b$, $a = 1 \cdot a + 0 \cdot b$, $b = 0 \cdot a + 1 \cdot b$.

б) Поскольку d является делителем чисел a и b, то существуют такие целые числа $k, l \in \mathbb{Z}$, что $a = kd$ и $b = ld$, откуда $a, b \in \mathbb{Z}(d)$. Кроме того, $0 = 0 \cdot d$ и $d = 1 \cdot d$.

4.14. *Решение:* а) По условию $k = x_1 a + y_1 b$ и $l = x_2 a + y_2 b$, так что

$$k \pm l = (x_1 \pm x_2)a + (y_1 \pm y_2)b \in \mathbb{Z}(a, b).$$

б) Аналогично: $k = xd$ и $l = yd$, откуда $k \pm l = (x + y)d \in \mathbb{Z}(d)$.

4.15. *Решение:* а) Если $k = xa + yb$, то $nk = (nx)a + (ny)b \in \mathbb{Z}(a, b)$.

б) Аналогично, если $k = xd$, то $nk = (nx)d \in \mathbb{Z}(d)$.

4.16. *Решение:* Модуль целого числа — натуральное число или нуль. Согласно принципу минимального элемента (раздел 3.1) в любом подмножестве натуральных чисел есть минимальный элемент.

4.17. *Решение:* Согласно алгоритму Евклида найдутся такие $x, y \in \mathbb{Z}$, что $bx + cy = 1$. Домножая это равенство на a, имеем $abx + acy = a$. Левая часть полученного равенства делится на bc, значит, и правая — тоже.

4.18. *Решение:* Проведём индукцию по n.

База индукции: при $n = 2$ утверждение очевидно.

Шаг индукции: пусть утверждение доказано для всех чисел, меньших n. Если n простое, то $n = n$ — его представление в таком виде. Если n не простое, то $n = n_1 \cdot n_2$, где $n_1 < n$ и $n_2 < n$ — натуральные числа, не равные единице. К каждому из них применимо предположение индукции, то есть они представимы в виде произведения простых чисел. Значит, и n — тоже.

4.19. *Решение:* Проведём индукцию по m.

База индукции: при $m = 2$ утверждение составляет формулировку леммы 4.9.

Шаг индукции: пусть утверждение верно для $m = k$. Заметим, что если $n_1(n_2 \dots n_{k+1}) \vdots p$, то либо $p \mid n_1$, либо $p \mid (n_2 \dots n_{k+1})$. Последнее же по предположению индукции означает, что $p \mid n_l$ для некоторого l.

4.20. *Ответ:* Нет.

Решение: Поскольку $64 = 2^6$, по основной теореме арифметики $x = 2^m$ и $y = 2^{6-m}$, причем $m \neq 0$. Таким образом, y – чётное число, но $yz = 405$ — нечётное.

4.21. *Решение:* Мы уже знаем, что $p \mid ab \;\Rightarrow\; p \mid a$ или $p \mid b$. В частном случае $a = b = x$ получаем $p \mid x$. Ясно, что если $p \mid x$, то $p^2 \mid x^2$.

12.5. Комбинаторика

5.1. *Ответ:* $20 \cdot 15 = 300$.

5.2. *Ответ:* а) $32 \cdot 32 = 1024$.

б) $32 \cdot 31 = 992$.

в) $(32 \cdot 31)/2 = 496$.

г) $(32 \cdot 31 \cdot 30 \cdot 29)/2 = 431\,520$.

5.3. *Решение:* Для упрощения введём такие обозначения: $A = (A_1 \cup \ldots \cup A_n) \cap A_{n+1}$ и $B = (A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \ldots \cup (A_n \cap A_{n+1})$. Воспользуемся критерием равенства

множеств: $A = B$ тогда и только тогда, когда $A \subset B$ и $B \subset A$. Допустим сначала, что $x \in A$. Тогда $x \in A_{n+1}$ и существует такое $k \in \{1, \ldots, n\}$, что $x \in A_k$. Отсюда вытекает, что $x \in (A_k \cap A_{n+1})$. Следовательно, $x \in B$, а значит, $A \subset B$. Для проверки обратного включения достаточно заметить, что все переходы в приведённом выше рассуждении обратимы.

