Материалы летней школы «Матфак: предисловие»

под редакцией Хайдара Нурлигареева

Москва, 30 августа 2021 г.

Предисловие к летней школе 2021

Настоящее пособие представляет собой раздаточные материалы летней школы математического факультета «Матфак: предисловие 2021». 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 2021 году.

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 2021 года приведён в соответствующем разделе. Объём предлагаемого видеоматериала довольно большой: так, в 2021 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.

   При желании участник может заменить просмотр видеолекций **чтением брошюры,** поскольку содержащийся в ней теоретический материал дублирует, а зачастую перекрывает информацию, поданную в видеоформате. Можно также дополнять или замещать ознакомление с видеолекциями и брошюрой какими-либо внешними источниками. Однако в последнем случае есть риск потерять систематичность изложения, поэтому мы бы не рекомендовали этот путь тем, кто видит предложенные темы впервые.

2. **Семинарские занятия.** Традиционно 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 2021 году наполненность групп составляла 8-10 человек в начале школы, а семинары проходили в формате видеоконференций при помощи платформ zoom и discord. Продолжительность одного семинарского занятия составляла 1 час 20 минут, посередине занятия был 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 2021 году для приёма задач использовалась платформа discord, в среднем на него отводилось около часа в день.

Нам бы хотелось особо подчеркнуть значимость математического практикума. К сожалению, часто случается, что участники недооценивают приносимую им пользу. 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 2021 года, снабжённый интерактивными ссылками на видео, размещённые на платформе youtube, — они помечены синим цветом. 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 задачам, 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 технических задач, прорешав которые, читатель может убедиться в том, что он усвоил основные понятия и методы, изложенные в главе. Помочь в достижении этой цели призваны Ответы и указания к упражнениям задачам, размещённые в конце брошюры для самоконтроля. Наконец, третья 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 потребностей аудитории. В том случае, когда задач по теме подобралось много, часть из них помечена символом **(С)**, что означает, что это задача предназначена 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 должны затрагивать 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.

Электронная версия этого пособия снабжена множеством активных гиперссылок. Часть из них отмечена синим — это касается, прежде всего, ссылок на различные разделы в оглавлении и ссылок на внешние ресурсы. Другие, такие как ссылки на теоремы, упражнения, задачи, рисунки и прочее, цветом не выделены, однако щелчок мыши по ним переведёт читателя на соответствующую объекту страницу брошюры. Мы надеемся, что подобный функционал поможет читателю быстрее находить нужную ему информацию и не тратить время на дополнительные поиски.

Отметим, что в 2021 году в некоторых аспектах видеолекции довольно заметно отличались от теоретического материала брошюры. Это связано с тем, что часть видео записывалась исходя из потребностей летних школ 2019-2020 годов, а возможности по внесению в них изменений в связи с непростой эпидемиологической ситуацией были ограничены. Также нельзя обойти вниманием тот факт, что заметная часть брошюры верстались 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 четыре 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, Андрей Коновалов, Семён Молоков, Иван Никитин, Анастасия Шепелевцева и Иван Яковлев. В не меньшей степени нужно благодарить авторов видеоматериалов, на основе которых была написана брошюра, — Владислава Балакирева, 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 первых 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 и выпускникам 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,
30 августа 2021 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], [17]). 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, при должном старании последних, 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, и поддавшись соблазну почивать на лаврах можно быть уверенным, что эта дорога рано или поздно 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) и Отображения (Владлен Тиморин)
   Рекомендованная скорость воспроизведения: 1.25.
3. Математическая индукция (Александр Штерн)
   Рекомендованная скорость воспроизведения: 1.25.
4. Делимость целых чисел (Владислав Балакирев)
   Рекомендованная скорость воспроизведения: 1.25.
5. Комбинаторика (Андрей Рябичев)
   Рекомендованная скорость воспроизведения: 1.5.
6. Делимость многочленов (Владислав Балакирев)
   Рекомендованная скорость воспроизведения: 1.25
7. Сравнения (Мария Матушко)
   Рекомендованная скорость воспроизведения: 1.5.
8. Действительные числа (Алексей Клименко)
   Рекомендованная скорость воспроизведения: 1.5.
9. Движения плоскости и векторы (Александр Тихомиров)
   Рекомендованная скорость воспроизведения: 1.75.
10. 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 — конструктивный подход (Алексей Клименко)
   Рекомендованная скорость воспроизведения: 1.5.
4. Мера: длина, площадь, объём (Алексей Клименко)
   Рекомендованная скорость воспроизведения: 1.5.

Вступительный тест

Задачи для оценки текущего уровня

1. Математическая логика

Задача 0.1. Для какой пары высказываний A и B ложно высказывание $A \to B$?
1) A : «5 — чётное число», B : «Все лебеди белые»;
2) A : «5 — чётное число», B : «Париж — столица Франции»;
3) A : «Париж — столица Франции», B : «5 — чётное число»;
4) A : «Все лебеди белые», B : «5 — чётное число»;
5) среди ответов 1)–4) нет верного;
6) среди ответов 1)–4) нет неверного.

Задача 0.2. Какая из пропозициональных формул ниже эквивалентна формуле $\neg(A \to B) \wedge C$?
1) $\neg(A \to (C \to B))$;
2) $A \vee \neg B \vee C$;
3) $\neg A \to (B \wedge C)$;
4) $\neg(X \to Y) \wedge Z$.

Задача 0.3. Сколько строк в таблице истинности для формулы $X \to Y \wedge \neg A \vee B \leftrightarrow P \vee Q$?

Задача 0.4. Какая из пропозициональных формул ниже эквивалентна пропозициональной формуле $X \to Y \wedge \neg A \vee B \leftrightarrow P \vee Q$?
1) $(X \to ((Y \wedge \neg A) \vee B)) \leftrightarrow (P \vee Q)$;
2) $(X \to (Y \wedge (\neg A \vee B))) \leftrightarrow (P \vee Q)$;
3) $X \to ((Y \wedge \neg A) \vee B) \leftrightarrow (P \vee Q))$;
4) $((X \to Y) \wedge (\neg A \vee (B \leftrightarrow P))) \vee Q$.

Задача 0.5. Какая из формул ниже является записью утверждения «Для любого целого числа x существует целое число y такое, что $x + 2y$ кратно 5»?
1) $\forall x \in \mathbb{Q}\ \exists y \in \mathbb{R} :\ 5 \mid (x + 2y)$;
2) $\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z} :\ 5 \mid (x + 2y)$;
3) $\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z} :\ 5 \mid 2y$;
4) $\exists x \in \mathbb{Z}\ \forall y \in \mathbb{Z} :\ 5 \mid (x + 2y)$.

Задача 0.6. Какой из формул ниже выражается отрицание утверждения «Для любого целого числа x существует целое число y такое, что $x + 2y$ кратно 5»?
1) $\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z} :\ 5 \nmid (x + 2y)$;
2) $\exists y \in \mathbb{Z}\ \forall x \in \mathbb{Z} :\ 5 \nmid (x + 2y)$;
3) $\exists x \in \mathbb{Z}\ \forall y \in \mathbb{Z} :\ 5 \nmid (x + 2y)$;
4) $\forall y \in \mathbb{Z}\ \exists x \in \mathbb{Z} :\ 5 \nmid (x + 2y)$.

2. Множества и отображения

Задача 0.7. Сколько элементов в множестве A, если $A = \{x \mid 1 \leqslant x \leqslant 45, x \text{ делится на } 5\}$?

Задача 0.8. Из скольких элементов состоит пересечение множеств

$$\{0, 17, 36, 99, 572\} \qquad \text{и} \qquad \{9n \mid n \in \mathbb{N}, 1 \leqslant n \leqslant 12\}?$$

Задача 0.9. На окружности отмечено несколько чёрных точек и одна белая. Чего больше: выпуклых многоугольников, у которых все вершины чёрные, или выпуклых многоугольников, у которых одна белая вершина, а все остальные чёрные?

1) у которых все вершины чёрные;
2) у которых одна белая вершина, а все остальные чёрные;
3) поровну;
4) зависит от количества чёрных точек.

Задача 0.10. Между какими из следующих множеств существует биекция?

1) $\{2, 4, 6\}$ и $\{8, 10\}$;
2) $\{x, y\}$ и $\{1, 2\}$;
3) $\{a, b, c\}$ и $\{m, n\}$.

Задача 0.11. Пусть T и C – множества всех треугольников и всех окружностей на плоскости соосвественно. Рассмотрим отбражение $f : T \to C$ ставящее треугольнику в соответствие его описанную окружность. Какими из перечисленных свойств обладает отображение f?

1) сюръективность;
2) инъективность;
3) обоими;
4) никаким.

Задача 0.12. Какое из следующих множеств является счётным?

1) множество всех подмножеств отрезка $(0, 1)$;
2) множество всех целых чисел без числа 3;
3) множество всех лучей на оси абсцисс;
4) никакое.

Задача 0.13. Какое из следующих множеств является счётным?

1) множество всех окружностей на плоскости;
2) множество квадратов площадью 1 на плоскости;
3) множество треугольников с вершинами в точках с целыми координатами на плоскости;
4) никакое.

Задача 0.14. В олимпиаде по математике приняло участие 40 учащихся. Им было предложено решить одну задачу по алгебре, одну по геометрии и одну по тригонометрии. Задачу по алгебре решили 20 человек, по геометрии — 18 человек, по тригонометрии — 18 человек. Задачи по алгебре и геометрии решили 7 человек, по алгебре и тригонометрии — 9 человек, по геометрии и тригонометрии — 7 человек. Ни одной задачи не решили 3 человека. Сколько учащихся решили все задачи?

3. Математическая индукция

Задача 0.15. Верно ли следующее рассуждение?

«Докажем по индукции, что все собаки красные. В самом деле, допустим, для любого $n \geqslant k$ утверждение доказано. Рассмотрим произвольную свору из $n = k + 1$ собаки. Отбросив последнюю из них, получим свору из k собак, которые, по предположению, все являются красными. Теперь, напротив, исключим из рассмотрения первую собаку. Снова получим свору из k собак, которые красные по предположению индукции. Объединяя эти два вывода, получаем, что все $n = k + 1$ собак красные, что и требовалось доказать.»

1) Утверждение верное, рассуждение верное.
2) Утверждение верное, но в базе индукции ошибка.
3) Утверждение верное, но в индукционном переходе ошибка.
4) Утверждение неверное, ошибка в базе индукции.
5) Утверждение неверное, ошибка в индукционном переходе.

Задача 0.16. Верно ли следующее рассуждение?

«Для любого натурального n произвольные n точек плоскости лежат на одной прямой. При $n = 1$ утверждение, очевидно, верно. Предположив, что утверждение верно для $n = k$, докажем его для $n = k + 1$. Возьмём произвольные $k + 1$ точек. Точки $1, \ldots, k$ лежат на одной прямой, точки $2, \ldots, k + 1$ лежат на одной прямой (по предположению индукции), следовательно, все они лежат на единственной прямой, проходящей через точки $2, \ldots, k$.»

1) Утверждение верное, рассуждение верное.
2) Утверждение верное, но в базе индукции ошибка.
3) Утверждение верное, но в индукционном переходе ошибка.
4) Утверждение неверное, ошибка в базе индукции.
5) Утверждение неверное, ошибка в индукционном переходе.

Задача 0.17. Верно ли следующее рассуждение?

«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 будет остроугольным. По индукции теорема доказана.»

1) Утверждение верное, рассуждение верное.
2) Утверждение верное, но в базе индукции ошибка.
3) Утверждение верное, но в индукционном переходе ошибка.
4) Утверждение неверное, ошибка в базе индукции.
5) Утверждение неверное, ошибка в индукционном переходе.

Задача 0.18. В колонию из 100 бактерий попал 1 вирус. Каждую секунду каждый из вирусов уничтожает одну бактерию, удваиваясь при этом. Все оставшиеся в живых бактерии тоже удваиваются. Правда ли, что через некоторое время все бактерии погибнут? Если да, то через сколько секунд?

Задача 0.19. На какое число частей делят плоскость 100 прямых, никакие две из которых не параллельны и никакие три из которых не проходят через одну точку?

Задача 0.20. Чему равна сумма углов выпуклого 100-угольника (в градусах).

4. Делимость целых чисел

Задача 0.21. Сколькими нулями оканчивается число 37!?

Задача 0.22. Сколько решений имеет диофантово уравнение $2x + 3y = 1$?

Задача 0.23. Найдите последнюю цифру числа $2^{2021} + 9^{2019}$.

Задача 0.24. Известно, что чётное число n имеет ровно 7 различных положительных делителей, включая 1 и само n. Найдите это число.

Задача 0.25. Сколько положительных делителей имеет число 900?

Задача 0.26. Найдите максимальное (натуральное) число n, такое что 40! делится на 2^n.

Задача 0.27. У числа 2020! посчитали сумму цифр, затем у получившегося числа тоже посчитали сумму цифр и т.д. Так продолжали до тех пор, пока не получилось однозначное (состоящее из одной цифры) число. Какое?

5. Комбинаторика

Задача 0.28. Имеется 12 волейбольных команд, каждая команда должна сыграть со всеми другими командами ровно один раз. Сколько матчей состоится в турнире?

Задача 0.29. Имеется 3 пары брюк, 4 пары ботинок и 5 рубашек. Сколькими способами можно одеться?

Задача 0.30. Сколько существует пятизначных чисел, в записи которых нет цифры 6?

6. Многочлены

Задача 0.31. Найдите коэффициент при x^{2018} многочлена $(1 + x)^{2020}$.

Задача 0.32. Найдите остаток от деления многочлена $f(x) = x^{150} + x + 4$ на $(x - 1)$.

Задача 0.33. Пусть $f(x) = x^2 + bx + c$, где b и c – целые числа. Известно, что число $\lambda = 1 + \sqrt{3}$ является корнем многочлена $f(x)$. Найдите $f(-1)$.

7. Сравнения

Задача 0.34. Решите в целых числах уравнение $x^2 + y^2 = 3z^2$.

Задача 0.35. Найдите минимальное трёхзначное решение сравнения $7x \equiv 3 \pmod{15}$.

Задача 0.36. Найдите остаток от деления 12^{100} на 13.

Задача 0.37. Найдите остаток от деления $14^{14^{14}}$ на 17.

Задача 0.38. Найдите остаток от деления $1 \cdot 2 \cdot 3 \cdot \ldots \cdot 96$ на 97.

Задача 0.39. Найдите наименьшее натуральное число, дающее при делении на $2, 3, 5, 7$ остатки $1, 2, 4, 6$ соответственно.

Задача 0.40. Найдите наименьшее четырёхзначное решение системы сравнений:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

9. Движения плоскости

Задача 0.41. Пусть K — фигура, изображенная на рис. 1. Сколько существует движений $f : \mathbb{R}^2 \to \mathbb{R}^2$ таких, что $f(K) = K$ (включая тривиальный случай)?

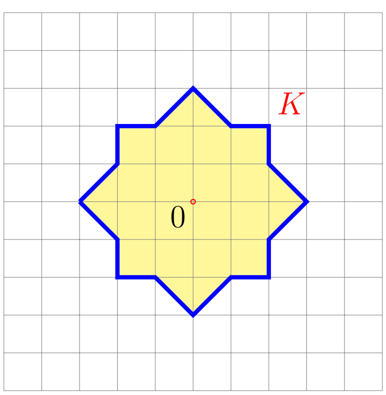

Рис. 1.

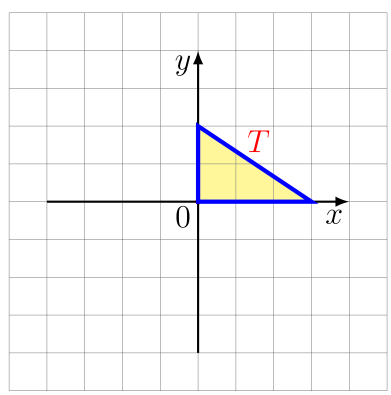

Рис. 2.

Задача 0.42. Пусть S_x и S_y — отражения относительно прямых Ox и Oy соответственно, а R_{90°, R_{180° и R_{270° — повороты против часовой стрелки на указанное число градусов. Среди всех композиций, состоящих из трёх указанных движений, найдите число тех, которые переводят треугольник T в себя (рис. 2).

10. Комплексные числа

Задача 0.43. Вычислите $5i^7 \cdot 7i^5$.

Задача 0.44. Найдите $\left|\dfrac{1+2i}{3-4i}\right|^2$.

Задача 0.45. Среди комплексных чисел, отмеченных на рис. 3, укажите обратное к z:

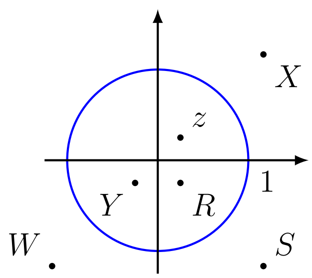

Рис. 3.

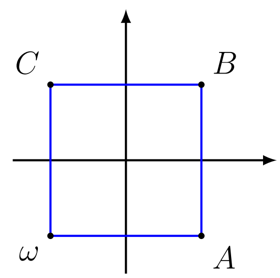

Рис. 4.

Задача 0.46. Вычислите $\left(\dfrac{1}{4}-\dfrac{\sqrt{3}}{4}i\right)^9$.

Задача 0.47. При условии, что $z^{2021}=1$ и $z\neq 1$, вычислите $\dfrac{1}{1+z}+\dfrac{1}{1+z^2}+\ldots+\dfrac{1}{1+z^{2021}}$.

Задача 0.48. На рис. 4 изображен квадрат, одна из его вершин соответствует комплексному числу ω. Установите соответствие между множествами $\{\overline{\omega}, -\omega, i\omega\}$ и $\{A, B, C\}$.

Задача 0.49. Какие из комплексных чисел, указанных ниже, лежат на прямой, проходящей через точки $1+i$ и $5-3i$?

1) $2+i$;
2) $-2+5i$;
3) $9-7i$.

Задача 0.50. Найдите произведение корней уравнения $x^3+x^2+x+1=0$.

Задача 0.51. Укажите верные утверждения.

1) Для любого комплексного числа z величина $z\cdot\bar{z}$ является вещественным.

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

3) Если p — многочлен, для которого $p(z)=i$, то $p(\bar{z})=i$.

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

5) Произведение всех корней 7-ой степени из единицы равно 1, а сумма равна (-1).

6) Пусть точка X имеет комплексную координату $27-4i$, точка Y — координату $2-10i$. Тогда прямая, проходящая через Y и точку с координатой $-4+15i$, перпендикулярна прямой XY.

Задача 0.52. Найдите наименьшее значение выражения $|z-5|+|z+7-5i|$.

11. Прочее

Задача 0.53. Существует ли натуральное N такое, что для всех n выполнено неравенство

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

Если да, укажите минимальное среди таких чисел.

Задача 0.54. Существует ли натуральное N такое, что для всех n выполнено неравенство

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} < N$$

Если да, укажите минимальное среди таких чисел.

1. 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* — это повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности.

Пример 1.2.
- A : «Все лебеди белые»;
- B : «5 – нечётное число»;
- C : «Нью-Йорк – столица США».

Определение 1.3. Есть 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. *Каковы истинностные значения высказываний в примере 1.2?*

Определение 1.4. *Логическая операция* – способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний.

Определение 1.5. 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 1.6. В отличие от математического языка, в естественном языке чаще используется так называемое «исключающее или». Иными словами, говоря «X или Y», скорее всего, мы имеем в виду, что истинно либо X, либо Y, но никак не оба высказывания.

Пример 1.7. 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 1.8. 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, запись «$\wedge)X\neg$» никакого смысла не имеет.

Определение 1.9. Элементарные высказывания, из которых строятся все остальные, называются *пропозициональными переменными*. Их мы обозначаем заглавными латинскими буквами.

Определение 1.10. *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 1.11. $X \wedge Y \vee Z$ и $X \wedge (Y \vee Z)$ — разные высказывания (см. пример 1.14).

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, содержащихся 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 1.12. 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 1.13. Формулы φ и ψ *эквивалентны*, если они истинны при одних и тех же значениях переменных.

Упражнение 1.4. *Докажите эквивалентность формул $X \wedge (X \to Y)$ и $X \wedge Y$ используя таблицы истинности.*

Пример 1.14. Построим и сравним таблицы истинности формул из примера 1.11. 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 1.15. Формула φ называется *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 1.16. 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 1.17. Аналогичным образом, 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 1.18. Если некоторое утверждение имеет вид импликации $X \to Y$, то утверждение $Y \to X$ называется *обратным* к нему.

Замечание 1.19. Истинность обратного утверждения никак не связана с истинностью прямого утверждения.

Пример 1.20. 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 1.21. Более того, даже если обратное утверждение верно, его доказательство может существенно отличаться от доказательства прямого, как по сложности, так и по содержанию.

Пример 1.22. 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 1.22.*

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. В самом деле, если Y ложно, то импликация $\neg X \to Y$ истинна тогда и только тогда, когда $\neg X$ ложно.

Определение 1.23. Рассмотренный выше метод доказательства называется *доказательством от противного.*

Пример 1.24. 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.*

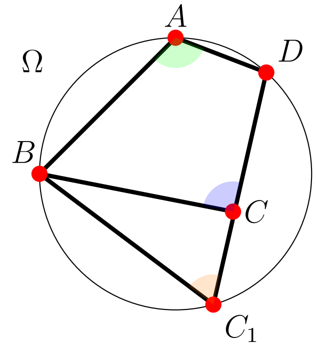

Рис. 5.

Доказательство. Рассмотрим четырёхугольник $ABCD$. Пусть, без ограничения общности, $\angle BAD + \angle BCD = 180°$. Рассмотрим окружность Ω, описанную около треугольника ABD. Допустим 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, откуда $\angle BCD = \angle BC_1D + \angle CBC_1$ (рис. 5). Если же точка C находится снаружи Ω, то внешним будет угол BC_1D в треугольнике BCC_1, что влечёт за собой $\angle BC_1D = \angle BCD + \angle CBC_1$. 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 1.25. 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 $n \vdots 5$, 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 $n = 10(m - 1) + 15$. Следовательно, 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 1.26. 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 1.27. Изменив порядок кванторов в предыдущем примере, получим следующую 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 1.26 и 1.27, 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 1.28. 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 1.29. 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, эквивалентные 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 которых равен 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

$$\bar{Q}_1 x_1 \ldots \bar{Q}_n x_n :\ \neg P(x_1, \ldots, x_n).$$

Здесь черта сверху означает замену квантора противоположным ($\forall$ на $\exists$ и наоборот).

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:

$A: \ (x \neq 1) \to (z \neq 2)$;
$B: \ ((y = 2) \vee (y = 3)) \to (x = 1)$;
$C: \ (y \neq 3) \to (z = 4)$;
$D: \ (t = 2) \to (y \neq 1)$;
$E: \ (t \neq 1) \to (y = 1)$.

Задача 1.11. Восьми мудрецам показали 5 красных, 4 синих и 2 белых колпака. В темноте на них надели 4 красных, 2 синих и 2 белых колпака, после чего включили свет и попросили назвать цвет надетых на них колпаков. Через некоторое время один из мудрецов правильно назвал цвет своего колпака. Какой на нём был колпак? (Мудрецы делают утверждения только в том случае, если уверены в их истинности.)

2. 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 2.1. $a \in A$ — 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 2.2. Множество чётных чисел можно записать как $\{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}:\, x = 2y\}$.

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) $\{$*Петя*$\}$,
г) $\{x \mid$ *буква* x *встречается в слове «крокодил»*$\}$*?*

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

2.2. Понятие подмножества. Критерий равенства множеств

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

Определение 2.3.
• Множество A называется *подмножеством* множества B (пишем $A \subset B$), если каждый элемент множества A является элементом множества B. Другими словами, $(x \in A) \to (x \in B)$.
• Два множества A и B *равны* ($A = B$), если они состоят из одних и тех же элементов: $(x \in A) \to (x \in B)$ и $(x \in B) \to (x \in A)$ 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 $y \in Y$.

Результаты операций удобно изображать схематическим образом с помощью *диаграмм Венна.* Так, на рис. 6 кружочками отмечены множества A, B и C, а красным закрашены области, соответствующие указанным снизу операциям. Диаграммы Венна можно использовать для проверки разных тождеств. Например, из рис. 6 д), б) и в) видно, что $(A \setminus B) \cup B = A \cup B$.

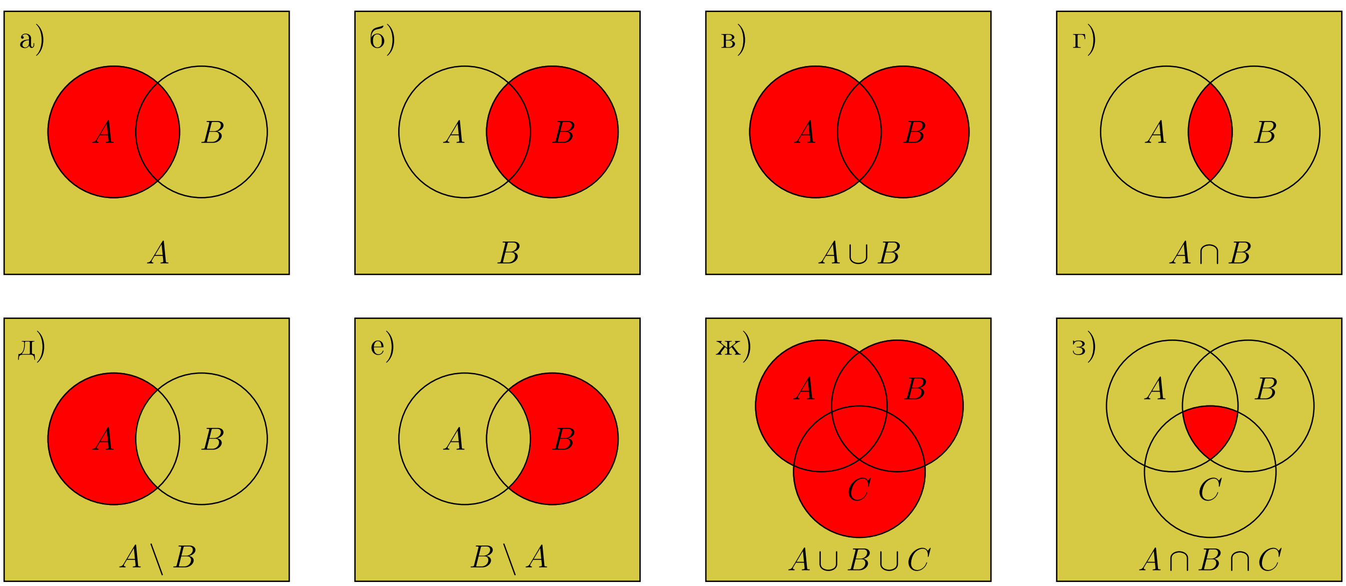

Рис. 6.

В общем случае для проверки тождеств используется критерий равенства множеств.

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

Упражнение 2.6. *Докажите, что для любых множеств A, B и C выполнены равенства:*
а) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$;
б) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

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.

Определение 2.4. *Бинарное отношение* на множестве X — это подмножество R декартова произведения $X \times X$.

Обозначение 2.5. Будем писать $x \sim y$, если $(x, y) \in R$.

Определение 2.6. Бинарное отношение называется *отношением эквивалентности*, если оно
а) *рефлексивно*: $x \sim x$ для каждого $x \in X$;
б) *симметрично*: $(x \sim y) \to (y \sim x))$ для всех $x, y \in X$;
в) *транзитивно*: $\big((x \sim y) \wedge (y \sim z)\big) \to (x \sim z)$ для всех $x, y, z \in X$.
Про элементы, связанные отношением эквивалентности, говорят, что они *эквивалентны*.

Пример 2.7. *Отношение равенства* $R = \{(x, x) \mid x \in X\}$ является важным примером отношения эквивалентности.

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

Определение 2.8. *Классом эквивалентности* элемента $x \in X$ называется множество

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

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.*

Пример 2.9. Рациональные числа можно рассматривать как классы эквивалентности декартова произведения $\mathbb{Z} \times \mathbb{N}$, если первый элемент пары $(m, n) \in \mathbb{Z} \times \mathbb{N}$ считать числителем, а второй — знаменателем. В самом деле, дробь не изменится, если домножить её числитель и знаменатель на одно и то же число. Поэтому отношение эквивалентности в этом случае задаётся следующим условием: $(m, n) \sim (p, q)$, если $mq = pn$.

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

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

$$k \equiv l \pmod m$$

на множестве всех целых чисел $\mathbb{Z}$ следующим образом: $(k - l)$ делится на m. Докажите, что отношение $\equiv$ является отношением эквивалентности.

б) Определим отношение на множестве $\mathbb{R}$ так: $x \sim y$, если существует $n \in \mathbb{Z}$ такое, что $(x - y) = \pi n$. Докажите, что это отношение эквивалентности. Каким объектам соответствуют классы эквивалентности по этому отношению?

2.5. Понятия отображения, функции и их графика

Неформально, мы хотим *сопоставлять* элементы двух множеств X и Y друг другу. Тогда интуитивно мы можем понимать *отображение* как некоторый способ это сделать. Формально:

Определение 2.10. *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 определения 2.10, отображение — это то же самое, что его *график*. Таким образом, запись $y = f(x)$ эквивалентна записи $(x, y) \in f$. Если множество Y — числовое, например, $\mathbb{Z}$, $\mathbb{Q}$ или $\mathbb{R}$, то отображение называют*функцией* и обозначают $f : X \to Y$.

Представление отображения с помощью стрелок: удобный способ изобразить отображение между конечными множествами — это нарисовать слева множество X, из которого бьёт наше отображение, а справа — множество Y, в которое бьёт наше отображение. Само же отображение мы можем представить в виде стрелок, то есть если при нашем отображении некоторая точка $x \in X$ переходит в некоторую точку $y \in Y$, то мы рисуем стрелку из x в y. Таким образом, из каждой точки множества X выходит ровно одна стрелка, и она ведет в множество Y (рис. 7).

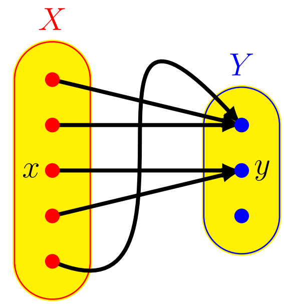

Рис. 7.

Упражнение 2.10. *Какие из чертежей, изображённых на рис. 8, соответствуют отображениям? Почему?*

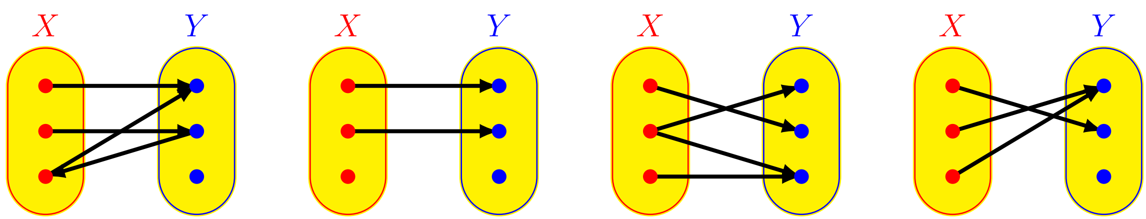

Рис. 8.

