УДК 51
ББК 74.200.58:22.1
Эл45

Эл45 Элементы математики в задачах: через олимпиады и кружки — к профессии / Под ред. А. А. Заславского, А. Б. Скопенкова и М. Б. Скопенкова. Изд. 2-е, исправленное и дополненное. — М.: МЦНМО, 2017. — 592 с.

ISBN 000-0-0000-0000-0

В данный сборник вошли материалы выездных школ по подготовке команды Москвы на Всероссийскую олимпиаду. Материалы сборника могут использоваться как школьниками для самостоятельных занятий, так и преподавателями. В большинстве материалов сборника приведены дававшиеся на занятиях задачи, а также решения или указания к ключевым задачам.

ББК 74.200.58:22.1

Элементы математики в задачах: через олимпиады и кружки — к профессии

Под редакцией А. А. Заславского, А. Б. Скопенкова и М. Б. Скопенкова

Подписано в печать ??.??.2017 г. Формат $60 \times 90\ {}^{1}/_{16}$. Бумага офсетная. Печать офсетная. Печ. л. ??. Тираж 2000 экз. Заказ № .

Издательство Московского центра непрерывного математического образования.
119002, Москва, Большой Власьевский пер., д. 11. Тел. (499) 241–08–04

Отпечатано ???

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. (495) 745–80–31. E-mail: biblio@mccme.ru,
http://biblio.mccme.ru

Оглавление

1 От редакторов

1.1 Зачем и для кого эта книга

Глубокое понимание математики полезно и математику, и профессионалу в наукоёмкой отрасли. В частности, «профессия» в названии этой книги не обязательно означает профессию математика.

Эта книга предназначена для старшеклассников и младшекурсников (в частности, ориентированных на олимпиады). См. подробнее § 26 «Олимпиады и математика». Книгу можно использовать как для самостоятельных занятий, так и для преподавания.

Книга содержит наиболее стандартный «базовый» материал (впрочем, частично, скорее, для повторения, чем для первоначального изучения). Основное содержание книги составляет более сложный материал. Некоторые темы малоизвестны в традиции математических кружков, но полезны как для математического образования, так и для подготовки к олимпиадам.

Книга основана на занятиях, проведённых авторами в разное время в школе им. А. Н. Колмогорова (СУНЦ МГУ), школе № 1543 г. Москвы, летней школе «Современная математика», Кировской и Костромской летних математических школах, Московской выездной олимпиадной школе, в кружках «Математический семинар» и «Олимпиады и математика», на летней конференции Турнира городов, при подготовке команды России к международной математической олимпиаде, в системе дистанционного обучения математике МИОО, а также в Независимом московском университете и на математическом факультете Высшей школы экономики.

Книга доступна уже старшеклассникам, интересующимся математикой[14]. Приводятся почти все определения, не входящие в школьную программу. Если где-то нужны дополнительные сведения, то приводятся ссылки.

[14] Часть материала в некоторых кружках и летних школах изучается теми, кто только знакомится с математикой (например, 6-классниками). Однако приводимое изложение рассчитано на читателя, уже имеющего хотя бы минимальную математическую культуру. Заниматься с 6-классниками нужно по-другому, см., например, [GIF].

При этом многие темы трудны, если изучать их «с нуля». Однако *последовательность изложения* помогает преодолевать трудности. В то же время многие темы *независимы* друг от друга. См. подробнее п. 1.3 «Как устроена книга».

1.2 Изучение путём решения и обсуждения задач

Мы следуем традиции изучения материала в виде решения и обсуждения задач. Эти задачи подобраны так, что в процессе их решения читатель (точнее, решатель) освоит основы важных теорий — как классических, так и современных. Основные идеи демонстрируются по одной и на «олимпиадных» примерах, т. е. на простейших частных случаях, свободных от технических деталей. Этим мы показываем, *как можно придумать* эти теории. См. подробнее § 26 «Олимпиады и математика».

Обучение путём решения задач не только характерно для серьёзного изучения математики, но и продолжает древнюю культурную традицию. Например, послушники дзенских монастырей обучаются, размышляя над загадками, данными им наставниками. Впрочем, эти загадки являются скорее парадоксами, а не задачами. См. подробнее [Su]; ср. [Pl, с. 26–33]. А вот некоторые «математические» примеры: [Ar01, BS, GDI, KK08, Pr07-1, DoSn, SCY, Sk09, Vag, Zv]; кое-где не только приведены задачи, но и изложены *принципы отбора* удачных задач.

Учиться, решая задачи, трудно. В частности, потому, что такое обучение обычно не создаёт *иллюзию* понимания. Однако усилия сполна вознаграждаются глубоким пониманием материала — в первую очередь, умением проводить аналогичные (и даже не очень аналогичные) рассуждения. Кое-где вслед за великими математиками в процессе изучения интересных задач читатель увидит, как естественно возникают важные понятия и теории. Надеемся, это поможет ему совершить собственные настолько же полезные открытия (не обязательно в математике)!

Для решения задач достаточно понимания их условий. Другие знания и теории не нужны. (Впрочем, такие знания и теории как раз появляются при решении подобранных задач.) Но может потребоваться владение другими частями книги, что отражено в под-

сказках и указаниях.

К важнейшим задачам приводятся подсказки, указания, решения и ответы. Они расположены в конце каждого пункта. Однако к ним стоит обращаться после прорешивания каждой задачи.

Если задача выделена словом «теорема» («лемма», «следствие» и т. д.) и жирным шрифтом, то её утверждение важное.

Как правило, мы приводим *формулировку* красивого или важного утверждения (в виде задачи) перед его *доказательством*. В таких случаях для доказательства утверждения могут потребоваться следующие задачи. Это всегда явно оговаривается в подсказках, а иногда и прямо в тексте. Поэтому если некоторая задача не получается, то читайте дальше. (На занятии задача-подсказка выдаётся только тогда, когда ученик немного подумал над самой задачей.) Такой процесс обучения полезен, поскольку моделирует реальную исследовательскую ситуацию. См. подробнее § 28 «О необходимости мотивировок».

Всё это — попытка продемонстрировать занятие в виде *диалога*, основанного на решении и обсуждении задач. Подробнее см. [KK15].

1.3 Как устроена книга

Книгу не обязательно изучать подряд. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана. Для занятия кружка можно использовать любой пункт (или подпункт) книги.

Книга разбита на главы, параграфы и пункты (некоторые пункты разбиты на подпункты). Структура параграфов приблизительно описана в их начале. Если в задаче используется материал другого пункта, то можно либо игнорировать эту задачу, либо посмотреть то место, на которое приводится ссылка. Это даёт большую свободу читателю при изучении книги, но одновременно может требовать его внимательности.

Пункты внутри каждого параграфа расположены примерно в порядке возрастания сложности материала. Цифры в скобках после названия пункта означают его «относительный уровень»: 1 — самый простой, 4 — самый сложный. Первые пункты (не отмеченные звёздочкой) являются базовыми; если не указано противное, с них

можно начать изучение главы. А к остальным пунктам (отмеченным звёздочкой) можно возвращаться потом; если не указано противное, то они независимы друг от друга. При изучении полезно *возвращаться* к пройденному материалу, но на новом уровне. Поэтому разные пункты одного параграфа можно изучать *не подряд*, а с перерывами на другие темы.

Обозначения, используемые в разных главах книги, приведены в конце введения. Понятия и обозначения, используемые в некоторой главе, вводятся в начале главы.

Последняя глава составлена из заметок об общих принципах преподавания, адресованных прежде всего учителям. Возможно, заметки окажутся полезными и ученикам.

В конце книги есть предметный указатель. Жирным шрифтом выделены номера страниц, на которых приводятся *формальные определения* понятий.

Обновляемая электронная версия части книги, выложенная с разрешения издательства:
`http://www.mccme.ru/circles/oim/materials/sturm.pdf`.

1.4 Напутствие. *А. Я. Канель-Белов*

Для успешного решения задач математических олимпиад высшего уровня необходимы в первую очередь общеукрепляющие средства: хорошая проработка алгебры (культура алгебраических преобразований), проработка школьной геометрии. Задачи этих олимпиад (кроме первых задач) практически всегда предполагают смешанный сценарий решения; редки задачи на применение некоторого метода или идеи в чистом виде. Решению таких «смешанных» задач должна предшествовать работа с ключевыми задачами, в которых идеи работают в чистом виде. См., например, литературу к п. 1.2 или настоящий сборник.

1.5 О литературе и источниках

В конце каждого параграфа приводится литература, относящаяся ко всему параграфу, и отдельно литература по каждому пункту. Ссылка на книгу [GKP], относящуюся и к комбинаторике, и к алгеб-

также ряд полезных идей и замечаний. Благодарим Д. А. Пермякова, редактора книги [ZPS]. Благодарим учеников за каверзные вопросы и указания на неточности. Благодарим Е. С. Горскую и П. В. Широкова за подготовку многих рисунков. Благодарности по отдельным материалам приводятся прямо в них.

Мы приносим извинения за допущенные неточности и будем благодарны читателям за указания на них.

Главы 1, 2 и 3 редактировали А. Б. Скопенков, А. А. Заславский и М. Б. Скопенков соответственно. Мы организовали рецензирование материалов главы 4, но редактировали их сами авторы.

М. Б. Скопенков и А. Б. Скопенков частично поддержаны грантами фонда Саймонса и фонда «Династия». М. Б. Скопенков частично поддержан грантом Президента РФ МК-6137.2016.1.

Места работы и интернет-страницы.

А. А. Заславский: ЦЭМИ РАН, школа 1543.

А. Б. Скопенков: Московский физико-технический институт (ГУ) и Независимый московский университет, `www.mccme.ru/~skopenko`.

М. Б. Скопенков: Национальный исследовательский университет Высшая школа экономики (факультет математики) и Институт проблем передачи информации РАН, `http://skopenkov.ru`.

1.7 Важные соглашения

Пункты внутри каждого параграфа расположены примерно в порядке возрастания сложности материала. Цифры в скобках после названия пункта означают его «относительный уровень»: 1 — самый простой, 4 — самый сложный. Первые пункты (не отмеченные звёздочкой) являются базовыми; если не указано противное, с них можно начать изучение главы. А к остальным пунктам (отмеченным звёздочкой) можно возвращаться потом; если не указано противное, то они независимы друг от друга.

Номера задач обозначаются жирным шрифтом. Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. *Загадкой* называется не сформулированный чётко вопрос; здесь нужно придумать и чёткую формулировку, и доказательство, ср. [VIN]. В задачах, отмеченных кружочком °, требуется привести только ответ без доказательства. Наибо-

лее трудные задачи отмечены звёздочкой *. Если в условии задачи написано «найдите», то нужно дать ответ без знака суммы и многоточия. *Указание и решение* к задаче может опираться на *подсказку* к ней. Если некоторая задача не получается, то читайте дальше — следующие задачи могут оказаться подсказками.

1.8 Основные обозначения

• $\lfloor x \rfloor = [x]$ — (нижняя) целая часть числа x («пол»), т. е. наибольшее целое число, не превосходящее x.

• $\lceil x \rceil$ — верхняя целая часть числа x («потолок»), т. е. наименьшее целое число, не меньшее x.

• $\{x\}$ — дробная часть числа x.

• $d \mid n$, или $n \vdots d$ — число n *делится* на число d, т. е. $d \neq 0$ и существует такое целое k, что $n = kd$ (число d называется *делителем* числа n).

• $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ — множества всех действительных, рациональных и целых чисел соответственно.

• $\mathbb{Z}_2$ — множество $\{0, 1\}$ остатков от деления на 2 с операциями сложения и умножения по модулю 2.

• $\mathbb{Z}_m$ — множество $\{0, 1, \ldots, m-1\}$ остатков от деления на m с операциями сложения и умножения по модулю m. (Специалисты по алгебре чаще обозначают это множество $\mathbb{Z}/m\mathbb{Z}$, а через $\mathbb{Z}_m$ обозначают множество *целых m-адических чисел* для простого m.)

• $\binom{n}{k}$ — количество k-элементных подмножеств n-элементного множества (другое обозначение: C_n^k).

• $|X|$ — число элементов во множестве X.

• $A - B = \{x \mid x \in A \text{ и } x \notin B\}$ — разность множеств A и B.

• $A \sqcup B$ — дизъюнктное объединение множеств A и B, т. е. объединение $A \cup B$ непересекающихся множеств A и B.

• $A \subset B$ — «множество A содержится в множестве B». (В некоторых других книгах это обозначают $A \subseteq B$, а $A \subset B$ означает «множество A содержится в множестве B и не равно B».)