5.4. *Ответ:* $33000 - 11000 - 6600 + 2200 = 17600$.

5.5. *Ответ:* $20 \cdot 19 \cdot 18 \cdot 17 = 116280$.

5.6. *Ответ:* $(25 \cdot 24 \cdot 23 \cdot 22 \cdot 21)/5! = 53130$.

5.8. *Решение:* Итак, проведём индукцию по параметру n.

База индукции: при $n = 0$ имеем $C_0^0 = 1 = 2^0$, при $n = 1$ получается $C_1^0 + C_1^1 = 1 + 1 = 2^1$.

Шаг индукции: пусть при $n = k$ верно $C_k^0 + C_k^1 + C_k^2 + \ldots + C_k^k = 2^k$. Рассмотрим сумму $C_{k+1}^0 + C_{k+1}^1 + C_{k+1}^2 + \ldots + C_{k+1}^{k+1}$ и заменим каждое слагаемое, кроме крайних, по формуле $C_{k+1}^{l+1} = C_k^l + C_k^{l+1}$. С учётом равенств на крайние члены, $C_{k+1}^0 = C_k^0 = 1$ и $C_{k+1}^{k+1} = C_k^k = 1$, мы получаем удвоенную сумму из индукционного предположения:

$$C_{k+1}^0 + C_{k+1}^1 + C_{k+1}^2 + \ldots + C_{k+1}^{k+1} = C_k^0 + (C_k^0 + C_k^1) + (C_k^1 + C_k^2) + \ldots + C_k^k = 2^{n+1}.$$

5.8. *Решение:* а) $0 = (1-1)^n = C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n$.

б) Доказательство аналогично решению упражнения 5.8 с тем отличием, что в шаге индукции вместо суммы одинаковых слагаемых мы получим их разность, то есть ноль:

$$C_{k+1}^0 - C_{k+1}^1 + C_{k+1}^2 - \ldots = C_k^0 - (C_k^0 + C_k^1) + (C_k^1 + C_k^2) - \ldots = 0.$$

5.9. *Ответ:* б) $C_k^0 + C_{k+1}^1 + C_{k+2}^2 + \ldots + C_{k+m}^m = C_{k+m+1}^m$.

Решение: а) Проведём индукцию по параметру m.

База индукции: для $m = 1$ и $m = 2$ проверка выполняется непосредственно: именно, имеем $C_k^0 = 1 = C_{k+1}^0$ и $C_k^k + C_{k+1}^k = 1 + (k+1) = (k+2) = C_{k+2}^{k+1}$.

Шаг индукции: пусть $C_k^k + C_{k+1}^k + \ldots + C_{k+m}^k = C_{k+m+1}^{k+1}$. Тогда для $m+1$ справедливо $C_k^k + C_{k+1}^k + \ldots + C_{k+m}^k + C_{k+(m+1)}^k = C_{k+m+1}^{k+1} + C_{k+(m+1)}^k = C_{k+m+2}^{k+1}$. Для проверки последнего равенства используется $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$, применённое к $n = k + m$.

5.10. *Ответ:* $C_{13}^3 = 286$.

5.11. *Решение:* а) На первом месте стоит один из n элементов. На втором и каждом из последующих — также один из n элементов. Значит, всего по правилу произведения получаем n^k наборов.

б) Рассмотрим $(n + k - 1)$ позицию, на каждой из которых может стоять один из k элементов или перегородка (всего перегородок $(n-1)$ штука). Перегородки делят элементы на n групп, упорядоченных по типу, в каждой из которых содержится от 0 до n элементов. Распределение элементов и перегородок по позициям соответствует одному набору. Количество таких распределений k элементов по $n + k - 1$ позициям составляет в точности C_{n+k-1}^k.

12.6. Многочлены

6.1. *Решение:* Ясно, что $x^k \cdot x^m = x^{k+m}$. При перемножении многочленов каждый одночлен многочлена $f(x)$ умножается на каждый одночлен многочлена $g(x)$, так что одночлен максимальной степени многочлена $f(x) \cdot g(x)$ получается как произведение одночленов степени $\deg f(x)$ и $\deg g(x)$.