2.6. Образы и прообразы

Введём важные понятия образа и прообраза отображения.

Определение 2.11. Пусть $f : X \to Y$ — некоторое отображение.

• Для всякого подмножества $A \subset X$ определим $f(A)$ как

$$f(A) = \{f(a) \mid a \in A\} \subset Y.$$

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

• Для всякого подмножества $B \subset Y$ определим $f^{-1}(B)$ как

$$f^{-1}(B) = \{x \mid f(x) \in B\} \subset X.$$

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

Пример 2.12. Рассмотрим отображение $f : X \to Y$, изображённое на рис. 9. Заметим, что X является прообразом Y, что мы можем записать как $X = f^{-1}(Y)$. Однако множество Y не является образом множества X при заданном отображении: $f(X) = \{a, b, c\} \neq Y$).

Рассмотрим теперь прообразы конкретных элементов:

$$f^{-1}(a) = \{1, 2, 4\};$$
$$f^{-1}(b) = \{3, 5\};$$
$$f^{-1}(c) = \{6\};$$
$$f^{-1}(d) = \varnothing.$$

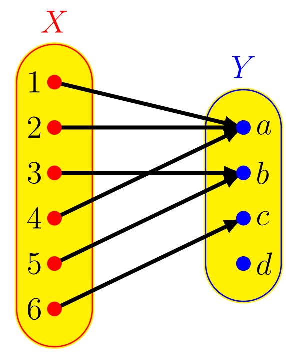

Рис. 9.

Таким образом, мы видим, что прообраз одного элемента (или даже подмножества) может состоять из какого угодно числа элементов.

Замечание 2.13. Когда множество состоит из одного элемента, то есть если $B = \{y\}$, фигурные скобки обычно опускают и пишут $f^{-1}(y)$ вместо $f^{-1}(\{y\})$.

Упражнение 2.11. *Для отображения $f : X \to Y$ из примера 2.12 укажите*
а) $f(A)$, если $A = \{1\}$, $A = \{1, 2\}$, $A = \{1, 2, 3\}$, $A = \{1, 3, 5\}$, $A = \{2, 4, 6\}$;
б) $f^{-1}(B)$, если $B = \{a\}$, $B = \{b, c\}$, $B = \{a, b, c\}$, $B = \{b, d\}$, $B = \{a, c, d\}$.

Упражнение 2.12. *Докажите, что для любого отображения $f : X \to Y$ всегда выполнено:*
а) $f^{-1}(Y) = X$;
б) $f^{-1}(\varnothing) = f(\varnothing) = \varnothing$.

2.7. Инъекция, сюръекция, биекция

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

Определение 2.14. Отображение $f : X \to Y$ называется

- *инъективным* (или *инъекцией*, или *вложением*), если для любых двух элементов $x, x' \in X$ равенство $f(x) = f(x')$ влечёт за собой $x = x'$;
- *сюръективным* (или *сюръекцией*, или *отображением НА*), если для всякого $y \in Y$ найдётся такой $x \in X$, что $f(x) = y$;
- *биективным* (или *биекцией*), если оно одновременно инъективно и сюръективно.

Биекции также называют *взаимно-однозначными соответствиями*.

Пример 2.15. Рассмотрим примеры со стрелками. На рис. 10 а) изображено отображение, которое является инъекцией, но не сюрьекцией. Инъекцией оно является по той причине, что разные стрелки заканчиваются в разных местах. А поскольку в элемент $c \in Y$ стрелка не входит, это не сюрьекция.

На рис. 10 б) мы можем видеть сюрьекцию, не являющуюся инъекцией. Дело в том, что во всех элементах множества Y заканчиваюся некоторые стрелки, но некоторые стрелки, исходящие из элементов 1 и 2, заканчиваются в одном и том же месте.

Наконец, в примере на рис. 10 в) мы видим биекцию (или взаимно-однозначное соответствие). То есть все стрелки ведут из разных точек в разные точки, и в каждой точке множества Y какая-то стрелка заканчивается. Вообще, термин взаимно-однозначное соответствие намекает на то, что все стрелки можно обратить. Если у нас есть биекция, то у всех стрелок можно поменять направление, так что получится новое отображение. Данное важное свойство *обратимости* будет подробно разобрано в следующем разделе.

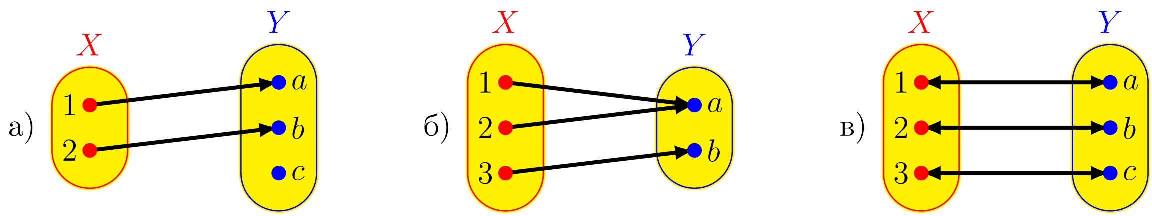

Рис. 10.

Оказывается, свойства отображений связаны с числом элементов в прообразах:

• 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 $y \in Y$).

Упражнение 2.13. *Постройте биекцию между множествами* $A \times B$ *и* $B \times A$.

Упражнение 2.14. *Перечислите все возможные отображения из множества* $\{7, 8, 9\}$ *в множество* $\{0, 1\}$. *Сколько среди них сюръекций, инъекций, биекций?*

2.8. 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:

Определение 2.16. Пусть $f : X \to Y$ и $g : Y \to Z$ — два отображения. Тогда их *композицией* называется отображение $g \circ f : X \to Z$, определенное формулой

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

для всякого $x \in X$.

Замечание 2.17. Обратите внимание, что в композиции $g \circ f$ сначала применяется отображение f, а потом — отображение g.

Для наглядности удобно изображать композицию в виде картинок со стрелками. Когда у нас есть два отображения f и g, мы рисуем три множества X, Y и Z, а также стрелки между ними. Стрелки между X и Y соответствуют отображению f, а стрелки между Y и Z — отображению g. Теперь нам нужно понять, как ведут себя стрелки, соответствующие композиции отбражений. Рассмотрим такие две стрелки из отображения f и из отображения g, что первая стрелка заканчивается там, где начинается вторая. Из этих двух стрелок можно составить *конкатенацию* (новую непрерывную стрелку, нарисованную «не отрывая карандаша»). Она и будет стрелкой композиции. Например, на рис. 11 слева.

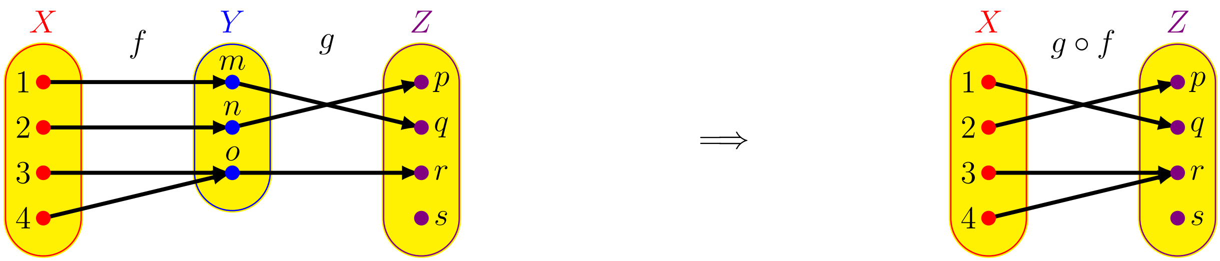

Рис. 11.

Дадим определения ещё двух понятий: тождественного и обратного отображений.

Определение 2.18.

• *Тождественное отображение* $\mathrm{id}_X : X \to X$ определяется формулой $f(x) = x$ для всякого $x \in X$ (рис. 12).

• Отображение $g : Y \to X$ называется *обратным* к отображению $f : X \to Y$, если выполнены следующие два условия:

$$g \circ f = \mathrm{id}_X \quad \text{и} \quad f \circ g = \mathrm{id}_Y.$$

Если такое отображение g существует, то отображение f называется *обратимым.*

• 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.

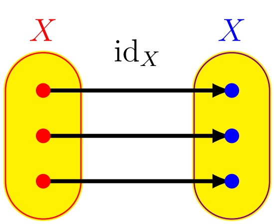

Рис. 12.

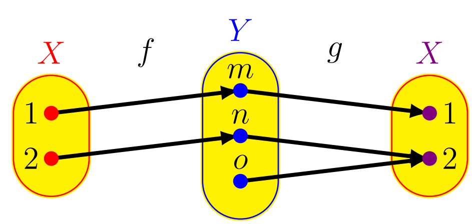

Рис. 13.

Пример 2.19. Если отображение $f : X \to Y$ инъективно, то у него есть левое обратное. В самом деле, для каждого элемента $x \in X$ рассмотрим $y = f(x)$ и положим $g(y) = x$. Для оставшихся элементов множества Y зададим отображение g произвольным образом (рис. 13). Из инъективности отображения f следует, что разным элементам из множества X соответствуют разные элементы множества Y, поэтому g определено корректно. И по построению $g(f(x)) = x$ для всех $x \in X$, то есть $g \circ f = \mathrm{id}_X$.

Упражнение 2.15. *Докажите, что если отображение $f : X \to Y$ сюръективно, то у него есть правое обратное.*

Объединяя пример 2.19 и упражнение 2.15, мы получаем нижеследующий критерий обратимости отображения.

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

Упражнение 2.16. *Убедитесь в том, что теорема 2.3 справедлива.*

Упражнение 2.17. *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?

2.9. Равномощные множества. Счётные множества и их свойства

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

Определение 2.20. 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:

Определение 2.21. Множество X называется *счётным*, если существует биекция между X и множеством $\mathbb{N}$ всех натуральных чисел.

Пример 2.22. Множества целых чисел $\mathbb{Z}$ и рациональных чисел $\mathbb{Q}$ счётны.

Упражнение 2.18. *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 2.19. *Убедитесь, что теоремы 2.4 и 2.5 справедливы.*

Упражнение 2.20. *Покажите, что множество рациональных чисел $\mathbb{Q}$ счётно.*

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

Обозначение 2.23. Пусть A — множество. Тогда $\mathcal{P}(A)$ — это *множество 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 2.21. *Приведите пример множества A из трёх элементов, для которого выполняется включение $A \subset \mathcal{P}(A)$.*

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. $\square$

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

Теорема 2.7. [Кантор] Множество бесконечных последовательностей из 0 и 1 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:

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

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.

2.11. (*) 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 $U \in U$. С одной стороны, если да, то U странное, но тогда по определению $U \notin U$. С другой стороны, если нет, то U обычное, а 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.

2.12. 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

Технические задачи

Задача 2.1. Даны множества $A = \{57, 91, 179, 239\}$, $B = \{91, 239, 2014\}$, $C = \{2, 57, 239, 2014\}$, $D = \{2, 91, 2014, 2017\}$. Найдите следующие множества:

а) $A \cup B$,
б) $A \cap B$,
в) $(A \cap B) \cup D$,
г) $C \cap (D \cap B)$,
д) $(A \cup B) \cap (C \cup D)$;
е) $(A \cap B) \cup (C \cap D)$,
ж) $(D \cup A) \cap (C \cup B)$;
з) $(A \cap (B \cap C)) \cap D$;
и) $(A \cup (B \cap C)) \cap D$,
к) $(C \cap A) \cup ((A \cup (C \cap D)) \cap B)$,
л) $(A \cup B) \setminus (C \cap D)$;
м) $(A \cup D) \setminus (B \cup C)$;
н) $A \setminus (B \setminus (C \setminus D))$;
о) $D \setminus ((B \cup A) \setminus C)$;
п) $((A \setminus (B \cup D)) \setminus C) \cup B$.

Задача 2.2. 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 2.3. Пусть A — множество чётных чисел, а B — множество чисел, делящихся на три. Найдите $A \cap B$.

Задача 2.4. Для каждого из указанных на рис. 14 отображений $f : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ найдите $f(\{1, 3\})$, $f(\{2, 3, 4\})$, $f^{-1}(a)$, $f^{-1}(\{a, b\})$ и $f^{-1}(\{b, d\})$.

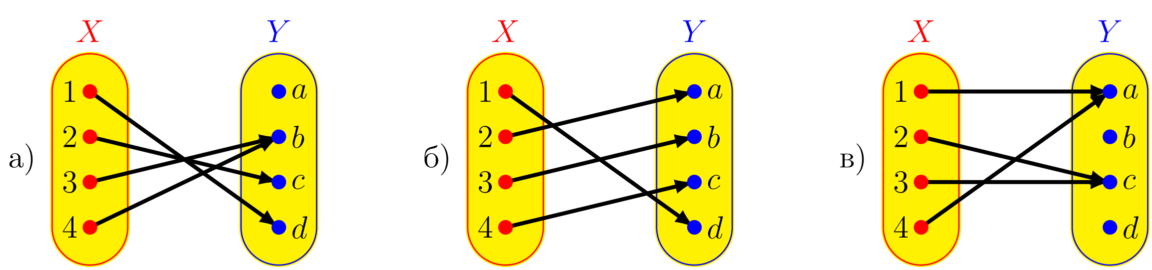

Рис. 14.

Задача 2.5. 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 2.6. Укажите все биекции из множества $\{1, 2, 3\}$ в себя.

Задача 2.7. Пусть $X = \{1, 2, 3, 5\}$, $Y = \{0, 1, 2\}$ и $Z = \{3, 7, 8, 9\}$. Отображения $f : X \to Y$, $g : Y \to Z$, $h : Z \to X$ изображены на рис. 15. Нарисуйте картинки для отображений:

а) $g \circ f$;
б) $f \circ g$;
в) $f \circ h$;
г) $h \circ g \circ f$;
д) $f \circ h \circ g$;
е) $g \circ h \circ f$;
ж) $f \circ h \circ g \circ f$;
з) $g \circ f \circ h \circ g$.

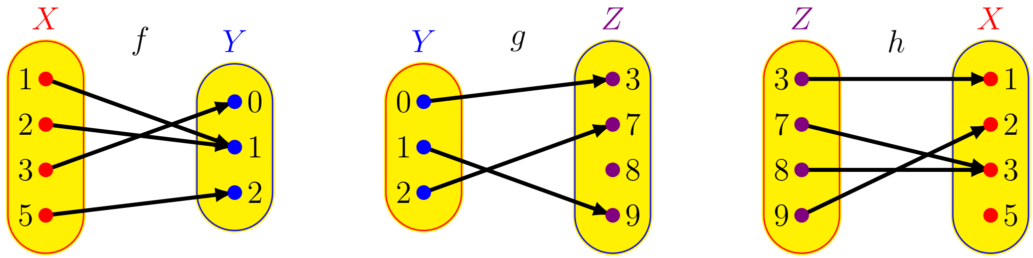

Рис. 15.

Задача 2.8. 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 $g \circ f$.

Множества и отображения

Задачи семинаров

2.1. Понятия множества и элемента. Различные способы задания множеств

Задача 2.9 (C)**.** 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 2.10 (C)**.** Верно ли, что множество летающих крокодилов является подмножеством множества ботинков на левую ногу? Обоснуйте ответ.

Задача 2.11 (C)**.** 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 2.12 (C)**.** Докажите, что для любых множеств A, B, C выполняется равенство:

а) $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$;

б) $(A \cap B) \setminus C = (A \setminus C) \cap B = (B \setminus C) \cap A$.

Задача 2.13. 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 2.14. 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 2.15 (С)**.** Выполнены ли свойства рефлексивности, симметричности и транзитивности для следующих отношений:

а) $x \sim y$, если x и y взаимно просты (см. определение 4.8), 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 $\mathbb{R}$?

Какие из рассмотренных отношений являются отношениями эквивалентности?

Задача 2.16. Является ли отношение $x < y$ на множестве всех действительных чисел отношением эквивалентности? Объясните ответ.

Задача 2.17. Постройте бинарное отношение C на 3-элементном множестве $\{x, y, z\}$ такое, что C рефлексивно и симметрично, но не транзитивно.

Задача 2.18. Сколько всего различных отношений эквивалентности на множестве из пяти элементов?

2.5. Понятия отображения, функции и их графика

Задача 2.19 (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. Образы и прообразы

Задача 2.20. 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 2.21 (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 2.22. 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. Инъекция, сюрьекция и биекция

Задача 2.23. Постройте биекцию между множествами $(A \times B) \times C$ и $A \times (B \times C)$.

Задача 2.24 (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 2.25. На окружности отмечено несколько черных точек и одна белая. Чего больше: выпуклых многоугольников, у которых все вершины черные, или выпуклых многоугольников, у которых одна белая вершина, а все остальные черные? Объясните ответ.

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

Задача 2.26 (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 2.27 (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 2.28. В цепочке отображений $A \to B \to C$ первое сюръективно, а второе не инъективно. Верно ли, что их композиция сюръективна? Не инъективна?

Задача 2.29. 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 2.30. 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 2.31. 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?

2.9. Равномощные множества. Счётные множества и их свойства

Задача 2.32 (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 2.33. Постройте биекцию между множеством $\mathbb{N} \times \mathbb{N}$ и множеством всех положительных чисел, которые делятся на 2 и 3, но не делятся на другие простые числа.

Дополнительные задачи

Задача 2.34. Докажите, что для любых множеств $A_1, \ldots, A_n$ и B выполняются равенства:
а) $(A_1 \cup \ldots \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \ldots \cup (A_n \cap B)$;
б) $(A_1 \cap \ldots \cap A_n) \cup B = (A_1 \cup B) \cap (A_2 \cup B) \cap \ldots \cap (A_n \cup B)$.

Задача 2.35. 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 2.36. Для каких множеств A, B выполнено равенство $\mathcal{P}(A \cup B) = \mathcal{P}(A) \times \mathcal{P}(B)$? Строго обоснуйте ответ.

3. Математическая индукция

Теоретический материал

3.1. Принцип минимального элемента

Мы принимаем за аксиому следующее утверждение.

Принцип минимального элемента: Каждое непустое подмножество множества натуральных чисел (в том числе, бесконечное) имеет минимальный элемент.

Замечание 3.1. Бесконечное подмножество множества натуральных чисел не имеет максимального элемента.

Пример 3.2. Пусть подмножество $S \subset \mathbb{N}$ состоит из чётных чисел. Тогда оно имеет минимальный элемент — это 2.

Упражнение 3.1. *Существует ли минимальный элемент в множестве S, если*
а) $S = \mathbb{Z}$ — множество целых чисел;
б) $S = [0, 1]$ — отрезок;
в) $S = (0, 1)$ — интервал.

3.2. Метод математической индукции

Метод математической индукции, которому посвящён этот раздел, очень полезен для доказательства различных результатов и является следствием принципа минимального элемента. По индукции мы доказываем утверждения, содержащие параметр n, который может принимать любые натуральные значения. А также утверждения, которые изначально выглядят иначе, но могут быть переформулированы таким образом.

Пример 3.3. При любом натуральном $n > 4$ выполнено неравенство $2^n > n^2$.

Пример 3.4. Число, десятичная запись которого состоит из 3^n единиц, делится на 3^n.

Пример 3.5. 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.

Схема метода математической индукции:
• *База индукции*: доказываем первое утверждение из последовательности.
• *Индукционный переход*: доказываем, что каждое из этих утверждений (кроме первого) 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. $\square$

На практике нумерация утверждений часто начинается не с единицы, как можно видеть, скажем, в примере 3.3, однако метод принципиально не меняется — изменения, которые нужно сделать в доказательстве, очевидны.

Упражнение 3.2. *Докажите утверждения из примеров 3.3, 3.4 и 3.5, используя метод математической индукции.*

3.3. Разбор базовых примеров

Для начала вернемся к примерам из предыдущего раздела.

Пример 3.3. 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:

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

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

Пример 3.4. 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 4.2) импликацию можно считать доказанной: каждый член последовательности содержит в разложении на множители на одну тройку больше, чем предыдущий. ◄

Замечание 3.6. 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 3.5. 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 каждого n-угольника для любой конфигурации стрелок на его сторонах и диагоналях найдётся корень. Докажем его по индукции.
База индукции: 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).
Шаг индукции: 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 3.7. 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 3.8. 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 3.3. *Доведите решение задачи из примера 3.8 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 3.9. *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 3.10. 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 3.11. *Индукция с нееденичным 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 (рис. 16).

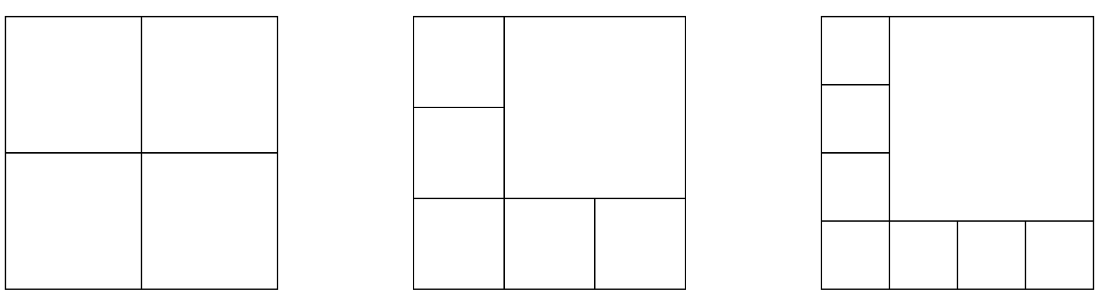

Рис. 16.

Пример 3.12. *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 3.4. *Докажите, что в действительности справедливо 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, 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 индукции: 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 (рис. 17). □

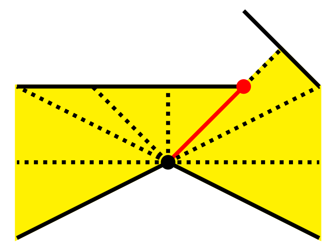

Рис. 17.

Упражнение 3.5. *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

Технические задачи

Задача 3.1. 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. 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 3.3. 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 $X_2, \ldots, X_k$.

Математическая индукция

Задачи семинаров

Доказательство неравенств

Задача 3.4. 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 3.5 (С)**.** Докажите, что при любого действительного числа $\alpha > -1$ и любого натурального числа выполнено *неравенство Бернулли*: $(1+\alpha)^n \geqslant 1 + n\alpha$.

Задача 3.6. Докажите, что при $n > 1$ выполняется неравенство:

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

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

Правдоподобные рассуждения

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.

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 две из них не параллельны и никакие три 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.

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. Имеется 2020 человек, которые 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.

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. 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 3.18. 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 3.19. 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 3.20. 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 3.21. 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 3.22. 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.

4. Делимость целых чисел

Теоретический материал

4.1. Основные определения и свойства

Целые числа знакомы читателю ещё со школы. В этом разделе мы напомним основные определения и обозначения, связанные с ними.

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 4.2. $8 \,\vdots\, 2$, 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, что такое *десятичная запись целого числа* (о десятичной записи действительных чисел, а также о записях с другими основаниями будет 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 4.3. $1467 = 1 \cdot 1000 + 4 \cdot 100 + 6 \cdot 10 + 7 = 1 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 7$.

В терминах десятичной записи формулируются признаки делимости на разные числа.

Утверждение 4.1.

- 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 двух 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 4.1.*

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

Утверждение 4.2.

- 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 4.2.*

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 4.3. 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 4.5. Обратите внимание, что $r \geqslant 0$, — это условие гарантирует единственность.

Мотивировка. Неформально, суть деления с остатком заключается в следующем. 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.*

Строгое доказательство теоремы 4.3. 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 читателю в качестве упражнения. Для доказательства воспользуемся индукцией по a.
База индукции: Случай $a < b$ тривиален, а именно, достаточно положить $q = 0$ и $r = a$.
Шаг индукции: 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

Определение 4.6. 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 $|n| \leqslant |a|$.*

Определение 4.7. *Наибольший общий делитель (НОД)* чисел $a, b \in \mathbb{Z}$ — это 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.

Определение 4.8. Целые числа a и b называются *взаимно простыми*, если $(a, b) = 1$.

Замечание 4.9. 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 более общее, 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 следующей последовательности шагов:

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

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 4.10. 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 4.4. 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,

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

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

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

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

Теорема 4.5. [Алгоритм Евклида] Последний остаток r_n в описанном выше алгоритме — это в точности НОД(a, b).

Доказательство. Благодаря лемме 4.4 имеем $(a, b) = (b, r_0) = (r_0, r_1) = \ldots = (r_n, 0)$. Остаётся заметить, что $(r_n, 0) = r_n$. □

Замечание 4.11. В доказательстве теоремы используется индукция, но 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 4.4.

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

Пример 4.12. 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 4.10 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:

$$\begin{array}{rcccc} 3 & = & 111 - 12 \cdot 9 & = & 111 - 12 \cdot (120 - 111) & = \\ & = & 13 \cdot 111 - 12 \cdot 120 & = & 13 \cdot (351 - 2 \cdot 120) - 12 \cdot 120 & = \\ & = & 13 \cdot 351 - 38 \cdot 120. & & & \end{array}$$

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 в качестве мотивировки такую задачу.

• Задача. Пусть в некоторой стране 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?

• Решение. 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 $d = (a,b) = 1$, то можно купить товар любой стоимости.

Перейдем теперь к теореме.

Теорема 4.6. [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.*

Пусть t — минимальный элемент множества $\mathbb{Z}(a, b)$, согласно упражнению 4.16 он существует. 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, получим $r = ax + by - qt$. 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, по построению 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 4.13. 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 4.14. 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 4.7. Если целые числа a и c взаимно просты и $ab \vdots c$, то $b \vdots c$.

Доказательство. Если $(a, c) = 1$, то по теореме 4.6 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 4.8. 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

$$x = x_0 + m\frac{b}{(a, b)}, \qquad y = y_0 - m\frac{a}{(a, b)}, \tag{2}$$

где m пробегает все целые числа.

Доказательство. Сокращая обе части на (a, b), можно 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 пара (x, y) является произвольным решением 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 4.7 следует, что $(x - x_0) \,\vdots\, b$ и $(y_0 - y) \,\vdots\, a$. Иными словами, существуют такие целые числа m и n, что

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

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.

Схема решения линейных диофантовых уравнений вида $ax + by = c$:
- Проверить, верно ли, что $c \,\vdots\, (a, b)$ — в противном случае решений нет. 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 формулу (2) из теоремы 4.8.

Пример 4.15. Рассмотрим уравнение $5x+2y = 17$. Легко убедиться, что $x_0 = 3, y_0 = 1$ является его частным решением. Значит, по теореме 4.8 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 $5x + 2y = (5, 2)$:

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

Домножая это частное решение уравнения $5x + 2y = (5, 2)$ на 17, мы найдём частное решение исходного уравнения: $x_0 = 17$, $y_0 = -34$. Остаётся применить теорему 4.8:

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

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

Определение 4.16. 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.

Упражнение 4.18. *Докажите, что для любого натурального числа $n > 1$ найдётся простое число p (возможно, равное n) такое, что n делится на p.*

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

Утверждение 4.9. Различных простых чисел бесконечно много.

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

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

Согласно упражнению 4.18 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 4.19. *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 4.10. 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 4.7 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 4.20. *Пусть p — некоторое простое число, $n_1, \ldots, n_m \in \mathbb{N}$. Докажите, что если $(n_1 n_2 \ldots n_m) \vdots p$, то существует $k \in \mathbb{N}$, для которого $n_k \vdots p$.*

Теорема 4.11. [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 $p_1, \ldots, p_k$ — простые числа (не обязательно различные).

Замечание 4.17. 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 4.19. 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 4.20 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 4.18. Число 12 разлагается в виде $12 = 2 \cdot 2 \cdot 3$, но допускаются и разложения $12 = 2 \cdot 3 \cdot 2$ или $12 = 3 \cdot 2 \cdot 2$. Или же можно написать $12 = 2^2 \cdot 3$.

Упражнение 4.21. *Существуют ли такие $x, y, z \in \mathbb{N}$, отличные от единицы, для которых были бы справедливы равенства $xy = 64$ и $yz = 405$?*

Упражнение 4.22. *Пусть p — простое число. Докажите, что для любого $n \in \mathbb{Z}$ наличие свойства $n^2 \,\vdots\, p$ влечёт за собой $n^2 \,\vdots\, p^2$.*

В качестве приятного приложения докажем следующий классический результат.

Утверждение 4.12. Число $\sqrt{2}$ не является рациональным.

Доказательство. Предположим, число $\sqrt{2}$ рационально, то есть

$$\sqrt{2} = \frac{m}{n}, \qquad m, n \in \mathbb{Z}.$$

Без ограничения общности можно считать эту дробь нескоратимой: $(m, n) = 1$. Возводя в квадрат, получим $2n^2 = m^2$. Следовательно, $m^2 \,\vdots\, 2$, откуда $m^2 \,\vdots\, 4$ согласно упражнению 4.22. Иными словами, $m^2 = 4s$ для некоторого натурального числа s. Значит,

$$2n^2 = 4s \quad \Longrightarrow \quad n^2 = 2s \quad \Longrightarrow \quad n^2 \,\vdots\, 2 \quad \Longrightarrow \quad n \,\vdots\, 2.$$

Однако 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

Технические задачи

Задача 4.1. Найдите остатки от деления:

а) 117 на 23;
б) -37 на 6;
в) 5863 на -37;
г) -3764 на -231;
д) 4^{123} на 5;
е) 13^{375} на 10;
ж) $(12^{14} + 14^{12})$ на 13;
з) $(2222^{5555} + 5555^{2222})$ на 7.

Задача 4.2. Какой цифрой оканчивается число

а) 14^{14};
б) $14^{14^{14}}$;
в) 3^{2020};
г) 7^7;
д) 7^{7^7};
е) $3^{3^{3^3}}$?

Задача 4.3. Вычислите наибольший общий делитель:

а) $(7777777, 7777)$;
б) $(3289, 969)$;
в) $(4352, 2091)$;
г) $(11391, 5673)$;
д) $(17711, 10946)$;
е) $(507885, 60808)$.

Задача 4.4. Решите линейные диофантовы уравнения:

а) $2x + 4y = 6$;
б) $21x + 9y = 7$;
в) $17x + 29y = 31$;
г) $17x + 23y = 36$;
д) $31x - 133y = 2$;
е) $85x + 145y = 505$;
ж) $1209x + 936y = 333$;
з) $7581x - 1767y = 171$.

Задача 4.5. Найдите каноническое разложение на множители числа:

а) 2187;
б) 1002001;
в) 17!;
г) C_{20}^{10};
д) 2021;
е) 18941.

Делимость целых чисел

Задачи семинаров

Свойства делимости

Задача 4.6. Верно ли, что если ab делится на c^2, то a делится на c или b делится на c?

Задача 4.7. а) Докажите, что число $\overline{a_n a_{n-1} \ldots a_1 a_0}$ делится на 11, если и только если знакопеременная сумма $\big(a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n\big)$ делится на 11.

б) Сформулируйте и докажите признак делимости на 111.