• Фраза «обозначим $x = a$» сокращается до $x := a$.

• id — отображение множества в себя, переводящее каждый элемент в себя (тождественное).

Глава 1

Теория чисел, алгебра и анализ

А. Б. Скопенков

Умение преобразовывать алгебраические выражения — одно из базовых. Его недостает «олимпиадникам», из-за его отсутствия часто возникают нелепые и обидные ошибки. Поэтому для успешного решения задач алгебраического и теоретико-числового типа рекомендуем нарабатывать культуру арифметических выкладок.

2 Делимость и деление с остатком

Из этого параграфа далее используются в основном алгоритм Евклида и его применения (задачи 2.5.7 и 2.5.9), язык сравнений (п. 2.4 «Деление с остатком и сравнения») и простые факты (типа задач 2.1.3 и 2.3.2).

В этом параграфе латинскими буквами обозначаются *целые* числа. Многие решения написаны с использованием текстов М. А. Прасолова.

2.1 Делимость (1)

2.1.1. (а) Сформулируйте и докажите признаки делимости на 2, 4, 5, 10, 3, 9, 11.

(b) Делится ли число $11\ldots1$ из 1993 единиц на 111111?
(c) Число $1\ldots1$ из 2001 единиц делится на 37.

2.1.2. Если a делится на 2 и не делится на 4, то количество чётных делителей числа a равно количеству его нечётных делителей.

2.1.3. Какие из следующих утверждений верны для любых a, b:
(a) $2|(a^2-a)$; (b) $4|(a^4-a)$; (c) $6|(a^3-a)$; (d) $30|(a^5-a)$;
(e) если $c|a$ и $c|b$, то $c|(a+b)$;
(f) если $b|a$, то $bc|ac$ для любого $c \neq 0$;
(g) если $bc|ac$ для некоторого c, то $b|a$?

При решении задачи 2.1.3 (c) вы использовали следующий факт 2.1.4 (a). Докажите его по определению делимости, не используя единственности разложения на простые множители (задача 2.2.7 (c))! Использование единственности может привести к порочному кругу, ведь обычно при доказательстве единственности используется факт, близкий к утверждению 2.1.4 (a).

2.1.4. (a) Если число a делится на 2 и на 3, то a делится на 6.
(b) Если число a делится на 2, на 3 и на 5, то a делится на 30.
(c) Если число a делится на 17 и на 19, то a делится на 323.

2.1.5. (a) Если k не кратно ни 2, ни 3, ни 5, то k^4-1 кратно 240.
(b) Если $a+b+c$ делится на 6, то и $a^3+b^3+c^3$ делится на 6.
(c) Если $a+b+c$ делится на 30, то и $a^5+b^5+c^5$ делится на 30.
(d) Если $n \geqslant 0$, то $20^{2n}+16^{2n}-3^{2n}-1$ делится на 323.

Подсказки

2.1.4. (a) Имеем $3a-2a=a$, поэтому a делится на 6.

Указания, ответы и решения

2.1.1. (a) Для доказательства нижеприведённых признаков обозначим упоминаемое в них число через

$$n = \pm(10^m a_m + 10^{m-1}a_{m-1} + \ldots + 10a_1 + a_0)$$

для некоторых a_i, $0 \leqslant a_i \leqslant 9$.

3.1 Малая теорема Ферма (2)

3.1.1. (a) Обозначим $\mathbb{Z}_{97} = \{0, 1, \ldots, 96\}$. Определим отображение $f\colon \mathbb{Z}_{97} \to \mathbb{Z}_{97}$ так: $f(a)$ равно остатку от деления числа $14a$ на 97. Тогда f — взаимно однозначное соответствие.

Обсуждение. Достаточно доказать либо сюръективность, либо инъективность. Обычно доказывают *инъективность*. Но необходимая для этого основная лемма арифметики 2.5.7.b обычно доказывается через разрешимость уравнения $97x + 14y = 1$, из которой сразу вытекает *сюръективность*.

(b) Справедливо соотношение $(14 \cdot 1) \cdot (14 \cdot 2) \cdot \ldots \cdot (14 \cdot 96) \equiv 96! \pmod{97}$.

(c) Справедливо соотношение $14^{96} \equiv 1 \pmod{97}$.

(d) **Малая теорема Ферма.** Если p простое, то $n^p - n$ делится на p для любого целого n.

Alio modo. Если p простое и n не делится на p, то $n^{p-1} - 1$ делится на p.

(f) Для простого p число $\binom{p}{k}$ делится на p для любого $k = 1, 2, \ldots, p-1$. (Из этого получается иное — по индукции — доказательство малой теоремы Ферма.)

3.1.2. Найдите остаток от деления

(a) 2^{100} на 101; (b) 3^{102} на 101; (c) 8^{900} на 29;

(d) 3^{2000} на 43; (e) 7^{60} на 143; (f) $2^{60} + 6^{50}$ на 143.

3.1.3. (a) Если p простое и $p > 2$, то $7^p - 5^p - 2$ делится на $6p$.

(b) Число $111\ldots11$ из 2002 единиц делится на 2003.

(c) Если p и q — различные простые числа, то $p^q + q^p - p - q$ делится на pq.

(d) Число $30^{239} + 239^{30}$ составное.

(e) Если p простое, то длина периода десятичной дроби $1/p$ делит $p - 1$.

3.1.4. Для простого p и a, не делящегося на p, назовём *порядком* $\operatorname{ord} a = \operatorname{ord}_p a$ числа (или вычета) a по модулю p наименьшее $k > 0$, для которого $a^k \equiv 1 \pmod{p}$:

$$\operatorname{ord} a = \operatorname{ord}_p a := \min\{k \geqslant 1 \mid a^k \equiv 1 \pmod{p}\}.$$

(a) Множество $\{m \geqslant 0\colon a^m \equiv 1 \pmod p\}$ состоит из целых неотрицательных чисел, кратных $\operatorname{ord} a$.

(b) Если $a^m \equiv a^n \pmod p$, то $m-n$ делится на $\operatorname{ord} a$.

(c) **Лемма.** Число $p-1$ делится на $\operatorname{ord} a$.

(d) Если $\operatorname{ord} x$ и $\operatorname{ord} y$ взаимно просты, то $\operatorname{ord}(xy) = \operatorname{ord} x \cdot \operatorname{ord} y$.

(e) Для любых ли a, x, p верно, что $a \operatorname{ord}_p x^a = \operatorname{ord}_p x$?

Заметим, что по простому модулю можно определить деление и отрицательные степени. Аналоги утверждений 3.1.4 (a, b) справедливы для отрицательных степеней.

3.1.5. В этой задаче буквами $p, q, p_1, \ldots, p_k$ обозначаются различные простые числа.

(a) Если $p \neq q$ и n не делится ни на p, ни на q, то $n^{(p-1)(q-1)} - 1$ делится на pq.

(b) Если n не делится на p, то $n^{p^\alpha(p-1)} - 1$ делится на $p^{\alpha+1}$.

(c) **Теорема Эйлера.** Если n взаимно просто с $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ и $\varphi(m) := (p_1-1)p_1^{\alpha_1-1} \cdot \ldots \cdot (p_k-1)p_k^{\alpha_k-1}$, то $n^{\varphi(m)} - 1$ делится на m.

(d) Число $\varphi(m)$ равно количеству чисел от 1 до m, взаимно простых с m.

3.1.6. (Загадка.) Известно, что n — нечётное число от 3 до 47, не делящееся на 5. Как быстро вычислять неизвестное n по известному $n^7 \bmod 50$?

Решение этой загадки показывает, почему для шифрования так важно быстро находить разложение числа на простые множители, в частности быстро распознавать простоту числа.

Указания, ответы и решения

3.1.1. (a) $14 \cdot 7k \equiv k \bmod 97$.

(b) $(14\cdot1)\cdot(14\cdot2)\cdot\ldots\cdot(14\cdot96) \equiv f(1)\cdot f(2)\cdot\ldots\cdot f(96) = 96! \bmod 97$.

(c) Сократите равенство из п. (b) на 96!.

3.1.2. *Ответы*: (a) 1; (b) 9; (c) 7; (d) 15; (e) 1; (f) 24.

По утверждению 3.1.4 (c) число $n-1=2^sk$ делится на $\operatorname{ord}_p a = 2^tl$. Значит, k делится на l. Если $t<s$, то $(n-1)/2=2^{s-1}k$ делится на 2^tl. Отсюда $a^{\frac{n-1}{2}}\equiv 1 \bmod p$, что противоречит делимости $a^{\frac{n-1}{2}}+1$ на n.

(d) Если n составное, то у него имеется простой делитель $p\leqslant\sqrt{n}$. По предыдущему пункту $p\geqslant 2^s+1$, а значит, $n\geqslant(2^s+1)^2$. Это противоречит тому, что $n=2^sk+1\leqslant(2^s)^2+1$.

3.2.4. (a) Действительно, $2^p=2\cdot(2^2)^{\frac{p-1}{2}}\equiv 2 \bmod 3$. Поэтому $n=(2^p-1)\frac{2^p+1}{3}$ составное.

Далее, $2^{2p}=2^2\cdot(2^{p-1})^2\equiv 4 \bmod p$. Значит, $2^{2p}-4$ делится на $2p$. Так как $p>3$, то число $n-1=(2^{2p}-4)/3$ также делится на $2p$. Следовательно, $2^{n-1}=(2^{2p})^{\frac{n-1}{2p}}\equiv 1 \bmod (2^{2p}-1)$. Итак, $2^{n-1}-1$ делится на $2^{2p}-1=3n$.

(b) Например, $n=561$.

3.3 Квадратичные вычеты (2*)

Цель этого цикла задач — мотивировать и обсудить проблему разрешимости сравнения $x^2\equiv a \pmod p$ для простого p. В этом пункте через p обозначается нечётное простое число.

3.3.1. (a) Какие остатки могут давать квадраты целых чисел при делении на 3, 4, 5, 6, 7, 8, 9, 10?

(b) Если a^2+b^2 делится на 3 (на 7), то a и b делятся на 3 (на 7).

(c) Число вида $4k+3$ не представимо в виде суммы двух квадратов.

(d) Существует бесконечно много чисел, не представимых в виде суммы трёх квадратов.

3.3.2. Решите уравнения в целых числах:

(a) $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2=y^2$ (в нечётных числах);

(b) $3x=5y^2+4y-1$; (c) $x^2+y^2=3z^2$; (d) $2^x+1=3y^2$;

(e) $x^2=2003y-1$; (f) $x^2+1=py$, где $p=4k+3$;

3.3.3. (a) Если $p=4k+3$ делит a^2+b^2, то $p|a$ и $p|b$.

(b) Число, в каноническое разложение которого некоторый простой делитель вида $4k+3$ входит в нечётной степени, не представимо в виде суммы двух квадратов (целых чисел).

(c)* Уравнение $x^2+1=py$ разрешимо в целых числах при $p=4k+1$ (и неразрешимо при $p=4k+3$).

(d)* Любое простое число вида $4k+1$ представимо в виде суммы двух квадратов.

(e)* Число, в каноническое разложение которого любой простой делитель вида $4k+3$ входит в чётной степени, представимо в виде суммы двух квадратов.

(f) Простых чисел вида $4k+1$ бесконечно много.

Доказательство Дон Загира утверждения (d) можно найти в книге [Pr07-1].

3.3.4. (Загадка.) «Сведите» уравнение $py=at^2+bt+c$, $a\neq 0$, к сравнению $x^2\equiv k \pmod p$.

Остаток $a\neq 0$ называется *квадратичным вычетом* (*квадратичным невычетом*) *по модулю* p, если сравнение $x^2\equiv a(p)$ разрешимо (неразрешимо). Слова «по модулю p» далее опускаются.

3.3.5. (a) Приведите пример таких a и p, что оба числа a и $-a$ являются квадратичными вычетами.

(b) Если a не делится на p, то сравнение $x^2\equiv a^2(p)$ имеет ровно два решения.

(c) **Лемма.** Число квадратичных вычетов равно числу квадратичных невычетов и равно $\frac{p-1}{2}$.

3.3.6. (a) **Лемма.** Для любого $a\neq 0$ существует и единственно такое b, что $ab\equiv 1(p)$.

Обозначение: $b=a^{-1}$.

(b) Решите сравнение $x\equiv x^{-1}(p)$.

(c) **Теорема Вильсона.** Число $(p-1)!+1$ делится на p.

3.3.7. (a) Если $a\neq 0$ — квадратичный вычет, то a^{-1} тоже квадратичный вычет.