Явно, если $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_0$, а $g(x) = g_m x^m + g_{m-1}x^{m-1} + \ldots + g_0$, то имеем $f(x) \cdot g(x) = f_n g_m x^{n+m} + (f_n g_{m-1} + f_{n-1}g_m)x^{n+m-1} + \ldots + (f_1 g_0 + f_0 g_1)x + f_0 g_0$.

6.2. *Решение:* Очевидно, что сумма (разность) многочленов разной степени имеет степень, равную степени наибольшего из них. Если же многочлены имеют одинаковую степень, то их сумма (разность) может иметь строго меньшую степень (если коэффициенты при старшей степени совпадают или отличаются знаком).

6.3. *Решение:* Прямо следует из упражнения 6.1.

6.4. *Ответ:* а) $x^2 - 4x + 3 = (x-1)(x-3) + 0$;

б) $x^2 - 4 = (x+5)(x-5) + 21$;

в) $x^4 - 2x + 5 = (x^2-1)(x^2+1) + (-2x+6)$.

6.5. *Решение:* Поскольку хотя бы один из многочленов $f(x)$ и $g(x)$ ненулевой, степень их общих делителей ограничена. При этом множество общих делителей не пусто, так как содержит константы. Значит, найдётся и общий делитель максимальной степени.

6.6. *Решение:* а) $0 = 0 \cdot f(x) + 0 \cdot g(x)$, $f(x) = 1 \cdot f(x) + 0 \cdot g(x)$, $g(x) = 0 \cdot f(x) + 1 \cdot g(x)$.

б) Если $u(x) = a_1(x)f(x) + b_1(x)g(x)$ и $v(x) = a_2(x)f(x) + b_2(x)g(x)$, то

$$u(x) \pm v(x) = \big(a_1(x) \pm a_2(x)\big)f(x) + \big(b_1(x) \pm b_2(x)\big)g(x).$$

в) Если $h(x) = a(x)f(x) + b(x)g(x)$, то $s(x)h(x) = \big(s(x)a(x)\big)f(x) + \big(s(x)b(x)\big)g(x)$.

6.7. *Решение:* $(f(x), g(x)) = (g(x), r_0(x)) = \ldots = (r_{n-1}(x), r_n(x)) = r_n(x)$.

6.8. *Решение:* Из условия $(f(x), h(x)) = 1$ вытекает, что существуют $a(x), b(x) \in \mathbb{K}[x]$ такие, что $a(x)f(x) + b(x)h(x) = 1$. Домножая это равенство на $g(x)$, получаем

$$a(x)f(x)g(x) + b(x)g(x)h(x) = g(x).$$

Видно, что левая часть делится на $h(x)$. Значит, и правая — тоже.

6.9. *Решение:* Индукция по количеству сомножителей n.

База индукции: случай $n = 2$ составляет утверждение 6.6.

Шаг индукции: предположим, мы умеем доказывать это утверждение для $n = m$. Рассмотрим $n = m + 1$. Если $f_1(x) \ldots f_{m+1}(x) \vdots h(x)$, то согласно утверждению 6.6 либо $f_1(x) \ldots f_m(x) \vdots h(x)$, либо $f_{m+1}(x) \vdots h(x)$. Во втором случае доказывать нечего, а в первом, применив предположение индукции, заключаем, что $f(x) \vdots f_k(x)$ для некоторого $k \in \{1, \ldots, m\}$, что и требовалось.

6.10. *Решение:* По теореме Безу $(x^2 + bx + c)$ делится на $(x - \lambda)$, то есть справедливо $x^2 + bx + c = q(x)(x - \lambda)$. Кроме того, ясно, что $\deg q(x) = 1$, то есть $q(x) = sx + r$ для некоторых $s, r \in \mathbb{K}$. В нашем случае, очевидно, $s = 1$, поскольку в противном случае при раскрытии скобок коэффициент перед x^2 был бы равен s. Сделав замену $r \mapsto -\mu$, получаем $x^2 + bx + c = (x - \mu)(x - \lambda)$.

Для доказательства второй части достаточно раскрыть скобки:

$$x^2 + bx + c = x^2 - (\mu + \lambda)x + \mu\lambda.$$

Многочлены равны в том и только в том случае, когда равны их коэффициенты, поэтому $b = -(\mu + \lambda)$ и $c = \mu\lambda$.