Задача 4.8. Докажите, что при любом натуральном n

а) $(n^3 - n)$ делится на 6;

б) $(n^5 - n)$ делится на 30;

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

г) $(7^{2n} - 4^{2n})$ делится на 33.

Деление с остатком

Задача 4.9. Докажите, что из любых 52 целых чисел можно выбрать 2 таких числа, что

а) их разность делится на 51;

б) их сумма или их разность делится на 100.

Задача 4.10. 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?

НОД, алгоритм Евклида и диофантовы уравнения

Задача 4.11. Пусть $a, b \in \mathbb{Z}$ и $d = (a, b)$. Докажите, что $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

Задача 4.12. 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?

Задача 4.13. По окружности длины a см катится колесо, длина обода которого равна b см (a и b натуральные, $(a, b) = d$). В колесо вбит гвоздь, он оставляет отметки на окружности. Сколько отметок оставит гвоздь?

Основная теорема арифметики

Задача 4.14. 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 4.15. Докажите, что число n не является квадратом натурального числа, если
а) $n = 25324851$;
б) $n = 39!$.

Задача 4.16. Существует ли 100 подряд идущих составных чисел?

Задача 4.17. Является ли рациональным число
а) $\sqrt{3}$;
б) $\sqrt{2} + \sqrt{3}$;
в) $\sqrt{2} + \sqrt{3} + \sqrt{6}$?

Дополнительные задачи

Задача 4.18. Сформулируйте и докажите признак делимости на 7.

Задача 4.19. Для всех пар неотрицательных целых чисел m и n вычислите:
а) $(2^m - 1,\, 2^n - 1)$;
б) $(2^{2^m} + 1,\, 2^{2^n} + 1)$.

Задача 4.20. 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 4.21. Даны m целых чисел. За один ход разрешается прибавить по единице к любым n из них. При каких m и n всегда можно за несколько таких ходов сделать все числа одинаковыми?

Задача 4.22. 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 4.23. Докажите, что из чисел, обратных к натуральным, можно составить арифметическую прогрессию произвольной длины.

5. 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 можно выбрать 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 можно выбрать 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 $\boxed{\text{А123БВ}}$, 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 могут стоять 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. Скольkими 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 (случаи двух и трёх множеств)

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. При этом по условию мы знаем, что $|A| = 50, |B| = 30, |A \cap B| = 20$. 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 (тех, кто входит 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. ◄

Формула

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$$

называется формулой включений-исключений для двух множеств. Её обоснование было получено в ходе обсуждения примера 5.2.

Для трёх множеств формула включений-исключений принимает следующий вид:

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

Доказательство. Пусть x, y, z — количества однократных элементов (входящих только в A, только в B, только в C соотвественно). Пусть, далее, p, q, r — количества двукратных элементов (входящих в точности в два множества: B и C, C и A, A и B), а s — число трёхкратных элементов (входящих во все три множества), см. рис. 18. Тогда

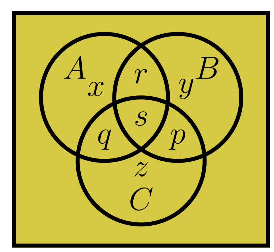

Рис. 18.

$$|A \cup B \cup C| = x + y + z + p + q + r + s$$

С другой стороны,

$$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| =$$
$$= (x + q + r + s) + (y + p + r + s) + (z + p + q + s) - (r + s) - (q + s) - (p + s) + s$$

после сокращения подобных даёт то же самое, что и требовалось доказать. □

Пример 5.5. В летнем лагере 70 ребят. Из них 27 занимаются в драмкружке, 32 поют в хоре, 22 увлекаются спортом. В драмкружке 10 ребят из хора, в хоре 6 спортсменов, в драмкружке 8 спортсменов; 3 спортсмена посещают и драмкружок, и хор. Сколько ребят не поют в хоре, не увлекаются спортом и не занимаются в драмкружке?

► Пусть A — множество студентов, занимабщихся в драмкружке, B — множество студентов, поющих в хоре, C — множество студентов, увлекающихся спортом. Тогда по формуле включений и исключений имеем:

$$|A \cup B \cup C| = 27 + 32 + 22 - 10 - 6 - 8 + 3 = 60.$$

Как и выше получаем, что $70 - 60 = 10$ не поют в хоре, не увлекаются спортом и не занимаются в драмкружке. ◄

Упражнение 5.3. *Сколько чисел в промежутке между 1 и 33000 включительно не делятся ни на 3, ни на 5?*

5.3. (*) Формула включений-исключений (общий случай)

Выше мы видели формулу включений-исключений для двух и трёх множеств. 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 была проверена в разделе 5.2 (см. пример 5.4).
Шаг индукции. Пусть для n множеств формула верна. Рассмотрим $(n + 1)$ множество, среди которых мы 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:

$$(A_1 \cup \ldots \cup A_n) \cap A_{n+1} = (A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \ldots \cup (A_n \cap A_{n+1}). \tag{3}$$

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 5.4. *Докажите формулу* (3).

5.4. Числа размещений и числа сочетаний

Определение 5.6. *Числом размещений из n по k* называется количество упорядоченных наборов из k различных элементов множества, состоящего из n элементов.

Обозначение 5.7. A_n^k.

Пример 5.8. 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 5.2. Для всех $k, n \in \mathbb{N}$ при $n \geqslant k$ выполняется $A_n^k = \dfrac{n!}{(n-k)!}$.

Доказательство. В качестве первого можно выбрать один из n возможных элементов, 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 5.9. *Числом сочетаний из n по k* называется количество k-элементных подмножеств множества, состоящего из n элементов.

Обозначение 5.10. C_n^k или $\binom{n}{k}$.

Пример 5.11. 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 5.3. 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

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

□

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

5.5. Свойства числа сочетаний и бином Ньютона

Утверждение 5.4. 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 состоит 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 5.5. 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 5.6. 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. □

Упражнение 5.7. *Докажите утверждения 5.4, 5.5 и 5.6, используя явные формулы для чисел сочетаний.*

Утверждение 5.7. [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 при $n = 1$ тривиальна. Индукционный переход: рассмотрим разложение $(x+y)^{n+1} = (x+y)^n(x+y)$ и применим к первому сомножителю предположение индукции:

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

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 сумме $C_n^k + C_n^{k+1}$. А согласно утверждению 5.5 это в точности C_{n+1}^{k+1}. □

Замечание 5.12. При $n = 2$ и $n = 3$ бином Ньютона превращается в хорошо известные из школьной алгебры формулы:

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

Утверждение 5.8. Для каждого $n \in \mathbb{N}$ выполнено $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n$.

Доказательство. Приведём доказаательство при помощи бинома Ньютона. После подстановки 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 5.8. *Докажите утверждение 5.8 при помощи математической индукции.*

Упражнение 5.9. *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.

5.6. (*) 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 $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$ (утверждение 5.8).

Замечание 5.13. 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.

Упражнение 5.10. *Докажите, что сумма чисел стоящих в n-й строки треугольника Паскаля равна 2^n.*

Упражнение 5.11. *Докажите, что любое число, кроме единицы, встречается в треугольнике Паскаля конечное число раз.*

Утверждение 5.9. Для любых $k, m \in \mathbb{N}$ выполнено $C_k^k + C_{k+1}^k + \ldots + C_{k+m}^k = C_{k+m+1}^{k+1}$.

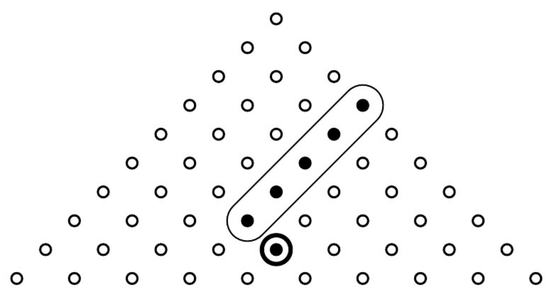

Рис. 19.

Доказательство. Заметим, что сумма, стоящая в левой части равенства, представляет собой сумму чисел на диагонали треугольника Паскаля (рис. 19). 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 рис. 19 кружочком). $\square$

Упражнение 5.12. *а) Проведите формальное доказательство утверждения 5.9 с помощью математической индукции.*

б) Какому равенству будет соответствовать картинка, полученная из рис. 19 отражением относительно его оси симметрии?

Утверждение 5.10. Все числа в N-й строке треугольника Паскаля нечётные тогда и только тогда, когда $N = 2^l - 1$ для некоторого целого l.

Доказательство. Рассмотрим треугольник Паскаля по модулю 2, то есть заменим все числа C_n^k на их остатки по модулю 2. Таким образом, чётным числам будут соответствовать нули, нечётным числам — единицы. Правила сложения по модулю 2 задаются следующим образом: $0 + 0 = 0$, $1 + 0 = 1$, $0 + 1 = 1$, $1 + 1 = 0$ (подробнее про язык сравнений по модулю написано в разделе 7.1). Поэтому после замены каждое внутреннее число треугольника по-прежнему равно сумме двух чисел, расположенных над ним.

Треугольник Паскаля по модулю 2 имеет следующий вид:

$$
\begin{array}{lccccccccccccccc}
n=0 & & & & & & & & 1 & & & & & & & \\
n=1 & & & & & & & 1 & & 1 & & & & & & \\
n=2 & & & & & & 1 & & 0 & & 1 & & & & & \\
n=3 & & & & & 1 & & 1 & & 1 & & 1 & & & & \\
n=4 & & & & 1 & & 0 & & 0 & & 0 & & 1 & & & \\
n=5 & & & 1 & & 1 & & 0 & & 0 & & 1 & & 1 & & \\
n=6 & & 1 & & 0 & & 1 & & 0 & & 1 & & 0 & & 1 & \\
n=7 & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1
\end{array}
$$

Мы хотим убедиться, что в его строках за номером $N = 2^l - 1$ стоят только единицы, а в каждой из остальных строк найдётся хотя бы один ноль. Докажем это индукцией по l.
База индукции: при $l = 0$ и $l = 1$ утверждение выполняется: в первых двух строках стоят только единицы, а в третьей есть ноль.
Шаг индукции: допустим, мы знаем, что в строке с номером $2^l - 1$ стоят только единицы. Рассмотрим строку с номером 2^l. В ней стоит $2^l + 1$ элемент, причём с каждого края находится по одной единице, а между ними стоит $2^l - 1$ нулей. В строке ниже под этими нулями тоже будут нули, которых уже на один меньше. И так далее, образуется равносторонний треугольник, состоящий только из нулей; этот треугольник занимает $2^l - 1$ строку (рис. 20).

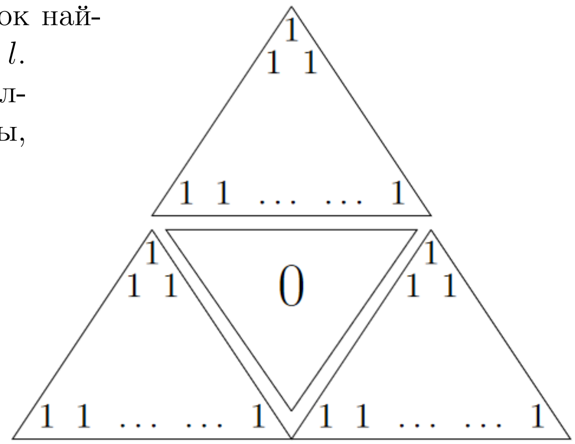

Рис. 20.

По краям строки с номером 2^l стоят единицы. Пока они разделены нулями — они не взаимодействуют, а значит, из них происходят точно такие же треугольники, как начало треугольника Паскаля по модулю 2. Через 2^l строк (то есть на строке с номером $2^l - 1 + 2^l = 2^{l+1} - 1$) нули посередине заканчиваются и два треугольника сливаются. Получается, что $(2^{l+1} - 1)$-ая строка состоит из строк с номерами $(2^l - 1)$ двух меньших треугольников, а по предположению индукции в этих строках стоят одни единицы. Значит, в строке с номером $(2^{l+1} - 1)$ будут только единицы. А наличие треугольника нулей означает, что для каждого $n \in \{2^l, \ldots, 2^{l+1} - 2\}$ в n-ой строке найдётся хотя бы один ноль. $\square$

5.7. Метод перегородок

Утверждение 5.11. 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:

$$\circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ$$

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. $\square$

Утверждение 5.12. 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 5.11. 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 5.11 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 5.14. 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 5.13. *В школьной столовой есть 4 вида пирожков. Сколькими способами можно купить 10 пирожков?*

Упражнение 5.14. [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.

5.8. (*) Понятие перестановки. Композиция и обратная перестановка

Определение 5.15. *Перестановкой* множества $S = \{1, 2, \ldots, n\}$ называется биекция

$$\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}.$$

Существует несколько способов для обозначения перестановок. Первый способ восходит к Коши: исходные элементы множества $S = \{1, 2, \ldots, n\}$ записываются в первой строке, а их образы во второй. Например,

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ k_1 & k_2 & k_3 & \ldots & k_n \end{pmatrix},$$

где $k_i = \sigma(i)$. Другой способ — записывать перестановку при помощи одной строки, а именно, $(\sigma(1)\ \sigma(2)\ \dots\ \sigma(n))$. Тем самым мы получаем эквивалентное определение:

Определение 5.16. *Перестановкой* множества $S = \{1, 2, \dots, n\}$ называется последовательность $\sigma(1),\ \sigma(2),\ \dots,\ \sigma(n)$, где $\sigma(i) \neq \sigma(j)$ для $i \neq j$, и для любого $k \in S$ существует $j \in S$ такой, что $\sigma(j) = k$. Множество перестановок множества S мы будем обозначать через S_n.

Упражнение 5.15. *Сколько всего существует перестановок множества $S = \{1, 2, \dots, n\}$?*

Определение 5.17. *Произведением* или *композицией* перестановой σ_1 и σ_2 называется композиция отображений $\sigma_2 \circ \sigma_1 : S \to S$.

Пример 5.18. Произведение перестановок не всегда коммутативно. Иными словами, меняя местами перестановки в произведении, мы можем получить другой результат. Скажем, пусть

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \qquad \text{и} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

Тогда после несложных вычислений получаем, что

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = \sigma_2 \circ \sigma_1.$$

Упражнение 5.16. *Вычислите* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$.

Пусть $\sigma \in S_n$. Как и для любой биекции, для неё существует обратное отображение, которое само является перестановкой: $\sigma^{-1} \in S_n$. Действительно, нам необходимо вернуть все элементы на свои прежние места. Если в перестановке σ элемент с позицией i переставляется в позицию j, то в обратной перестановке элемент с позиции j переставляется в позицию i. С точки зрения записи перестановки в виде таблицы $2 \times n$ это означает, что мы меняем строки местами. Тождественная перестановка традиционно обозначается буквой e, то есть

$$e = \mathrm{id}_S,$$

и таким образом, $\sigma^{-1}\sigma = \sigma \circ \sigma^{-1} = e$.

Упражнение 5.17. *Вычислите* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}^{-1}$.

5.9. (*) Перестановки: чётность и циклическое разложение

Определение 5.19. Перестановка, в которой два элемента меняются местами, а все остальные остаются на месте, называется *транспозицией*. Если мы меняем местами элементы i и j, где $i < j$, то стандартная запись транспозиции имеет вид

$$\begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}.$$

Это длинно, и поэтому мы будем сокращённо записывать её как (ij).

Утверждение 5.13. Любая перестановка σ может быть представлена как произведение транспозиций.

Доказательство. Доказательство почти очевидно, если переформулировать его на следующий язык: пусть имеется n стульев, на каждом из которых сидит человек, и нам разрешено пересаживать сидящих на стульях по двое, то есть на каждом шаге двое меняются местами, а остальные не двигаются. Тогда можно в итоге пересадить людей в любом порядке. Действительно, сначала поместим на первый стул того, кто там должен сидеть (обменяв его с другим, если он ещё не там), и больше уже его никогда не будем трогать. Затем посадим на второй стул того, кто должен там сидеть, и так далее, пока все не будут сидеть на своих местах. □

Определение 5.20. Будем называть перестановку *чётной*, если она раскладывается в чётное число транспозиций, и *нечётной*, если она представляется произведением нечётного числа транспозиций.

Для корректности определения нам необходимо проверить, что перестановка не может быть чётной и нечётной одновременно. В качестве первого шага докажем следующее утверждение.

Утверждение 5.14. Произведение нечётного числа транспозиций не может быть тождественной перестановкой.

Доказательство. Заметим, что утверждение достаточно доказать для транспозиций соседних элементов. Действительно, допустим, что элементы i и j не соседние и между ними находится k промежуточных элементов: $i + k = j$. Тогда транспозицию (ij) можно заменить на произведение $2k - 1$ траспозиций соседних элементов:

$$(ij) = (i\,i+1)(i+1\,i+2)\dots(j-2\,j-1)(j-1\,j)(j-2\,j-1)\dots(i+1\,i+2)(i\,i+1).$$

При этом вместо одной транспозиции, мы получаем $2k+1$ транспозицию, тем самым увеличивая их совокупное число на $2k$. Однако чётность числа транспозиций от такой замены не меняется. Следовательно, если произведение нечётного числа траспозиций было тождественным, то используя замену, описанную выше, мы получим произведение нечётного числа соседних траспозиций, равное тождественной перестановке.

Допустим теперь, что произведение нечётного числа соседних траспозиций (обменов местами людей, сидящих на стульях) является тождественной перестановкой. Выберем двух произвольных людей и рассмотрим моменты, когда они менялись друг с другом. Каждый такой обмен меняет их порядок. Поэтому, если эти два человека в итоге остались на своих местах, то общее число таких обменов обязано быть чётным.

Теперь заметим, что каждая соседняя траспозиция — это обмен какой-то пары. Если разбить все обмены на группы по этому признаку (какая пара людей менялась), то, как мы показали выше, в каждой группе будет чётное число обменов. Но сумма чётных чисел всегда чётна, получаем противоречие. □

Упражнение 5.18. *Используя утверждение 5.14, докажите, что перестановка не может быть чётной и нечётной одновременно.*

Определение 5.21. *Знак* перестановки σ — это $\varepsilon_\sigma = (-1)^t$, где t — число транспозиций в каком-нибудь разложении σ. Из утверждения 5.14 и упражнения 5.18 следует, что данное определение корректно.

Будем обозначать $\sigma^k = \sigma \circ \ldots \circ \sigma$ произведение k копий перестановки $\sigma \in S_n$.

Определение 5.22. Пусть $\sigma \in S_n$, $j \in S$. *Циклом* называется последовательность

$$j,\ \sigma(j),\ \sigma^2(j),\ \ldots,\ \sigma^k(j) = j,$$

в которой все элементы кроме первого и последнего различны. Число k называется *длиной* цикла.

Пример 5.23. Перестановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}$ разлагается в произведение (1345)(2), где запись (1345) обозначает перестановку-цикл $1 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1$ длины 4, а (2) — перестановку-цикл длины 1.

Упражнение 5.19. *Докажите, что любая перестановка может быть представлена в виде произведения циклов.*

Теорема 5.15. Пусть $\sigma \in S_n$ — произвольная перестановка. Тогда существует такое $m \in \mathbb{N}$, что $\sigma^m = e$ — тождественная перестановка.

Доказательство. Рассмотрим последовательность перестановок

$$\sigma^0 = e, \quad \sigma^1 = \sigma, \quad \sigma^2, \quad \sigma^3, \quad \ldots$$

Так как число перестановок конечно, то рано или поздно в этой последовательности должна повториться какая-то перестановка. Это означает, что существуют $k < l$ такие, что $\sigma^k = \sigma^l$. Умножив на обратную перестановку, получим

$$\sigma^{l-1} = \sigma^{-1} \circ \sigma^l = \sigma^{-1} \circ \sigma^k = \sigma^{k-1}.$$

Действуя аналогично, мы приходим к равенству $e = \sigma^0 = \sigma^{l-k}$, что и требовалось доказать. $\square$

Определение 5.24. Минимальное натуральное число $m > 0$, такое что $\sigma^m = e$, называется *порядком* перестановки σ.

Упражнение 5.20. *Вычислите порядок перестановки* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$.

5.10. 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.
- *Шень А. Х.*, Перестановки — Москва, МЦНМО, 2020.

Комбинаторика

Технические задачи

Задача 5.1. Вычислите: A_4^2; A_5^3; A_7^4.

Задача 5.2. Вычислите: C_4^2; C_5^4; C_7^3.

Задача 5.3. В пассажирском поезде 17 вагонов. Сколькими способами можно распределить по вагонам 17 проводников, если за каждым вагоном закрепляется один проводник?

Задача 5.4. Сколькими способами 28 учеников могут выстроиться в очередь в столовую?

Задача 5.5. а) Из класса, в котором учатся 28 человек, назначаются на дежурство в столовую 4 человека. Сколькими способами это можно сделать?

б) Сколько существует способов набрать команду дежурных, в которую попадет ученик этого класса Коля Васин?

Задача 5.6. Из двух математиков и десяти экономистов надо составить комиссию из восьми человек. Сколькими способами можно составить комиссию, если в неё должен войти хотя бы один математик?

Задача 5.7. В классе 25 человек. Из них 13 ходит на черчение, 15 человек ходят на географию, а 7 человек не посещают эти два предмета. Сколько человек посещают оба предмета?

Задача 5.8. Из 100 студентов института английский язык знают 28 студентов, немецкий — 30, французский — 42, английский и немецкий — 8, английский и французский — 10, немецкий и французский — 5, все три языка знают — 3 студента. Сколько студентов не знают ни одного из трёх языков?

Задача 5.9. Выпишете бином Ньютона:

а) для $n = 4$;
б) для $n = 5$;
с) для $n = 6$.

Задача 5.10. Вычислите:

а) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; в) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^2$

Задача 5.11. Разложите в произведение независимых циклов следующие перестановки:

а) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$; в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 6 & 7 & 2 & 1 & 9 & 4 & 8 \end{pmatrix}$.

Задача 5.12. Для всех $n, k \in \mathbb{N}$ укажите, сколько в S_n циклов длины k.

Комбинаторика
Задачи семинаров

Основные задачи

Задача 5.13. 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 1 и n).

Задача 5.14. 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 дополнительно, чтобы хоть одна из досок обязательно была синей?

Задача 5.15. 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 5.16. 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 5.17. 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 5.18. Каждая сторона квадрата разбита на n частей. Сколько можно построить треугольников с вершинами в точках деления (не включая вершины квадрата)?

Задача 5.19. Имеется 6 красок. Сколькими способами можно раскрасить ими грани кубика так, чтобы все цвета присутствовали? Способы, отличающиеся вращениями кубика, считаются одинаковыми.

Задача 5.20. Пусть есть n шариков разных цветов. Сколько можно собрать наборов из нечётного числа шариков?

Задача 5.21. Сколько существует целых чисел от 1 до 33000, которые не делятся ни на 3 ни на 5, но делятся на 11?

Задача 5.22. У Нины 7 разных шоколадных конфет, у Коли 9 разных карамелек. Сколькими способами они могут обменяться друг с другом пятью конфетами?

Дополнительные задачи

Задача 5.23. На столе площади 1 лежит три журнала, площадь каждого из которых составляет не меньше 1/2. Среди их попарных пересечений рассмотрим наибольшее по площади. Какую наименьшую площадь оно может иметь?

Задача 5.24. 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 5.25. 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 5.26. 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 5.27. 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 5.28. Пусть $n < 2^k$. Докажите, что число n встречается в треугольнике Паскаля не более, чем $2k-2$ раз.

Задача 5.29. В каких строках треугольника Паскаля все числа, кроме единиц, будут кратны данному простому числу p?

Задача 5.30. 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 5.31. Сколько существует десятизначных чисел, все цифры которых различны и которые делятся на 11111?

Задача 5.32. Какие из следующих перестановок являются чётными:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$; в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 7 & 2 & 1 & 9 & 5 & 8 \end{pmatrix}$?

Задача 5.33. Вычислите: а) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^{1000}$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}^{-1000}$; в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}^{500}$; г) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}^{-127}$;

Задача 5.34. Пусть $\sigma = (1, 2, \ldots, n)$ — цикл длины n. На какое количество независимых циклов раскладывается перестановка σ^k? Каковы длины этих циклов?

6. 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.

Определение 6.1. *Многочленом* от переменной x с коэффициентами в множестве $\mathbb{K}$ называется *формальное выражение* вида

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

Обозначение 6.2. Множество многочленов с коэффициентами в $\mathbb{K}$ обозначается $\mathbb{K}[x]$.

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 (раздел 10).

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

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

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.

Определение 6.3. *Нулевой многочлен* (на языке формальных выражений) — это многочлен, все коэффициенты которого равны нулю.

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

Определение 6.4. 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.*

Обозначение 6.5. Степень многочлена $f(x)$ обозначается $\deg f(x)$.

Пример 6.6. 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 $\mathbb{K} \subset \mathbb{K}[x]$. Иными словами, подмножество многочленов нулевой степени — это как раз и есть $\mathbb{K}$ (с естественной оговоркой, что нулевой многочлен соответствует нулю). И правда, 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.

Определение 6.7. 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 6.8. Согласно утверждению 4.12 корень многочлена $(x^2 - 2) \in \mathbb{Q}[x]$ не лежит в $\mathbb{Q}$.

Определение 6.9. 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 6.10. $(x^3 - 1) \in \mathbb{Q}[x]$ делится на $(x - 1)$. И правда, $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

Определение 6.11. 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

Определение 6.12. 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 6.13. 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

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

Доказательство. Начнём 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, имеет место первый вариант: $r_2(x) - r_1(x) = 0$. 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. Можно считать, что $\deg g(x) > 0$, поскольку на любые многочлены степени 0 можно делить с нулевым остатком. Воспользуемся индукцией по степени многочлена $f(x)$. Введём обозначения:

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

База индукции: 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 6.14. 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

Определение 6.15. 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 $h(x) \mid g(x)$.

Любые два многочлена имеют хотя бы один общий делитель — постоянный многочлен 1.

Определение 6.16. *Наибольшим общим делителем* (НОД) многочленов $f(x),\ g(x) \in \mathbb{K}[x]$ называется их общий делитель, имеющий наибольшую степень. Если НОД имеет нулевую степень, то $f(x)$ и $g(x)$ называются *взаимно простыми.*

Обозначение 6.17. Для наибольшего общего делителя многочленов применяют те же обозначения, что и для целых чисел:

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

Оба означают, что $d(x)$ — НОД многочленов $f(x)$ и $g(x)$.

Замечание 6.18. В отличие от целых чисел, НОД многочленов определён неоднозначно. Действительно, пусть $d(x) = (f(x), g(x))$. Тогда для любого ненулевого числа $t \in \mathbb{K} \setminus \{0\}$ многочлен $t \cdot d(x)$ — 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).*

Определение 6.19. Многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ называется *приведённым*, если его *старший коэффициент* равен единице: $a_n = 1$.

Пример 6.20. $x^3 + 6x + 1$ — 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, для которого многочлен $\alpha \cdot d(x)$ является приведённым. 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 $d(x)$, в то время как $\mathbb{K}(f(x), g(x))$ — 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 $f(x), g(x) \in \mathbb{K}[x]$ — 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. Включение $\mathbb{K}(f(x), g(x)) \subset \mathbb{K}(d(x))$ очевидно, поэтому достаточно 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. $\square$

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 $g(x)$. $\square$

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:

$$\begin{array}{cc}
f(x) = q_0(x)g(x) + r_0(x) & \text{нулевой шаг} \\
g(x) = q_1(x)r_0(x) + r_1(x) & \text{первый шаг} \\
\dots & \\
r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x) & n\text{-й шаг} \\
r_{n-1}(x) = q_{n+1}(x)r_n(x) & (n+1)\text{-й шаг}
\end{array}$$

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 $f(x), g(x), h(x) \in \mathbb{K}[x]$ — такие 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 утверждение 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. Докажите, что 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 нескольким фундаментальным результатам, среди которых мы дадим описание неприводимых многочленов с коэффициентами в $\mathbb{R}$ и $\mathbb{C}$ (правда, без доказательства).

Теорема 6.7. [Теорема Безу] Число $\lambda \in \mathbb{K}$ является корнем многочлена $f(x) \in \mathbb{K}[x]$, тогда и только тогда, когда $f(x) \vdots (x - \lambda)$.

Доказательство. Если $f(x) \vdots (x-\lambda)$, то $f(x) = q(x)(x-\lambda)$ для некоторого $q(x) \in \mathbb{K}$. Подставляя $x = \lambda$, получаем $f(\lambda) = q(\lambda) \cdot 0 = 0$.

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. $\square$

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: очевидно, 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. $\square$

Конкретный вид неприводимых многочленов в $\mathbb{K}[x]$ существенно зависит от $\mathbb{K}$.

Пример 6.21. 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, как было доказано в утверждении 4.12, $\sqrt{2}$ — иррациональное число.

Тот же самый многочлен как элемент $\mathbb{R}[x]$ приводим: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Пример 6.22. 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

$$f(x) = a(x^2 + b_1x + c_1) \cdot \ldots \cdot (x^2 + b_kx + c_k) \cdot (x - \lambda_1) \cdot \ldots \cdot (x - \lambda_m),$$

где $a, b_i, c_i, \lambda_j \in \mathbb{R}$, а дискриминанты всех квадратичных многочленов отрицательны.

Многочлены

Задачи семинаров

Задача 6.1. Пусть $f(x) \in \mathbb{R}[x]$, причём $\deg f(x) = 3$.

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 $x(x+1)(2x+1)$.

7. Сравнения

Теоретический материал

7.1. Язык сравнений

Определение 7.1. Пусть n натуральное число. Введём отношение эквивалентности $\equiv$ на множестве целых чисел $\mathbb{Z}$ 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 по отношению $\equiv$, говорят, что *a сравнимо с b по модулю n*.

Замечание 7.2. 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 7.3. Множество классов эквивалентности обозначается как $\mathbb{Z}/n\mathbb{Z}$.

Замечание 7.4. 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 отождествить со множеством остатков $\{0, 1, 2, ..., n-1\}$.

Пример 7.5. При $n = 2$ в $\mathbb{Z}/n\mathbb{Z}$ существует всего два класса эквивалентности: чётные числа 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).

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 7.6. $726 = 11 \cdot 11 \cdot 6 \equiv (-2) \cdot (-2) \cdot 6 \equiv 2 \cdot 12 \equiv 2 \cdot (-1) \equiv 11 \pmod{13}$.