(b) Число квадратичных вычетов чётно тогда и только тогда, когда -1 является квадратичным вычетом.

(e), (f) Используйте малую теорему Ферма.

3.3.5. (c) Квадратичных вычетов не более $\frac{p-1}{2}$, так как $a^2 \equiv (-a)^2 (p)$.

Предположим, что существуют такие $1 \leqslant l < k \leqslant \frac{p-1}{2}$, что $k^2 \equiv l^2 \pmod{p}$. Тогда одно из чисел $k-l$ и $k+l$ делится на p. Но $0 < k-l < k+l < p$. Противоречие! Значит, наше предположение неверно, т. е. вычетов ровно $\frac{p-1}{2}$. Следовательно, невычетов $p-1-\frac{p-1}{2} = \frac{p-1}{2}$. Требуемое доказано.

3.3.8. (c) В отличие от п. (a), (b) доказательство не проводится напрямую. Используйте п. (a), (b) и лемму 3.3.5 (c).

3.4 Квадратичный закон взаимности (3*)

Здесь строится алгоритм выяснения разрешимости сравнения $x^2 \equiv a \pmod{p}$ для простого p. Используется п. 3.3 «Квадратичные вычеты».

3.4.1. Если число $p = 8k+5$ простое, то

(a) $2^{4k+2} \equiv -1 \pmod{p}$;

(b) уравнение $x^2 - 2 = py$ неразрешимо в целых числах.

3.4.2. Если число $p = 8k+1$ простое, то

(a) $2^{4k} \equiv 1 \pmod{p}$;

(b) уравнение $x^2 - 2 = py$ разрешимо в целых числах.

3.4.3. (a) Если число $p = 8k \pm 1$ простое, то $2^{(p-1)/2} \equiv 1 \pmod{p}$.

(b) Если число $p = 8k \pm 3$ простое, то $2^{(p-1)/2} \equiv -1 \pmod{p}$.

(c) Для каких простых p разрешимо в целых числах уравнение $x^2 - 2 = py$?

3.4.4. (a) Если число $p = 12k \pm 1$ простое, то $3^{(p-1)/2} \equiv 1 \pmod{p}$.

(b) Если число $p = 12k \pm 5$ простое, то $3^{(p-1)/2} \equiv -1 \pmod{p}$.

(c) Для каких простых p разрешимо в целых числах уравнение $x^2 - 3 = py$?

3.5.1. (2–7) Сформулируйте и обоснуйте алгоритм решения сравнения $a^x \equiv b\ (m)$ для заданных a, b, взаимно простых с заданным $m \in \{2, 3, 4, 5, 6, 7\}$.

(Решение такого сравнения — одна из основных мотивировок этого занятия.)

3.5.2. (a) Если $(a, 35) = 1$, то $a^{12} \equiv 1 \pmod{35}$.

(b) Если m делится на два различных простых нечётных числа и $(a, m) = 1$, то $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$.

Пусть $(g, m) = 1$. Вычет g называется *первообразным корнем* по модулю m, если остатки от деления на m чисел $g^1, g^2, \ldots, g^{\varphi(m)} \equiv 1$ различны. Например,

• число 2 является первообразным корнем по модулю 5, а число 4 — нет;

• по задаче 3.5.2 (b) если m делится на два различных простых нечётных числа, то не существует первообразного корня по модулю m.

3.5.3. Докажите существование первообразного корня по простому модулю следующего вида:

(a) 257; (b) $2^l + 1$; (c) $2^k \cdot 3^l + 1$; (d) 151; (e) $2^k \cdot 3^l \cdot 5^m + 1$.

Простой метод решения пунктов (a), (b), (c), не проходит для (d), (e). Продемонстрируем метод решения пунктов (d), (e) на примерах.

3.5.4. (a) Вычет g — первообразный корень по модулю 97 тогда и только тогда, когда ни g^3, ни g^{32} не сравнимы с 1 по модулю 97.

(b) Сравнение $x^3 \equiv 1 \pmod{97}$ имеет ровно 3 решения.

(c) Сравнение $x^{32} \equiv 1 \pmod{97}$ имеет ровно 32 решения.

(d) Существует первообразный корень по модулю 97.

(e) Количество первообразных корней по модулю 97 равно 63.

3.5.5. (a) Вычет g — первообразный корень по модулю 151 тогда и только тогда, когда ни g^2, ни g^3, ни g^{25} не сравнимы с 1 по модулю 151.

(b) Сравнение $x^k \equiv 1 \pmod{151}$ имеет ровно k решений для $k \in \{30, 50, 75\}$.

(c) Имеет место равносильность

$$\begin{cases} x^{30} \equiv 1 \pmod{151}, \\ x^{50} \equiv 1 \pmod{151} \end{cases} \Leftrightarrow x^{10} \equiv 1 \pmod{151}.$$

(d) Существует первообразный корень по модулю 151.

(e) Количество первообразных корней по модулю 151 равно 40.

3.5.6. (a) Если p простое и $p-1$ делится на d, то сравнение $x^d \equiv 1 \pmod{p}$ имеет ровно d решений.

(b) **Теорема о первообразном корне.** Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1} = 1$ различны.

(c) Сколько существует первообразных корней по простому модулю p?

Указания, ответы и решения

3.5.3. (b) Если первообразного корня нет, то сравнение $x^{2^{l-1}} \equiv 1 \pmod{p}$ имеет $p - 1 = 2^l > 2^{l-1}$ решений.

3.5.6. (a) Заметьте, что многочлен $x^{p-1} - 1$ над $\mathbb{Z}_p$ имеет ровно $p-1$ корень и делится на $x^d - 1$. Докажите, что если многочлен степени a имеет ровно a корней и делится на многочлен степени b, то этот многочлен степени b имеет ровно b корней.

Другое решение можно получить, заметив, что если $p = kd$, то для любого a сравнение $y^k \equiv a \pmod{p}$ имеет не более k решений.

(c) *Ответ*: $\varphi(p-1)$.

3.6 Высокие степени (3*). *А. Я. Канель-Белов, А. Б. Скопенков*

3.6.1. (a) Для любых n и нечетного k число $k^{2^n} - 1$ делится на 2^{n+2}.

(b) Для любого n число $2^{3 \cdot 7^n} - 1$ делится на 7^{n+1}.

3.6.2. При каких a

(a) $2^a - 1$ делится на 3^{100}; (b) $2^a + 1$ делится на 3^{100};

(c) $5^a - 1$ делится на 2^{100}; (d) $2^a - 1$ делится на 5^{100}?

Утверждение 3.6.1 (a) означает, что ни при каком $n \geqslant 3$ не существует первообразного корня по модулю 2^n (см. определение в п. 3.5). Ответы к задачам 3.6.2.(a),(d),(c) и утверждение 3.6.1.(b) означают, что для любого n число 2 является первообразным корнем по модулю 3^n и по модулю 5^n, а числа 5 и 2 не являются первообразными корнями по модулю 2^n и по модулю 7^n.

3.6.3. (a) Найдите первообразный корень по модулю 7^{100}.

(b) **Теорема.** Первообразные корни существуют только по модулям $2, 4, p^n, 2p^n$.

3.6.4. Пусть $p > 2$ простое, g — первообразный корень по модулю p и $g^{p-1} - 1$ не делится на p^2. Тогда g — первообразный корень по модулю

(a) p^2; (b) p^3; (c) p^n для любого n.

3.6.5. Пусть $p > 2$ простое.

(a) Если g — первообразный корень по модулю p, то одно из чисел $g^{p-1} - 1$ и $(g + p)^{p-1} - 1$ не делится на p^2.

(b) Если g — первообразный корень по модулю p^2, то g — первообразный корень по модулю p^n для любого n.

(c) Для любого целого положительного n существует первообразный корень по модулю p^n.

(d) То же по модулю $2p^n$.

3.6.6. Лемма об уточнении показателя. Пусть p — простое число, $p > 2$ или $n > 1$, q не делится на p и $x - 1$ делится на p^n, но не на p^{n+1}.

(a) Число $x^q - 1$ делится на p^n, но не на p^{n+1}.

(b) Число $x^p - 1$ делится на p^{n+1}, но не на p^{n+2}.

(c) Число $x^{p^k q} - 1$ делится на p^{n+k}, но не на p^{n+k+1}.

(Близкое утверждение называется *леммой Гензеля.*)

3.6.7. Найдите длину периода дроби (a) $1/3^{100}$; (b) $1/7^{100}$.

3.6.8. (a) При циклической перестановке цифр в периоде дроби $1/7 = 0{,}(142857)$ получатся дроби вида 1/7, 2/7, 3/7, 4/7, 5/7, 6/7. Докажите аналогичный факт для дроби $1/p$, если в ней длина периода равна $p - 1$.

4.2.1. (a) Уравнение $x^3+3x^2+5x+7=0$ «сводится» заменой переменной к уравнению $y^3+py+q=0$ с некоторыми числами p, q.

(b) Уравнение $ax^3+bx^2+cx+d=0$ при $a\neq 0$ «сводится» заменой переменной к уравнению $y^3+py+q=0$ с некоторыми числами p, q.

(c) Уравнение $ax^4+bx^3+cx^2+dx+e=0$ при $a\neq 0$ «сводится» заменой переменной к уравнению $y^4+py^2+qy+r=0$ с некоторыми числами p, q, r.

4.2.2. (a) Докажите, что $\sqrt[3]{2+\sqrt{5}}-\sqrt[3]{\sqrt{5}-2}=1$.

(b) Найдите хотя бы одно решение уравнения $x^3-3\sqrt[3]{2}x+3=0$.

Указание. **Метод дель Ферро.** Так как

$$(u+v)^3=u^3+v^3+3uv(u+v),$$

то число $u+v$ является корнем уравнения $x^3-3uvx-(u^3+v^3)=0$.

(c) Решите уравнение $x^3-3\sqrt[3]{2}x+3=0$.

4.2.3. (a) Разложите на множители выражение $a^3+b^3+c^3-3abc$.

(b) Справедливо неравенство $a^2+b^2+c^2\geqslant ab+bc+ca$. Когда достигается равенство?

(c) Справедливо неравенство $a^3+b^3+c^3\geqslant 3abc$ при $a, b, c>0$.

(d) Разложите выражение $a^3+b^3+c^3-3abc$ на линейные множители с комплексными коэффициентами.

Задачи этого пункта о комплексных числах можно пропустить. Но для их решения необходимы лишь минимальные сведения о комплексных числах: достаточно уметь решать задачи 4.5.1 и 4.5.2.

4.2.4. (a) Сформулируйте и докажите теоремы, описывающие все вещественные (все комплексные) решения уравнения $x^2+px+q=0$.

(b) Сформулируйте и докажите теоремы, описывающие все вещественные (все комплексные) решения уравнения $x^3+px+q=0$ в том случае, когда работает метод дель Ферро (см. задачу 4.2.2). А при каком условии на p, q применим этот метод для вещественных решений, если квадратные корни разрешается извлекать только из положительных чисел?

(c) Составьте алгоритм (точного, или символьного) нахождения всех вещественных корней уравнения $ax^3+bx^2+cx+d=0$, где $a\neq 0$.

При решении некоторых кубических уравнений методом дель Ферро в формулах неожиданным образом возникают комплексные числа — как раз тогда, когда все корни исходного уравнения вещественны. Такие уравнения можно также решать следующим «чисто вещественным» методом. Он также интересен тем, что подводит к *трансцендентным методам* решения уравнений [PSo].

4.2.5. (a) Решите уравнение $4x^3 - 3x = \frac{1}{2}$.

(b) Решите уравнение $x^3 - 3x - 1 = 0$.

(c) Используя функции cos и arccos, напишите общую формулу для решения уравнения $x^3 + px + q = 0$ методом, намеченным в этой задаче. При каком условии уравнение $x^3 + px + q = 0$ решается этим методом?

4.2.6. Решите уравнение

(a) $(x^2 + 2)^2 = 9(x - 1)^2$; (b) $x^4 + 4x - 1 = 0$;

(c) $x^4 + 2x^2 - 8x - 4 = 0$; (d) $x^4 - 12x^2 - 24x - 14 = 0$.

Указание к задаче 4.2.6 (b). **Метод Феррари.** Подберите такие α, b, c, что

$$x^4 + 4x - 1 = (x^2 + \alpha)^2 - (bx + c)^2.$$

Для этого найдите хотя бы одно α, для которого квадратный трёхчлен $(x^2 + \alpha)^2 - (x^4 + 4x - 1)$ от x является полным квадратом. Для этого найдите дискриминант этого квадратного трёхчлена. Он является кубическим многочленом от α и называется *кубической резольвентой* многочлена $x^4 + 4x - 1$.