6.11. *Решение:* а) Предположим противное: пусть $\lambda_1, \ldots \lambda_{n+1}$ — корни многочлена $f(x)$, но $\deg f(x) = n$. Тогда согласно теореме Безу $f(x) = q_1(x)(x-\lambda_1)$. Далее, $(x-\lambda_2) \mid f(x)$, а кроме того, поскольку $(x - \lambda_2) \nmid (x - \lambda_1)$, отсюда следует, что $(x - \lambda_2) \mid q_1(x)$. Таким образом, $f(x) = q_2(x)(x - \lambda_2)(x - \lambda_1)$. Продолжая в том же духе, получим

$$f(x) = q_{n+1}(x)(x - \lambda_{n+1}) \cdot \ldots \cdot (x - \lambda_1)$$

но $\deg(x - \lambda_{n+1}) \cdot \ldots \cdot (x - \lambda_1) = n + 1 > \deg f(x)$ — противоречие.

б) Любой ненулевой многочлен имеет конечное число корней. Тождественно равная нулю фукция же обладает бесконечным числом корней, так что она не может быть реализована ненулевым многочленом согласно пункту а).

6.12. *Ответ:* а) $f(x) = (x^2 + 2)(x^2 - 2)$ — разложение в $\mathbb{Q}[x]$.

б) $f(x) = (x^2 + 2)(x + \sqrt{2})(x - \sqrt{2})$ — разложение в $\mathbb{R}[x]$.

в) $f(x) = (x + \sqrt{2})(x - \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$ — разложение в $\mathbb{C}[x]$.

12.7. Сравнения

7.1. *Решение:* а) $(a - b) \vdots n$ и $(c - d) \vdots n$, поэтому сумма $(a + c) - (b + d)$ тоже делится на n, что и означает, что $a + c \equiv b + d \pmod n$.

б) Аналогично пункту а).

в) Существуют такие $k, l \in \mathbb{Z}$, что $a = b + kn$ и $c = d + ln$. Перемножая, имеем $ac = bd + n(bl + dk + kln)$, откуда $(ac - bd) \vdots n$.

г) Следует индукцией из пункта в).

7.2. *Указание:* Воспользуетесь признаками делимости на эти числа.

7.3. *Решение:* Перебор вариантов: $2 \cdot 0 \equiv 2 \cdot 2 \equiv 0 \pmod 4$; $2 \cdot 1 \equiv 2 \cdot 3 \equiv 2 \pmod 4$.

7.4. *Ответ:* По модулю 3: 0, 1. По модулю 8: 0, 1, 4. По модулю 24: 0, 1, 4, 9, 12, 16.

7.5. *Решение:* Заметим, что $3^4 = 81 \equiv 1 \pmod 5$. Поэтому $3^{2020} = (3^4)^{505} \equiv 1 \pmod 5$.

7.6. *Ответ:* По модулю 7: 1, 2, 4. По модулю 13: 1, 3, 4, 9, 10, 12.

7.7. *Ответ:* Если p не является простым числом, то разные раскраски круга посчитаны разное число раз. Например, если $p \vdots 2$, то мы можем раскрасить круг в два цвета «в шахматном порядке», чередуя цвета. Такая раскраска при повороте круга даст всего 2 разных варианта, а не p, как это было в случае простого p.

7.8. *Решение:* а) Достаточно заметить, что $C_p^k = \frac{p!}{k!(p-k)!}$, причём число $p!$ делится на p, а числа $k!$ и $(p - k)!$ не делятся, если $1 < k < p$.

б) Достаточно раскрыть скобки в выражении $(a + b)^p$ с помощью бинома Ньютона и воспользоваться пунктом а).

в) Будем вести индукцию по a.
База индукции: $a = 1$. Тривиальным образом выполняется: $1^p = 1$.
Шаг индукции: пусть мы умеем доказывать, что $a^p \equiv a \pmod p$. Тогда для $(a+1)$ имеет место следующая цепочка сравнений: $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$.

12.8. Действительные числа

8.1. *Решение:* Достаточно заметить, что функция $f(x) = x^5 + x + 1$ является монотонно возрастающей.