Замечание 7.7. Чтобы сложить или перемножить два числа по модулю 10, достаточно 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 7.8. 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 7.9. 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 7.10. 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 целого 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 4.8 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 $x=r(x_0)$. $\square$

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 7.11. Теорема 4.8 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 7.12. 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 7.13. 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 7.3. 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, каждый остаток в строке $1^2, 2^2, \ldots, (p-1)^2$ выписан ровно два раза. □

Следствие 7.4. 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 7.5. [Малая теорема Ферма]
Если p — простое число, то 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:

$$\begin{array}{rcl} a & \equiv & r_1 \pmod p \\ 2a & \equiv & r_2 \pmod p \\ & \ldots & \\ (p-1)a & \equiv & r_{p-1} \pmod p \end{array}$$

Перемножая левые и правые части между собой, 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. Если при этом отождествлять раскраски, получающиеся друг из друга поворотом, то каждая раскраска, кроме a одноцветных, будет посчитана p раз. Это значит, что неодноцветных раскрасок в точности $(a^p-a)/p$. Поскольку 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 7.6. [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,

$$(p-1)! \equiv 1 \cdot (2 \cdot 2^{-1}) \cdot (3 \cdot 3^{-1}) \cdot \ldots \cdot (p-1) \pmod{p}$$

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 7.14. Если $n = 17$, то остатки в числе 16! разбиваются на пары обратных друг к другу следующим образом:

$$17! = 1 \cdot (2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14) \cdot 16 \equiv 16 \pmod{17}.$$

7.4. Китайская теорема об остатках

Пример 7.15. 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 7.7. [Китайская теорема об остатках]
Пусть $n_1, n_2, \ldots, n_m$ — попарно взаимно простые натуральные числа. Тогда для любых целых чисел $a_1, a_2, \ldots, a_m \in \mathbb{Z}$ 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 $k \in \{1, 2, \ldots, m\}$ положим

$$N_k = \frac{N}{n_k} \qquad \text{и} \qquad b_k \equiv N_k^{-1} \pmod{n_k}.$$

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 стоящее в правой части равенства выражение 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 7.16. 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

$$f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_m\mathbb{Z}$$

$$a \mapsto \big(r_{n_1}(a), r_{n_2}(a) \ldots, r_{n_m}(a)\big)$$

является биекцией. На самом деле верно 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 7.17. 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 $(x-3) \,\vdots\, 6$, в частности x делится на 3. Но из первого сравнения $(x - 1) \,\vdots\, 3$. Следовательно, искомая система сравнений решений не имеет.

Сравнения

Технические задачи

Задача 7.1. Вычислите

а) $8 \cdot 9 \cdot 15 + 8 \pmod{17}$;
б) $3 : 8 + 4 \cdot 4 \pmod{11}$;
в) $11 \cdot 17 \cdot 35 \cdot 21 \cdot 41 \cdot 15 \cdot 13 \cdot 37 \pmod{50}$;
г) $8 \cdot 491 \cdot 771 \cdot 8 \cdot 491 \cdot 771 \pmod{1001}$.

Задача 7.2. Какие остатки от деления на 7 и на 9 может давать

а) полный квадрат;
б) полный куб?

Задача 7.3. Решите уравнение

а) $x + 7 \equiv 2 \pmod{11}$;
б) $2x + 5 \equiv 2 \pmod{13}$;
в) $7x \equiv 3 \pmod{15}$;
г) $6x \equiv 5 \pmod{9}$;
д) $4x \equiv 2 \pmod{18}$;
е) $x^2 + x + 1 \equiv 0 \pmod{2}$;
ж) $x^2 + x + 1 \equiv 0 \pmod{3}$;
з) $x^2 + x + 1 \equiv 0 \pmod{19}$;
и) $x^2 \equiv 1 \pmod{8}$;
к) $x^5 - x + 1 = 0 \pmod{5}$;
л) $x^4 = x \pmod{4}$;
м) $x^n = x \pmod{4}$.

Задача 7.4. 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) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x^2 \equiv 1 \pmod{6} \end{cases}$;

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 7.5. 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;
д) 7^{7^7} на 10.

Сравнения

Задачи семинаров

Основные задачи

Задача 7.6. 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 7.7. Сколько решений имеет сравнение $21x \equiv 14 \pmod{91}$?

Задача 7.8. Пусть n — нечётное число. Найдите остаток от деления на n следующей суммы: $1^3 + 2^3 + \ldots + (n-1)^3$.

Задача 7.9. 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.

Задача 7.10. а) Сколько существует квадратичных вычетов по модулю p?

б) Что можно сказать о произведении двух квадратичных (не)вычетов?

в) Что можно сказать о произведении вычета и невычета?

Задача 7.11. а) Докажите, что $x(x-1)\ldots(x-(p-1)) \equiv x^p - x \pmod{p}$.

б) Оставим в многочлене слева только те скобки $(x - a)$, где a – квадратичный вычет. Что получится после раскрытия скобок?

(В обоих случаях мы рассматриваем многочлены с коэффициентами по модулю p.)

Задача 7.12. Докажите, что существует бесконечно много натуральных чисел, которые не представимы в виде суммы двух квадратов.

Задача 7.13. Докажите, что число $\dfrac{n^7}{7} + \dfrac{n^{11}}{11} + \dfrac{59n}{77}$ является целым.

Задача 7.14. Найдите наименьшее натуральное число, дающее при делении на 2, 3, 5, 7 остатки 1, 2, 4, 6 соответственно.

Задача 7.15. При каких целых n число $n^2 + 3n + 1$ делится на 55?

(*) Квадратичный закон взаимности

Определение 7.18. Пусть a не делится на простое p. *Символ Лежандра* — это число

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{если } a \equiv 0 \pmod p \\ 1, & \text{если } a \text{ вычет по модулю } p \\ -1, & \text{иначе} \end{cases}$$

Задача 7.16. Проверьте, что символ Лежандра удовлетворяет следующим свойствам:

а) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;

б) $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Для нечётного простого p будем называть остатки $1, 2, \ldots, \frac{p-1}{2}$ положительными (по модулю p), а остальные ненулевые остатки – отрицательными.

Задача 7.17. а) (Лемма Гаусса) Рассмотрим отображение множества ненулевых остатков по модулю нечётного простого p, заданное умножением на ненулевой a. Пусть c — количество положительных остатков с отрицательным образом. Докажите, что $(\frac{a}{p}) = (-1)^c$.

б) Вычислите $(\frac{2}{p})$.

в) Докажите, что $(\frac{a}{p}) = (-1)^t$, где

$$t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$$

.

Задача 7.18. Пусть p, q — различные нечётные простые числа.

а) Рассмотрим множество пар (x, y), где x, y – положительные остатки по модулю p и q соответственно (рассматриваемые как натуральные числа). Сколько таких пар, что $qx > py$?

б) (**Квадратичный закон взаимности**) Докажите, что

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

в) Вычислите: $(\frac{1000}{53})$, $(\frac{2021}{37})$.

г) Решите уравнение $x^2 - x + 30 \equiv 0 \pmod{101}$.

Дополнительные задачи

Задача 7.19. Найдите остаток от деления числа, состоящего из 19 девяток, на 19.

Задача 7.20. Пусть m и n — взаимно простые натуральные числа, a и b — целые числа.

а) Докажите, что числа a, $a+m$, …, $a+(n-1)m$ 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.

Определение 7.19. Пусть $n \in \mathbb{N}$. *Функция Эйлера* $\phi(n)$ — это количество чисел от 1 до n включительно, взаимно простых с n.

Задача 7.21. 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 7.22. [Теорема Эйлера] Пусть натуральные числа a и n взаимно просты. Докажите, что $a^{\phi(n)} \equiv 1 \pmod{n}$.

Определение 7.20. 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 7.23. 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 7.24. 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 7.25. 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, y, z), для которого $x \equiv y \equiv z \equiv 0 \pmod{p}$).

8. Действительные числа

Теоретический материал

8.1. Введение

Этот раздел посвящён действительным (вещественным) числам. Из школьной программы хорошо известны понятия натуральных чисел $\mathbb{N}$, целых чисел $\mathbb{Z}$ и рациональных чисел $\mathbb{Q}$. Действительные числа $\mathbb{R}$ — следующий, ещё более широкий класс чисел.

Переход от одного класса чисел к другому, более широкому, обычно нужен 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 числах, в отличие от целых, — делить одно на другое (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. Например, мы бы хотели, чтобы выполнялись такие свойства:

$$\begin{array}{ccc} a+b=b+a, \qquad ab=ba & & \textit{(коммутативность)},\\ (a+b)+c=a+(b+c), \quad (ab)c=a(bc) & & \textit{(ассоциативность)},\\ a(b+c)=ab+ac & & \textit{(дистрибутивность)},\\ (a \leqslant b) \wedge (b \leqslant c) & \Rightarrow & a \leqslant c,\\ (a \leqslant b) \wedge (c \leqslant d) & \Rightarrow & a+c \leqslant b+d,\\ (0 \leqslant a \leqslant b) \wedge (0 \leqslant c \leqslant d) & \Rightarrow & 0 \leqslant ac \leqslant bd. \end{array}$$

В отличие от целых и рациональных чисел, которые строятся более или менее единственным естественным образом, проблема с действительными числами заключается в том, что определить их можно несколькими разными способами, каждый из которых является достаточно сложным. Имеется два основных подхода.

• **Аксиоматический:** перечисляем требуемые свойства (*аксиомы*) и выводим остальные утверждения из них. При этом возникают следующие два важных вопроса.

(а) Существует ли объект с перечисленными свойствами (*непротиворечивость*)?

(б) Является ли такой объект единственным (*категоричность*)?

• **Конструктивный:** строим новый объект из уже имеющихся «деталей». В этом случае возникающие вопросы таковы.

(а) Почему построенный объект интересен?

(б) Почему для разных конструкций получится один и тот же объект?

Так для чего же нам нужны действительные числа? Что это за свойство, ради которого нужно расширять множество рациональных чисел? Ответить на этот вопрос оказывается тоже не так просто. 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 априори это совершенно 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 разделе 10. 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 произвольной 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 в концах некоторого отрезка значения разных знаков, то можно получить его корень на этом отрезке. Числа, получающиеся из целых чисел с помощью этого набора операций, называются *алгебраическими.*

Ещё одно 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.

8.2. Аксиомы сложения и умножения

Для того, чтобы определить множество действительных чисел, мы воспользуемся аксиоматическим подходом. Согласно этому подходу множеством *действительных чисел* мы назовём множество $\mathbb{R}$, которое

- наделено операциями «+» и «·», удовлетворяющими *аксиомам сложения и умножения*;
- наделено отношением порядка, удовлетворяющим *аксиомам порядка*;
- дополнительно удовлетворяет *аксиоме полноты.*

В этом разделе мы обсудим аксиомы сложения и умножения, оставив аксиомы порядка до раздела 8.3, а аксиому полноты — до раздела 8.4.

1. Аксиомы сложения:

   (a) $\forall\, a, b \in \mathbb{R}: \quad a + b = b + a$ (*коммутативность сложения*),

   (b) $\forall\, a, b, c \in \mathbb{R}: \quad (a + b) + c = a + (b + c)$ (*ассоциативность сложения*),

   (c) $\exists\, 0 \in \mathbb{R}\, \forall\, a \in \mathbb{R}: \quad a + 0 = a$ (*существование нуля*),

   (d) $\forall\, a \in \mathbb{R}\, \exists\, b \in \mathbb{R}: \quad a + b = 0$ (*существование противоположного элемента*).

2. Аксиомы умножения:

   (a) $\forall\, a, b \in \mathbb{R}: \quad a \cdot b = b \cdot a$ (*коммутативность умножения*),

   (b) $\forall\, a, b, c \in \mathbb{R}: \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*ассоциативность умножения*),

   (c) $\exists\, 1 \in \mathbb{R}\, \forall\, a \in \mathbb{R}: \quad a \cdot 1 = a$ (*существование единицы*),

   (d) $\forall\, a \in \mathbb{R} \setminus \{0\}\, \exists\, b \in \mathbb{R}: \quad a \cdot b = 1$ (*существование обратного элемента*).

3. Связь сложения с умножением:

   (a) $\forall\, a, b, c \in \mathbb{R}: \quad a \cdot (b + c) = a \cdot b + a \cdot c$ (*дистрибутивность*),

   (b) $1 \neq 0$ (*нетривиальность* $\mathbb{R}$).

Обозначение 8.1. Для данного элемента $a \in \mathbb{R}$ его противоположный элемент обозначается $(-a)$. Если $a \neq 0$, то его обратный элемент обозначается a^{-1}. Таким образом,

$$a + (-a) = 0 \qquad \text{и} \qquad a \cdot a^{-1} = 1.$$

Упражнение 8.2. *Каким из вышеперечисленных аксиом удовлетворяют*
а) натуральные числа;
б) целые числа;
в) рациональные числа;
г) комплексные числа (см. раздел 10)?

Из аксиом сложения и умножения выводятся привычные нам «естественные» свойства действительных чисел. Посмотрим, как это работает, на нескольких примерах, касающихся операции сложения.

Пример 8.2. *Нулевой элемент единственен.* В самом деле, предположим, что существует два различных нуля: 0_1 и 0_2. Тогда

$$0_1 \overset{(1c)}{=} 0_1 + 0_2 \overset{(1a)}{=} 0_2 + 0_1 \overset{(1c)}{=} 0_2.$$

Здесь над каждым знаком равенства мы подписали, какой именно аксиомой мы воспользовались. Таким образом, $0_1 = 0_2$, и нулевой элемент на самом деле только один.

Пример 8.3. *Противоположный элемент единственен.* В самом деле, допустим, что для некоторого элемента $a \in \mathbb{R}$ существует два различных противоположных элемента b и c. Тогда

$$b \overset{(1c)}{=} b + 0 \overset{(1d)}{=} b + (a + c) \overset{(1b)}{=} (b + a) + c \overset{(1a)}{=} (a + b) + c \overset{(1d)}{=} 0 + c \overset{(1a)}{=} c + 0 \overset{(1c)}{=} c.$$

Таким образом, $b = c$, и противоположный элемент тоже на самом деле только один.

Пример 8.4. Для любых двух элементов $a, b \in \mathbb{R}$ справедливо

$$-(a + b) = (-a) + (-b).$$

Действительно, $\big(-(a + b)\big)$ — это элемент, противоположный элементу $(a + b)$, то есть

$$(a + b) + \big(-(a + b)\big) \overset{(1d)}{=} 0.$$

С другой стороны,

$$(a + b) + \big((-a) + (-b)\big) \overset{(1b)}{=} \big((a + b) + (-a)\big) + (-b) \overset{(1a)}{=} \big((b + a) + (-a)\big) + (-b) \overset{(1b)}{=}$$
$$\overset{(1b)}{=} \big(b + (a + (-a))\big) + (-b) \overset{(1d)}{=} (b + 0) + (-b) \overset{(1c)}{=} b + (-b) \overset{(1c)}{=} 0.$$

Таким образом, $(-a) + (-b)$ — это тоже элемент, противоположный элементу $(a + b)$. Поскольку противоположный элемент единственен, отсюда и следует, что $-(a + b) = (-a) + (-b)$.

Упражнение 8.3. *Докажите, что для любого элемента $a \in \mathbb{R}$ справедливо равенство*

$$-(-a) = a.$$

Упражнение 8.4. *Докажите, что операция умножения обладает следующими свойствами:*
а) единичный элемент единственен;
б) для каждого ненулевого числа $a \in \mathbb{R}$ обратный элемент единственен;
в) для каждого ненулевого числа $a \in \mathbb{R}$ выполняется равенство $\big(a^{-1}\big)^{-1} = a$;
г) для любых двух ненулевых чисел $a, b \in \mathbb{R}$ выполняется равенство $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

Любопытно также взглянуть на свойства, связывающие между собой сложение и умножение.

Пример 8.5. Для любого элемента $a \in \mathbb{R}$ справедливо равенство

$$a \cdot 0 = 0.$$

В самом деле, заметим сначала, что

$$a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a \cdot (0 + 1) = a \cdot (1 + 0) = a \cdot 1 = a.$$

Следовательно, прибавив к полученному равенству $(-a)$, мы получим

$$a \cdot 0 = a \cdot 0 + 0 = a \cdot 0 + \big(a + (-a)\big) = (a \cdot 0 + a) + (-a) = a + (-a) = 0.$$

Упражнение 8.5. *а) Над каждым знаком равенства в примере 8.5 подпишите, какая именно аксиома была использована.*
б) Используя пример 8.5, покажите, что для любого $a \in \mathbb{R}$ выполняется $a \cdot (-1) = -a$.

8.3. Аксиомы порядка

В предыдущем разделе мы обсудили аксиомы сложения и умножения. В этом разделе пришла очередь аксиом, связанных с отношением порядка $\geqslant$.

4. Аксиомы порядка:

   (a) $\forall\, a \in \mathbb{R}: \quad a \geqslant a \quad$ (*рефлексивность*),

   (b) $\forall\, a, b \in \mathbb{R} \quad \big((a \geqslant b) \wedge (b \geqslant a)\big) \to (a = b) \quad$ (*антисимметричность*),

   (c) $\forall\, a, b, c \in \mathbb{R}: \quad \big(a \geqslant b) \wedge (b \geqslant c)\big) \to (a \geqslant c) \quad$ (*транзитивность*),

   (d) $\forall\, a, b \in \mathbb{R}: \quad (a \geqslant b) \vee (b \geqslant a) \quad$ (*линейная упорядоченность*),

   (e) $\forall\, a, b, c \in \mathbb{R}: \quad (a \geqslant b) \to (a + c \geqslant b + c)$ (*связь порядка и сложения*),

   (f) $\forall\, a, b, c \in \mathbb{R}: \quad \big((a \geqslant 0) \wedge (b \geqslant 0)\big) \to (a \cdot b \geqslant 0) \quad$ (*связь порядка и умножения*).

Обозначение 8.6. Если $a \geqslant b$, но при этом $a \neq b$, то пишут $a > b$.

Пример 8.7. Покажем, что если для элементов $a, b, c, d \in \mathbb{R}$ выполнено $a \geqslant b$ и $c \geqslant d$, то

$$a + c \geqslant b + d.$$

В самом деле,

$$a + c \overset{(4e)}{\geqslant} b + c \overset{(1a)}{=} c + b \overset{(4e)}{\geqslant} d + b \overset{(1a)}{=} b + d.$$

Пример 8.8. Покажем, что если для элементов $a, b \in \mathbb{R}$ выполнено $a \geqslant b$, то

$$(-a) \leqslant (-b).$$

В самом деле, достаточно прибавить к обеим частям исходного неравенства $(-a)+(-b)$. С формальной точки зрения, мы пользуемся цепочкой следующих аксиом:

$$(-a) \overset{(1c)}{=} (-a) + 0 \overset{(1d)}{=} (-a) + \big(b + (-b)\big) \overset{(1b)}{=} \big((-a) + b\big) + (-b) \overset{(1a)}{=} \big(b + (-a)\big) + (-b) \overset{(1b)}{=}$$
$$\overset{(1b)}{=} b + \big((-a) + (-b)\big) \overset{(4e)}{\leqslant} a + \big((-a) + (-b)\big) \overset{(1b)}{=} \big(a + (-a)\big) + (-b) \overset{(1d)}{=} 0 + (-b) \overset{(1c)}{=} (-b).$$

Упражнение 8.6. *Проверьте, что*
а) если $a \geqslant b \geqslant 0$ и $c \geqslant d \geqslant 0$, то $a \cdot c \geqslant b \cdot d \geqslant 0$;
б) если дополнительно $b \neq 0$, то $b^{-1} \geqslant a^{-1} > 0$.

Пример 8.9. Покажем, что $1 > 0$. Прежде всего, заметим, что согласно аксиоме (4d) о линейной упорядоченности имеет место одна из двух возможностей: $1 \geqslant 0$ или $0 \geqslant 1$ С учётом того, что аксиома ($3b$) запрещает равенство $1 = 0$, аксиома антисимметричности ($2b$) оставляет только две взаимоисключающие возможности: либо $1 > 0$, либо $1 < 0$.

Предположим, что $0 > 1$. Тогда, как мы видели в примере 8.8, $-1 > 0$. Применяя аксиому (4f) в этому неравенству, взятому дважды, мы получим

$$(-1) \cdot (-1) > 0 \cdot 0 = 0.$$

Однако $(-1) \cdot (-1) = 1$, откуда $1 > 0$, что противоречит изначальному предположению.

Упражнение 8.7. *Проверьте, что* $(-1) \cdot (-1) = 1$.

Замечание 8.10. Аксиомы порядка выделяют в множестве действительных чисел специальное подмножество $P \subset \mathbb{R}$ — множество его *положительных* элементов. Иными словами,

$$P = \{a \in \mathbb{R} \mid a > 0\}.$$

Можно показать, что множество положительных чисел удовлетворяет следующим свойствам:

(P1) Для любого $a \in \mathbb{R}$ верно ровно одно из трёх утверждений: $a \in P$; $a = 0$; $(-a) \in P$.

(P2) Если $a, b \in P$, то $a + b \in P$ и $a \cdot b \in P$.

С другой стороны, оказывается, что свойства (P1) и (P2) можно назначить аксиомами вместо аксиом порядка. Иными словами, если $P \subset \mathbb{R}$ — подмножество, удовлетворяющее условиям (P1) и (P2), то свойства (4a)-(4f) выполняются автоматически.

8.4. Аксиома полноты

Этот подраздел посвящён *аксиоме полноты* — тому свойству, которое и выделяет множество действительных чисел. Однако прежде чем переходить к аксиоме полноты, обсудим ещё одно утверждение, на первый взгляд настолько очевидное, что не требует особой формулировки.

Аксиома Архимеда. Для любого числа $c \in \mathbb{R}$ существует $n \in \mathbb{N}$ такое, что $n > c$.

Следствие 8.1. Для любого числа $\varepsilon > 0$ существует $n \in \mathbb{N}$ такое, что $1/n < \varepsilon$.

Доказательство. Достаточно рассмотреть $c = 1/\varepsilon$ и воспользоваться аксиомой Архимеда:

$$n > \frac{1}{\varepsilon} \qquad \Rightarrow \qquad \frac{1}{n} < \varepsilon.$$

□

Перейдём теперь к полноте. Есть несколько эквивалентных формулировок этого понятия (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). Не доказывая эквивалентность, мы обсудим некоторые из них.

8.4.1. В терминах разделяющих чисел

Аксиома 8.2. [Аксиома полноты]
Пусть $A, B \subset \mathbb{R}$ — два непустые подмножества такие, что для всех $a \in A$ и $b \in B$ справедливо неравенство $a \leqslant b$. Тогда существует такое число $c \in \mathbb{R}$, что

$$\forall\, a \in A \;\forall\, b \in B:\; a \leqslant c \leqslant b.$$

Замечание 8.11. Аксиома полноты в этой формулировке называется *аксиомой непрерывности* или *теоремой о разделяющем числе.*

8.4.2. В терминах последовательностей

Определение 8.12. *Последовательность* — это отображение $x\colon \mathbb{N} \to \mathbb{R}$. Образы натуральных чисел при этом отображении называются *элементами последовательности* и обозначаются x_n, а саму последовательность обозначают (x_n). Последовательность называется

- *неубывающей*, если $x_n \leqslant x_{n+1}$ при всех $n \in \mathbb{N}$;
- *ограниченной сверху*, если существует такое $C \in \mathbb{R}$, для которого $x_n \leqslant C$ при всех $n \in \mathbb{N}$.

Упражнение 8.8. *Дайте определения*

а) невозрастающей последовательности;

б) убывающей последовательности;

в) возрастающей последовательности;

г) ограниченной снизу последовательности.

Аксиома 8.3. [Аксиома полноты]
Пусть последовательность (x_n) неубывающая и ограниченная сверху. Тогда множество чисел

$$S = \{a \mid \forall\, n : \quad x_n \leqslant a\}$$

имеет наименьший элемент $A = \min S$, который называют *пределом* последовательности (x_n).

Обозначение 8.13. Обозначение: $A = \lim\limits_{n\to\infty} x_n$.

Предупреждение. В курсе матанализа будет дано другое определение предела последовательности, которое работает не только для монотонных последовательностей. Однако для монотонных последовательностей наше определение будет эквивалентно этому более общему.

Упражнение 8.9. *Как бы вы определили предел невозрастающей ограниченной снизу последовательности? Почему он всегда существует?*

Вообще говоря, не во всяком множестве есть наименьший элемент. Например, множество $Z = \{x \mid x > 0\}$ такого элемента не имеет. И правда, если взять произвольный элемент $a \in Z$, то для $b = a/2$ верно, что $b \in Z$ и $b < a$, а потому a не может быть минимальным элементом множества Z. Формулировка аксиомы полноты утверждает, что в нашем случае множество S наименьшим элементом обладает. Заметим, кстати, что множество S непусто тогда и только тогда, когда последовательность (x_n) ограничена сверху, так что это условие отбросить нельзя.

Упражнение 8.10. *Проверьте, что множество $\{x > 0 \mid x^2 > 2\}$ не имеет наименьшего элемента, не используя существования $\sqrt{2}$.*

8.4.3. В терминах вложенных отрезков

Аксиома 8.4. [Аксиома полноты]
Любая последовательность вложенных отрезков

$$[a_1, b_1] \supset [a_2, b_2] \supset [a_3, b_3] \supset [a_4, b_4] \supset \ldots$$

имеет общую точку:

$$\exists\, x \in \mathbb{R}\ \ \forall\, n \in \mathbb{N} :\ x \in [a_n, b_n].$$

Замечание 8.14. Аксиома полноты в этой формулировке называется *принципом вложенных отрезков.*

8.4.4. В терминах точных верхних граней

Определение 8.15. Пусть $S \subset \mathbb{R}$. Будем называть число $s \in \mathbb{R}$
- *верхней гранью* множества S, если $\forall\, a \in S :\ s \geqslant a$;
- *нижней гранью* множества S, если $\forall\, a \in S :\ s \leqslant a$.

Множество S называется
- *ограниченным сверху*, если у него существует верхняя грань;
- *ограниченным снизу*, если у него существует нижняя грань;
- *ограниченным*, если оно ограничено как сверху, так и снизу.

Упражнение 8.11. *Докажите, что множество $S \subset \mathbb{R}$ ограничено тогда и только тогда когда существует такое число M, что $\forall\, a \in S :\ |a| \leqslant M$.*

Определение 8.16. Число $C \in \mathbb{R}$ называется *точной верхней гранью* ограниченного множества S, если C есть наименьшая из всех верхних граней множества S.

Обозначение 8.17. $C = \sup S$ (читается: *супремум*).

Упражнение 8.12. *Докажите, что $C \in \mathbb{R}$ является точной верхней гранью множества S тогда и только тогда, когда выполняются следующие два условия:*
1) $\forall\, x \in M :\ x \leqslant C$;
2) $\forall\, \varepsilon > 0\ \exists\, x \in M :\ x > C - \varepsilon$.

Аксиома 8.5. [Аксиома полноты]
Всякое непустое ограниченное сверху подмножество $S \in \mathbb{R}$ имеет в $\mathbb{R}$ точную верхнюю грань.

Замечание 8.18. Аксиома полноты в этой формулировке называется *аксиомой о точной верхней грани.*

Упражнение 8.13. *Дайте определение точной нижней грани ограниченного снизу множества и докажите, что всякое непустое ограниченное снизу множество $S \in \mathbb{R}$ имеет в $\mathbb{R}$ точную нижнюю грань.*

Обозначение 8.19. $C = \inf S$ (читается: *инфимум*).

8.5. Бесконечные десятичные дроби

Как мы обсуждали во введении к этой главе, когда мы используем аксиоматический подход для задания объекта, всегда возникает вопрос, почему этот объект существует. Идея этого раздела — предъявить искомый действительные числа явным образом, построив их на основе рациональных, после чего проверить, что они удовлетворяют описанным выше аксиомам. Строго эту проверку мы делать не будем, лишь наметив общее направление.

Определение 8.20. Запись вида $\overline{\alpha_n\alpha_{n-1}\ldots\alpha_1\alpha_0}$, где α_i — цифры и $\alpha_n \neq 0$, называется *десятичной записью натурального числа* $10^n \cdot \alpha_n + 10^{n-1} \cdot \alpha_{n-1} + \ldots + 10 \cdot \alpha_1 + \alpha_0$. Запись вида $\pm A{,}a_1a_2\ldots a_n$, где A — десятичная запись натурального числа или ноль, а a_i — цифры, называется *конечной десятичной дробью* и обозначает число $\pm\left(A + \dfrac{a_1}{10} + \dfrac{a_2}{10^2} + \ldots + \dfrac{a_n}{10^n}\right)$.

Определение 8.21. Пусть $A \in \mathbb{N}$ и (a_n) — последовательность цифр. *Бесконечной десятичной дробью* с разрядами a_n будем называть (бесконечную) запись $\pm A{,}a_1a_2\ldots a_na_{n+1}\ldots$

Замечание 8.22. По формальным причинам мы запретим запись $-0{,}000\ldots$, поскольку ясно, что она должна означать то же самое, что и $0{,}000\ldots$. Кроме того, как мы увидим чуть ниже, стоит запретить записи с «хвостом девяток», поскольку они дублируют записи с «хвостом нулей», например $0{,}999\ldots = 1{,}000\ldots$ Другой способ — ввести отношение эквивалентности, отождествив пары записей подобного вида, и считать действительными числами не сами бесконечные десятичные дроби, а их классы эквивалентности.

Определив множество бесконечных десятичных дробей, нужно объяснить, как его элементы складывать и умножать. Для этого используются алгоритмы сложения и умножения «в столбик», сначала применительно к конечным кускам дробей. Например,

$$
+\begin{array}{r} 0,3 \\ 0,4 \\ \hline 0,7 \end{array}
\qquad
+\begin{array}{r} 0,34 \\ 0,45 \\ \hline 0,79 \end{array}
\qquad
+\begin{array}{r} 0,347 \\ 0,452 \\ \hline 0,799 \end{array}
\qquad
+\begin{array}{r} 0,3476 \\ 0,4525 \\ \hline 0,8001 \end{array}
\qquad
+\begin{array}{r} 0,34760 \\ 0,45259 \\ \hline 0,80019 \end{array}
\qquad
+\begin{array}{r} 0,347603 \\ 0,452592 \\ \hline 0,800195 \end{array}
$$

Как можно увидеть, рассматривая конечные куски сумм, значение результата постепенно стабилизируется (в примере выше уже стабилизировавшиеся цифры отмечены зелёным): как только цифра в очередном разряде суммы оказывается отличной от 9, мы можем с уверенностью сказать, что все предыдущие разряды стабилизировались. Единственное исключение составляет случай, когда в результате получается «хвост девяток», например

$$0{,}11111\ldots + 0{,}88888\ldots = 0{,}99999\ldots$$

В этом случае стабилизация происходит в самом конце уже по факту.

После того, как операции были определены, нужно доказывать выполнение аксиом сложения и умножения. Какие-то из них, как коммутативность, совсем очевидны. Какие-то, как ассоциативность или дистрибутивность, требуют больших усилий. Сложнее всего обосновать существование обратного элемента (аксиома (2d)) — для этого используется алгоритм деления «столбиком», однако более хитрый, чем известный всем со школы, поскольку делим мы не на конечные десятичные дроби, а на бесконечные.

Следующий шаг — ввести отношение порядка. Это делается естественным образом. Пусть имеется две бесконечные десятичные дроби без «хвостов девяток»:

$$A{,}a_1a_2\ldots \qquad \text{и} \qquad B{,}b_1b_2\ldots$$

Тогда первая дробь больше второй, если либо $A > B$, либо $A = B$ и найдётся такое натуральное $k \in \mathbb{N}$, что для всех индексов $i < k$ выполнено $a_i = b_i$, а для индекса k справедливо $a_k = b_k$. Иными словами, мы сравниваем бесконечные десятичные дроби поразрядно, и в какой дроби впервые цифра в каком-то разряде больше — ту дробь мы и объявляем большей. После этого проверяются аксиомы порядка, но мы это тоже делать не будем.