4.2.7.* (a) Сформулируйте и докажите теорему, описывающую все вещественные решения уравнения $x^4 + px^2 + qx + s = 0$. Можно использовать корень α кубической резольвенты.

(b) То же для комплексных решений.

Замечание. Уравнение $x^4 + ax^3 + bx^2 + cx + d = 0$ можно также решить, подобрав такие α, A, B, что

$$x^4 + ax^3 + bx^2 + cx + d = \left(x^2 + \frac{ax}{2} + \alpha\right)^2 - (Ax + B)^2.$$

В подсказках и указаниях к задачам этого пункта использован материал из [ABG].

Пусть $k_i \leqslant k_{i+1}$ для некоторого i. Вместе с u многочлен f должен содержать член $ax_1^{k_1} \dots x_i^{k_{i+1}} x_{i+1}^{k_i} \dots x_n^{k_n}$, который старше u. Противоречие. Поэтому $k_1 \geqslant k_2 \geqslant \dots \geqslant k_n$.

По п. (a) старший член многочлена $g := a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3} \dots \sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}$ совпадает с u. Поэтому мультистепень многочлена $f - g$ меньше мультистепени многочлена f. Осталось применить предположение индукции. □

4.7 Диофантовы уравнения и гауссовы числа (4*). *А. Я. Канель-Белов*

Всем хорошо знаком алгоритм Евклида. Даны два числа a, b. Из них выбирается большее, из большего вычитается меньшее, большее заменяется на разность, и с новой парой чисел производится та же процедура. См. задачу 2.5.9 (b). С помощью алгоритма Евклида доказываются арифметические свойства чисел и это Вы изучали раньше (см. п. 2.5 «Линейные диофантовы уравнения» и п. 4.4 «Делимость для многочленов»). Приведём принципиально новые (для большинства школьников) его применения.

4.7.1. Решите уравнения в целых числах:
(a) $x^2 + 4 = y^3$; (b) $x^2 + 2 = y^n$; (c)* $x^3 + y^3 = z^3$.

Попробуйте порешать их, не читая дальнейшего! Впрочем, у Вас вряд ли получится. Возвращайтесь к этой задаче по мере чтения дальнейшего материала.

При решении уравнения $x^2 + 4 = y^3$ в целых числах хочется действовать так: $x^2 + 4 = (x + 2i)(x - 2i)$. При нечётном x оба эти множители взаимно просты, и потому оба являются кубами. Из этого получается решение. (Случай чётного x хитрее: обе скобки могут делиться на $(1 + i)^3$.) Попробуйте довести решение до конца, а затем сравнить с приведённым в конце темы.

Одним словом, хочется наслаждаться дополнительными возможностями при разложении на множители за счёт использования *гауссовых чисел*, т. е. чисел вида $a + bi$ с целыми a и b. Однако не всё коту масленица — так получается не всегда (см. задачи 2.2.7 (b) и 4.7.3 (b)), но иногда получается. Чтобы применять разложение на

множители для решения уравнений, нужна *однозначность разложения на простые множители*. Если она имеет место, то мы имеем всё те же арифметические удовольствия, что и для целых чисел. Следующая задача показывает удивительный факт: для *арифметических* удовольствий достаточно доказать *геометрический* факт о возможности деления с остатком.

4.7.2. Гауссово число называется *простым*, если оно не разлагается на два множителя, каждый из которых отличен от ± 1 и $\pm i$. В этой задаче латинские буквы обозначают гауссовы числа.

(a) Однозначность разложения на простые множители вытекает из следующего свойства (аналога леммы Евклида 2.5.7 (c)).

Факториальность. Для любых a, b если простое число p делит ab, то p делит a или p делит b.

(b) Факториальность вытекает из следующего свойства (аналога леммы о представлении НОД 2.5.7 (a)).

Главноидеальность. Для любых a, b существуют такие x, y, что $xa + yb = \gcd(a, b)$. (Дайте определение наибольшего общего делителя $gcd(a, b)$ чисел a, b самостоятельно!)

(c) Главноидеальность обеспечивается следующим свойством (аналогом теоремы о делении с остатком 2.4.1 (b)).

Евклидовость. Для любых $b \neq 0$ и a существует такое k, что $|a - kb| < |b|$.

4.7.3. Верна ли евклидовость (и, значит, факториальность!) для множества $\mathbb{Z}[\xi]$ чисел вида $a + b\xi$ с целыми a, b, если ξ есть

(a) $\sqrt{-2}$; (b) $\sqrt{-3}$; (c) $(1 - \sqrt{-3})/2$; (d) $(1 - \sqrt{-5})/2$;
(e) $(1 - \sqrt{-7})/2$?

4.7.4. (a) Никакое простое число вида $4k-1$ не разлагается в сумму двух квадратов.

(b) Любое простое число вида $4k + 1$ разлагается в сумму двух квадратов, причём ровно одним способом.

(b) Существует целое число, ровно 1024 способами разлагающееся в сумму двух квадратов.

Эту задачу проще решать без гауссовых чисел (см. п. 3.3), однако полезно потренироваться в их применении!

Подробнее см. [Pos, § 4]. См. также задачу 4.4.7.

5 Разрешимость в радикалах

Основное содержание этого параграфа — простые элементарные доказательства знаменитых теорем Гаусса, Абеля, Галуа и Кронекера о построимости правильных многоугольников и неразрешимости уравнений в радикалах. На примере этих доказательств иллюстрируются некоторые основные идеи алгебры. Определения построимости и разрешимости в радикалах, а также формулировки указанных теорем, приводятся. Этот параграф адресован всем любителям изложения глубоких идей на примерах красивых результатов и доказательств: старшеклассникам, студентам, учителям и профессиональным математикам. Хороший опыт в работе с комплексными числами и многочленами получит и тот, кто не дойдёт до полного доказательства основных результатов.

5.1 Введение

5.1.1 О чём этот параграф

Основное содержание этого параграфа — простые элементарные доказательства

• теоремы Гаусса о построимости правильных многоугольников (и даже более сильного результата — теоремы Гаусса о понижении);

• существования уравнения 3-й степени, неразрешимого в *вещественных* радикалах (и даже более сильного результата — сильной вещественной теоремы о неразрешимости);

• теоремы Галуа о существовании уравнения 5-й степени, неразрешимого в *комплексных* радикалах (и даже более сильного результата — теоремы Кронекера).

Определения построимости и разрешимости в радикалах, а также формулировки указанных теорем приведены в п. 5.1.2 и 5.1.3. Я не привожу историю этих знаменитых теорем, отсылая заинтересованного читателя к текстам [Gi, Gi1, Ma].

Приводимые доказательства интересны тем, что для их понимания достаточно уметь доказывать иррациональность (п. 4.1), делить многочлены с остатком (п. 4.3 и задачи 4.4.3, 4.4.4), извлекать

корни из комплексных чисел (задача 4.5.4) и решать системы линейных уравнений. Эти прямые доказательства интересны тем, что на них ясно видны базовые идеи важной *теории Галуа* (см. п. 5.2.1 и § 27).

Приводимые доказательства не претендуют на новизну (хотя в этом тексте имеется много методических находок, см. п. 5.2.1 и 5.2.2). Однако, к сожалению, они малоизвестны. Как следствие, малоизвестно, что не только решать квадратные и кубические уравнения, но и доказывать указанные теоремы экономнее не строя и затем применяя теорию Галуа (как, например, в [Kh13, Kir]), а напрямую — но при этом, конечно, открывая и используя базовые идеи этой теории.

Параграф адресован тем, кому интересен хотя бы один из этих результатов. Разбор доказательств (или их начала) полезен для закрепления тем «иррациональность», «многочлены», «комплексные числа» и «основы линейной алгебры». Старшеклассник найдёт здесь задачи для исследования, не претендующие на научную новизну, подробнее см. п. 5.2.1. Пункты 5.3.3 и 5.5 могут быть интересны профессиональному математику.

Как устроен параграф, написано в п. 5.1.4. Впрочем, начать изучать параграф можно не с п. 5.1, а с решения задач в п. 5.4, поскольку большинство из них использует предыдущий материал только в качестве мотивировки.

Благодарю А. Я. Белова-Канеля, И. И. Богданова, Э. Б. Винберга, В. В. Волкова, М. Н. Вялого, А. С. Голованова, П. А. Дергача, Д. Зунга, А. А. Казначеева, А. Л. Канунникова, Г. А. Мерзона, А. А. Пахарева, В. В. Прасолова, А. Д. Руховича, Л. М. Самойлова, М. Б. Скопенкова, Г. Р. Челнокова, Л. А. Шабанова, В. В. Шувалова и особенно В. А. Клепцына за полезные замечания и предложения.

5.1.2 Разрешимость в квадратных радикалах: формулировки (1)

Известно, что

$$\cos\frac{2\pi}{3}=-\frac{1}{2},\quad \cos\frac{2\pi}{4}=0,\quad \cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4},\qquad \cos\frac{2\pi}{6}=\frac{1}{2},\quad \cos\frac{2\pi}{8}=\frac{1}{\sqrt{2}}. \tag{$*$}$$

Как обобщить эти формулы (используя только четыре арифметических действия и извлечения корней)? Для формализации этого вопроса введём следующие определения.

Определение вещественного калькулятора. Рассмотрим калькулятор с кнопками

$$1,\quad +,\quad -,\quad \times,\quad :\quad \text{и}\quad \sqrt[n]{\ }\quad \text{для любого } n.$$

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдаёт ошибку.

Вещественный калькулятор оперирует с вещественными числами и при извлечении корня чётной степени из отрицательного числа выдаёт ошибку.

Определение вещественной построимости. Вещественное число называется *вещественно построимым*, если его можно получить на вещественном калькуляторе так, чтобы при этом извлекались корни только второй степени (т. е. получить из 1 при помощи сложений, вычитаний, умножений, делений и извлечений квадратного корня из положительных чисел).

Например, вещественно построимы числа

$$\sqrt[4]{2}=\sqrt{\sqrt{2}},\quad \sqrt{2\sqrt{3}},\quad \sqrt{2}+\sqrt{3},\quad \sqrt{1+\sqrt{2}},\quad 1+\sqrt{3-2\sqrt{2}},\quad \frac{1}{1+\sqrt{2}},$$

числа из формулы $(*)$ и даже число $\cos\frac{\pi}{60}=\cos 3^\circ$. Про последнее число это не совсем очевидно (но мы это увидим в п. 5.3.1).

Вопрос об обобщении формул $(*)$ формализуется так: для каких n число $\cos(2\pi/n)$ вещественно построимо? Ответ даётся следующей теоремой.

Теорема 5.1 (Гаусса). *Число* $\cos(2\pi/n)$ *вещественно построимо тогда и только тогда, когда* $n = 2^\alpha p_1 \dots p_l$, *где* $p_1, \dots, p_l$ *— различные простые числа вида* $2^{2^s} + 1$.

Построимость в теореме Гаусса доказана в п. 5.3.1 и 5.3.3, а непостроимость — в п. 5.5.2.

Вещественная построимость числа равносильна его *построимости циркулем и линейкой*. Поэтому теорема Гаусса равносильна критерию построимости циркулем и линейкой правильных многоугольников. Мы обсудим эту равносильность в п. 5.2.3; впрочем, она не используется в остальном тексте.

Из вещественной непостроимости числа $\cos(2\pi/9)$ вытекает следующий результат.

Следствие. *Трисекция угла невозможна на вещественном калькуляторе, если можно извлекать корни только второй степени, или, формально, на нём невозможно получить число* $\cos(\alpha/3)$, *имея число* $\cos\alpha$ (*например, для* $\alpha = 2\pi/3$).

Замечания. (a) Строго говоря, теорема Гаусса не даёт настоящего решения проблемы построимости, поскольку неизвестно, какие числа вида $2^{2^s} + 1$ являются простыми. Однако теорема Гаусса даёт, например, быстрый алгоритм выяснения построимости числа $\cos(2\pi/n)$.

(b) Для практики приближённые методы вычисления тригонометрических функций и решения уравнений более полезны, чем радикальные формулы. Кроме того, уравнения степени выше 4 разрешимы при помощи трансцедентных функций (см. метод Виета в п. 4.2 и [PSo]; о развитии этих идей рассказывается, например, в [Sk10]). Однако проблема разрешимости в радикалах интересна как пробная задача современных теорий символьных вычислений и сложности вычислений.

5.1.3 Неразрешимость в радикалах: формулировки (2)

Следующее утверждение даёт достаточное условие разрешимости уравнений третьей степени «в вещественных радикалах».