8.2. *Указание:* Для произвольного $a \in \{x > 0 \mid x^2 > 2\}$ возьмите $b = \dfrac{1}{2}\left(a + \dfrac{2}{a}\right)$.

8.3. *Указание:* Рассмотрите последовательность $y_n = -x_n$.

8.4. *Решение:* а) Согласно *неравенству Коши* $(a + b \geqslant 2\sqrt{ab})$ имеем:

$$x_{n+1}^2 = \frac{1}{4}\left(x_n^2 + \frac{4}{x_n^2} + 4\right) \geqslant \frac{4+4}{4} = 2. \tag{7}$$

б) Так как $x_n^2 \geqslant 2$, то $x_n \geqslant 2/x_n$. Поэтому среднее арифметическое x_n и $2/x_n$ (которое суть x_{n+1}) не превышает x_n.

8.5. *Решение:* Поскольку (x_n) невозрастает и $x_1 = 2$, предел (x_n) меньше двух, а значит, $(x_n + x) \leqslant 4$, откуда умножением на неотрицательную величину $(x_n - x)$ следуют требуемое неравенство. Теперь если $x^2 < 2$, скажем, $2 - x^2 = 4\varepsilon > 0$, то $x_n - x > \varepsilon$, что противоречит предположению, что x — предел последовательности (x_n).

8.6. *Решение:* Из формулы (7), а также из $x_n^2 \geqslant 2$ следует, что

$$4x_{n+1} = x_n^2 + 4 + \frac{4}{x_n^2} \leqslant x_n^2 + 4 + 2.$$

Перегруппировкой отсюда получаем требуемое неравенство. Следовательно, последовательность $y_n = x_n^2 - 2$ ограничена последовательностью $z_n = 1/4^n$. Последняя же стремится к нулю (строго этот факт доказывается в разделе 8.4).

8.7. *Указание:* б) Полезно рассмотреть d-ичную запись натурального числа $(-p) + d^m$.

8.8. *Решение:* Имеют место следующие неравенства:

$$x_n = A + \sum_{j=1}^{n} a_j d^{-j} \leqslant A + \sum_{j=0}^{n} (d-1)d^{-j} = A + \sum_{j=1}^{n} (d^{-j+1} - d^{-j}) = A + 1 - d^{-n} \leqslant A + 1.$$

8.9. *Ответ:* Если $\alpha = \overline{A, a_1 a_2 \ldots}0$, то $-\alpha = \overline{(-A-1), b_1 b_2 \ldots}$, где $b_j = 9 - a_j$.

12.9. Движения плоскости и векторы

9.1. *Решение:* Пусть векторы $\overrightarrow{u} = (u_1, u_2)$ и $\overrightarrow{v} = (v_1, v_2)$ неколлинеарны (то есть ни один из них не получается из другого умножением на некоторое число). Чтобы найти выражение вектора $\overrightarrow{w} = (a, b)$ в виде линейной комбинации $\overrightarrow{w} = x\overrightarrow{u} + y\overrightarrow{v}$, достаточно решить систему линейных уравнений:

$$\begin{cases} a &= u_1x + v_1y \\ b &= u_2x + v_2y \end{cases} \qquad \Longrightarrow \qquad x = \frac{av_2 - bv_1}{u_1v_2 - u_2v_1},\ \ y = \frac{u_1a - u_2b}{u_1v_2 - u_2v_1}.$$

Неколлинеарность гарантирует, что знаменатель не обратится в ноль.

9.2. *Ответ:* а) $\overrightarrow{w} = 2\overrightarrow{v}$;
б) $\overrightarrow{w} = \overrightarrow{u} - 2\overrightarrow{v}$;
в) $\overrightarrow{w} = \frac{4}{7}\overrightarrow{u} - \frac{1}{7}\overrightarrow{v}$.

9.3. *Решение:* Пусть точки A', B' и C' являются образами точек A, B и C при движении f. Согласно определению движения $A'B' = AB$, $B'C' = BC$ и $C'A' = CA$. Следовательно, $\triangle A'B'C' = \triangle ABC$ по трём сторонам, откуда $\angle A'B'C' = \angle ABC$, что и требовалось.