Последний шаг — проверка аксиомы Архимеда и аксиомы полноты. Аксиома Архимеда здесь очевидна:

$$A{,}a_1a_2\ldots \leqslant A+1 = (A+1){,}000\ldots$$

Посмотрим на аксиому полноты в формулировке 8.3. Пусть $x_n = \overline{A^{(n)},a_1^{(n)}a_2^{(n)}\ldots}$ — неубывающая последовательность бесконечных десятичных дробей без «хвостов девяток», ограниченная сверху каким-то числом. По аксиоме Архимеда можно вместо него взять натуральное M. Тогда $A^{(n)}$ — неубывающая последовательность целых чисел, ограниченная сверху целым числом M. 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 9, а потому она стабилизируется на $a_1^{(n_1)} = b_1$. Теперь смотрим на $a_2^{(n)}$ при $n \geqslant n_1$ и так далее. 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 так далее. 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 $y = \overline{C, c_1\ldots}$ отличается от $\overline{B, b_1\ldots}$: $c_k < b_k$. Тогда при $n \geqslant n_k$ верно, что $x_n = \overline{B, b_1\ldots b_k a_{k+1}^{(n)}\ldots}$, 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. Построение корня из двух и числа пи

В этом разделе мы объясним, почему во множестве действительных чисел существуют такие числа, как $\sqrt{2}$ и π.

Напомним, что $\sqrt{2}$ — это положительное решение уравнения $x^2 = 2$. Нам будет удобно искать его, пользуясь аналогом аксиомы 8.3 для невозрастающих последовательностей, который формулируется так (см. упражнение 8.9): 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 $A = \max\{c \mid x_n \geqslant c \ \ \forall n\}$.

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 8.14. *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 8.15. *Докажите, что*

$$x_n^2 - x^2 \leqslant 4(x_n - x).$$

Выведите отсюда, что $x^2 \geqslant 2$.

Упражнение 8.16. *Докажите, что*

$$x_{n+1}^2 - 2 \leqslant \frac{x_n^2 - 2}{4}.$$

Выведите отсюда, что $x^2 = 2$.

Теперь обсудим построение числа π. Напомним его определение. 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. Если мы теперь сложим такие неравенства для всех сторон 2^n-угольника, то как раз и получим $P_{n+1} \geqslant P_n$.

Покажем, что $P_n \leqslant 8$ при всех n. Рассмотрим часть 2^n-угольника, попадающую в первый квадрант: это ломаная $A_0A_1 \ldots A_{2^{n-2}}$, 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,

$$A_sA_{s+1} = \sqrt{(x_s - x_{s+1})^2 + (y_s - y_{s+1})^2} \leqslant |x_s - x_{s+1}| + |y_s - y_{s+1}| = (x_s - x_{s+1}) + (y_{s+1} - y_s)$$

(неравенство на втором шаге вытекает из того, что длина гипотенузы короче суммы длин катетов). Суммируя полученные неравенства при всех $s = 0, \ldots, (2^{n-2} - 1)$, мы получим неравенство $L_n \leqslant (x_0 - x_{2^{n-2}}) + (y_{2^{n-2}} - y_0) = 2$, что и требовалось.

Таким образом, последовательность $P_n = 4L_n$ возрастает и ограничена сверху, а потому, согласно аксиоме полноты 8.3, стремится к некоторому пределу, который и называется *длиной окружности* и обозначается π.

8.7. Литература для дальнейшего изучения

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

Действительные числа

Задачи семинаров

Основные задачи

Задача 8.1. Какие из следующих последовательностей являются невозрастающими, неубывающими, ограниченными сверху, ограниченными снизу?

а) $a_n = 1$.
б) $a_n = n$.
в) $a_n = -n^2$.
г) $a_n = 1,$ если $n = 2021,$ $a_n = 0,$ иначе.
д) $a_n = (-1)^n$.
е) $a_n = q^n$, $q \in \mathbb{R}$.

Задача 8.2. Верно ли, что если последовательности (a_n) и (b_n) являются неубывающими, то этим же свойством обладает их

а) сумма;
б) разность;
в) произведение;
г) частное?

Если нет, можно ли наложить какое-либо дополнительное условие, чтобы это стало верным?

Задача 8.3. а) Пусть последовательности (a_n) и (b_n) неограничены. Значит ли это, что неограничены последовательности $(a_n + b_n)$ и $(a_n \cdot b_n)$?

б) Пусть последовательность (a_n) ограничена, а последовательность (b_n) неограничена. Что можно сказать про последовательность $(a_n + b_n)$?

в) Пусть последовательности (a_n) и (b_n) ограничены, причём $b_n \neq 0$ при всех $n \in \mathbb{N}$. Что можно сказать про последовательность (a_n / b_n)?

г) Пусть последовательность $(a_n \cdot b_n)$ ограничена и никогда не равна нулю. Что можно сказать про последовательности (a_n) и (b_n)?

Задача 8.4. Пусть множества A и B непустые и ограниченные. Докажите следующие свойства точных верхних и нижних граней:

а) если $A \subset B$, то $\sup A \leqslant \sup B$;
б) если $r > 0$, то $\sup(rA) = r \sup A$, где $rA = \{ra \mid a \in A\}$;
в) если $r < 0$, то $\inf(rA) = r \sup A$;
г) $\sup(A + B) = \sup A + \sup B$, где $A + B = \{a + b \mid a \in A, b \in B\}$;
д) если $A \subset (0, \infty)$, то $1/\sup(A) = \inf(1/A)$, где $1/A = \{1/a \mid a \in A\}$;
е) если $A, B \subset (0, \infty)$, то $\sup(A \cdot B) = \sup(A) \cdot \sup(B)$, где $A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$;

ж) приведите примеры, когда свойства из пунктов д) и е) нарушаются для множеств, содержащих не только положительные числа.

Задача 8.5. Найдите бесконечные десятичные записи чисел $1/7$ и $1/17$.

Задача 8.6. Найдите 99-ю цифру после запятой в десятичной записи числа 5/7.

Определение 8.23. Бесконечная десятичная 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 8.24. $\pm A{,}\alpha_1\alpha_2 \dots \alpha_k(\alpha_{k+1} \dots \alpha_{k+l})$.

Задача 8.7. а) Докажите, что десятичной дроби $0,(\beta_1 \dots \beta_m)$ соответствует число $\dfrac{\overline{\beta_1 \dots \beta_m}}{d^m - 1}$.

б) Найдите число, соответствующее десятичной дроби $A, \alpha_1 \dots \alpha_{k-1}(\beta_1 \dots \beta_m)$.

Задача 8.8 (С)**.** Докажите, что:

а) всякая периодическая десятичная дробь задаёт рациональное число;

б) всякое рациональное число задаётся периодической десятичной дробью.

Задача 8.9. Пусть $k, n \in \mathbb{N}$. Докажите, что сумма длин предпериода и минимального периода дроби k/n не больше n.

Задача 8.10. 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 8.11. При каких натуральных n десятичная дробь $1/n$

а) является конечной;

б) не имеет предпериода?

Задача 8.12. Пусть натуральные числа k и n взаимно просты. Докажите, что минимальные периоды у k/n и $1/n$ имеют одинаковую длину.

Дополнительные задачи

Задача 8.13. Докажите, что множество всех точек отрезка $[0, 1]$ равномощно множеству всех бесконечных последовательностей нулей и единиц (а значит, несчётно).

9. Движения плоскости

Теоретический материал

9.1. Преобразования плоскости, движения и их свойства

Пусть α — плоскость.

Определение 9.1. *Преобразованием плоскости* называется биекция вида $\phi : \alpha \to \alpha$. Если для какой-либо точки $A \in \alpha$ справедливо $\phi(A) = A$, то такая точка называется *неподвижной*.

Обозначение 9.2. Множество неподвижных точек преобразования ϕ обозначается $\mathrm{Fix}\,(\phi)$. Иными словами,

$$\mathrm{Fix}\,(\phi) = \{A \in \alpha \mid \phi(A) = A\}.$$

Изучать произвольные преобразования плоскости практически бессмысленно: они могут быть устроены сколь угодно плохо (переставьте, например, несколько точек местами). Поэтому мы будем изучать такие преобразования плоскости, которые сохраняют некоторые её геометрические свойства и структуры.

Определение 9.3. Преобразование плоскости $\phi : \alpha \to \alpha$ называется *движением*, если для любых точек $A, B \in \alpha$ расстояние между ними равно расстоянию между их образами.

Обозначение 9.4. Расстояние между точками A и B мы будем обозначать $\rho(A, B)$ или $|AB|$. Таким образом, ϕ — движение, если для любых двух точек A и B выполнено соотношение

$$\rho\big(\phi(A), \phi(B)\big) = \rho(A, B).$$

Пример 9.5. *Тождественное отображение* id_α, оставляющее каждую точку плоскости на месте, является простейшим примером движения. Очевидно, $\mathrm{Fix}\,(\mathrm{id}_\alpha) = \alpha$.

Утверждение 9.1. Пусть ϕ и ψ — движения плоскости. Тогда
- композиция $\psi \circ \phi$ также является движением;
- преобразование ψ^{-1}, обратное к движению ψ, снова является движением.

Доказательство. Рассмотрим произвольную пару точек A, B на плоскости. Тогда

$$\rho\big(\psi \circ \phi(A), \psi \circ \phi(B)\big) = \rho\big(\psi(\phi(A)), \psi(\phi(B))\big) = \rho\big(\phi(A), \phi(B)\big) = \rho(A, B),$$

а также

$$\rho\big(\psi^{-1}(A), \psi^{-1}(B)\big) = \rho\big(\psi(\psi^{-1}(A)), \psi(\psi^{-1}(B))\big) = \rho(A, B).$$

Значит, преобразования $\psi \circ \phi$ и ψ^{-1} сохраняют расстояния, то есть являются движениями. $\square$

Каждое движение ϕ сохраняет прямые, то есть образ прямой под действием ϕ — это снова прямая (подумайте, почему это так). Кроме того, любое движение сохраняет углы и их градусные меры.

9.2. Виды движений: параллельный перенос

Определение 9.6. *Параллельным переносом* $T_{\overrightarrow{v}}$ на вектор $\overrightarrow{v}$ называется движение, при котором каждая точка A отображается в такую точку A', что вектор $\overrightarrow{AA'}$ равен вектору $\overrightarrow{v}$.

Иными словами, если A и B — две точки плоскости, а A' и B' — их образы при параллельном переносе $T_{\overrightarrow{v}}$, то середины отрезков AB' и $A'B$ совпадают. В частности, если прямая AB не параллельна вектору $\overrightarrow{v}$, то $ABB'A'$ — параллелограмм (рис. 21). Это свойство можно использовать в качестве определения параллельного переноса.

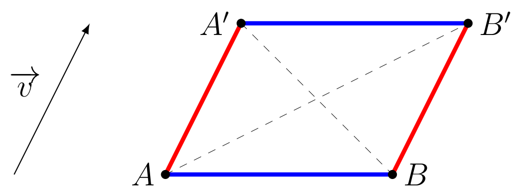

Рис. 21.

Утверждение 9.2. Определение 9.6 корректно, то есть параллельный перенос действительно является движением.

Доказательство. Пусть A и B — две произвольные точки плоскости, а A' и B' — их образы при параллельном переносе соответственно. Как мы видели выше, если AB и $\overrightarrow{v}$ не параллельны, то $ABB'A'$ — параллелограмм. Следовательно, $|AB| = |A'B'|$. □

Упражнение 9.1. *Завершите доказательство утверждения 9.1 для случая, когда* $AB \parallel \overrightarrow{v}$.

Определение 9.7. Мы будем говорить, что движение ϕ можно *восстановить* в своём классе по n точкам, если, зная образы произвольного набора точек $A_1, \ldots, A_n \in \alpha$, можно найти $\phi(B)$ для любой точки $B \in \alpha$.

Определение 9.7 означает, что для заданного набора точек $A_1, \ldots, A_n \in \alpha$ и их образов $A'_1, \ldots, A'_n \in \alpha$ существует единственное движение ϕ из рассматриваемого класса такое, что $\phi(A_k) = A'_k$ для $k = 1, \ldots, n$.

Утверждение 9.3. Параллельные переносы восстанавливаются по одной точке: для каждой пары $A, A' \in \alpha$ существует единственный параллельный перенос T, для которого $T(A) = A'$.

Доказательство. Параллельный перенос однозначно определяется вектором сдвига $\overrightarrow{v}$. То есть чтобы восстановить параллельный перенос, нужно определить, чему равен вектор $\overrightarrow{v}$. Как несложно догадаться, $\overrightarrow{v} = \overrightarrow{AA'}$. Другими словами, зная, что движение T — параллельный перенос, а также что $T(A) = A'$, мы можем для каждой точки B однозначно определить её образ $B' = T(B')$: это такая точка, для которой середины отрезков AB' и BA' совпадают. □

Упражнение 9.2. *а) Каково множество неподвижных точек параллельного переноса* $T_{\overrightarrow{v}}$*?*

б) Для каких прямых m *выполняется равенство* $T_{\overrightarrow{v}}(m) = m$*?*

в) Для каких окружностей ω *выполняется равенство* $T_{\overrightarrow{v}}(\omega) = \omega$*?*

9.3. Виды движений: осевая симметрия

Определение 9.8. *Осевая симметрия* S_l с осью l — это движение, переводящее каждую точку A в такую точку A', что прямая l является серединным перпендикуляром к отрезку AA'. Также её называют *отражением* относительно прямой l.

Утверждение 9.4. Определение 9.8 корректно, то есть осевая симметрия в самом деле является движением.

Доказательство. Рассмотрим точки $A, B \in \alpha$ и их образы A' и B' под действием S_l. Докажем, что $|AB| = |A'B'|$. Для этого рассмотрим все возможные случаи расположения точек A и B.

1) Если $A, B \in l$, то $A' = A$, $B' = B$ и доказывать нечего.

2) Пусть теперь $A \in l$, но $B \notin l$. Тогда $A' = A$, но $B' \neq B$. Обозначим за O точку пересечения отрезка BB' и прямой l (рис. 22). Так как B и B' симметричны относительно l, то

$$|BO| = |B'O|, \qquad \measuredangle AOB = \measuredangle AOB' = \frac{\pi}{2}.$$

Значит, треугольники $\triangle ABO$ и $\triangle AB'O$ прямоугольны и имеют равные катеты. Следовательно, они равны, и $|AB| = |A'B'|$.

3) Предположим, что $A, B \notin l$ и при этом прямые AB и l пересекаются. Обозначим их точку пересечения за C (рис. 23). Тогда $S_l(C) = C$, и нам достаточно доказать, что

$$|AC| = |A'C|, \qquad |BC| = |B'C|.$$

А это уже напрямую следует из разобранного выше случая 2). □

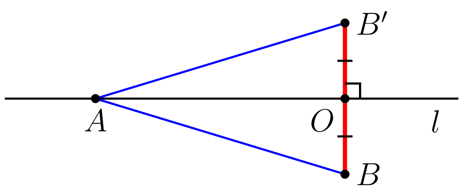

Рис. 22.

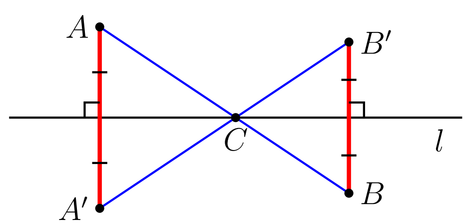

Рис. 23.

Упражнение 9.3. *Завершите доказательство утверждения 9.3, то есть разберите случай, когда $A, B \notin l$ и при этом $AB \parallel l$.*

Утверждение 9.5. Осевые симметрии восстанавливаются по двум точкам: существует единственная осевая симметрия S_l, для которой $S_l(A) = A'$ и $S_l(B) = B'$ при данных $A, B, A', B \in \alpha$.

Доказательство. Чтобы восстановить осевую симметрию по точкам A и B, достаточно построить её ось l. Если A и B неподвижны, то $l = AB$. Если же A не является неподвижной точкой данной осевой симметрии, то l — это серединный перпендикуляр к отрезку AA'. □

Упражнение 9.4. *а) Каково множество неподвижных точек осевой симметрии S_l?*

б) Для каких прямых m выполняется равенство $S_l(m) = m$?

в) Для каких окружностей ω выполняется равенство $S_l(\omega) = \omega$?

9.4. Виды движений: поворот

Определение 9.9. *Поворотом* $R_{O,\varphi}$ около точки O на угол φ называется движение, оставляющее точку O на месте и переводящее каждую точку $A \neq O$ в такую точку A', что $|OA| = |OA'|$ и $\measuredangle AOA' = \varphi$ (рис. 24). Поворот на угол $\varphi = \pi$ около точки O также называется *центральной симметрией* относительно точки O и обозначается S_O.

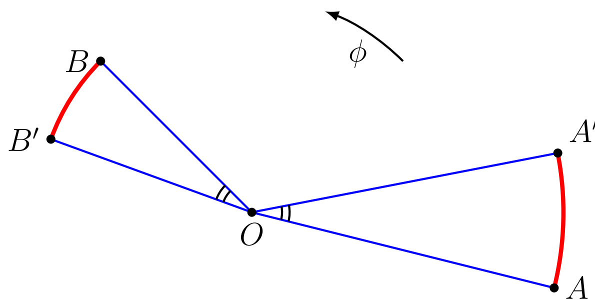

Рис. 24.

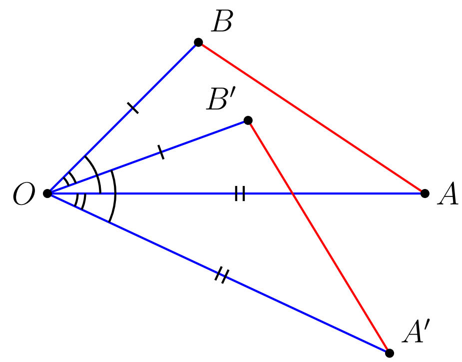

Рис. 25.

Утверждение 9.6. Определение 9.9 корректно, то есть поворот является движением.

Доказательство. Рассмотрим точки $A, B \in \alpha$ и их образы A' и B' под действием $R_{O,\varphi}$. Если одна из точек A и B совпадает с O, то равенство $|AB| = |A'B'|$ следует из определения. Пусть теперь A, O и B образуют треугольник (рис. 25). Тогда

$$\measuredangle A'OB' = \measuredangle AOA' + \measuredangle AOB - \measuredangle B'OB = \varphi + \measuredangle AOB - \varphi = \measuredangle AOB.$$

Учитывая, что $|AO| = |A'O|$ и $|BO| = |B'O|$, получаем, что треугольники $\triangle AOB$ и $\triangle A'OB'$ равны по двум сторонам и углу между ними. Следовательно $|AB| = |A'B'|$. $\square$

Упражнение 9.5. *Завершите доказательство утверждения 9.5, рассмотрев случай, когда точки A, B и O лежат на одной прямой.*

Утверждение 9.7. Повороты восстанавливаются по двум точкам: существует единственный поворот $R_{O,\varphi}$, для которого $R_{O,\varphi}(A) = A'$ и $R_{O,\varphi}(B) = B'$ при данных $A, B, A', B \in \alpha$.

Доказательство. Для того, чтобы восстановить поворот, нам нужно определить два параметра: его центр O и угол поворота φ. Будем строить их в зависимости от взаимного расположения данных точек A и B и их образов.

1) Если обе точки A и B неподвижны, то $\varphi = 0$, а в качестве центра поворота можно взять любую точку. В этом вырожденном случае поворот на самом деле является тождественным преобразованием id_α.

2) Если точка A неподвижна, а точка B — нет, то $O = A$, а угол поворота φ восстанавливается как $\measuredangle BOB'$.

3а) Пусть теперь $A \neq A'$ и $B \neq B'$. Обозначим за l и m серединные перпендикуляры к отрезкам AA' и BB' соответственно. Так как $\triangle AOA'$ равнобедренный, то высота и медиана, опущенные из O, совпадают, так что $O \in l$. Аналогично, O лежит на прямой m. Если l и m

пересекаются в единственной точке, то центр найден (рис. 26). Угол поворота, как и выше, восстанавливается как $\varphi = \measuredangle BOB'$.

3b) Предположим, что l и m параллельны. Так как $O \in l \cap m$, они совпадают. Докажем, что O лежит на прямой AB. Обозначим за A'' середину отрезка AA', то есть точку пересечения прямых AA' и l. Так как луч OA'' является биссектрисой угла $\measuredangle AOA'$, угол между прямыми AO и l равен половине $\measuredangle AOA'$:

$$\measuredangle AOA'' = \frac{\measuredangle AOA'}{2} = \frac{\varphi}{2}.$$

Аналогично, угол между прямыми BO и l равен $\varphi/2$, так что $AO = BO$ и O лежит на прямой AB (рис. 26). С другой стороны, обратное отображение к повороту также является поворотом с центром в O. Поэтому, применяя это же рассуждение к обратному отображению, получаем, что O лежит также и на рямой $A'B'$. Если прямые AB и $A'B'$ различны, то это позволяет нам построить точку O. В противном случае искомый поворот имеет инвариантную прямую, а значит, это центральная симметрия. Тогда $\varphi = \pi$, а O — это середина отрезка AA'. $\square$

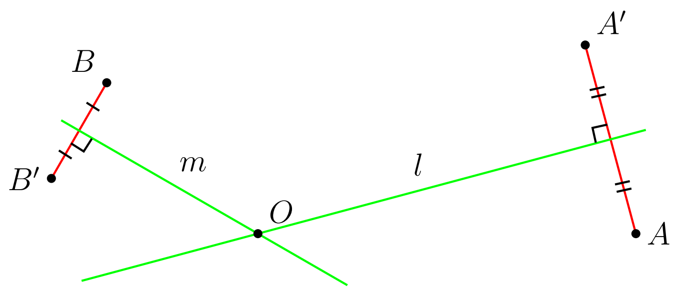

Рис. 26.

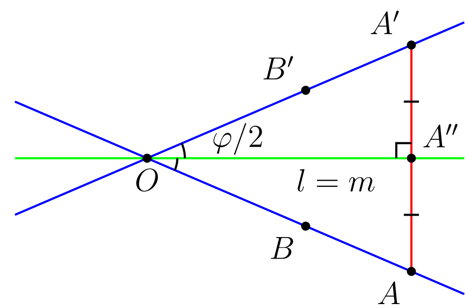

Рис. 27.

Упражнение 9.6. *а) Каково множество неподвижных точек поворота $R_{O,\varphi}$?*

б) Для каких прямых m выполняется равенство $R_{O,\varphi}(m) = m$?

в) Для каких окружностей ω выполняется равенство $R_{O,\varphi}(\omega) = \omega$?

9.5. Композиции движений

Как следует из утверждения 9.1, композиция движений ϕ и ψ, а также отображение, обратное к данному движению ψ, также являются движениями. В этом разделе мы поговорим о том, какими могут быть движения $\psi \circ \phi$ и ψ^{-1} в зависимости от движений ϕ и ψ.

Пример 9.10. 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 A перешла в точку A' такую, что прямая l является серединным перпендикуляром к отрезку AA', то при повторном применении S_l для точки A' такой точкой станет точка A. Таким образом, $S_l \circ S_l = \mathrm{id}_\alpha$ или $(S_l)^{-1} = S_l$, то есть осевая симметрия S_l сама себе обратна. Отображения, обратные сами себе, называются *инволюциями.*

Пример 9.11. 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 $\overrightarrow{u}+\overrightarrow{v}$. В самом деле, пусть точка A под действием $T_{\overrightarrow{u}}$ отобразилась в точку A', а точка A' под действием $T_{\overrightarrow{v}}$ — в точку A''. По определению параллельного переноса $\overrightarrow{AA'}=\overrightarrow{u}$ и $\overrightarrow{A'A''}=\overrightarrow{v}$, а значит, $\overrightarrow{AA''}=\overrightarrow{u}+\overrightarrow{v}$. Таким образом, мы показали, что $T_{\overrightarrow{v}}\circ T_{\overrightarrow{u}}=T_{\overrightarrow{u}+\overrightarrow{v}}$.

Упражнение 9.7. *Какое движение будет обратным к параллельному переносу $T_{\overrightarrow{v}}$?*

Пример 9.12. Композиция поворотов с центром в одной и той же точке O является поворотом с тем же центром. Более точно,

$$R_{O,\varphi_1}\circ R_{O,\varphi_2}=R_{O,\varphi_1}\circ R_{O,\varphi_2}=R_{O,\varphi_1+\varphi_2}.$$

В частности, обратное отображение к повороту $R_{O,\varphi}$ — это поворот вокруг той же точки и на тот же угол, но в противоположную сторону: $R_{O,\varphi}^{-1}=R_{O,-\varphi}$.

Упражнение 9.8. *Рассмотрим композицию $\phi=S_l\circ S_m$ двух осевых симметрий относительно прямых l и m. Докажите следующие утверждения.*

- *Если $l\parallel m$, то ϕ — это параллельный перенос. Как найти вектор этого параллельного переноса?*
- *, Если прямые l и m не параллельны, то ϕ — это поворот вокруг их точки пересечения. Чему равен угол поворота?*

Замечание 9.13. Обратите внимание, что порядок, в котором мы применяем движения S_l и S_m, вообще говоря, важен, то есть $S_l\circ S_m\neq S_m\circ S_l$. Оказывается, для движений это довольно типичная ситуаций. В задачах ниже мы увидим, что порядок применяемых отображений часто играет существенную роль.

9.6. Виды движений: скользящая симметрия

До сих пор мы имели дело только с тремя классами движений: параллельными переносами, отражениями относительно прямых и поворотами вокруг точек. Однако оказывается, что если рассматривать их композиции, могут возникнуть движения, не принадлежащие ни одному из этих классов. Этот раздел посвящён именно таком движениям — скользящим симметриям.

Определение 9.14. *Скользящая симметрия $H_{l,\overrightarrow{v}}$* вдоль прямой l — это композиция движений

$$H_{l,\overrightarrow{v}}=T_{\overrightarrow{v}}\circ S_l=S_l\circ T_{\overrightarrow{v}},$$

где вектор $\overrightarrow{v}$ и прямая l параллельны.

Замечание 9.15. Так как тождественное преобразование можно рассматривать как параллельный перенос на нулевой вектор, $T_{\overrightarrow{0}}=\mathrm{id}_\alpha$, отражение S_l — это частный случай скользящей симметрии вдоль оси l.

Рассмотрим скользящую симметрию $H_{l,\overrightarrow{v}}$ и точку A, не лежащую на прямой l. Обозначим за B основание высоты, опущенной из A на l, а за O — точку пересечения l и отрезка, соединяющего A и его образ A' (рис. 28). Образ B' точки B лежит на l, и кроме того, $|AB| = |A'B'|$ и $A'B' \perp l$, так что треугольники $\triangle ABO$ и $\triangle A'B'O$ равны как прямоугольные треугольники с равными катетами и гипотенузами. Следовательно, отрезки AA' и BB' пересекаются на прямой l и точка пересечения O делит их пополам.

Отметим также, что если точки A_1 и A_2 являются образами точки A при отражении S_l и параллельном переносе $T_{\overrightarrow{v}}$ соответственно, то $AA_1A'A_2$ — прямоугольник со сторонами, параллельными прямой l (рис. 28).

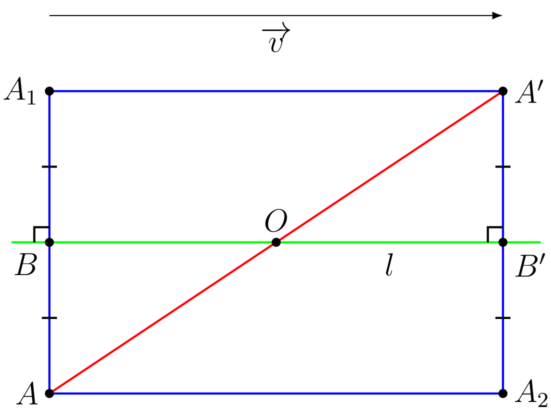

Рис. 28.

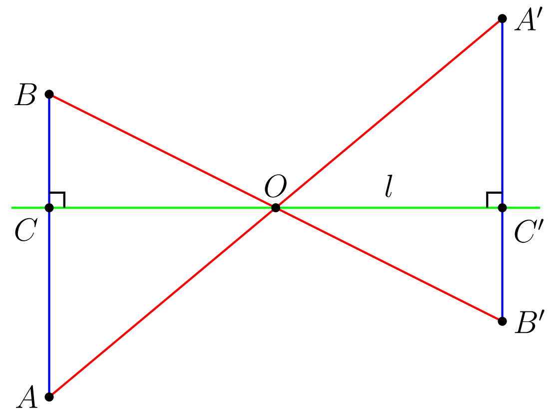

Рис. 29.

Утверждение 9.8. Скользящая симметрия $H_{l,\overrightarrow{v}}$ восстанавливается по двум точкам.

Доказательство. Рассмотрим пару точек $A, B \in \alpha$ и их образы A' и B' при данной скользящей симметрии. Мы хотим восстановить её ось l и определить вектор сноса $\overrightarrow{v}$. Пусть точки O и K — середины отрезков AA' и BB' соответственно. Имеется два возможных случая.

1) Если точки O и K различны, то прямая l восстанавливается как $l = OK$.

2) Пусть теперь O и K совпадают. Рассмотрим основания C и D высот, опущенных на l из A и B. Тогда векторы CC' и DD' равны, сонаправлены и имеют общую середину. Значит, $C = D$ и $AB \perp l$ (рис. 29). Теперь мы можем восстановить l как прямую, перпендикулярную прямой AB и проходящую через точку O. А параллельный перенос $T_{\overrightarrow{v}}$ определяется тем, что точка O является серединой отрезка CC', то есть $\overrightarrow{v} = \overrightarrow{CC'}$. □

9.7. Теорема Шаля

Теорема 9.9. [Теорема Шаля.]
Всякое движение плоскости представляет собой одно из следующих движений:

- тождественное преобразование id_α;
- параллельный перенос $T_{\overrightarrow{v}}$ на некоторый ненулевой вектор $\overrightarrow{v}$;
- поворот $R_{\phi,O}$ на некоторый ненулевой угол ϕ;
- осевая симметрия S_l относительно некоторой прямой l;
- скользящая симметрия $T_{\overrightarrow{v}} \circ S_l$, где $\overrightarrow{v}$ и l — параллельные друг другу вектор и прямая.

Движения плоскости

Задачи семинаров

Движения прямой

Пусть l — прямая. Этот раздел посвящён движениям на прямой.

Задача 9.1. По аналогии с движениями плоскости, дайте определение движения прямой

$$\phi : l \to l.$$

Задача 9.2. Докажите, что движение ϕ прямой l — это

- параллельный перенос, если ϕ не имеет неподвижных точек;
- отражение с центром в A, если A — единственная неподвижная точка ϕ;
- тождественное преобразование, если ϕ имеет хотя бы 2 неподвижные точки.

Задача 9.3. Докажите следующие утверждения.