Утверждение о разрешимости в вещественных радикалах. *Если многочлен третьей степени с рациональными коэффициентами имеет ровно один вещественный корень, то этот корень можно получить на вещественном калькуляторе*[1]*. Более того, это можно сделать так, чтобы извлечение корня происходило только два раза, один раз второй и один раз третьей степени.*

Это утверждение доказывается *методом дель Ферро* (оно вытекает из теоремы, приведённой в подсказке к задаче 4.2.4, и результата задачи 8.1.5 (d)).

Теорема 5.2 (о неразрешимости в вещественных радикалах)**.** *Существует многочлен 3-й степени с рациональными коэффициентами (например,* $x^3 - 3x + 1$*), ни один из корней которого невозможно получить на вещественном калькуляторе.*

Эта теорема доказана в п. 5.5.3.

Следствие. *Трисекция угла невозможна на вещественном калькуляторе, или, формально, на нём невозможно получить число* $\cos(\alpha/3)$*, имея число* $\cos\alpha$ *(например, для* $\alpha = 2\pi/3$*).*

Доказательство. По формуле 4.1.5 (a) косинуса тройного угла каждое из чисел $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ удовлетворяет уравнению $8y^3 - 6y + 1 = 0$. Замена $x = 2y$ превращает его в уравнение $x^3 - 3x + 1 = 0$. Значит, по теореме ни одно из них невозможно получить на вещественном калькуляторе. □

Перейдём теперь к формулам, которые могут содержать комплексные числа.

Определение комплексного калькулятора. *Комплексный* калькулятор имеет те же кнопки, что и вещественный, но оперирует с комплексными числами и при нажатии кнопки $\sqrt[n]{\ }$ выдаёт все значения корня. На комплексном калькуляторе *можно получить число*, если на нём можно получить множество чисел, содержащих заданное число.

[1] Стандартная терминология: уравнение *разрешимо в вещественных радикалах.*

Оказывается, уравнение третьей степени (например, x^3-3x+1), неразрешимое на вещественном калькуляторе, разрешимо на комплексном.

Утверждение о разрешимости в комплексных радикалах. *Все корни любого многочлена третьей или четвёртой степени с рациональными коэффициентами можно получить на комплексном калькуляторе*[2]. *Более того, это можно сделать так, чтобы извлечение корня происходило только*

- *два раза, причём один раз третьей степени и один раз второй — для многочлена третьей степени;*
- *четыре раза, причём один раз третьей степени и три раза второй — для многочлена четвёртой степени.*

Это утверждение доказывается *методами дель Ферро и Феррари* (оно вытекает из теорем, приведённых в указании к задачам 4.2.4 и 4.2.7).

Однако аналог этого утверждения для более высоких степеней неверен.

Теорема 5.3 (Галуа)**.** *Существует многочлен 5-й степени с рациональными коэффициентами (например, x^5-4x+2), ни один из корней которого невозможно получить на комплексном калькуляторе*[3].

Из приведённых теорем о неразрешимости тривиально следует, что *для любого $n \geqslant 3$ ($n \geqslant 5$) существует многочлен n-й степени, один из корней которого невозможно получить на вещественном (комплексном) калькуляторе.* Более сложно доказывается аналог этого утверждения с заменой слов «один из корней» на «ни один из корней». При этом корни *некоторых* уравнений высоких степеней вполне могут получаться на калькуляторе, см. например, п. 5.3.3.

Теорема Галуа вытекает из следующего результата. Он интересен и нетривиален даже для многочленов пятой степени.

[2]Стандартная терминология: уравнение *разрешимо в радикалах.*

[3]Немного ранее была доказана более слабая теорема Руффини–Абеля. Она сложнее формулируется [Al, FT, Sk11, Sk15], но именно она решила знаменитую проблему о разрешимости уравнений в радикалах.

Теорема 5.4 (Кронекера). *Если многочлен простой степени неприводим над $\mathbb{Q}$, имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней невозможно получить на комплексном калькуляторе.*

Эта теорема доказана в п. 5.5.4. Для её доказательства необходимо следующее обобщение теоремы Гаусса (которое доказывается аналогично, см. задачу 5.3.11). Обозначим

$$\varepsilon_n := \cos(2\pi/n) + i\sin(2\pi/n).$$

Теорема 5.5 (Гаусса о понижении). (a) *Если n простое, то на комплексном калькуляторе можно получить ε_n так, чтобы корни извлекались только $(n-1)$-й степени.*

(b) *Для любого n на комплексном калькуляторе можно получить ε_n так, чтобы корни извлекались только степеней, строго меньших n.*

Вещественный аналог теоремы Кронекера следующий.

Теорема 5.6 (Сильная вещественная теорема о неразрешимости). *Если многочлен простой нечётной степени неприводим над $\mathbb{Q}$ и имеет более одного вещественного корня, то ни один из его корней невозможно получить на вещественном калькуляторе.*

Доказательство этой «вещественной» теоремы приведено в п. 5.5.5. Оно *сложнее* доказательства «комплексной» теоремы Кронекера.

5.1.4 План параграфа

Этот параграф не обязательно изучать подряд. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана. К плану разумно вернуться, если читатель потеряет нить изложения.

Пункт 5.2 независим от остального текста (т. е. он не используется в остальном тексте и для его изучения достаточно прочитать п. 5.1). В п. 5.2.3 приводится переформулировка теоремы Гаусса (упомянутая в п. 5.1.2).

Этот несложный результат (доказанный лишь в XIX веке) показывает, что из непостроимости числа $\cos(2\pi/n)$ вытекает непостроимость правильного n-угольника циркулем и линейкой. Для доказательства этого результата можно рассмотреть все возможные случаи появления новых объектов (точек, прямых, окружностей) и показать, что координаты всех построенных точек и коэффициенты уравнений всех проведённых прямых и окружностей являются построимыми. Детали читатель сможет восполнить самостоятельно или найти в [Kol, CR, Ma, Pr07-2]. Ср. п. 14.3.

5.3 Доказательство построимости в теореме Гаусса

В п. 5.3.1 и п. 5.3.3 доказана построимость в теореме Гаусса. В п. 5.3.2 идеи из п. 5.3.3 иллюстрируются на примерах и задачах. Материал п. 5.3.4 не используется далее.

5.3.1 Переформулировка построимости в теореме Гаусса (2)

Начнём с простых задач, подводящих к основному результату этого пункта — лемме о комплексификации.

5.3.1. Число $\cos(2\pi/n)$ вещественно построимо для n =3, 4, 5, 6, 8, 10, 15.

5.3.2. Лемма об умножении (вещественная версия).
(a) Если число $\cos(2\pi/n)$ вещественно построимо, то число $\cos(\pi/n)$ вещественно построимо.
(b) Если числа $\cos(2\pi/n)$ и $\cos(2\pi/m)$ вещественно построимы и m, n взаимно просты, то число $\cos(2\pi/mn)$ вещественно построимо.

Из этой леммы вытекает, что вещественная построимость в теореме Гаусса следует из вещественной построимости чисел $\cos(2\pi/n)$ для простых n вида $2^{2^s}+1$.

Определение построимости. Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе так, чтобы при этом извлекались корни только второй степени.

5.3.3. Число $\cos(2\pi/n)$ построимо тогда и только тогда, когда число $\varepsilon_n := \cos(2\pi/n) + i\sin(2\pi/n)$ построимо.

5.3.4. (a) **Лемма о комплексификации.** Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.

(b)* Можно ли получить число e на калькуляторе, если уже есть число $e + \pi i$? (Используйте без доказательства тот факт, что числа e и π невозможно получить на калькуляторе.)

Из этой леммы вытекает, что вещественное число построимо тогда и только тогда, когда оно вещественно построимо[4]. Значит, построимость в теореме Гаусса достаточно доказать с заменой «вещественной построимости» на «построимость».

5.3.2 Метод резольвент Лагранжа (2)

5.3.5. (a) Число ε_5 построимо.

(b) На комплексном калькуляторе можно получить число ε_7 так, что при этом извлекаются только корни второй и третьей степени.

(b′)* Можно ли получить на комплексном калькуляторе число ε_7 так, что при этом извлекаются только корни второй и третьей степени, причём только по одному разу?

(c) На комплексном калькуляторе можно получить число ε_{11} так, что при этом извлекаются только корни второй и пятой степени.

(d) Число ε_{17} построимо.

---

[4]Заметим, что на комплексном калькуляторе нет кнопок Re и Im. Однако их можно «реализовать», доказав, что если можно получить число z, то можно получить и $\overline{z}$. Но так будет доказана *построимость* вещественной и мнимой частей, а не их *вещественная построимость*. Для доказательства вещественной построимости нужно научиться извлекать корень из комплексного числа при помощи вещественного калькулятора. Это возможно только для корней второй степени. Если в определении построимости и вещественной построимости допускать извлечения корней третьей степени, то аналог леммы о комплексификации будет неверен (ибо $\varepsilon_9 \in \sqrt[3]{\sqrt[3]{1}}$ получается на комплексном калькуляторе с извлечением корней только третьей степени, а $\cos(2\pi/9)$ не получается на вещественном калькуляторе, см. п. 5.1.3).

Пункты (a), (b) и (b′) можно решить непосредственно. Для решения пунктов (c), (d) уже нужна новая идея, изложенная далее. Оказывается, в задачах 5.3.5 (c, d) (и во многих других ситуациях!) вместо работы с набором корней удобнее работать с некоторыми выражениями от корней — *резольвентами Лагранжа*, которые мы скоро определим.

5.3.6. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны, $\varepsilon_3 = \dfrac{-1+i\sqrt{3}}{2}$):

$$\text{(a)}\quad \begin{cases} x+y+z+t=a,\\ x+y-z-t=b,\\ x-y+z-t=c,\\ x-y-z+t=d; \end{cases} \qquad \text{(b)}\quad \begin{cases} x+y+z+t=a,\\ x+iy-z-it=b,\\ x-y+z-t=c,\\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)}\quad \begin{cases} x+y+z=a,\\ x+\varepsilon_3 y+\varepsilon_3^2 z=b,\\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

Выражения из задачи 5.3.6 и называются *резольвентами Лагранжа*. Они «лучше» корней, поскольку «симметричнее» в следующем смысле.

Решение кубического уравнения при помощи резольвент Лагранжа. Для нахождения корней x, y, z кубического уравнения достаточно найти выражения a, b, c из задачи 5.3.6 (c). (Заметим, что метод дель Ферро из п. 4.2 фактически приводит к тому же результату.) По теореме Виета $a = a(x, y, z)$ — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлен $b = b(x, y, z)$ переходит в $\varepsilon_3 c$, а $c = c(x, y, z)$ в $\varepsilon_3^2 b$ (проверьте!). Значит, многочлены bc и $b^3 + c^3$ не меняются при этой замене. Аналогично они не меняются при замене $z \leftrightarrow y$. Поэтому многочлены bc и $b^3 + c^3$ *симметрические*, т. е. не меняются при любой перестановке переменных. Тогда из теоремы Виета и теоремы о представимости симметрического многочлена в виде многочлена от элементарных симметрических многочленов (утверждение 4.6.3 (c)) следует, что эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая квадратное уравнение, можно получить b^3 и c^3. Далее легко получить сами b и c.

Решение уравнения 4*-й степени при помощи резольвент Лагранжа.* Для нахождения корней x, y, z, t уравнения 4-й степени достаточно найти выражения a, b, c, d от корней из задачи 5.3.6 (a). По теореме Виета a — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлены c^2 и d^2 меняются местами, а многочлен b^2 переходит в себя. При циклической замене $x \to y \to z \to t \to x$ многочлены b^2 и d^2 меняются местами, а многочлен c^2 переходит в себя. Значит, многочлены b^2, c^2, d^2 переставляются при любой перестановке переменных. Поэтому виетовские многочлены от них, т. е.

$$b^2 + c^2 + d^2, \quad b^2c^2 + b^2d^2 + c^2d^2, \quad b^2c^2d^2,$$

симметрические. Тогда эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая кубическое уравнение, можно получить сами b^2, c^2, d^2. Далее легко получить b, c, d.

Сообразите, почему же этот метод не работает для общего уравнения 5-й степени!