9.4. *Решение:* Пусть точки A, B и C лежат на одной прямой, причём B — между A и C, а точки A', B' и C' являются их образами при движении f. Заметим, что тогда $A'C' = AC = AB + BC = A'B' + B'C'$. Следовательно, неравенство треугольника ($A'C' < A'B' + B'C'$) не выполняется и точки A', B' и C' лежат на одной прямой.

9.5. *Решение:* Пусть точки X и Y перешли в точки X' и Y' под действием осевой симметрии S_l. Если $X, Y \in l$, то они неподвижны и доказывать нечего. Если $X \in l$, но $Y \notin l$, то $X' = X$ и треугольник XYY' — равнобедренный, поскольку его высота совпадает с медианой, откуда $XY = X'Y'$. Наконец, если ни одна из исходных точек не лежит на прямой, обозначим за Z точку пересечения YY' и l. Как было показано выше, $XZ = X'Z$, а $\angle XZY = \angle X'ZY'$ как углы, дополняющие равные углы до 90°. Значит, $\triangle XZY = \triangle X'ZY'$ по двум сторонам и углу между ними, откуда $XY = X'Y'$.

Пусть точки X и Y перешли в точки X' и Y' при повороте вокруг точки O на угол ϕ. Тогда $XO = X'O$, $YO = Y'O$ по определению, а кроме того, $\angle XOY = \angle X'OY'$. Поэтому $\triangle XOY = \triangle X'OY'$ по двум сторонам и углу между ними, откуда $XY = X'Y'$.

9.6. *Ответ:* а) Векторы $\overrightarrow{XY}$ и $\overrightarrow{X'Y'}$ имеют одинаковую длину и являются противоположно направленными.

б) Композиция центральных симметрий S_{O_1} и S_{O_2} суть параллельный перенос на вектор $2\overrightarrow{O_1O_2}$.

9.7. *Ответ:* Параллельный перенос на вектор $\overrightarrow{O_1O'}$, где $O' = R_{-\varphi,O_2}(O_1)$.

9.8. *Ответ:* б) Точку O можно найти как пересечение срединных перпендикуляров к отрезкам $O_1R_{\varphi_2,O_2}(O_1)$ и $O_2R_{-\varphi_1,O_1}(O_2)$.

9.9. *Решение:* Достаточно заметить, что тождественное отображение и осевая симметрия имеют бесконечно много неподвижных точек.

9.10. *Решение:* Зная образ $f(A)$, мы понимаем, что $f(D)$ лежит на окружности с центром $f(A)$ радиуса AD. Зная образы $f(A)$ и $f(B)$, мы локализуем $f(D)$ как точку

пересечения двух таких окружностей. Добавляя точку C, мы вводим в рассмотрение третью окружность, а поскольку $f(A)$, $f(B)$ и $f(C)$ не лежат на одной прямой, все три окружности не могут пересекаться более чем в одной точке. Что и означает, что образ точки D определён однозначно.

12.10. Комплексные числа

10.1. *Ответ:* Комплексное сопряжение является движением, а именно, это осевая симметрия относительно вещественной оси Ox.

10.2. *Решение:* Прямое вычисление: если $z = x + iy$, то

$$\frac{z+\bar{z}}{2} = \frac{x+iy+x-iy}{2} = \frac{2x}{2} = x \qquad \text{и} \qquad \frac{z-\bar{z}}{2i} = \frac{x+iy-x+iy}{2i} = \frac{2iy}{2i} = y.$$

Осталось воспользоваться определением: $x = \operatorname{Re}(z)$ и $y = \operatorname{Im}(z)$.

10.3. *Ответ:* $-6 + 5i$.

10.4. *Ответ:* $5 - 5i$.

10.5. *Ответ:* $r = \sqrt{x^2+y^2}$, $\theta = \operatorname{arctg}(y/x)$.

10.6. *Решение:* Проведём доказательство индукцией по n.

База индукции: при $n = 1$ тривиальным образом выполняется.