- Параллельный перенос T, переводящий A в B, единственен.
- Для $A, B \in l$ композиция $\mathcal{S}_B \circ \mathcal{S}_A$ это такой параллельный перенос T, что

$$T(A) = \mathcal{S}_B(A).$$

- Композиция параллельных переносов T_1 и T_2 это такой параллельный перенос, что

$$T(A) = T_2(T_1(A)).$$

  Параллельные переносы коммутируют: $T_2 \circ T_1 = T_1 \circ T_2$.

- Композиция T и $\mathcal{S}_A$ является отражением относительно центра отрезка $AT^{-1}(A)$. Композиция $\mathcal{S}_A$ и T является отражением относительно центра отрезка $AT(A)$.

Теперь мы можем составить **таблицу умножения** для движений прямой

$\circ$	S	T
S	T	S
T	S	T

Задача 9.4. Покажите, что произвольное движение прямой l может быть представлено в виде композиции отражений, число "сомножителей" в котором не больше двух.

Движения плоскости

Задача 9.5. Опишите множество движений плоскости, совмещающих прямые l и n.

Задача 9.6. Докажите, что движение T плоскости α является параллельным переносом тогда и только тогда, когда выполнено одно из трех следующих условий

- T отображает каждый луч на сонаправленный ему;
- для любых $A, B \in \alpha$ середины отрезков $AT(B)$ и $BT(A)$ совпадают;
- либо T сохраняет каждую прямую, параллельную l и $\mathrm{Fix}\,(T) = \varnothing$, либо $T = \mathrm{id}_\alpha$.

Задача 9.7. Докажите, что ϕ — скользящая симметрия тогда и только тогда, когда

- середина отрезка AA', соединяющего точку $A \in \alpha$ и ее образ A', лежит на l;
- ограничение ϕ определяет параллельный перенос на прямой l;

Задача 9.8. Докажите, что для произвольного движения ϕ множество неподвижных точек

- пусто $\Leftrightarrow$ ϕ параллельный перенос либо скользящая симметрия (на ненулевой вектор);
- состоит из одной точки $\Leftrightarrow$ ϕ поворот вокруг этой точки на ненулевой угол;
- состоит из прямой $\Leftrightarrow$ ϕ это отражение относительно этой прямой;
- совпадает со всей плоскостью $\Leftrightarrow$ ϕ тождественное преобразование.

Задача 9.9. Докажите, что множество инвариантных прямых движения ϕ

- пусто $\Leftrightarrow$ ϕ это поворот на ненулевой угол;
- состоит из прямой l $\Leftrightarrow$ ϕ это скользящая симметрия с осью l (на ненулевой вектор);
- состоит из прямых, проходящих через O $\Leftrightarrow$ ϕ это центральная симметрия Z_O;
- состоит из прямых, параллельных l $\Leftrightarrow$ ϕ это параллельный перенос на ненулевой вектор вдоль l;
- состоит из прямой l и прямых, перпендикулярных l $\Leftrightarrow$ ϕ это отражение S_l;
- совпадает со всем $\mathcal{L}$ $\Leftrightarrow$ ϕ тождественное преобразование.

Какие движения могут относиться сразу к нескольким типам нашей классификации?

Задача 9.10. 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 9.11. Пусть ABC — равнобедренный прямоугольный треугольник с гипотенузой BC. Дайте точное описание композиции движений $S_{CA} \circ S_{BC} \circ S_{AB}$.

Задача 9.12. 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?

Задача 9.13. 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.

Задача 9.14. 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 точку O с помощью циркуля и линейки по точкам O_1, O_2 и углам φ_1, φ_2.

Задача 9.15. Преобразованием какого типа может являться композиция двух скользящих симметрий? Какой из типов реализуется при каких условиях на взаимное расположение осей исходных симметрий?

Задача 9.16. 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.

Задачи на построение

Задача 9.17. Рассмотрим прямую l и пару точек $A, B \in \alpha$. Для какого $C \in l$ сумма длин

$$f(C) := |AC| + |CB|$$

принимает наименьшее значение? Сколько таких точек?

Задача 9.18. Для точки A внутри острого угла $\measuredangle BOC$ рассмотрим периметр

$$f(D, F) = P_{ADF}$$

как функцию от пары точек $D \in OB$, $E \in OC$ на сторонах угла.
Для каких D и E функция f принимает наименьшее значение?

Задача 9.19. Рассмотрим точку M, лежащую внутри угла $\measuredangle AOB$. На сторонах угла постройте пару точек $C \in OA$ и $D \in OB$ таких, что M лежит на середине отрезка CD.

Задача 9.20. В условия предыдущей задачи постройте точки $C \in OA$ и $D \in OB$ так, чтобы точка M лежала на отрезке CD и площадь треугольника $\triangle OCD$ была наименьшей.

10. Комплексные числа

Теоретический материал

10.1. Алгебраическая форма комплексного числа

В этой главе мы займёмся построением 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.

Определение 10.1. *Комплексным числом* называется точка вещественной плоскости.

Обозначение 10.2. Множество комплексных чисел обозначается буквой $\mathbb{C}$.

Если зафиксировать на этой плоскости декартову систему координат Oxy, то каждая точка M будет иметь некоторые координаты (x, y), которые мы обозначим одним символом (рис. 30):

$$z = (x, y).$$

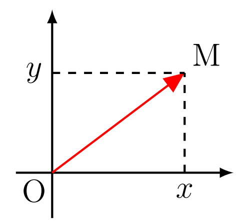

Рис. 30.

Запись $M(z)$ означает, что z — комплексная координата точки M.

Определение 10.3. Вещественные координаты x и y комплексного числа z 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.

Определение 10.4. *Комплексно сопряженным* к числу $z = x + iy$ называется число

$$\bar{z} = x - iy.$$

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:

$$z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2).$$

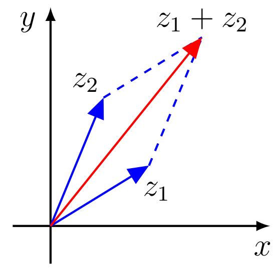

Рис. 31.

Упражнение 10.2. *Покажите, что для любого $z \in \mathbb{C}$ справедливо*

$$\mathrm{Re}\,(z) = \frac{z + \bar{z}}{2} \qquad и \qquad \mathrm{Im}\,(z) = \frac{z - \bar{z}}{2i}.$$

$\cdot$	1	i
1	1	i
i	i	-1

Табл. 1.

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 вид изображённый на табл. 1.

Для остальных чисел воспользуемся дистрибутивностью умножения относительно сложения. Иначе говоря, определим умножение, пользуясь обычными правилами раскрытия скобок и приведения подобных:

$$z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + y_1 x_2).$$

Пример 10.5. $(5 + 2i)(3 - i) = 5 \cdot 3 - 5 \cdot i + 2i \cdot 3 - 2i \cdot i = 15 - 5i + 6i + 2 = 17 - i.$

Упражнение 10.3. *Найти все $t \in \mathbb{R}$, для которых величина $(2 + 3i)(2 + ti)$ — вещественная.*

Упражнение 10.4. *Докажите, что для любых $z_1, z_2 \in \mathbb{C}$ выполнено*

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 \qquad и \qquad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2.$$

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 10.6. $\dfrac{5 + 2i}{3 - i} = \dfrac{(5 + 2i)(3 + i)}{(3 - i)(3 + i)} = \dfrac{15 + 5i + 6i - 2}{9 + 1} = \dfrac{13 + 11i}{10} = 1{,}3 + 1{,}1i.$

Упражнение 10.5. *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 вектор задаётся двумя параметрами: длиной и направлением. Поэтому применительно к комплексной плоскости уместно рассмотреть следующие две величины.

Определение 10.7. • *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:

$$\arg(z) = \theta.$$

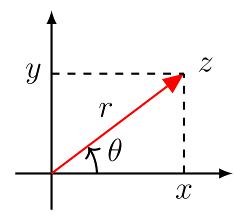

Рис. 32.

Очевидно, что аргумент комплексного числа определен не однозначно, а с точностью до 2π.[1] Удобно брать значения $\theta \in [0; 2\pi)$.

Определение 10.8. Пусть r и θ обозначают модуль и аргумент ненулевого комплексного числа $z = x + iy$ соответственно. Тогда число z записывается через *полярные координаты* (r, θ):

$$z = r(\cos\theta + i\sin\theta).$$

Такая форма записи называется *тригонометрической формой* комплексного числа.

Упражнение 10.6. *Выразите модуль r и аргумент θ числа $z = x + iy \neq 0$ 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

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1) \qquad \text{и} \qquad z_2 = r_2(\cos\theta_2 + i\sin\theta_2).$$

Вычислим их произведение:

$$z_1 \cdot z_2 = \big(r_1(\cos\theta_1 + i\sin\theta_1)\big)\big(r_2(\cos\theta_2 + i\sin\theta_2)\big) = \\ = r_1 \cdot r_2\big((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)\big).$$

Тем самым, получаем

$$z_1 \cdot z_2 = r_1 \cdot r_2\big(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\big).$$

Таким образом, для того, чтобы перемножить два ненулевых комплексных числа, нужно перемножить их модули, а аргументы — сложить.

[1] С формальной точки зрения на множестве $\mathbb{R}$ вводится отношение эквивалентности. Именно, мы полагаем $a \sim b$, если разность $(a - b)$ представима в виде $2\pi k$, для некоторого $k \in \mathbb{Z}$. Тогда аргумент — это класс эквивалентности по такому отношению. См. также пункт б) упражнения 2.9.

Пример 10.9. 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,

$$w = \left(1\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)\right)\left(\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)\right)^2 = \\ = 1\cdot(\sqrt{2})^2\left(\cos\left(\frac{\pi}{2} + 2\cdot\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2} + 2\cdot\frac{\pi}{2}\right)\right) = 2\big(\cos\pi + i\sin\pi\big) = -2.$$

В качестве следствия получается формула для возведения в степень.

Теорема 10.1. [Формула Муавра] Пусть r и θ — модуль и аргумент ненулевого комплексного числа z соответственно. Тогда для любого $n \in \mathbb{Z}$ имеет место формула:

$$\boxed{z^n = r^n\big(\cos(n\theta) + i\sin(n\theta)\big).}$$

Упражнение 10.7. *Докажите формулу Муавра.*

Упражнение 10.8. *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

$$z^n = w. \tag{4}$$

Для начала, воспользуемся формулой Муавра:

$$z^n = r^n(\cos n\alpha + i\sin n\alpha).$$

Следовательно,

$$\begin{cases} r^n &= \rho \\ n\alpha &= \theta + 2\pi k \end{cases} \quad\Longrightarrow\quad \begin{cases} r &= \sqrt[n]{\rho} \\ \alpha &= (\theta + 2\pi k)/n \end{cases}, \qquad k \in \{0, \ldots n-1\}.$$

Таким образом, существует ровно n решений уравнения (4) — *корней n-ой степени* из числа w. Поскольку они могут быть вычислены по формуле

$$z_k = \sqrt[n]{\rho}\left(\cos\frac{\theta + 2\pi k}{n} + i\sin\frac{\theta + 2\pi k}{n}\right), \quad k \in \{0, \ldots n-1\}, \tag{5}$$

это означает, что корни лежат на окружности радиуса $\sqrt[n]{\rho}$ и являются вершинами правильного n-угольника, вписанного в эту окружность.

Пример 10.10. Найдем корни четвертой степени из числа $w = 1 + i$. Прежде всего, найдём его модуль и аргумент:

$$r = |w| = |1+i| = \sqrt{1^2+1^2} = \sqrt{2} \qquad \text{и} \qquad \theta = \arg(w) = \arg(1+i) = \operatorname{arctg}\frac{1}{1} = \frac{\pi}{4}.$$

Следовательно в тригонометрической форме число w имеет вид

$$w = r(\cos\theta + \sin\theta) = \sqrt{2}\left(\cos\frac{\pi}{4} + \sin\frac{\pi}{4}\right).$$

Найдём корни уравнения $z^4 = w$, используя формулу (5). У нас $k \in \{0, \ldots, 3\}$, поэтому

$$\begin{aligned}
z_0 &= \sqrt[4]{\sqrt{2}}\left(\cos\frac{\frac{\pi}{4}+2\pi\cdot 0}{4} + i\sin\frac{\frac{\pi}{4}+2\pi\cdot 0}{4}\right) &= \sqrt[8]{2}\left(\cos\frac{\pi}{16} + \sin\frac{\pi}{16}\right);\\
z_1 &= \sqrt[4]{\sqrt{2}}\left(\cos\frac{\frac{\pi}{4}+2\pi\cdot 1}{4} + i\sin\frac{\frac{\pi}{4}+2\pi\cdot 1}{4}\right) &= \sqrt[8]{2}\left(\cos\frac{9\pi}{16} + \sin\frac{9\pi}{16}\right);\\
z_2 &= \sqrt[4]{\sqrt{2}}\left(\cos\frac{\frac{\pi}{4}+2\pi\cdot 2}{4} + i\sin\frac{\frac{\pi}{4}+2\pi\cdot 2}{4}\right) &= \sqrt[8]{2}\left(\cos\frac{17\pi}{16} + \sin\frac{17\pi}{16}\right);\\
z_3 &= \sqrt[4]{\sqrt{2}}\left(\cos\frac{\frac{\pi}{4}+2\pi\cdot 3}{4} + i\sin\frac{\frac{\pi}{4}+2\pi\cdot 3}{4}\right) &= \sqrt[8]{2}\left(\cos\frac{25\pi}{16} + \sin\frac{25\pi}{16}\right).
\end{aligned}$$

Таким образом, корни лежат в вершинах квадрата с центром в начале координат (рис. 33).

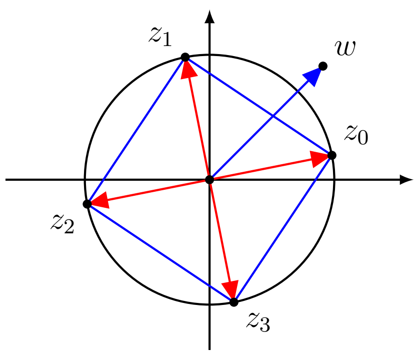

Рис. 33.

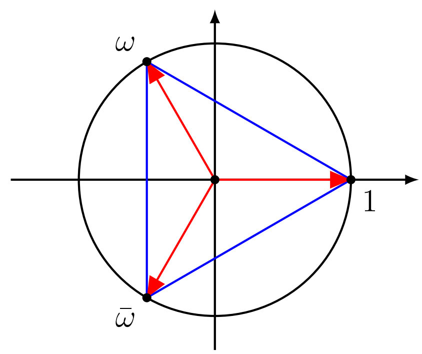

Рис. 34.

Как видно, как и в случае с действительными числами, извлечение корня из комплексного числа почти всегда дает «эстетически неприятный» ответ. Однако, следующий пример показывает, для корней из единицы не все так плохо.

Пример 10.11. Кубические корни из единицы удовлетворяют уравнению $z^3 = 1$. Один них равен 1. Другие два — комплексно сопряженные числа $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ и $\bar{\omega} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$ (рис. 34).

Упражнение 10.9. *а) Пусть ω_1 и ω_2 – корни n-ой степени из единицы. Докажите, что числа $\omega_1 \cdot \omega_2$ и $\frac{\omega_1}{\omega_2}$ 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.

Упражнение 10.10. *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:

$$a\left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Таким образом, видно, что 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 10.12. 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 10.13. 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 10.11. *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 $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$ с комплексными коэффициентами, степень которого $n \geqslant 1$, имеет комплексный корень.

Набросок доказательства. На комплексной плоскости $\mathbb{C}$ рассмотрим окружность радиуса R с центром нуле. Если для всех $\omega \in \mathbb{C}$ имеет место $p(\omega) \neq 0$, то образ этой окружности при отображении $p : \mathbb{C} \to \mathbb{C}$ — некоторая кривая, не проходящая через ноль (рис. 35).

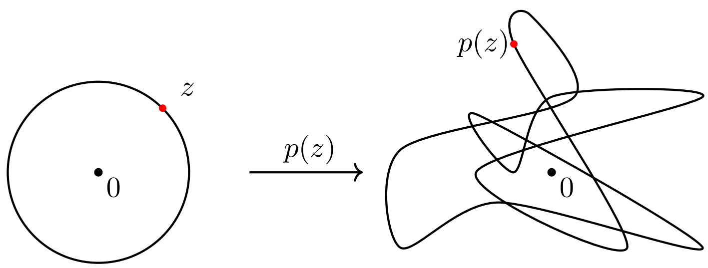

Рис. 35.

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, поскольку

$$p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0 = z^n \left(1 + \frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n}\right),$$

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 (рис. 36).

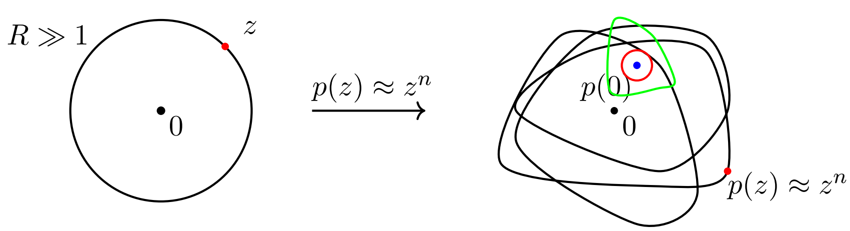

Рис. 36.

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 10.12. *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 $b = \left(\frac{\alpha}{2} - i\cdot\frac{\beta}{2}\right)$ 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 уравнение 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:

$$z\bar{z} + bz + \bar{b}\bar{z} + c = 0, \qquad b \in \mathbb{C},\ c \in \mathbb{R}.$$

Определение 10.14. *Обобщенной окружностью* на комплексной плоскости $\mathbb{C}$ называется его подмножество, являющееся прямой или окружностью.

Как следует из рассуждений выше, обобщённая окружность задаётся уравнением

$$\boxed{az\bar{z} + bz + \bar{b}\bar{z} + c = 0, \qquad a, c \in \mathbb{R},\ b \in \mathbb{C}.}$$

Упражнение 10.13. *Изобразите на комплексной плоскости множество точек z, задаваемое следующими 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 записываются в комплексных координатах. Начнём наш небольшой обзор с движений. Напомним, что *движением* (комплексной) плоскости назывется 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 10.14. *Пусть* $z = \dfrac{1}{2} + i\dfrac{1}{2}$. *Изобразите* $-i\bar{z} - 1 + 3i$.

Другим важным преобразованием плоскости является гомотетия.

Определение 10.15. *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 10.16. H_A^k.

Упражнение 10.15. *Докажите, что гомотетия*
а) переводит прямые в прямые, а окружности — в окружности;
б) сохраняет величины углов между лучами;
в) переводит треугольники в подобные треугольники с коэффициентом подобия k.

При $k = 1$ гомотетия H_A^k представляет собой тождественное преобразование плоскости, 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 10.16. *Как в комплексных координатах записывается гомотетия с произвольным 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.

Определение 10.17. *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 соотношение

$$(a-z)(\bar{a}-\bar{z})(a-w)(\bar{a}-\bar{w}) = R^4.$$

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':

$$w = \frac{R^2}{\bar{z}-\bar{a}} + a, \qquad \text{где } R \in \mathbb{R},\ a \in \mathbb{C}.$$

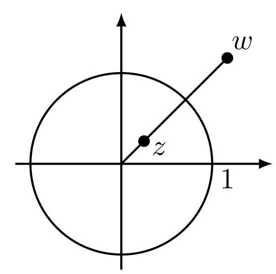

Рис. 37.

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 10.17. *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

Технические задачи

Задача 10.1. Вычислите:

а) $i + i^2 + i^3 + i^4$;

б) $i + 2i^2 + 3i^3 + \cdots + 10i^{10}$.

Задача 10.2. Найти действительную и мнимую части комплексного числа:

а) $\dfrac{i-7}{3i+6}$;

б) $\dfrac{i}{(3i+1)(3+i)}$;

в) $\dfrac{i+1}{i-1}$;

г) $(2+i\sqrt{5})^2$;

д) $(1+i)^4$.

Задача 10.3. Найдите множество значений:

а) $\sqrt{-1}$;

б) $\sqrt{-i}$;

в) $\sqrt{1-i}$;

г) $\sqrt[3]{i}$;

д) $(1+i)^{16}$.

Задача 10.4. Решите уравнения:

а) $\bar{z} = z^2$;

б) $z^2 = 2i$;

в) $z^3 = \dfrac{1-i}{1+i}$.

Задача 10.5. Пусть $\alpha \in \mathbb{R}$. Найдите тригонометрическую форму чисел

а) $\cos\alpha - i\sin\alpha$;

б) $\sin\alpha + i\cos\alpha$;

в) $1 + \cos\alpha + i\sin\alpha$.

Задача 10.6. Пусть $\arg(z) = \theta$. Вычислите:

а) $\arg(\bar{z})$;

б) $\arg(z) + \arg(\bar{z})$;

в) $\arg(z\bar{z})$;

г) $\arg\left(\dfrac{z}{\bar{z}}\right)$;

д) $\arg\left(z^2\right)$.

Задача 10.7. Изобразите на комплексной плоскости множество точек z таких, что:

а) $|z| \leqslant 2$;

б) $|1-z| > 1$;

в) $|z-2+i| = 3$;

г) $|z-i| = |z+1|$;

д) $\mathrm{Im}\,(z) \geqslant \mathrm{Re}\,(z)$;

е) $\mathrm{Im}\,(z) = |z-2|$;

Комплексные числа

Задачи семинаров

Комплексное сопряжение

Задача 10.8. Докажите, что если $|z| = 1$, то число $w = -i\frac{z-1}{z+1}$ вещественное.

Задача 10.9. Пусть функция $f : \mathbb{C} \to \mathbb{C}$ опеределена на множестве всех комплексных чисел и принимает комплексные значения. Докажите, что если она удовлетворяет двум условиям:

- для любых $z, w \in \mathbb{C}$ выполняется $f(z + w) = f(z) + f(w)$ и $f(zw) = f(z)f(w)$;
- для любого $x \in \mathbb{R}$ справедливо $f(x) = x$;

то $f(z) = z$ или $f(z) = \bar{z}$ для любого комплексного числа z.

Параллельность и перпендикулярность на комплексной плоскости

Задача 10.10. Даны две различные точки $A(a)$ и $B(b)$, отличные от начала координат O. Напишите условие коллинеарности точек O, A и B в терминах комплексных чисел a и b.

Задача 10.11. Даны две различные точки $A(a)$ и $B(b)$, отличные от начала координат O. Напишите условие перпендикулярности прямых OA и OB.

Задача 10.12. Напишите условие коллинеарности трех различных точек $A(a)$, $B(b)$ и $C(c)$.

Задача 10.13. Даны четыре различные точки $A(a)$, $B(b)$, $C(c)$ и $D(d)$. Напишите условие коллинеарности векторов $\overrightarrow{AB}$ и $\overrightarrow{CD}$.

Прямые и окружности

Задача 10.14. 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 10.15. Запишите в виде функции комплексной переменной:

а) ортогональную проекцию на ось Ox,

б) симметрию относительно оси y,

в) поворот на угол φ относительно точки A,

г) скользящую симметрию относительно прямой $y = 3$ со сдвигом на 1 влево,

д) поворот, переводящий ось x в прямую $y = 2x + 1$,

е) симметрию относительно прямой $y = 2x + 1$.

Уравнения и основная теорема алгебры

Задача 10.16. Пусть $1, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ – корни n-ой степени из единицы. Чему равна их сумма? Произведение?

Задача 10.17. Пусть $1, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ являются корнями уравнения $z^n = 1$. Докажите, что

$$(1 - \alpha_1)(1 - \alpha_2) \ldots (1 - \alpha_{n-1}) = n.$$

Задача 10.18. 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 10.19. Пусть $f(x)$ – многочлен с вещественными коэффициентами, степень которого не превосходит 4, и при этом $f(1 + i) = f(33 - i) = 0$. Найдите все возможные корни f.

Задача 10.20. 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 все возможные значения z.

Суммирование

Задача 10.21. Вычислите:

а) $\sin x + \sin 2x + \cdots + \sin nx$;

б) $\cos x + 2 \cos 2x + 3 \cos 3x + \cdots + n \cos nx$;

в) $\sin x + C_n^1 \sin 2x + C_n^2 \sin 3x + \cdots + C_n^n \sin{(n + 1)x}$

Задача 10.22. Для каждого натурального числа k найдите представления $\cos k\alpha$ и $\sin k\alpha$ в виде многочленов от $\cos \alpha$ и $\sin \alpha$

Дополнительные задачи

Задача 10.23. Найдите натуральное k, такое, что

$$\operatorname{arctg}\frac{1}{3}+\operatorname{arctg}\frac{1}{5}+\operatorname{arctg}\frac{1}{7}+\operatorname{arctg}\frac{1}{k}=\frac{\pi}{4}.$$

Задача 10.24. Найдите $\operatorname{Im}\big((\cos 17^\circ+\mathrm{i}\sin 17^\circ+\cos 43^\circ+\mathrm{i}\sin 43^\circ)^6\big)$.

11. Математический практикум

Задачи для индивидуального обсуждения

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, которые были бы эквивалентны 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. Может ли у множества A быть на 2020 подмножеств больше, чем у множества B?

Задача 11.6. 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 11.7. Пусть $A = \{b, c, d, e\}$, $B = \{c, e, k\}$, $C = \{a, b, e, k\}$, $D = \{a, c, k, l\}$. Сколько различных множеств можно получить из них при помощи операций $\cup$, $\cap$ и $\setminus$?

Задача 11.8. Верно ли, что $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$? Докажите или приведите контрпример.

Задача 11.9. 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 11.10. 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 11.11. Пусть $f : X \to Y$ — отображение, и A, $B \subset X$. Всегда ли верно, что:
а) $f(A \setminus B) \subset f(A) \setminus f(B)$;
б) $f(A \setminus B) \supset f(A) \setminus f(B)$?
Докажите или приведите контрпримеры.

Задача 11.12. 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 11.13. 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 11.14. 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 11.15. Постройте биекцию между множеством всех последовательностей натуральных чисел и множеством всех возрастающих последовательностей натуральных чисел.

Задача 11.16. 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 11.17. 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 11.18. 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 11.19. $n > 4$ 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 11.20. Найдётся ли натуральное число, произведение цифр которого равно 528?

Задача 11.21. 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 11.22. Опишите все такие натуральные числа n, что
а) НОД$(n, n+12) = 6$;
б) НОД$(n, n+12) = 1$.

Задача 11.23. Пусть $d(k)$ обозначает наибольший нечётный делитель целого числа k. Докажите, что $d(n+1) + d(n+2) + \ldots + d(2n) = n^2$.

Задача 11.24. Пусть $a, b, c \in \mathbb{N}$. Докажите, что если $ab \,\vdots\, c$, то $a \,\vdots\, \dfrac{c}{(c,b)}$.

Задача 11.25. 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 11.26. 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 11.27. Сколькими способами три взрослых человека могут поделить между собой
а) 15 различных конфет;
б) 15 одинаковых конфет?
(Делят не обязательно поровну, человеку может достаться ноль конфет.)

Задача 11.28. 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 11.29. На сколько нулей оканчивается число $11^{100} - 1$?

Задача 11.30. В ожесточенном бою 70 из 100 пиратов Флинта потеряли один глаз, 75 — одно ухо, 80 — одну руку и 85 — одну ногу. Каково минимальное число потерявших одновременно глаз, ухо, руку и ногу?

Задача 11.31. Найдите остаток от деления многочлена $(x-1)^{2019}$ на многочлен $(x-2)$.

Задача 11.32. 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 11.33. Приведите пример многочлена $f(x) \in \mathbb{Z}[x]$ такого, что $f(\sqrt{2} + \sqrt{5}) = 0$.

Задача 11.34. Найдите остаток от деления многочлена $x^{81} + x^{27} + x^9 + x^3 + x$ на $x^2 - 1$.

Задача 11.35. Пусть $f(x) = x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$. Найдите все рациональные корни многочлена $f(x)$.

Задача 11.36. 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 соотношение $l^a \equiv l^b \pmod{n}$?

Задача 11.37. Сколько различных решений имеет сравнение $123x \equiv 321 \pmod{777}$? (Имеются в виду решения, различные по модулю 777.)

Задача 11.38. Найдите наименьшее нечётное натуральное число n такое, что $(n+1)$ делится на 3, $(n+4)$ делится на 5, а $(n+7)$ делится на 11.

Задача 11.39. 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 11.40. Пусть p — простое число, $k \in \mathbb{N}$. Докажите, что $C_{p-1}^{k} \equiv (-1)^{k-1} \pmod p$.

Задача 11.41. Укажите такое k-значное число $N \in \mathbb{N}$, для которого десятичные записи чисел $N, 2N, \ldots, kN$ отличаются только порядком цифр, если

а) $k = 6$;
б) $k = 16$.

Задача 11.42. Докажите, что число 0,1234567891011121314151617... иррационально.

Задача 11.43. Докажите, что любое положительное число можно представить в виде суммы девяти чисел, десятичные записи которых содержат только цифры 0 и 7.

Задача 11.44. 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 11.45. Может ли геометрическая фигура иметь ровно два центра симметрии?

Задача 11.46. Пусть l и m — две прямые на плоскости, $\vec{v}$ — некоторый вектор. К какому из типов движений 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 11.47. Докажите, что любое движение, меняющее направления лучей на противоположные, является центральной симметрией.

Задача 11.48. Докажите, что композиция трёх осевых симметрий является осевой симметрией тогда и только тогда, когда оси пересекаются в одной точке или параллельны, а в остальных случаях являются скользящей симметрией.

Задача 11.49. 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 выполняются равенства?

Задача 11.50. 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 11.51. Дан квадрат $ABCD$ и комплексные координаты a и b его вершин A и B. Найдите комплексные координаты вершин C и D.

Задача 11.52. Пусть f — многочлен с действительными коэффициентами. Докажите, что если $f(i) = 0$, то f делится на $x^2 + 1$.

Задача 11.53. Найдите число упорядоченных пар (x, y), $x, y \in \mathbb{R}$, таких, что $(x+iy)^{2020} = x-iy$.

Задача 11.54. Можно ли ввести на комплексных числах отношение порядка $>$, согласованное со сложением и умножением?

Указание: Согласованность отношения $>$ с операциями 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 $ab > 0$.

Дополнительные задачи

Задача 11.55. 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 11.56. 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 11.57. Пусть $n > 1$. Может ли быть целым число $1 + \dfrac{1}{2} + \dfrac{1}{3} + \ldots + \dfrac{1}{n}$?

Задача 11.58. Выведите формулу для суммы квадратов делителей числа $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$.

Задача 11.59. Найдите все натуральные числа $n \in \mathbb{N}$, для каждого из которых существует число $k \in \{1, 2, \ldots, n-1\}$ такое, что выполняется равенство $2C_n^k = C_n^{k-1} + C_n^{k+1}$.

Задача 11.60. 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 11.61. Для каждого натурального n определите, сколько существует троек натуральных чисел, сумма которых равна $6n$.

Задача 11.62. Докажите, что если p — простое число, не равное двум, то числитель дроби

$$1 + \frac{1}{2} + \frac{1}{3} \ldots + \frac{1}{p-1}$$

делится на p.

Задача 11.63. Докажите, что последовательность остатков чисел $1^1, 2^2, 3^3, \ldots$ по модулю простого числа p периодична. Оцените её период.