5.3.7. (a) Если $x_1, \dots, x_5$ — корни многочлена $f \in \mathbb{Q}[x]$ 5-й степени, то

$$T(y) := \prod_{\tau \in S_5} (y - x_{\tau(1)} - \varepsilon_5 x_{\tau(2)} - \varepsilon_5^2 x_{\tau(3)} - \varepsilon_5^3 x_{\tau(4)} - \varepsilon_5^4 x_{\tau(5)}) \in \mathbb{Q}[\varepsilon_5][y].$$

(b) Для некоторого $G \in \mathbb{Q}[\varepsilon_5][y]$ выполнено равенство $T(y) = G(y^5)$. Такой многочлен G называется *разрешающим многочленом* для f.

(c)* На комплексном калькуляторе можно получить все корни разрешающего многочлена для $f(x) = x^5 + 15x + 11$ (а значит, и самого многочлена f).

5.3.8.* На комплексном калькуляторе можно получить хотя бы один корень уравнения $x^5 + ax + b = 0$ для

(a) $(a, b) = (15, 11)$; (b) $(a, b) = (-5, 52)$; (c) $(a, b) = (35, 36)$;

(d) $(a, b) = \frac{(15 \pm 20c, 44 \mp 8c)}{c^2+1}$, $c \in \mathbb{Q}$, $c \geqslant 0$.

(Для других (a, b) этого сделать нельзя [PSo].)

Идея доказательства построимости числа $\varepsilon := \varepsilon_5$. Во-первых,

$$T_0 := \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1.$$

Сначала докажем построимость числа

$$T_2 := \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8.$$

При замене ε на ε^2 число T_2 переходит в $-T_2$. Значит, T_2^2 не меняется при этой замене. Поэтому T_2^2 не меняется при двукратной и трехкратной таких заменах, т. е. при заменах ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_2^2 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_2^2 и заменим ε^5 на 1. Получим равенство

$$T_2^2 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z}.$$

Так как для любого k число T_2^4 не меняется при замене ε на ε^k, то $a_1 = a_2 = a_3 = a_4$. Поэтому $T_2^2 = a_0 - a_1 \in \mathbb{Z}$. Значит, T_2 построимо.

Обозначим

$$T_1 := \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8 \qquad \text{и} \qquad T_3 := \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8.$$

Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать построимость чисел T_1 и T_3. Сделаем это для T_1; доказательство для T_3 аналогично.

При замене ε на ε^2 число T_1 переходит в $-iT_1$. Значит, T_1^4 при этой замене не меняется. Поэтому T_1^4 не меняется при двукратной и трёхкратной замене такого вида, т. е. при замене ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_1^4 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_1^4 и заменим ε^5 на 1. Получим равенство

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Так как для любого k число T_1^4 не меняется при замене ε на ε^k, то $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Значит, T_1 построимо.

В приведённом рассуждении нужно обосновать вывод равенства $a_1 = a_2 = a_3 = a_4$ и строго определить, что такое «замена ε на ε^2». Обоснование для общего случая трудное; читатель может найти пример такого рассуждения в [E1, § 24]. Поэтому вместо того, чтобы его приводить, мы немного изменим доказательство; именно этим изменением приводимое доказательство отличается от данного в [E1], [PSo, § 6.4]. Для этого вместо того, чтобы работать с *числами*, мы будем работать с *многочленами* и подставлять в них ε в качестве аргумента.

5.3.9. Обозначим $T_1(x) := x + ix^2 - x^4 - ix^8$. Тогда[5]
(a) $iT_1(x^2) \equiv T_1(x) \bmod (x^5 - 1)$;
(b) $T_1^4(x^2) \equiv T_1^4(x) \bmod (x^5 - 1)$;
(c) $T_1^4(x^k) \equiv T_1^4(x) \bmod (x^5 - 1)$ для любого k.

Доказательство построимости числа $\varepsilon := \varepsilon_5$. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Имеем

$$iT_1(x^2) \underset{x^5-1}{\equiv} T_1(x) \quad \Longrightarrow \quad T_1^4(x^2) \underset{x^5-1}{\equiv} T_1^4(x) \quad \Longrightarrow$$
$$\Longrightarrow \quad T_1^4(x^k) \underset{x^5-1}{\equiv} T_1^4(x) \quad \text{для любого } k.$$

Возьмём многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z} + i\mathbb{Z}$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$.

Тогда $a_1 = a_2 = a_3 = a_4$. Поэтому[6] $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$.

Значит, $T_1(\varepsilon)$ построимо. Аналогично $T_2(\varepsilon)$ и $T_3(\varepsilon)$ построимы. □

[5] Два многочлена называются *сравнимыми по модулю многочлена* $x^5 - 1$, если их разность делится на $x^5 - 1$.

[6] Другой способ, предложенный М. Ягудиным:

$$T_1^4(\varepsilon) = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 = a_0 + a_1\varepsilon^2 + a_2\varepsilon^4 + a_3\varepsilon + a_4\varepsilon^3 =$$
$$= a_0 + a_1\varepsilon^3 + a_2\varepsilon + a_3\varepsilon^4 + a_4\varepsilon^2 = a_0 + a_1\varepsilon^4 + a_2\varepsilon^3 + a_3\varepsilon^2 + a_4\varepsilon.$$

Суммируя эти выражения, получим $4T_1^4(\varepsilon) = a_0 - a_1 - a_2 - a_3 - a_4 \in \mathbb{Z} + i\mathbb{Z}$.

5.3.3 Доказательство построимости в теореме Гаусса (3)

Читатель, изучивший (точнее, прорешавший) два предыдущих пункта, подготовлен к доказательству. Напомним, что формально оно независимо от п. 5.3.1, а из п. 5.3.2 используется только лемма 5.3.4 о комплексификации.

Лемма об умножении. (a) *Если ε_n построимо, то ε_{2n} построимо.*

(b) *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{mn} построимо.*

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. □

При решении задач 5.3.5 (a) мы использовали различность остатков от деления чисел $2, 2^2, 2^3, 2^4$ на 5. При решении задач 5.3.5 (c, d) и 5.3.10 (a) мы использовали аналогичное свойство чисел 2 и 11, 6 и 17, 3 и 7. Для общего случая необходимо следующее обобщение.

Теорема 5.8 (о первообразном корне)**.** *Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1}$ различны.*

Указание к доказательству для $p = 2^m+1$ (только этот случай нужен для теоремы Гаусса). Если первообразного корня нет, то сравнение $x^{2^{m-1}} \equiv 1 \bmod p$ имеет $p - 1 = 2^m > 2^{m-1}$ решений. Это противоречит теореме Безу.

Заинтересованный читатель может получить и полное доказательство, см. п. 3.5.

Доказательство построимости в теореме Гаусса. По лемме 5.3.4 о комплексификации и по лемме об умножении достаточно доказать, что ε_n построимо для любого простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме об умножении $\beta := \varepsilon_{n-1}$ построимо. Обозначим

$$\mathbb{Z}[\beta] := \{a_0 + a_1\beta + a_2\beta^2 + \ldots + a_{n-2}\beta^{n-2} \mid a_0, \ldots, a_{n-2} \in \mathbb{Z}\}.$$

Обозначим через g первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \ldots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

Тогда $(T_0 + T_1 + \ldots + T_{n-2})(\varepsilon) = (n-1)\varepsilon$. Кроме того, $T_0(\varepsilon) = -1$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Имеем

$$\beta^r T_r(x^g) \underset{x^n-1}{\equiv} T_r(x) \quad \Longrightarrow \quad T_r^{n-1}(x^g) \underset{x^n-1}{\equiv} T_r^{n-1}(x) \quad \Longrightarrow$$
$$\Longrightarrow \quad T_r^{n-1}(x^k) \underset{x^n-1}{\equiv} T_r^{n-1}(x) \quad \text{для любого } k.$$

Возьмём многочлен $a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_2 = \ldots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$. Значит, $T_r(\varepsilon)$ построимо. □

5.3.11.* Докажите теорему Гаусса о понижении (a,b).

Подсказки

5.3.11. (a) Аналогично доказательству построимости в теореме Гаусса.

(b) Докажем теорему при помощи индукции по n.

Если $n = ab$ для некоторых целых a, b, $0 < a, b < n$, то шаг индукции следует из равенства $\varepsilon_n = \sqrt[a]{\varepsilon}_b$.

Если же n простое, то шаг индукции следует из п. (a).

5.3.4 Эффективные доказательства построимости (4*)

Здесь приводятся другие доказательства построимости в теореме Гаусса и теоремы Гаусса о понижении 5.3.11 (a). Они сложнее вышеприведённых, но дают более реальную возможность получить явные формулы [BK, Saf]. Именно они принадлежит Гауссу. Интересно бы получить явные формулы и при помощи вышеприведённого метода.

Эффективное доказательство построимости в теореме Гаусса для $n = 5$. Сразу выразить число $\varepsilon := \varepsilon_5$ через радикалы трудно,

в F называется *неприводимым* над множеством F, если он не раскладывается в произведение многочленов меньшей степени с коэффициентами в F. Числа $v_1, \ldots, v_n \in \mathbb{C}$ называются *линейно зависимыми над* $\mathbb{Q}$, если найдутся $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$, не все равные нулю, для которых $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$.

В подсказках и указаниях к некоторым задачам этого пункта использован материал [ABG].

5.4.1 Одно извлечение квадратного корня (1)

Перед решением задач этого пункта полезно прорешать п. 4.1.

5.4.1. Представимо ли следующее число в виде $a+\sqrt{b}$, где $a, b \in \mathbb{Q}$:

(a) $\sqrt{3+2\sqrt{2}}$; (b) $\frac{1}{7+5\sqrt{2}}$;

(c) $\sqrt[3]{7+5\sqrt{2}}$; (d) $\cos(2\pi/5)$; (e) $\sqrt[3]{2}$; (f) $\sqrt{2}+\sqrt[3]{2}$;

(g) $\cos(2\pi/9)$; (h)* $\sqrt{2+\sqrt{2}}$; (i)* $\cos(2\pi/7)$.

Задачи 5.4.1 и 5.4.3 интересны в связи с неразрешимостью в радикалах, поскольку нам нужно придумать многочлен, корни которого невозможно получить на калькуляторе, а числа из задачи 5.4.1 являются корнями многочленов (подумайте, каких).

5.4.2. Пусть $r \in \mathbb{R} - \mathbb{Q}$ и $r^2 \in \mathbb{Q}$.

(a) **Лемма о неприводимости.** Многочлен $x^2 - r^2$ неприводим над $\mathbb{Q}$.

(b) **Лемма о линейной независимости.** Если $a, b \in \mathbb{Q}$ и $a + br = 0$, то $a = b = 0$.

(c) Если многочлен имеет корень r, то этот многочлен делится на $x^2 - r^2$.

(d) **Теорема о сопряжении.** Если многочлен имеет корень r, то корнем этого многочлена является также число $-r$.

(e) **Следствие.** Если $a, b \in \mathbb{Q}$ и многочлен имеет корень $a + br$, то корнем этого многочлена является также число $a - br$.

(f) **Следствие.** Если $a, b \in \mathbb{Q}$ и кубический многочлен имеет корень $a + br$, то он имеет рациональный корень.

5.4.3. Утверждение. Если многочлен степени выше второй неприводим над $\mathbb{Q}$, то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

5.5 Доказательства неразрешимости в радикалах

Читатель, изучивший (точнее, прорешавший) предыдущий параграф, подготовлен к доказательствам. Напомним, что формально они независимы от предыдущего параграфа. Для понимания этого параграфа достаточно прочитать п. 5.1.2 и 5.1.3 (кроме того, в п. 5.5.2 понадобится простая лемма 5.3.4 о комплексификации). *План доказательства* в каждом пункте получается из текста пункта пропуском доказательств лемм.

5.5.1 Лемма о калькуляторе и понятие поля (2*)

Если $F \subset \mathbb{C}$, $r \in \mathbb{C}$ и $r^q \in F$ для некоторого целого положительного q, то обозначим

$$F[r] := \{a_0 + a_1 r + a_2 r^2 + \ldots + a_{q-1} r^{q-1} \mid a_0, \ldots, a_{q-1} \in F\}.$$

Лемма о калькуляторе. *Пусть $F \in \{\mathbb{R}, \mathbb{C}\}$. Число $x \in F$ можно получить на F-калькуляторе тогда и только тогда, когда существуют такие $r_1, \ldots r_{s-1} \in F$ и такие простые $q_1, \ldots q_{s-1}$, что*

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_{s-1} \subset F_s \ni x,$$

где $r_k^{q_k} \in F_k$, $r_k \notin F_k$ и $F_{k+1} = F_k[r_k]$ для любого $k = 1, \ldots, s-1$.

Такая последовательность называется *башней* (радикальных) *расширений.*

Эта лемма доказывается несложно (аналогично леммам о калькуляторе из п. 5.4).