Шаг индукции: пусть $(\cos\varphi + i\sin\varphi)^k = \cos k\varphi + i\sin k\varphi$ справедливо для некоторого натурального k. Тогда для $k+1$:

$$(\cos\varphi + i\sin\varphi)^{k+1} = (\cos\varphi + i\sin\varphi)^k(\cos\varphi + i\sin\varphi) = \\ (\cos k\varphi + i\sin k\varphi)(\cos\varphi + i\sin\varphi) = \cos(k+1)\varphi + i\sin(k+1)\varphi.$$

10.7. *Ответ:* $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$, $\sin 3\alpha = 3\sin\alpha - 4\sin^3\alpha$.

Указание: Воспользуйтесь формулой Муавра и биномом Ньютона.

10.8. *Решение:* Прямое вычисление:

а) $(\omega_1 \cdot \omega_2)^n = \omega_1^n \cdot \omega_2^n = 1 \cdot 1 = 1$, $\left(\dfrac{\omega_1}{\omega_2}\right)^n = \dfrac{\omega_1^n}{\omega_2^n} = \dfrac{1}{1} = 1$.

б) $(\varepsilon \cdot \omega)^n = \varepsilon^n \cdot \omega^n = 1 \cdot w = w$.

10.9. *Решение:* Раскроем скобки в правой части и воспользуемся тем, что ω — корень уравнения $z^3 = 1$, не равный единице, то есть $\omega^3 = 1$ и $\omega^2 + \omega = -1$:

$$(x+y)(x+\omega y)(x+\omega^2 y) = (x+y)(x^2+\omega xy+\omega^2 xy+\omega^3 y) = (x+y)(x^2-xy+y^2) = x^3+y^3.$$

10.10. *Ответ:* а) $\left\{-\dfrac{1}{2} \pm i\dfrac{\sqrt{3}}{2}\right\}$;

б) $\{1+i,\ -2i\}$;

в) $\{\pm\sqrt{2} \pm \sqrt{i}\}$.

10.11. *Ответ:* а) $z^2 + 1 = (z+i)(z-i)$;

б) $z^3+z-2=(z-1)\left(z+\dfrac{1+i\sqrt{7}}{2}\right)\left(z+\dfrac{1-i\sqrt{7}}{2}\right)$;

в) $z^n-1=\prod\limits_{k=0}^{n-1}\left(z-\cos\dfrac{2\pi k}{n}-i\sin\dfrac{2\pi k}{n}\right)$.

10.12. *Ответ:* а) Прямая $x=3$, канонический вид: $z-\bar{z}-6=0$.

б) Окружность с центром в точке $(2,-1)$ и радиусом 3,
канонический вид: $z\bar{z}+(-2-i)z+(-2+i)\bar{z}-4=0$.

в) Срединный перпендикуляр к отрезку с концами в точках $(-1,0)$ и $(0,1)$,
канонический вид: $(1-i)z+(1+i)\bar{z}=0$.

10.13. *Решение:* Примените к числу z последовательно отражение относительно оси Ox, поворот на 90° по часовой стрелке и параллельный перенос на $-1+3i$. В результате получится $-\dfrac{3}{2}+\dfrac{5}{2}i$.

10.14. *Ответ:* а) Пусть точки A, B и C лежат на одной прямой, а A', B' и C' — их образы при гомотетии. Тогда

$$\frac{OA}{AA'}=\frac{OB}{BB'}=\frac{OC}{CC'},$$

откуда по теореме обратной к теореме о пропорциональных отрезках имеем $A'B'\parallel AB$ и $BC\parallel B'C'$. Поэтому точки A', B' и C' лежат на одной прямой.

Для проверки второго утверждения выберем систему координат, в которой центр гомотетии O совпадает с началом координат. Тогда при гомотетии произвольная точка плоскости (x,y) перейдёт в точку $(x',y')=(kx,ky)$. Следовательно, окружность

$$(x-a)^2+(y-b)^2=R^2 \qquad \Leftrightarrow \qquad (kx-ka)^2+(ky-kb)^2=(kR)^2$$

перейдёт в окружность $(x-ka)^2+(y-kb)^2=(kR)^2$.

б), в) Пусть треугольник ABC перешёл в треугольник $A'B'C'$ при гомотетии с коэффициентом k. Тогда

$$\frac{A'B'}{AB}=\frac{B'C'}{BC}=\frac{C'A'}{CA}=|k|,$$

откуда треугольники ABC и $A'B'C'$ подобны с коэффициентом k по трём сторонам. В частности, их соответствующие углы равны.