Задача 11.64. Является ли счётным любое бесконечное множество непересекающихся

а) интервалов на прямой;

б) кругов на плоскости?

Задача 11.65. Может ли длина периода дроби $1/n$ быть равной $(n - 1)$, если n является составным числом?

Задача 11.66. 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.

Задача 11.67. Пусть α и β — случайно выбранные решения уравнения $z^{2021} - 1 = 0$. Найдите вероятность того, что $|\alpha + \beta| \geqslant 2$.

Ответы и указания к упражнениям и задачам

Вступительный тест

Задача 0.1. *Ответ:* Вариант 3).
Задача 0.2. *Ответ:* Вариант 1).
Задача 0.3. *Ответ:* 64.
Задача 0.4. *Ответ:* Вариант 1).
Задача 0.5. *Ответ:* Вариант 2).
Задача 0.6. *Ответ:* Вариант 3).
Задача 0.7. *Ответ:* 9.
Задача 0.8. *Ответ:* 2.
Задача 0.9. *Ответ:* Вариант 2).
Задача 0.10. *Ответ:* Вариант 2).
Задача 0.11. *Ответ:* Вариант 1).
Задача 0.12. *Ответ:* Вариант 2).
Задача 0.13. *Ответ:* Вариант 3).
Задача 0.14. *Ответ:* 4.
Задача 0.15. *Ответ:* Вариант 4).
Задача 0.16. *Ответ:* Вариант 5).
Задача 0.17. *Ответ:* Вариант 5).
Задача 0.18. *Ответ:* Правда. Через 100 секунд.
Задача 0.19. *Ответ:* 5051.
Задача 0.20. *Ответ:* 17740.
Задача 0.21. *Ответ:* 8.
Задача 0.22. *Ответ:* Бесконечно много.
Задача 0.23. *Ответ:* 1.
Задача 0.24. *Ответ:* 64.
Задача 0.25. *Ответ:* 27.
Задача 0.26. *Ответ:* 38.
Задача 0.27. *Ответ:* 9.
Задача 0.28. *Ответ:* 66.
Задача 0.29. *Ответ:* 60.
Задача 0.30. *Ответ:* $90000 - 8 \cdot 9 \cdot 9 \cdot 9 \cdot 9 = 37512$.
Задача 0.31. *Ответ:* $C_{2020}^2 = 2039190$.
Задача 0.32. *Ответ:* 6.
Задача 0.33. *Ответ:* 1.
Задача 0.34. *Ответ:* $\{(0, 0, 0)\}$.
Задача 0.35. *Ответ:* $\{-6 + 15t \mid t \in \mathbb{Z}\}$; минимальное трёхзначное решение: 114.
Задача 0.36. *Ответ:* 1.
Задача 0.37. *Ответ:* 1.
Задача 0.38. *Ответ:* 96.
Задача 0.39. *Ответ:* 209 (а наименьшее по модулю — (-1)).
Задача 0.40. *Ответ:* 1073.

Задача 0.41. *Ответ:* 8.
Задача 0.42. *Ответ:* 12.
Задача 0.43. *Ответ:* 35.
Задача 0.44. *Ответ:* $5/25 = 1/5$.
Задача 0.45. *Ответ:* S.
Задача 0.46. *Ответ:* $-1/512$.
Задача 0.47. *Ответ:* $2021/2$.
Задача 0.48. *Ответ:* $\overline{\omega} \mapsto C,\ -\omega \mapsto B,\ i\omega \mapsto A$.
Задача 0.49. *Ответ:* Вариант 3).
Задача 0.50. *Ответ:* -1.
Задача 0.51. *Ответ:* Варианты 1) и 6).
Задача 0.52. *Ответ:* 13.
Задача 0.53. *Ответ:* Существует. Минимальное число равно 2.
Задача 0.54. *Ответ:* Не существует.

1. Математическая логика

Упражнение 1.1. *Ответ:* A и C ложны, B истинно.
Упражнение 1.2. *Ответ:* $X \wedge Y$: «n равно 3»; $X \vee Y$: «n — натуральное число».
Упражнение 1.3. *Ответ:* Всего 48 формул.
Решение: Рассмотрим несколько случаев.

- Пусть 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.

- Пусть 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 перестановкой переменных. 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 шестью способов: $\mathrm{var} \wedge \mathrm{var} \wedge \mathrm{var}$, $\mathrm{var} \vee \mathrm{var} \vee \mathrm{var}$, $\mathrm{var} \wedge \mathrm{var} \vee \mathrm{var}$, $\mathrm{var} \vee \mathrm{var} \wedge \mathrm{var}$, $\mathrm{var} \wedge (\mathrm{var} \vee \mathrm{var})$, $(\mathrm{var} \vee \mathrm{var}) \wedge \mathrm{var}$. 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, получается 18 формул. Другие 18 формул получим, подставляя переменные Y, Y, X.

Суммируя, имеем всего $12 + 18 + 18 = 48$ формул.
Упражнение 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

Упражнение 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

Упражнение 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 1.13, 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 1.15.

Упражнение 1.7. *Ответ:* $\neg X \vee Y$.

Упражнение 1.8. *Решение:* Пусть (a_n) — арифметическая прогрессия со знаменателем d. Предположим, $q = (a_1, d)$ — наибольший общий делитель чисел a_1 и d. Тогда любой член арифметической 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 $a_1 = p$.

Упражнение 1.9. *Решение:* Предположим, что $a \neq b$. 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, поскольку a и b — строго положительные вещественные числа. Противоречие. Следовательно, $a = b$, что и требовалось доказать.

Упражнение 1.10. *Решение:* Верно первое. И правда, для каждого $n \in \mathbb{N}$ верно неравенство $n + 1 > n$. Второе утверждение с помощью этого неравенства можно опровергнуть. В самом деле, если бы существовало указанное во втором утверждении натуральное число N, большее всех натуральных чисел, то было бы выполнено очевидно неверное неравенство $N + 1 < N$.

2. Множества и отображения

Упражнение 2.1. *Ответ:* а) 1. б) 3. в) 1. г) 6.

Упражнение 2.2. *Ответ:* $5, 10, 15, 20, 25, 30, 35, 40, 45$.

Упражнение 2.3. *Ответ:* $\varnothing$, $\{\varnothing\}$, $\{\{0\}\}$, $\{1\}$, $\{\varnothing, \{0\}\}$, $\{\varnothing, 1\}$, $\{\{0\}, 1\}$, $\{\varnothing, \{0\}, 1\}$.

Упражнение 2.4. *Ответ:* $2^4 = 16$.
Упражнение 2.5. *Ответ:* Объединением является множество $\mathbb{N}$, а пересечением – $\varnothing$.
Упражнение 2.6. *Решение:* Используем диаграммы Венна (рис. 38).

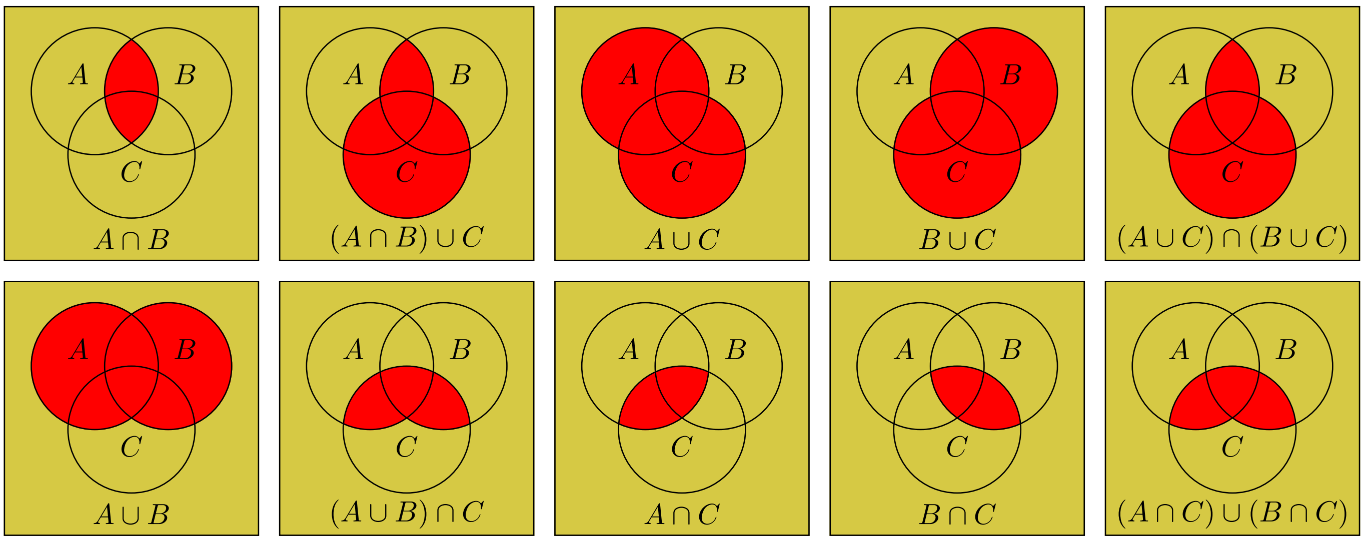

Рис. 38.

Упражнение 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 $w \in C(x)$.
Упражнение 2.8. *Ответ:* Направленные отрезки $\overrightarrow{AB}$ и $\overrightarrow{CD}$ называются эквивалентными, если они коллинеарны, имеют одинаковые направления и $|AB| = |CD|$.
Упражнение 2.9. *Решение:* а) Воспользуемся результатом упражнения 4.2.
Рефлексивность: $(k - k) = 0$ делится на m.
Симметричность: если $(k - l)$ делится на m, то и $(l - k)$ делится на m.
Транзитивность: если $(k - l)$ и $(l - n)$ делятся на m, то и $(k - n)$ делится на m.
Указание: б) Проверьте рефлексивность, симметричность и транзитивность как в пункте а).
Упражнение 2.10. *Решение:* Первый чертёж — не отображение, поскольку одна из стрелок ведёт из Y в X. Второй чертёж — не отображение, поскольку одному из элементов в X не соответствует ни одного элемента из Y. Третий чертёж — не отображение, поскольку одному из элементов в X соотвествует два элемента из Y. Четвёртый чертёж — отображение.
Упражнение 2.11. *Ответ:*
а) $f(\{1\}) = f(\{1, 2\}) = \{a\}$,
$f(\{1, 2, 3\}) = f(\{1, 3, 5\}) = \{a, b\}$,
$f(\{2, 4, 6\}) = \{a, c\}$;
б) $f^{-1}(\{a\}) = \{1, 2, 4\}$,
$f^{-1}(\{b, c\}) = \{3, 5, 6\}$,
$f^{-1}(\{a, b, c\}) = \{1, 2, 3, 4, 5, 6\} = Y$,
$f^{-1}(\{b, d\}) = \{3, 5\}$,
$f^{-1}(\{a, c, d\}) = \{1, 2, 4, 6\}$.
Упражнение 2.12. *Решение:* а) Заметим, что $f^{-1}(Y) \subset X$ по определению прообраза. С другой стороны, каждый элемент $x \in X$ при отображении f переходит в некоторый элемент $y \in Y$,

а значит, $x \in f^{-1}(Y)$. Следовательно, $X \subset f^{-1}(Y)$, и согласно критерию равенства множеств $X = f^{-1}(Y)$.

б) Предположим, что $f(\varnothing) \neq \varnothing$. Тогда найдётся лежащий там элемент $y \in f(\varnothing)$, а значит, существует $x \in \varnothing$ такой, что $f(x) = y$. Однако в $\varnothing$ нет никаких элементов — противоречие. Аналогично доказывается, что $f^{-1}(\varnothing) = \varnothing$.

Упражнение 2.13. *Ответ:* $(x, y) \mapsto (y, x)$.

Упражнение 2.14. *Ответ:* Всего 8 отображений (рис. 39). Среди них 6 сюрьекций (все, кроме первого и последнего отображения), инъекций и биекций нет.

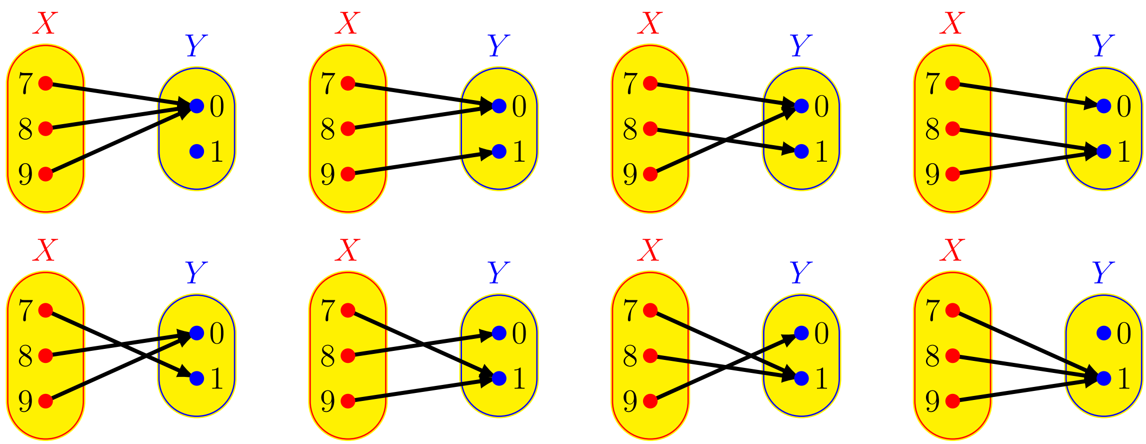

Рис. 39.

Упражнение 2.15. *Решение:* Если $f : X \to Y$ сюрьективно, то у каждого элемента $y \in Y$ найдётся прообраз: $x \in X$ такой, что $y = f(x)$. Положив $g(y) = x$, по построению получим $f(g(y)) = y$ для всех $y \in Y$, то есть $f \circ g = \mathrm{id}_Y$ (рис. 40).

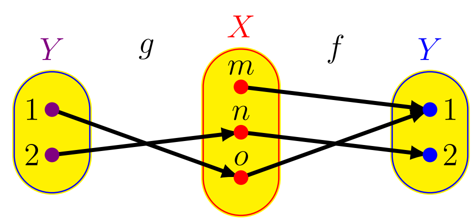

Рис. 40.

Упражнение 2.16. *Решение:* Если f не инъективно, то найдутся элементы $x \neq x'$ 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 сюрьективно, 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 сюрьективность 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.

Упражнение 2.17. *Ответ:* Отображение f не инъективно (в множестве A больше элементов, чем в его образе), поэтому ни обратного, ни левого обратного нет. Однако f сюрьективно, поэтому существует правое обратное, например, $g(x) = x + 5$.

Упражнение 2.18. *Ответ:* а) Биекция для целых чисел:

$$\begin{array}{cccccccccccccccccccc}
\mathbb{Z}: & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & 5 & -5 & 6 & -6 & 7 & -7 & 8 & -8 & 9 & -9 \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\mathbb{N}: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19
\end{array}$$

б) Биекцию $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ можно задать формулой $f(a, b) = 2^{a-1}(2b - 1)$.

Упражнение 2.19. *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. Предположим 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 $A \times B = \bigcup\limits_{k=1}^{\infty} A \times \{b_k\}$.

Упражнение 2.20. *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).

Упражнение 2.21. *Ответ:* $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$.

Задача 2.1. *Ответ:*

а) $\{57, 91, 179, 239, 2014\}$;
б) $\{91, 239\}$;
в) $\{2, 91, 239, 2014, 2017\}$;
г) $\{2014\}$;
д) $\{57, 91, 239, 2014\}$;
е) $\{2, 91, 239, 2014\}$;
ж) $\{2, 57, 91, 239, 2014\}$;
з) $\emptyset$;
и) $\{91, 2014\}$;
к) $\{57, 91, 239, 2014\}$;
л) $\{57, 91, 179, 239\}$;
м) $\{179, 2017\}$;
н) $\{57, 179, 239\}$;
о) $\{2, 2014, 2017\}$;
п) $\{91, 179, 239, 2014\}$.

Задача 2.2. *Ответ:*

$\{0, 1\} \times \{9\} = \{(0, 13), (1, 13)\}$;
$\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$;
$\varnothing \times \varnothing = \varnothing$;
$\{5, 7\} \times \{1, 3, 17\} = \{(5, 1), (5, 3), (5, 13), (7, 1), (7, 3), (7, 13)\}$;
$\{16, 41\} \times \varnothing = \varnothing$.

Задача 2.3. *Ответ:* $A \cap B$ — множество чисел, делящихся на шесть.

Задача 2.4. *Ответ:*

а) $f(\{1, 3\}) = \{b, d\}$,
$f(\{2, 3, 4\}) = \{b, c\}$,
$f^{-1}(a) = \varnothing$,
$f^{-1}(\{a, b\}) = \{3, 4\}$,

$f^{-1}(\{b,d\}) = \{1,3,4\};$

б) $f(\{1,3\}) = \{b,d\},$
$f(\{2,3,4\}) = \{a,b,c\},$
$f^{-1}(a) = \{2\},$
$f^{-1}(\{a,b\}) = \{2,3\},$
$f^{-1}(\{b,d\}) = \{1,3\};$

в) $f(\{1,3\}) = \{a,c\},$
$f(\{2,3,4\}) = \{a,c\},$
$f^{-1}(a) = \{1,4\},$
$f^{-1}(\{a,b\}) = \{1,4\},$
$f^{-1}(\{b,d\}) = \varnothing.$

Задача 2.5. *Ответ:* $f(\mathbb{R}) = [0,+\infty)$; $f^{-1}(x) = \begin{cases} \{-\sqrt{x}, \sqrt{x}\}, & \text{если } x > 0, \\ \{0\}, & \text{если } x = 0, \\ \varnothing, & \text{если } x > 0. \end{cases}$

Задача 2.6. *Ответ:* Все возможные 6 биекций изображены на рис. 41.

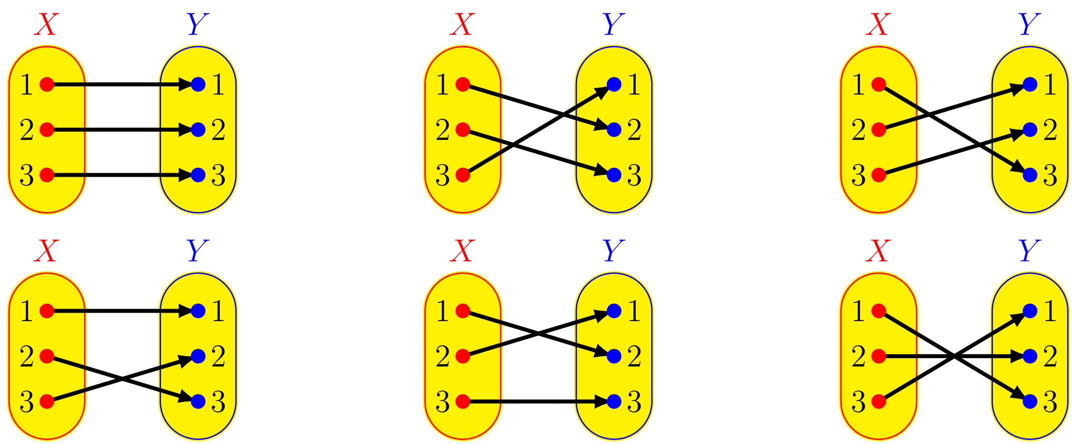

Рис. 41.

Задача 2.7. *Ответ:* В пунктах б) и е) отображения не определены. Для остальных пунктов они изображены на рис. 42.

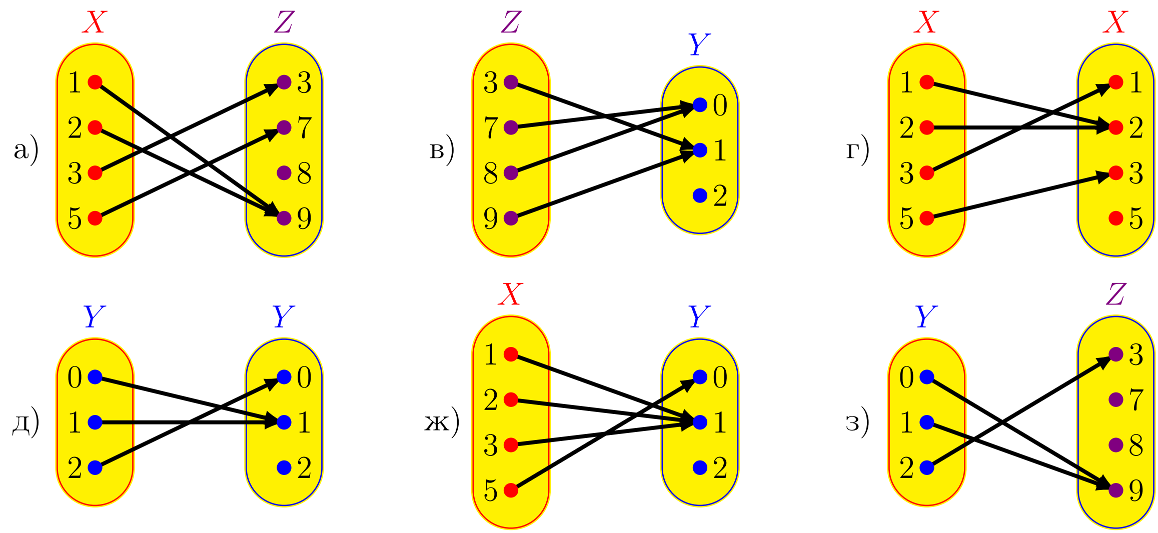

Рис. 42.

Задача 2.8. *Ответ:* $(f \circ g)(x) = -x - 1$, $(g \circ f)(x) = -x + 1$.

3. Математическая индукция

Упражнение 3.1. *Ответ:* а) Нет. б) Да. в) Нет.
Упражнение 3.2. *Указание:* Решение изложено в разделе 3.3.
Упражнение 3.3. *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 мы 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, воспользовавшись математической индукцией.
База индукции: если в системе только один город, то дорог там нет (откуда следует, что дорог на одну меньше, чем городов).
Шаг индукции: 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 одну меньше, чем городов. А значит, и для исходной системы это было верно.
Упражнение 3.4. *Решение:*
База индукции: при $n = 2$ равенство очевидно.
Шаг индукции: 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.

Упражнение 3.5. *Решение:* а) Проведём доказательство по индукции.
База индукции: при $n=3$ в триангуляции $(n-1)=1$ треугольник.
Шаг индукции: пусть доказано, что при каждом $n<k$ в любую триангуляцию n-угольника входит ровно $(n-2)$ треугольника. 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 его углов суть сумма углов входящих в него треугольников, а она равна $(n-2)\pi$.

Задача 3.1. *Решение:* а) Проведём доказательство по индукции.
База индукции: при $n=1$ равенство справедливо, поскольку

$$1=\frac{1\cdot(1+1)}{2}.$$

Шаг индукции: пусть при $n=k$ выполнено равенство

$$1+2+3+4+\ldots+k=\frac{k(k+1)}{2}.$$

Тогда при $n=k+1$ имеем

$$1+2+3+4+\ldots+k+(k+1)=\frac{k(k+1)}{2}+(k+1).$$

Приводя правую часть к общему знаменателю, получаем

$$\frac{k(k+1)}{2}+(k+1)=\frac{k(k+1)+(k+1)}{2}=\frac{(k+1)(k+2)}{2},$$

что и требовалось.

Указание: Остальные пункты решаются аналогично. Ключевые соображения таковы:

б) $\dfrac{n(n+1)(2n+1)}{6}+(n+1)^2=\dfrac{(n+1)\big((2n^2+n)+6(n+1)\big)}{6}=\dfrac{(n+1)(n+2)(2n+3)}{6}.$

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

г) $\dfrac{n(n+1)(n+2)}{3}+(n+1)(n+2)=\dfrac{(n+1)(n+2)(n+3)}{3}.$

д) $\big((n+1)!-1\big)+(n+1)(n+1)!=(n+1)!\big(1+(n+1)\big)-1=(n+2)!-1.$

е) $\dfrac{n(n+3)}{4(n+1)(n+2)}+\dfrac{1}{(n+1)(n+2)(n+3)}=\dfrac{n(n+3)^2+4}{4(n+1)(n+2)(n+3)}=\dfrac{(n+1)^2(n+4)}{4(n+1)(n+2)(n+3)}.$

ж) $\dfrac{3}{4}-\dfrac{1}{2n+2}-\dfrac{1}{2n+4}+\dfrac{1}{(n+1)(n+3)}=\dfrac{3}{4}-\dfrac{1}{2n+4}-\dfrac{1}{2n+6}$, поскольку

$$\frac{1}{(n+1)(n+3)}=\frac{1}{2}\left(\frac{1}{n+1}-\frac{1}{n+3}\right)=\frac{1}{2n+2}-\frac{1}{2n+6}.$$

Задача 3.2. *Ответ:* Не работает переход $A_1 \to A_2$: если отбросить второе число, то останется только первое число, которое, вообще говоря, не равно второму.
Задача 3.3. *Ответ:* Не работает переход $A_2 \to A_3$: при $k=2$ множество $\{X_2,\ldots,X_k\}$ состоит из одной точки, а потому через неё проходит бесконечно много различных прямых (а вовсе не одна единственная).

4. Делимость целых чисел

Упражнение 4.1. *Ответ:* Отношение порядка рефлексивно и транзитивно, но не симметрично.
Упражнение 4.2. *Решение:* По условию $a=q_1n, b=q_2n$, поэтому

$$a+b=q_1n+q_2n=(q_1-q_2)n \qquad \text{и} \qquad a-b=q_1n+q_2n=(q_1-q_2)n.$$

Упражнение 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.
Упражнение 4.4. *Решение:* По определению $a=q_1b$ и $b=q_2c$, так что $a=q_1b=q_1q_2c$.
Упражнение 4.5. *Указание:* Следует использовать 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 упражнениям 4.2 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.

Упражнение 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 сможет её обобщить. Представим искомое число в виде

$$\overline{a_2a_1a_0}=a_2\cdot 100+a_1\cdot 10+a_0=a_2\cdot 99+a_1\cdot 9+(a_2+a_1+a_0).$$

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.

Упражнение 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 $|b|$.

Упражнение 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 и 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.

Упражнение 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 нижеследующую 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

Упражнение 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 $a_1 a_2 = (q_1 q_2 b + q_1 r_2 + q_2 r_1)b + r_1 r_2$. 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 $3^4 = 81 \equiv 1 (\mathrm{mod}\ 5)$.

Упражнение 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.

Упражнение 4.12. *Ответ:* $(372, 69) = 3$.

Решение: Проведём выкладки:

$$\begin{gathered} 372 = 5 \cdot 69 + 27, \\ 69 = 2 \cdot 27 + 15, \\ 27 = 1 \cdot 15 + 12, \\ 15 = 1 \cdot 12 + 3, \\ 12 = 4 \cdot 3. \end{gathered}$$

Упражнение 4.13. *Решение:* а) $0 = 0 \cdot a + 0 \cdot b, \quad a = 1 \cdot a + 0 \cdot b, \quad b = 0 \cdot a + 1 \cdot b$.

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 $d = 1 \cdot d$.

Упражнение 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 $k \pm l = (x+y)d \in \mathbb{Z}(d)$.

Упражнение 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 $nk = (nx)d \in \mathbb{Z}(d)$.

Упражнение 4.16. *Решение:* Модуль целого числа — натуральное число или ноль. Согласно принципу минимального элемента (раздел 3.1) в любом подмножестве натуральных чисел есть минимальный элемент.

Упражнение 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.

Упражнение 4.18. *Решение:* Проведём доказательство индукцией по числу n.

База индукции: при $n = 2$ утверждение очевидно, $n \vdots 2$.

Шаг индукции: допустим, что мы умеем доказывать искомое утверждение для всех чисел, меньших n. Само n может быть либо простым — тогда доказывать нечего, — либо 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.

Упражнение 4.19. *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 искомом виде. Если же n составное, то $n = n_1 \cdot n_2$, где натуральные числа n_1 и n_2 таковы, что $1 < n_1 \leqslant n_2 < n$. К каждому из них применимо предположение индукции, то есть они представимы в виде произведения простых чисел. Значит, и n — тоже.

Упражнение 4.20. *Решение:* Проведём индукцию по m.

База индукции: при $m = 2$ утверждение составляет формулировку леммы 4.7.

Шаг индукции: пусть утверждение верно для $m = k$. Заметим, что если $n_1(n_2 \ldots n_{k+1}) \vdots p$, то либо $p \mid n_1$, либо $p \mid (n_2 \ldots n_{k+1})$. Последнее же по предположению индукции означает, что $p \mid n_l$ для некоторого l.

Упражнение 4.21. *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.

Упражнение 4.22. *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 $p^2 \mid x^2$.

Задача 4.1. *Ответ:*

а) 2;
б) 5;
в) 17;
г) 163;
д) 4;
е) 7;
ж) 2;
з) 0.

Задача 4.2. *Ответ:*

а) 6;
б) 6;
в) 1;

г) 3;
д) 3;
е) 7.

Задача 4.3. *Ответ:*
а) 7;
б) 1;
в) 17;
г) 3;
д) 1;
е) 691.

Задача 4.4. *Ответ:*
а) $\{(1+2m, 2-m) \mid m \in \mathbb{Z}\}$;
б) $\varnothing$;
в) $\{(372+29m, -217-17m) \mid m \in \mathbb{Z}\} = \{(-5+29m, 4-17m) \mid m \in \mathbb{Z}\}$;
г) $\{(-144+23m, 108-17m) \mid m \in \mathbb{Z}\} = \{(-6+23m, 6-17m) \mid m \in \mathbb{Z}\}$;
д) $\{(-60+133m, -14+31m) \mid m \in \mathbb{Z}\} = \{(73+133m, 17+31m) \mid m \in \mathbb{Z}\}$;
е) $\{(1212+29m, -707-17m) \mid m \in \mathbb{Z}\} = \{(-6+29m, 7-17m) \mid m \in \mathbb{Z}\}$;
ж) $\varnothing$;
з) $\{(21+31m, 90+133m) \mid m \in \mathbb{Z}\} = \{(-10+31m, -43+133m) \mid m \in \mathbb{Z}\}$.

Задача 4.5. *Ответ:*
а) $2187 = 3^7$;
б) $1002001 = 1001^2 = 7^2 \cdot 11^2 \cdot 13^2$;
в) $17! = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$;
г) $C_{20}^{10} = 2^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$;
д) $2021 = 43 \cdot 47$;
е) $18941 = 13 \cdot 31 \cdot 47$.

5. Комбинаторика

Упражнение 5.1. *Ответ:* $20 \cdot 15 = 300$.

Упражнение 5.2. *Ответ:*
а) $32 \cdot 32 = 1024$.
б) $32 \cdot 31 = 992$.
в) $(32 \cdot 31)/2 = 496$.
г) $(32 \cdot 31 \cdot 30 \cdot 29)/2 = 431\,520$.

Упражнение 5.3. *Ответ:* $33000 - 11000 - 6600 + 2200 = 17600$.