В этом пункте *полем* называется подмножество множества $\mathbb{C}$, замкнутое относительно операций сложения, умножения, вычитания и деления на ненулевое число. Общепринятое название: числовое поле (а *полем* в математике называется немного другой объект). Это понятие полезно для нас тем, что теорема делении с остатком верна для многочленов с коэффициентами в поле.

Если F — поле, q простое, $r \notin F$ и либо $F = \mathbb{Q}$, либо $\varepsilon_q \in F$, то многочлен $t^q - r^q$ неприводим над F (это фактически доказано в леммах о линейной независимости далее в п. 5.5.3 и 5.5.4 аналогично лемме о неприводимости 5.4.22 (а) и задаче 5.4.27). Тогда $F[r]$ — поле.

Напомним, что $\varepsilon_n := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

5.5.2 Доказательство непостроимости в теореме Гаусса (3*)

Так как $\varepsilon_n = \varepsilon_{nk}^k$, то из построимости числа ε_{nk} вытекает построимость числа ε_n. Поэтому и по лемме 5.3.4 о комплексификации для доказательства вещественной непостроимости в теореме Гаусса достаточно показать, что ε_n непостроимо для

(A) простого числа n, не представимого в виде $2^m + 1$;

(B) квадрата простого числа, т. е. $n = p^2$.

Лемма о степенях двойки. *Если неприводимый над $\mathbb{Q}$ многочлен P с рациональными коэффициентами имеет построимый корень, то $\deg P$ есть степень двойки.*

Эта лемма доказана далее. Для её применения нужны следующие результаты.

Признак Эйзенштейна. *Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$.*

Лемма Гаусса. *Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.*

И признак Эйзенштейна, и лемма Гаусса легко доказываются переходом к многочленам с коэффициентами $\mathbb{Z}_p$ (для леммы Гаусса рассмотрим разложение $P = P_1P_2$ данного полинома P над $\mathbb{Q}$, возьмём такие целые n_1 и n_2, что и n_1P_1, и n_2P_2 имеют целые коэффициенты, и возьмём простой делитель p числа n_1n_2).

Доказательство непостроимости числа ε_n. Непостроимость числа ε_n следует из леммы о калькуляторе и леммы о степенях двойки для корня ε_n многочлена

- $P(x) := x^{n-1} + x^{n-2} + \ldots + x + 1$ в случае (A) и
- $P(x) := x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1$ в случае (B).

Неприводимость этих многочленов $P(x)$ над $\mathbb{Q}$ вытекает из их неприводимости над $\mathbb{Z}$ и леммы Гаусса. Неприводимость этих многочленов $P(x)$ над $\mathbb{Z}$ вытекает из неприводимости многочленов $P(x+1)$ над $\mathbb{Z}$. Последняя неприводимость доказывается применением

признака Эйзенштейна. Выполнение предположений признака Эйзенштейна для многочленов $P(x+1)$ легко проверяется с помощью сравнения $(a+b)^p \equiv a^p + b^p \bmod p$. □

Лемма о степенях двойки является случаем $k = 1$ следующего утверждения.

Обобщённая лемма о степенях двойки. *Если*

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_{s-1} \subset F_s \ni \alpha,$$

где $r_k^2 \in F_k$, $r_k \notin F_k$ *и* $F_{k+1} = F_k[r_k]$ *для любого* $k = 1, \ldots, s-1$, *то для каждого* $k = 1, 2, \ldots, s$ *степень любого неприводимого над* F_k *многочлена с коэффициентами из* F_k *и корнем* α *есть степень двойки.*

Доказательство. Индукция по k вниз. База $k = s$ очевидна. Докажем шаг. Для $j \in \{k, k+1\}$ обозначим через P_j любой неприводимый над F_k многочлен с коэффициентами из F_k и корнем α. Предположение индукции заключается в том, что $\deg P_{k+1}$ есть степень двойки. Будем рассматривать делимость и НОД в F_{k+1}. Так как $P_k(\alpha) = 0$, то многочлен P_k делится на P_{k+1}.

Будем использовать следующий простой результат.

Лемма о сопряжении. *Пусть* $F \subset \mathbb{C}$ *— поле,* $r \in \mathbb{C} - F$ *и* $r^2 \in F$. *Определим отображение сопряжения* $\bar{\cdot} : F[r] \to F[r]$ *формулой* $\overline{x + yr} := x - yr$. *Это отображение корректно определено,* $\overline{z+w} = \overline{z} + \overline{w}$ *и* $\overline{zw} = \overline{z} \cdot \overline{w}$.

Применим эту лемму о сопряжении к $F = F_k$ и $F[r] = F_{k+1}$. Получим, что $P_k = \overline{P_k}$ делится на $\overline{P_{k+1}}$. Обозначим $D := \gcd(P_{k+1}, \overline{P_{k+1}})$. Так как многочлен P_{k+1} неприводим над F_{k+1} и делится на D, то либо $D = 1$, либо $P_{k+1} = D$.

Во втором случае из того, что $\overline{D} = D$, получаем, что $P_{k+1} = D \in F_k[x]$. Значит, $P_k = P_{k+1}$ и шаг индукции доказан.

В первом случае P_k делится на $M := P_{k+1}\overline{P_{k+1}}$. Из того, что $\overline{M} = M$, следует, что $M \in F_k[x]$. Так как многочлен P_k неприводим над F_k, то $P_k = M$. Значит, $\deg P_k = 2 \deg P_{k+1}$ есть степень двойки. □

5.5.3 Доказательство неразрешимости в вещественных радикалах (3*)

Основная лемма (вещественный случай). *Пусть q простое, $F \subset \mathbb{R}$ — поле, $r \in \mathbb{R} - F$ и $r^q \in F$.*

(a) (линейная независимость). *Если $P(r) = 0$ для некоторого многочлена $P \in F[\varepsilon_q][t]$ степени меньше q, то $P = 0$.*

(b) (сопряжение). *Если $P \in F[\varepsilon_q][t]$ и $P(r) = 0$, то $P(r\varepsilon_q^k) = 0$ для любого $k = 0, 1, \ldots, q-1$.*

Доказательство части (a). Оба многочлена P и $t^q - r^q$ с коэффициентами из $F[\varepsilon_q]$ имеют корень r. Значит, их НОД имеет корень r и степень k, $0 < k \leqslant \deg P < q$. Все корни многочлена $t^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Свободный член наименьшего общего делителя равен произведению некоторых k из этих корней. Тогда $r^k \in F[\varepsilon_q]$. Так как q простое, то $kx + qy = 1$ для некоторых целых x, y. Тогда $r = (r^k)^x (r^q)^y \in F[\varepsilon_q]$.

Поэтому[10] $r^2, r^3, \ldots, r^{q-1} \in F[\varepsilon_q]$. Составим таблицу $a_{kl} \in F$ размера $q \times (q-1)$ из разложений чисел r^k по степеням числа ε_q:

$$r^k = \sum_{l=0}^{q-2} a_{kl} \varepsilon_q^l, \quad 0 \leqslant k \leqslant q-1.$$

При помощи нескольких операций прибавления к одной строке другой, умноженной на число из F, можно получить таблицу с нулевой строкой.

Значит, имеется ненулевой многочлен P_1 степени меньше q с коэффициентами из F и корнем r. Дальнейшие рассуждения аналогичны первому абзацу этого доказательства. Нужно только заменить P на P_1 и $F[\varepsilon_q]$ на F. Получаем, что $r \in F$, — противоречие.

Доказательство части (b). Так как $P(r) = 0$, то остаток от деления многочлена $P(t)$ на $t^q - r^q$ принимает значение 0 в точке r. Значит, по части (a) этот остаток равен нулю. Отсюда вытекает заключение части (b).

[10] Другая запись этого абзаца с использованием понятия размерности: тогда $\dim_F F[r] \leqslant \dim_F F[\varepsilon_q] \leqslant q - 1$.

Доказательство теоремы о неразрешимости в вещественных радикалах. Предположим, напротив, что некоторый корень x_0 уравнения $x^3-3x+1=0$ можно получить на вещественном калькуляторе. Тогда по лемме о калькуляторе для $F=\mathbb{R}$ существует наименьшее s, для которого найдётся башня расширений, последнее поле $F_s\subset\mathbb{R}$ которой содержит некоторый корень x_1 уравнения $x^3-3x+1=0$ (возможно, $x_1\neq x_0$). Обозначим $F:=F_{s-1}$, $q:=q_{s-1}$ и $r:=r_{s-1}$. Тогда $x_1=H(r)$ для некоторого многочлена H с коэффициентами в F степени больше 0 и меньше q.

Применим часть (b) основной леммы (вещественный случай) к многочлену $P(t):=H(t)^3-3H(t)+1$. Так как $H(r)^3-3H(r)+1=0$, то $H(r\varepsilon_q^k)$ является корнем уравнения $x^3-3x+1=0$ для любого $k=0,1,\dots,q-1$. Если $H(r\varepsilon_q^k)=H(r\varepsilon_q^l)$ для некоторых k,l, $0\leqslant k<l\leqslant q-1$, то по части (a) основной леммы (вещественный случай) получим, что $\deg H=0$ — противоречие. Итак, числа $H(r\varepsilon_q^k)$, $0\leqslant k\leqslant q-1$, — попарно различные корни уравнения $x^3-3x+1=0$. Значит, $q=2$ или $q=3$.

Если $q=2$, то по теореме Виета третий корень уравнения $x^3-3x+1=0$ равен $-2H(0)\in F$ — противоречие с минимальностью числа s.

Если $q=3$, то возьмём $h_0,h_1,h_2\in F$, для которых $h_0+h_1t+h_2t^2=H(t)$. Так как

$$H(r\varepsilon_3)\in\{2\cos(2\pi/9),2\cos(8\pi/9),2\cos(14\pi/9)\}\subset\mathbb{R},$$

то $0=\operatorname{Im}H(r\varepsilon_3)=\frac{\sqrt{3}}{2}(h_1r-h_2r^2)$. Так как $r\notin F$, то $h_1=h_2=0$. Противоречие с неравенством $\deg H>0$[11]. □

5.5.4 Доказательство неразрешимости в радикалах (4*)

Из следующих лемм только основная лемма (части (a), (c)) и лемма об уплотнении прямо используются в доказательстве теоремы Кронекера. Часть (b) основной леммы используется для доказательства части (c).

[11] *Другое завершение доказательства для $q=3$.* Если $q=3$, то из равенство $\overline{\varepsilon_3}=\varepsilon_3^2$ вытекает, что $\overline{H(r\varepsilon_3)}=H(r\varepsilon_3^2)$. Это противоречит вещественности и различности последних двух чисел.

6.3.2. (a) **Весовое неравенство Коши.** Если $a_1 > 0, \ldots, a_n > 0$ и $a_1 + \ldots + a_n = 1$, то $a_1x_1 + \ldots + a_nx_n \geqslant x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$. (Это обобщение неравенства Юнга 6.2.5 (b).)

(b)* Определим *среднее степенное порядка* m *чисел* $x_1, \ldots, x_n$ *с весами* $a_1, \ldots, a_n > 0$, где $a_1 + \ldots + a_n = 1$, как

$$S_m := \sqrt[m]{a_1x_1^m + \ldots + a_nx_n^m} \quad \text{при} \quad m \neq 0, \quad S_0 := x_1^{a_1} \cdot \ldots \cdot x_n^{a_n},$$
$$S_{-\infty} := \min\{x_1, \ldots, x_n\} \quad \text{и} \quad S_{+\infty} := \max\{x_1, \ldots, x_n\}.$$

Докажите, что $S_a \leqslant S_b$ при $a \leqslant b$ для любых $a, b \in \mathbb{R} \cup \{-\infty, +\infty\}$.

(c) Остаётся ли справедливым неравенство $S_a \leqslant S_b$ при $a \leqslant b$ и любых положительных значениях переменных $x_1, \ldots, x_n$, если одно из чисел a_i меньше нуля?

6.3.3. Докажите неравенства

(a) $\frac{a_1^2}{a_2} + \frac{a_2^2}{a_3} + \ldots + \frac{a_n^2}{a_1} \geqslant a_1 + a_2 + \ldots + a_n$;

(b) $\frac{a_1^2}{a_1+a_2} + \frac{a_2^2}{a_2+a_3} + \ldots + \frac{a_n^2}{a_n+a_1} \geqslant \frac{1}{2}(a_1 + a_2 + \ldots + a_n)$.