10.15. *Ответ:* $z\mapsto k(z-a)+a$.

10.16. *Ответ:* Выберем систему координат так, чтобы инверсия производилась относительно единичной окружности с центром в начале координат. Поскольку при этом

$$z\mapsto z'=\frac{1}{\bar{z}} \qquad \text{и} \qquad \bar{z}\mapsto \bar{z'}=\frac{1}{z},$$

то обобщённая окружность, заданная формулой

$$az\bar{z}+bz+\bar{b}\bar{z}+c=0 \qquad \Leftrightarrow \qquad a+\frac{b}{\bar{z}}+\frac{\bar{b}}{z}+\frac{c}{z\bar{z}},$$

перейдёт в обобщённую окружность $a'z'\bar{z'}+b'z'+\bar{b'}\bar{z'}+c'=0$, где $a'=c$, $b'=\bar{b}$ и $c'=a$.

Литература

[1] *Верещагин Н.К., Шень А.*, Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств (4-е издание) — Москва, МЦНМО, 2012.

[2] *Верещагин Н.К., Шень А.*, Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления (4-е издание) — Москва, МЦНМО, 2012.

[3] *Виленкин Н.Я.*, Комбинаторика — Москва, Наука, 1969.

[4] *Виленкин Н.Я.*, Рассказы о множествах (3-е издание) — Москва, МЦНМО, 2005.

[5] *Генкин С.А., Итенберг И.В., Фомин Д.В.*, Ленинградские математические кружки — Киров, АСА, 1994.

[6] *Голенищева–Кутузова Т.И., Казанцев А.Д., Кудряшов Ю.Г., Кустарёв А.А., Мерзон Г.А., Ященко И.В.*, Математический анализ в 57-й школе. Четырехгодичный курс. Часть I — Москва, МЦНМО, 2010.

[7] *Голенищева–Кутузова Т.И., Казанцев А.Д., Кудряшов Ю.Г., Кустарёв А.А., Мерзон Г.А., Ященко И.В.*, Математический анализ в 57-й школе. Четырехгодичный курс. Часть II — Москва, МЦНМО, 2010.

[8] *Головина Л.И., Яглом И.М.*, Индукция в геометрии (Выпуск 21 из серии «Популярные лекции по математике») — Москва, Физматгиз, 1961.

[9] *Давидович Б.М., Пушкарь П.Е., Чеканов Ю.В.*, Математический анализ в 57-й школе. Четырехгодичный курс. — Москва, МЦНМО, 2008.

[10] *Заславский А.А., Пермяков Д.А., Скопенков А.Б., Скопенков М.Б., Шаповалов А.В.*, Математика в задачах. — Москва, МЦНМО, 2009.

[11] *Калужин Л.А.*, Основная теорема арифметики (Выпуск 47 из серии «Популярные лекции по математике») — Москва, Наука, 1969.

[12] *Канель-Белов А.Я., Ковальджи А.К.*, Как решают нестандартные задачи. (4-е издание) — Москва, МЦНМО, 2008.

[13] *Курант Р., Робинс Г.*, Что такое математика? (3-е издание) — Москва, МЦНМО, 2001.

[14] *Понарин Я.П.*, Алгебра комплексных чисел в геометрических задачах — Москва, МЦНМО, 2004.

[15] *Соминский И.С.*, Метод математической индукции (Выпуск 3 из серии «Популярные лекции по математике») — Москва, Наука, 1965.

[16] *Успенский В.А.*, Простейшие примеры математических доказательств, Библиотека «Математическое просвещение», выпуск 34 (2-е издание) — Москва, МЦНМО, 2012.

[17] *Фомин С.В.*, Системы счисления (Выпуск 40 из серии «Популярные лекции по математике») — Москва, Физматгиз, 1987.

[18] *Шень А.*, Задачи по математике, предлагавшиеся ученикам математического класса 57 школы (выпуск 2000 года, класс «В») — Москва, МЦНМО, 2000.

[19] *Шень А.*, Математическая индукция (5-е издание) — Москва, МЦНМО, 2016.