Упражнение 5.4. *Решение:* Для упрощения введём 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, во-первых, $x \in A_{n+1}$, а во-вторых, существует такое $k \in \{1, \ldots, n\}$, что $x \in A_k$. Следовательно, $x \in (A_k \cap A_{n+1})$, а значит, $x \in B$, откуда вытекает, что $A \subset B$. Для проверки обратного включения достаточно заметить, что все переходы в приведённом выше рассуждении обратимы.

Упражнение 5.5. *Ответ:* $20 \cdot 19 \cdot 18 \cdot 17 = 116280$.

Упражнение 5.6. *Ответ:* $(25 \cdot 24 \cdot 23 \cdot 22 \cdot 21)/5! = 53130$.

Упражнение 5.7. *Ответ:*

а) $C_n^k = \dfrac{n!}{k!(n-k)!} = \dfrac{n!}{(n-(n-k))!(n-k)!} = C_n^{n-k}$.

б) $C_n^k + C_n^{k+1} = \dfrac{n!}{k!(n-k)!} + \dfrac{n!}{(k+1)!(n-k-1)!} = \dfrac{n!}{k!(n-k-1)!}\left(\dfrac{1}{n-k}+\dfrac{1}{k+1}\right) =$

$= \dfrac{n!}{k!(n-k-1)!}\dfrac{n+1}{(n-k)(k+1)} = \dfrac{(n+1)!}{(k+1)!(n-k)!} = C_{n+1}^{k+1}$.

в) $C_n^m \cdot C_m^k = \dfrac{n!}{m!(n-m)!}\cdot\dfrac{m!}{k!(m-k)!} = \dfrac{n!}{(n-k)!k!}\cdot\dfrac{(n-k)!}{(m-k)!(n-m)!} = C_n^k \cdot C_{n-k}^{m-k}$.

Упражнение 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:

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

Упражнение 5.9. *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:

$$C_{k+1}^0 - C_{k+1}^1 + C_{k+1}^2 - \ldots = C_k^0 - (C_k^0 + C_k^1) + (C_k^1 + C_k^2) - \ldots = 0.$$

Упражнение 5.10. *Решение:* Это в точности результат утверждения 5.8.
Упражнение 5.11. *Решение:* Понятно, что любое число (кроме крайних единиц) в i-ой строке треугольника Паскаля больше либо равно i. Так произвольное число $n \neq 1$ может встречаться лишь в строках с номерами не больше n, но число элементов в таких строках конечно. Следовательно, число n встречается в треугольнике Паскаля конечное число раз.
Упражнение 5.12. *Решение:* а) Проведём индукцию по параметру m.
База индукции: для $m=1$ и $m=2$ проверка выполняется непосредственно: $C_k^0 = 1 = C_{k+1}^0$ 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 равенство $C_k^k + C_{k+1}^k + \ldots + C_{k+m}^k + C_{k+(m+1)}^k = C_{k+m+1}^{k+1} + C_{k+(m+1)}^k = C_{k+m+2}^{k+1}$. Для проверки последнего равенства используется $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$, применённое к $n = k+m$.
Ответ: б) $C_k^0 + C_{k+1}^1 + C_{k+2}^2 + \ldots + C_{k+m}^m = C_{k+m+1}^m$.
Упражнение 5.13. *Ответ:* $C_{10+4-1}^{4-1} = C_{13}^3 = 286$.
Упражнение 5.14. *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.
Упражнение 5.15. *Ответ:* $n!$.

Упражнение 5.16. *Ответ:* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$.

Упражнение 5.17. *Ответ:* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$.

Упражнение 5.18. *Решение:* Пусть $\sigma = T_n \circ \ldots \circ T_1 = T'_k \circ \ldots \circ T'_1$, где σ — некая перестановка, T_i и T'_j — транспозиции. Умножим равенство слева на $T_1 \circ \ldots \circ T_n$:

$$T_1 \circ \ldots \circ T_n \circ T_n \circ \ldots \circ T_1 = T_1 \circ \ldots \circ T_n \circ T'_k \circ \ldots \circ T'_1.$$

Поскольку $T_i \circ T_i = e$, в левой части мы получаем тождественную перестановку (все члены левого части равенства сокращаются). А правая часть равна произведению $n+k$ транспозиций. Согласно утверждению 5.14 число $n+k$ чётно, поэтому n и k имеют одинаковую чётность.

Упражнение 5.19. *Решение:* Для каждого элемента $j \in S$ рассмотрим последовательность

$$j,\ \sigma(j),\ \sigma^2(j),\ \sigma^3(j),\ \ldots$$

В ней найдутся повторяющиеся элементы, то есть $\sigma^m(j) = \sigma^l(j)$ для некоторых $l < m$, откуда $\sigma^{m-l}(j) = j$. Таким образом, существуют такие числа $k \in \mathbb{N}$, что $\sigma^k(j) = j$, и если мы выберем среди них минимальное, то элементы в ряду

$$j,\ \sigma(j),\ \sigma^2(j),\ \sigma^3(j),\ \ldots,\ \sigma^{k-1}(j)$$

не будут повторяться. Поэтому эти элементы образуют цикл, который мы обозначим $C(j)$.

Остаётся показать, что любые два цикла либо не пересекаются, либо совпадают. Это следует из леммы 2.1. Действительно, рассмотрим на множестве S отношение: $i \sim j$, если найдётся m такое, что $\sigma^m(j) = i$. Это отношение обладает всеми свойствами отношения эквивалентности:
Рефлексивность: $\sigma^0(j) = j$.
Симметричность: если $\sigma^k(j) = j$ и $\sigma^m(j) = i$, то $\sigma^{k-m}(i) = j$.
Транзитивность: если $\sigma^m(j) = i$ и $\sigma^s(i) = l$, то $\sigma^{sm}(j) = l$.
Таким образом, $\sim$ — это отношение эквивалентности, и по лемме 2.1 всё множество S распадается на циклы.

Задача 5.1. *Ответ:* 12; 60; 840.
Задача 5.2. *Ответ:* 6; 5; 35.
Задача 5.3. *Ответ:* 17!.
Задача 5.4. *Ответ:* 28!.
Задача 5.5. *Ответ:*
а) $C_{28}^4 = 20475$;
б) $C_{27}^3 = 2925$.
Задача 5.6. *Ответ:* $2 \cdot C_{10}^7 + 1 \cdot C_{10}^6 = 330$.
Задача 5.7. *Ответ:* 10.
Задача 5.8. *Ответ:* 20.
Задача 5.9. *Ответ:*
а) $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$;
б) $(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$;
в) $(x+y)^6 = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6$.
Задача 5.10. *Ответ:*

а) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$;
б) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$;
в) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Задача 5.11. *Ответ:*
а) $(1,3)$;
б) $(1,4,3)(2,5)$;
в) $(4,7,9,8)(1,3,6)(2,5)$.

Задача 5.12. *Ответ:* Если $n \geqslant k$, то $C_n^k \cdot (k-1)! = \dfrac{n!}{k \cdot (n-k)!}$. Иначе 0.

6. Многочлены

Упражнение 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 $f(x) \cdot g(x) = f_n g_m x^{n+m} + (f_n g_{m-1} + f_{n-1} g_m)x^{n+m-1} + \ldots + (f_1 g_0 + f_0 g_1)x + f_0 g_0$.

Упражнение 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).

Упражнение 6.3. *Решение:* Прямо следует из упражнения 6.1.

Упражнение 6.4. *Ответ:*
а) $x^2 - 4x + 3 = (x-1)(x-3) + 0$;
б) $x^2 - 4 = (x+5)(x-5) + 21$;
в) $x^4 - 2x + 5 = (x^2-1)(x^2+1) + (-2x+6)$.

Упражнение 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.

Упражнение 6.6. *Решение:*
а) $0 = 0 \cdot f(x) + 0 \cdot g(x), \qquad f(x) = 1 \cdot f(x) + 0 \cdot g(x), \qquad g(x) = 0 \cdot f(x) + 1 \cdot g(x)$.
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 $s(x)h(x) = \big(s(x)a(x)\big)f(x) + \big(s(x)b(x)\big)g(x)$.

Упражнение 6.7. *Решение:* $(f(x), g(x)) = (g(x), r_0(x)) = \ldots = (r_{n-1}(x), r_n(x)) = r_n(x)$.

Упражнение 6.8. *Решение:* Из условия $(f(x), h(x)) = 1$ вытекает, что существуют такие многочлены $a(x), b(x) \in \mathbb{K}[x]$, 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.
Упражнение 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 $f_1(x) \dots f_{m+1}(x) \vdots h(x)$, то согласно утверждению 6.6 либо $f_1(x) \dots f_m(x) \vdots h(x)$, 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 $k \in \{1, \dots, m\}$, что и требовалось.
Упражнение 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 $c = \mu\lambda$.
Упражнение 6.11. *Решение:* а) Предположим противное: пусть $\lambda_1, \dots \lambda_{n+1}$ — 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).
Упражнение 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 $\mathbb{C}[x]$.

7. Сравнения

Упражнение 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, эти два равенства, имеем $ac = bd + n(bl + dk + kln)$, откуда $(ac - bd) \vdots n$.

г) Следует индукцией из пункта в).
Упражнение 7.2. *Указание:* Воспользуетесь признаками делимости на эти числа.
Упражнение 7.3. *Решение:* Перебор вариантов: $2 \cdot 0 \equiv 2 \cdot 2 \equiv 0 \pmod 4$; $2 \cdot 1 \equiv 2 \cdot 3 \equiv 2 \pmod 4$.
Упражнение 7.4. *Ответ:*

По модулю 3: 0, 1.

По модулю 8: 0, 1, 4.

По модулю 24: 0, 1, 4, 9, 12, 16.

Упражнение 7.5. *Решение:* Так как $3^4 = 81 \equiv 1 \pmod 5$, то $3^{2020} = (3^4)^{505} \equiv 1 \pmod 5$.

Упражнение 7.6. *Ответ:*

По модулю 7: 1, 2, 4.

По модулю 13: 1, 3, 4, 9, 10, 12.

Упражнение 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.

8. Действительные числа

Упражнение 8.1. *Указание:* Достаточно заметить, что функция $f(x) = x^5 + x + 1$ является монотонно возрастающей.

Упражнение 8.2. *Ответ:*

а) В $\mathbb{N}$ выполнены (1a), (1b), (2a), (2b), (2c), (3a).

б) В $\mathbb{Z}$ выполнены все аксиомы, кроме (2d).

в) В $\mathbb{Q}$ выполнены все аксиомы.

г) В $\mathbb{C}$ выполнены все аксиомы.

Упражнение 8.3. *Решение:* Заметим, что $\big(-(-a)\big)$ — это элемент, противоположный элементу $(-a)$, то есть

$$(-a) + \big(-(-a)\big) \overset{(1d)}{=} 0.$$

С другой стороны,

$$0 \overset{(1d)}{=} a + (-a) \overset{(1a)}{=} (-a) + a,$$

то есть a — это тоже элемент, противоположный элементу $(-a)$. Поскольку, как мы видели в примере 8.3, противоположный элемент единственен, отсюда следует, что $\big(-(-a)\big) = a$.

Упражнение 8.4. *Решение:*

а) Если есть две различные единицы 1_1 и 1_2, то

$$1_1 \overset{(2c)}{=} 1_1 \cdot 1_2 \overset{(2a)}{=} 1_2 \cdot 1_1 \overset{(2c)}{=} 1_2.$$

б) Если для элемента $a \in \mathbb{R} \setminus \{0\}$ существует два обратных элемента b и c, то

$$b \overset{(2c)}{=} b \cdot 1 \overset{(2d)}{=} b \cdot (a \cdot c) \overset{(2b)}{=} (b \cdot a) \cdot c \overset{(2a)}{=} (a \cdot b) \cdot c \overset{(2d)}{=} 1 \cdot c \overset{(2a)}{=} c \cdot 1 \overset{(2c)}{=} c.$$

Указание: в) Аналогично упражнению 8.3 достаточно показать, что как $\big(a^{-1}\big)^{-1}$, так и a являются элементами обратными к a^{-1}.

г) Аналогично примеру 8.4 достаточно показать, что как $\big(a \cdot b\big)^{-1}$, так и $a^{-1} \cdot b^{-1}$ являются элементами обратными к $a \cdot b$.

Упражнение 8.5. *Решение:*

а) В первом равенстве используются следующие аксиомы:

$$a \cdot 0 + a \overset{(2c)}{=} a \cdot 0 + a \cdot 1 \overset{(3a)}{=} a \cdot (0+1) \overset{(1a)}{=} a \cdot (1+0) \overset{(1c)}{=} a \cdot 1 \overset{(2c)}{=} a.$$

Во втором равенстве используются первое равенство (I) и следующие аксиомы:

$$a \cdot 0 \overset{(1c)}{=} a \cdot 0 + 0 \overset{(1d)}{=} a \cdot 0 + \big(a + (-a)\big) \overset{(1b)}{=} (a \cdot 0 + a) + (-a) \overset{(I)}{=} a + (-a) \overset{(1d)}{=} 0.$$

б) Заметим, что элемент $(-a)$ является противоположным к элементу a. Однако $a \cdot (-1)$ также является обратным к элементу a, поскольку

$$a + a \cdot (-1) \overset{(2c)}{=} a \cdot 1 + a \cdot (-1) \overset{(3a)}{=} a \cdot \big(1 + (-1)\big) \overset{(1d)}{=} a \cdot 0 = 0$$

(в последнем равенстве мы воспользовались результатом примера 8.5). Так как противоположный элемент единственен, получаем $a \cdot (-1) = -a$.

Упражнение 8.6. *Решение:*

а) Сначала докажем, что $a \cdot c \geqslant a \cdot d$. В самом деле,

$$\Big(c \geqslant d\Big) \overset{(4e)}{\to} \Big(c + (-d) \geqslant d + (-d) \overset{(1c)}{=} 0\Big) \overset{(4f)}{\to} \Big(a \cdot \big(c + (-d)\big) \geqslant 0\Big).$$

В последнем переходе мы воспользовались ещё и аксиомой (4c), которая позволила нам сделать вывод $\big((a \geqslant b) \wedge (b \geqslant 0)\big) \to (a \geqslant 0)$. Раскрыв скобки по дистрибутивности (3a) и перенеся слагаемое со знаком «минус» в правую часть по аксиоме (4e), получим $a \cdot c \geqslant a \cdot d$. Аналогично доказывается неравенство $a \cdot d \geqslant b \cdot d$, которое вместе с первым по транзитивности (4c) даёт нам искомое $a \cdot c \geqslant b \cdot d$. Что касается неравенства $b \cdot d \geqslant 0$, то оно следует непосредственно из аксиомы (4f).

Замечание: Обратите внимание, что попутно мы доказали свойство

$$\forall\, a, b, c \in \mathbb{R}: \quad \big((a \geqslant b) \wedge (c \geqslant 0)\big) \to (a \cdot c \geqslant b \cdot c).$$

Мы им воспользуемся при доказательстве пункта б).

б) Сначала заметим, что $a^{-1} \neq 0$, так как иначе $a \cdot a^{-1} = 0$ согласно примеру 8.5, в то время как $a \cdot a^{-1} = 1$. Затем, применив аксиому (4f) к неравенству $a > 0$, взятому дважды, мы получим $a^2 > 0$. Теперь предположение $a^{-1} < 0$ привело бы нас к противоречию, поскольку по аксиоме (4f), домножая обе части неравенства на a^2, мы бы получили $a < 0$.

Для доказательства второго неравенства достаточно заметить, что

$$\Big((a \geqslant b) \wedge (b > 0)\Big) \overset{(4c)}{\to} \Big((a > 0) \wedge (b > 0)\Big) \to \Big((a^{-1} > 0) \wedge (b^{-1} > 0)\Big) \overset{(4f)}{\to} \Big(a^{-1} \cdot b^{-1} > 0\Big).$$

Поэтому можно домножить неравенство $a \geqslant b$ на $a^{-1} \cdot b^{-1}$, и знак у результата не изменится:

$$b^{-1} \overset{(2c)}{=} b^{-1} \cdot 1 \overset{(2a)}{=} 1 \cdot b^{-1} \overset{(2d)}{=} \big(a \cdot a^{-1}\big) \cdot b^{-1} \overset{(2b)}{=} a \cdot \big(a^{-1} \cdot b^{-1}\big) >$$
$$> b \cdot \big(a^{-1} \cdot b^{-1}\big) \overset{(2a)}{=} b \cdot \big(b^{-1} \cdot a^{-1}\big) \overset{(2b)}{=} \big(b \cdot b^{-1}\big) \cdot a^{-1} \overset{(2d)}{=} 1 \cdot a^{-1} \overset{(2a)}{=} a^{-1} \cdot 1 \overset{(2c)}{=} a^{-1}.$$

Упражнение 8.7. *Решение:* Заметим, что 1 является противоположным к элементу (-1):

$$(-1) + 1 \overset{(1a)}{=} 1 + (-1) \overset{(1d)}{=} 0.$$

Однако $(-1)\cdot(-1)$ также является обратным к элементу (-1), поскольку

$$(-1)+(-1)\cdot(-1) \overset{(2c)}{=} (-1)\cdot 1+(-1)\cdot(-1) \overset{(3a)}{=} (-1)\cdot\big(1+(-1)\big) \overset{(1d)}{=} (-1)\cdot 0 = 0.$$

Так как противоположный элемент единственен, получаем $(-1)\cdot(-1)=1$.
Замечание: Также для доказательства этого равенства можно было воспользоваться результатами упражнений 8.3 и 8.5.
Упражнение 8.8. *Ответ:* Последовательность (x_n) называется
а) невозрастающей, если $x_n \geqslant x_{n+1}$ при всех $n \in \mathbb{N}$;
б) убывающей, если $x_n > x_{n+1}$ при всех $n \in \mathbb{N}$;
в) возрастающей, если $x_n < x_{n+1}$ при всех $n \in \mathbb{N}$;
г) ограниченной снизу, если существует такое $C \in \mathbb{R}$, для которого $x_n \geqslant C$ при всех $n \in \mathbb{N}$.
Упражнение 8.9. *Решение:* Пусть последовательность (x_n) невозрастающая и ограниченная снизу. Тогда множество чисел

$$S = \{b \mid \forall\, n: \quad x_n \geqslant b\}$$

имеет наибольший элемент $B = \max S$, который называют *пределом* последовательности (x_n). Этот предел всегда существует, поскольку по аксиоме 8.3 существует предел A неубывающей ограниченной сверху последовательности (y_n), заданной формулой $y_n = -x_n$, а $B = -A$.
Упражнение 8.10. *Указание:* Для произвольного $a \in \{x > 0 \mid x^2 > 2\}$ возьмите

$$b = \frac{1}{2}\left(a + \frac{2}{a}\right).$$

Упражнение 8.11. *Решение:* Если множество S ограничено, то у него есть верхняя грань s_1 и нижняя грань s_2. Положим $M = \max(|s_1|, |s_2|)$. Тогда для каждого $x \in S$ выполнено

$$M \geqslant s_1 \geqslant x \geqslant s_2 \geqslant -M,$$

а значит, $|x| \leqslant M$. Обратно, если $|x| \leqslant M$ для всех $x \in S$, то M является верхней гранью множества S, а $(-M)$ — его нижней гранью.
Упражнение 8.12. *Решение:* Если C — точная верхняя грань множества S, то она является его верхней гранью, а значит, условие 1) выполнено по определению. Предположим, что условие 2) наружается. Тогда существует некоторое число $\varepsilon > 0$ такое, что для всех $x \in S$ справедливо $x \leqslant C - \varepsilon$. Но это означает, что $(C - \varepsilon)$ тоже является верхней гранью множества S, а значит, C — не точная. Противоречие.

Обратно, пусть выполняются условия 1) и 2). Рассмотрим какое-нибудь число $C' < C$ и положим $\varepsilon = C - C'$. Тогда найдётся $x \in S$ такой, что $x > C - \varepsilon = C'$. Следовательно, C' не является верхней гранью, и среди чисел, меньших C, верхних граней множества S нет. Поэтому C — его точная верхняя грань.
Упражнение 8.13. *Решение:* Элемент $C \in \mathbb{R}$ называется *точной нижней гранью* множества S, если C есть наибольшая из всех его нижних граней.

Если S ограничено снизу, то множество $-S = \{-a \mid a \in S\}$ ограничено сверху, а значит, существует $\sup(-M) = \inf M$.
Упражнение 8.14. *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.

Упражнение 8.15. *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).

Упражнение 8.16. *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 так: (z_n) убывает и ограничена снизу нулём, поэтому она имеет предел. Но предел не может быть больше нуля, потому что элементы последовательности (z_n) бывают сколь угодно малы: для любого $\varepsilon > 0$ согласно аксиоме Архимеда найдётся такое $n \in \mathbb{N}$, что $n > 1/\varepsilon$, и с учётом неравенства $4^n > n$, доказываемого по индукции, получаем

$$\frac{1}{4^n} < \frac{1}{n} < \varepsilon.$$

9. Движения плоскости

Упражнение 9.1. *Решение:* Если $AB \parallel \overrightarrow{v}$, то точки A, B, A' и B' лежат на одной прямой. Считая без ограничения общности, что векторы $\overrightarrow{AB}$ и $\overrightarrow{v}$ сонаправлены, и пользуясь равенством $\overrightarrow{AA'} = \overrightarrow{BB'} = \overrightarrow{v}$, мы получаем

$$\overrightarrow{A'B'} = \overrightarrow{A'A} + \overrightarrow{AB} + \overrightarrow{BB'} = -\overrightarrow{AA'} + \overrightarrow{AB} + \overrightarrow{BB'} = -\overrightarrow{v} + \overrightarrow{AB} + \overrightarrow{v} = \overrightarrow{AB}.$$

Упражнение 9.2. *Ответ:*

а) $\operatorname{Fix}(T_{\overrightarrow{v}}) = \varnothing$ — у параллельного переноса нет неподвижных точек.

б) Это $\{l \mid l \parallel \overrightarrow{v}\}$ — прямые, параллельные вектору $\overrightarrow{v}$.

в) Таких окружностей нет.

Упражнение 9.3. *Решение:* Если $AB \parallel l$, то рассмотрим основания O_A и O_B перпендикуляров, опущенных на l из точек A и B. Из условия параллельности вытекает, что все углы в четырёхугольнике ABO_BO_A прямые, а потому это прямоугольник. Аналогичным образом, прямоугольниками являются $A'B'O_BO_A$ и $ABB'A'$, а значит, $A'B' = AB$.

Упражнение 9.4. *Ответ:*

а) $\operatorname{Fix}(S_l) = l$ — множество неподвижных точек осевой симметрии суть её ось.

б) Это $\{l\} \cup \{m \mid m \perp l\}$ — прямые, перпендикулярные прямой l, и сама прямая l.

в) Это окружности с центром на прямой l.

Упражнение 9.5. *Решение:* Если A, B и O лежат на одной прямой, возможно два случая.

1) Точка O находится между точками A и B. Тогда, согласно определению поворота,

$$A'B' = A'O + B'O = AO + BO = AB.$$

2) Точка O не находится между точками A и B. Для определённости будем считать, что точка B находится между точками A и O. Тогда, согласно определению поворота,

$$A'B' = A'O - B'O = AO - BO = AB.$$

Упражнение 9.6. *Ответ:*

а) $\mathrm{Fix}\,(R_{O,\varphi}) = \{O\}$ — множество неподвижных точек поворота суть его центр.

б) Если $\varphi = \pi$ (то есть поворот является центральной симметрией), то это прямые, проходящие через центр O. В противном случае инвариантных прямых нет.

в) Это концентрические окружности с центром в точке O.

Упражнение 9.7. *Ответ:* Обратным движением к параллельному переносу $T_{\overrightarrow{v}}$ является параллельный перенос на вектор, противоположный исходному: $T_{-\overrightarrow{v}}$.

Упражнение 9.8. *Ответ:*

а) Вектор $\overrightarrow{v}$ параллельного переноса $T_{\overrightarrow{v}} = S_l \circ S_m$ перпендикулярен прямым $l \parallel m$, направлен от m к l, а длина его равна удвоенному расстоянию между прямыми l и m.

б) Угол поворота φ поворота $R_{O,\varphi} = S_l \circ S_m$ равен удвоенному углу между прямыми l и m, а центр этого поворота суть точка пересечения прямых: $O = l \cap m$.

10. Комплексные числа

Упражнение 10.1. *Ответ:* Комплексное сопряжение является движением, а именно, это осевая симметрия относительно вещественной оси Ox.

Упражнение 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: $x = \mathrm{Re}\,(z)$ и $y = \mathrm{Im}\,(z)$.

Упражнение 10.3. *Ответ:* -3.

Упражнение 10.4. *Решение:* Прямое вычисление: если $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$, то

$$\overline{z_1+z_2} = (x_1+x_2) + i(y_1+y_2) = \bar z_1 + \bar z_2 \qquad \text{и} \qquad \overline{z_1 z_2} = (x_1x_2 - y_1y_2) - i(x_1y_2 + y_1x_2) = \bar z_1 \bar z_2.$$

Упражнение 10.5. *Ответ:* $5 - 5i$.

Упражнение 10.6. *Ответ:* $r = \sqrt{x^2+y^2}$, $\theta = \mathrm{arctg}(y/x)$.

Упражнение 10.7. *Решение:* Проведём доказательство индукцией по n.

База индукции: при $n = 1$ тривиальным образом выполняется.

Шаг индукции: пусть $(\cos\theta + i\sin\theta)^k = \cos k\theta + i\sin k\theta$ справедливо для некоторого натурального k. Тогда для $k+1$:

$$(\cos\theta + i\sin\theta)^{k+1} = (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta) =$$
$$(\cos k\theta + i\sin k\theta)(\cos\theta + i\sin\theta) = \cos{(k+1)\varphi} + i\sin{(k+1)\theta}.$$

Упражнение 10.8. *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 для $(\cos\alpha + i\sin\alpha)^3$, после чего приравняйте друг к другу действительные и мнимые части полученных выражений соответственно.

Упражнение 10.9. *Решение:* Прямое вычисление:

а) $(\omega_1 \cdot \omega_2)^n = \omega_1^n \cdot \omega_2^n = 1 \cdot 1 = 1, \quad \left(\dfrac{\omega_1}{\omega_2}\right)^n = \dfrac{\omega_1^n}{\omega_2^n} = \dfrac{1}{1} = 1.$

б) $(\varepsilon \cdot \omega)^n = \varepsilon^n \cdot \omega^n = 1 \cdot w = w.$

Упражнение 10.10. *Решение:* Раскроем скобки в правой части и воспользуемся тем, что ω является корнем уравнения $z^3 = 1$, не равным единице, то есть $\omega^3 = 1$ и $\omega^2 + \omega = -1$:

$$(x+y)(x+\omega y)(x+\omega^2 y) = (x+y)(x^2+\omega xy+\omega^2 xy+\omega^3 y) = (x+y)(x^2-xy+y^2) = x^3+y^3.$$

Упражнение 10.11. *Ответ:*

а) $\left\{-\dfrac{1}{2} \pm i\dfrac{\sqrt{3}}{2}\right\}$;

б) $\{1+i,\ -2i\}$;

в) $\{\pm\sqrt{2} \pm \sqrt{i}\}$.

Упражнение 10.12. *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) $z^n - 1 = \prod\limits_{k=0}^{n-1}\left(z - \cos\dfrac{2\pi k}{n} - i\sin\dfrac{2\pi k}{n}\right)$.

Упражнение 10.13. *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) Серединный перпендикуляр к отрезку с концами в точках $(-1,0)$ и $(0,1)$, канонический вид: $(1-i)z + (1+i)\bar{z} = 0$.

Упражнение 10.14. *Ответ:* Примените к числу z последовательно отражение относительно оси Ox, поворот на 90° по часовой стрелке и параллельный перенос на $-1+3i$. В результате получится $-\dfrac{3}{2} + \dfrac{5}{2}i$.

Упражнение 10.15. *Решение:* а) Пусть точки A, B и C лежат на одной прямой, а их образами при гомотетии являются точки A', B' и C'. Тогда

$$\frac{OA}{AA'} = \frac{OB}{BB'} = \frac{OC}{CC'},$$

откуда по теореме, обратной к теореме о пропорциональных отрезках, $A'B' \parallel AB$ 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.

Упражнение 10.16. *Ответ:* $z\mapsto k(z-a)+a$.

Упражнение 10.17. *Решение:* Выберем систему координат так, чтобы инверсия производилась относительно единичной окружности с центром в начале координат. Поскольку при этом
$$z\mapsto z'=\frac{1}{\bar z}\qquad \text{и}\qquad \bar z\mapsto \bar{z}'=\frac{1}{z},$$
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 $c'=a$.

Задача 10.1. *Ответ:*

а) 0;

б) $-6+5i$.

Задача 10.2. *Ответ:*

а) $-\dfrac{13}{15}+\dfrac{3}{5}i$;

б) $\dfrac{1}{10}$;

в) $-i$;

г) $-1+4i\sqrt{5}$;

д) -4.

Задача 10.3. *Ответ:*

а) $\{\pm i\}$;

б) $\left\{\pm\left(\dfrac{\sqrt2}{2}+i\dfrac{\sqrt2}{2}\right)\right\}$;

в) $\left\{\sqrt[4]{2}\left(\cos\left(\dfrac{7\pi}{8}\right)+i\sin\left(\dfrac{7\pi}{8}\right)\right),\ \sqrt[4]{2}\left(\cos\left(\dfrac{15\pi}{8}\right)+i\sin\left(\dfrac{15\pi}{8}\right)\right)\right\}$;

г) $\left\{\dfrac{\sqrt3}{2}+i\dfrac12,\ -\dfrac{\sqrt3}{2}+i\dfrac12,\ -i\right\}$;

д) 256.

Задача 10.4. *Ответ:*

а) $-\dfrac12\pm\dfrac{\sqrt3}{2}$;

б) $\pm(1+i)$;

в) i; $\dfrac{\pm\sqrt{3}-i}{2}$.

Задача 10.5. *Ответ:*

а) $\cos(-\alpha) + i\sin(-\alpha)$;

б) $\cos\left(\dfrac{\pi-\alpha}{2}\right) + i\sin\left(\dfrac{\pi-\alpha}{2}\right)$;

в) $2\cos\dfrac{\alpha}{2}\left(\cos\dfrac{\alpha}{2} + i\sin\dfrac{\alpha}{2}\right)$.

Задача 10.6. *Ответ:*

а) $-\theta$;

б) 0;

в) 0;

г) 2θ;

д) 2θ.

Задача 10.7. *Ответ:*

а) круг с центром в 0, радиуса 2 вместе с граничной окружностью;

б) все точки плоскости вне круга с границей с центром в 1 радиуса 1;

в) окружность радиуса 3 с центром в $2-i$;

г) серединный перпендикуляр к отрезку, соединяющему точки -1 и i;

д) область с границей над прямой $y = x$;

е) парабола с вершиной в точке $(2;0)$, ветвями вверх.

Список литературы

[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] *Шень А.*, Задачи по математике, предлагавшиеся ученикам математического класса 57 школы (выпуск 2000 года, класс «В») — Москва, МЦНМО, 2000.

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

[19] *Шень А. Х.*, Перестановки — Москва, МЦНМО, 2020.