6.3.4. Докажите неравенство

$$\frac{a^2}{b(a+c)} + \frac{b^2}{c(b+d)} + \frac{c^2}{d(c+a)} + \frac{d^2}{a(d+b)} \geqslant 2.$$

6.3.5. Докажите неравенства

(a) $a^3b + b^3c + c^3a \geqslant abc(a + b + c)$;

(b) $a^3b^2 + b^3c^2 + c^3a^2 \geqslant abc(ab + bc_ca)$.

6.3.6. Докажите неравенства

(a) $\frac{a_1^3}{a_1+a_2} + \frac{a_2^3}{a_2+a_3} + \ldots + \frac{a_n^3}{a_n+a_1} \geqslant \frac{1}{2}(a_1^2 + a_2^2 + \ldots + a_n^2)$;

(b) $\frac{a}{b+2c+d} + \frac{b}{c+2d+a} + \frac{c}{d+2a+b} + \frac{d}{a+2b+c} \geqslant 1$.

6.3.7. Докажите неравенства

(a) $\frac{a}{b+c} + \frac{b}{c+d} + \frac{c}{d+a} + \frac{d}{a+b} \geqslant 2$;

(b) $\frac{a+c}{a+b} + \frac{b+d}{b+c} + \frac{c+a}{c+d} + \frac{d+b}{d+a} \geqslant 4$.

6.3.8. Если $ab + bc + cd + da = 1$, то

$$\frac{a^3}{b+c+d} + \frac{b^3}{c+d+a} + \frac{c^3}{d+b+a} + \frac{d^3}{a+b+c} \geqslant \frac{1}{3}.$$

Применения основных неравенств

[DY] *Дворянинов С.*, *Ясиновый Э.* Как получаются симметрические неравенства // Квант. 1985. № 7. С. 33–36.

[Gor09] *Горелов М.* Неравенства и ... параллельный перенос // Квант. 2009. № 2. С. 41–45.

[Khr00] *Храбров А. И.* Вокруг монгольского неравенства // Мат. Просвещение. 2003. No 7. С. 149–162.

Геометрическая интерпретация

[AK] *Алексеев Р.*, *Курляндчик Л.* Стороны треугольника. // Квант. 1993. № 5. С. 69–70. Квант (N5,1993)

Следующие классические источники ориентированы не на школьников.

[BB] *Беккенбах Э.*, *Беллман Р.* Неравенства. М.: Мир, 1965.

[HLP] *Харди Г. П.*, *Литтльвуд Д. Е.*, *Полиа Г.* Неравенства. М.: ИЛ, 1948.

[MO] *Маршалл А.*, *Олкин И.* Неравенства: теория мажоризации и её приложения. М.: Мир, 1983.

7 Последовательности и пределы

Этот параграф почти независим от остальной части книги. В других местах из него используются лишь простые факты.

7.1 Конечные суммы и разности (3)

Последовательностью сумм последовательности $\{a_n\}_{n=1}^{\infty}$ называется последовательность $b_n = \Sigma a_n := a_1 + \ldots + a_n$, а *последовательностью разностей* — последовательность $c_n = \Delta a_n := a_{n+1} - a_n$.

Например, $\Delta 2^n = 2^n$ и $\Sigma 2^n = 2^{n+1} - 2$.

(Сумма и разность — аналоги *интеграла* и *производной*.)

В этом пункте n обозначает номер члена последовательности, «по которому» берётся сумма и разность. Так, например, $\Delta 2^k = 0$.

7.1.1. Найдите

(a) Δn^k для каждого целого $k \geqslant -1$; (b) $\Delta \cos n$; (c) $\Delta(n \cdot 2^n)$.

7.1.2. Найдите

(a) $\Sigma \sin n$; (b) $\Sigma \frac{1}{n(n+1)\ldots(n+k)}$ для каждого целого $k > 0$.

7.1.3. Какие из указанных равенств выполняются для некоторой непостоянной последовательности a_n:

(a) $\Delta a_n = 0$; (b) $\Delta a_n = 1$; (c) $\Delta a_n = a_n$;

(d) $\Sigma a_n = a_n$; (e) $\Sigma \Delta a_n = a_n$; (f) $\Delta \Sigma a_n = a_n$?

7.1.4. (a) Найдите $\sum\limits_{k=0}^{n} (-1)^k k^2 \binom{n}{k}$.

(b) **Лемма.** k-я разность многочлена k-й степени есть постоянная, а $(k+1)$-я равна 0.

(c) (Загадка.) Выразите $\Delta^k a_n$ через $a_n, a_{n+1}, \ldots, a_{n+k}$.

(d) **Лемма.** Равенство $\Delta^k a_n = 0$ имеет место тогда и только тогда, когда a_n — многочлен от n степени не выше $k-1$.

(e) Для некоторого многочлена $P_\lambda(n)$, имеющего степень l при $\lambda \neq 1$ и степень $l-1$ при $\lambda \neq 1$, выполняется равенство $\Delta(n^l \lambda^n) = P_\lambda(n)\lambda^n$.

(f) **Формула Лейбница.** Справедливо равенство

$$\Delta(a_n b_n) = a_{n+1}\Delta b_n + b_n \Delta a_n.$$

(g)* Сформулируйте и докажите аналогичную формулу для $\Delta^l(a_n b_n)$.

7.1.5. (a) Найдите Σn^k для $k = 0, 1, 2, 3, 4$.

(b) **Лемма.** Последовательность сумм многочлена степени $k \geqslant 0$ есть многочлен степени $k+1$.

7.1.6. (a) Найдите $\Sigma(n \cdot 2^n)$.

7.2.5. *Ответы,* в которых $a := a_2$:

(a) $(a-10)3^{n-1} + (15-a)2^{n-1}$;

(b) $\left(a - \frac{19}{2}\right)3^{n-1} + (14-a)2^{n-1} + \frac{1}{2}$;

(c) $\left(a - \frac{37}{4}\right)3^{n-1} + (13-a)2^{n-1} + \frac{n}{2} + \frac{3}{4}$;

(d) $(n+a-14)3^{n-1} + (18-a)2^{n-1}$;

(e) $(a-8)3^{n-1} + (14-a-n)2^{n-1}$;

(f) $\left(\frac{n^2-7n}{2} + a - 1\right)3^{n-1} + (9-a)2^{n-1}$.

7.3 Конкретная теория пределов (4*)

Задачи этого пункта интересны не только как простейший способ разобраться в теории пределов. Похожие задачи о конкретных, хотя и грубых оценках часто возникают и на олимпиадах, и в прикладной математике, и в теоретической математике.

В решении этих задач нельзя пользоваться функциями $\sqrt[n]{x}$, a^x, $\log_a x$, $\arcsin x$ и т. п. без определения этих функций (поскольку для их определения — например, для доказательства существования такого x, что $x^2 = 2$, — фактически нужно эти задачи решить). Исключение: если некоторая функция используется в условии, то её можно использовать и в решении. Можно пользоваться без доказательства свойствами неравенств.

7.3.1. Найдите хотя бы одно такое N, чтобы для любого $n > N$ выполнялось неравенство $a_n > 10^9$, если

(a) $a_n = \sqrt{n}$; (b) $a_n = n^2 - 3n + 5$; (c) $a_n = 1{,}02^n$;

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

7.3.2. Неравенство Бернулли. Докажите, что $(1+x)^a \geqslant 1 + ax$ для любых $x \geqslant -1$ и

(a) целого $a \geqslant 1$; (b) рационального $a \geqslant 1$;

(c) действительного $a \geqslant 1$.

7.3.3. Найдите хотя бы одну пару таких a и N, чтобы для любого $n > N$ выполнялось неравенство $|a_n - a| < 10^{-8}$, если

(a) $a_n = \frac{n^2-n+28}{n-2n^2}$; (b) $\sqrt{5 + \dfrac{2}{n}}$; (c) $a_n = n\left(\sqrt{1 + \frac{1}{n}} - 1\right)$;

(h) Используйте п. (g).

(i) Найдите и используйте аналогичное равенство для $\frac{1}{(\log_2 n)^t} - \frac{1}{(\log_2(n+1))^t}$.

(j) Используйте признак расходимости Раабе 7.6.2 (e, f).

7.6.3. (b) См. задачу 7.6.4.

(c) Решение аналогично задаче 7.6.4.

(d, e) Используйте признак Дирихле-Абеля 7.6.5 (b).

(f) «Варьируйте» на тему признака Дирихле-Абеля 7.6.5 (b) и его доказательства.

7.6.5. (a) Аналогично задаче 7.6.4.

(b) Используйте преобразование Абеля 7.5.6 (c).

7.7 Примеры трансцендентных чисел (3*)

7.7.1. Следующие числа иррациональны:

(a) $e := \sum\limits_{n=0}^{\infty} \frac{1}{n!}$; (b) $\lambda := \sum\limits_{n=0}^{\infty} 2^{-n!}$; (c) $\mu := \sum\limits_{n=0}^{\infty} 2^{-2^n}$.

(Используемые здесь бесконечные суммы определены в п. 7.5.)

7.7.2. (e), (λ), (μ) Ни одно из чисел e, λ, μ не является корнем квадратного уравнения с целыми коэффициентами.

7.7.3. Для любого рационального числа p/q, не являющегося корнем многочлена f степени t с целыми коэффициентами, выполнено неравенство $|f(p/q)| \geqslant q^{-t}$.

Число x называется *трансцендентным*, если оно не является корнем уравнения $a_t x^t + a_{t-1}x^{t-1} + \ldots + a_1 x + a_0 = 0$ с целыми коэффициентами $a_t \neq 0$, $a_{t-1}, \ldots, a_0$.

7.7.4. (a) **Теорема Лиувилля.** Число λ трансцендентно.

(b) **Общая теорема Лиувилля.** Для любых многочлена степени t с рациональными коэффициентами и его иррационального корня α существует такое $C > 0$, что для любых целых p, q выполнено неравенство $\left|\alpha - \frac{p}{q}\right| > Cq^{-t}$.

7.7.5. (a) Число μ не является корнем кубического уравнения с целыми коэффициентами.

(b) Справедливо равенство $\mu^q = \sum\limits_{n=0}^{\infty} d_n(q)2^{-n}$, где $d_n(q)$ есть количество упорядоченных представлений числа n в виде суммы q степеней двойки (не обязательно различных степеней):

$$d_n(q) = \#\{(w_1, \ldots, w_q) \in \mathbb{Z}^q \mid n = 2^{w_1} + \ldots + 2^{w_q} \text{ и } w_1, \ldots, w_q > 0\}.$$

Например, $d_3(2) = 2$, поскольку $3 = 2^0 + 2^1 = 2^1 + 2^0$. По определению полагаем $d_0(0) = 1$.

(c) Справедливо неравенство $d_n(q) \leqslant (q!)^2$.

(d) Число μ трансцендентно.

Следующая задача — удачная тема для исследовательских работ старшеклассников. Описание удачных примеров этой деятельности читатель может найти в материалах Московской математической конференции школьников [M]. Пункты (a), (b), (c) заведомо не претендуют на научную новизну. Решение остальных пунктов мне неизвестно, но наверняка доступно сильному старшекласснику.

7.7.6. Является ли число $\sum\limits_{n=0}^{\infty} a_n$ трансцендентным, если

(a) $a_n = 2^{-3^n}$;

(b) $a_n = d_n 2^{-2^n}$ для некоторой ограниченной последовательности $d_n > 0$ целых чисел;

(c) $a_n = 2^{-f_n}$, где $f_{n+2} = f_{n+1} + f_n$, $f_0 = f_1 = 1$ — последовательность Фибоначчи;

(d)* $a_n = 2^{-[1,1^n]}$; (e)* $a_n = n2^{-2^n}$; (f)* $a_n = 2^{n-2^n}$;

(g)* $a_n = (-1)^n 2^{-2^n}$.

Подсказки

7.7.1. (a) Предположим, напротив, что существует линейный многочлен $f(x) = bx + c$ с целыми коэффициентами $b \neq 0$ и c, для которого $f(e) = 0$. Обозначим $e_s = \sum\limits_{n=0}^{s} \frac{1}{n!}$. Заметим, что уравнение $bx + c = 0$ имеет только один корень, значит, $f(e_s) \neq 0$. Мы получим

8.1.1. (a) График любого кубического многочлена имеет центр симметрии.

(b) Найдите координаты центра симметрии графика функции $y = -2x^3 - 6x^2 + 4$.

(c) Верно ли, что график любого многочлена 4-й степени имеет ось симметрии?

Известно, что квадратное уравнение $ax^2 + bx + c = 0$ имеет два решения при $D > 0$, имеет одно решение при $D = 0$ и не имеет решений при $D < 0$. Здесь $D = b^2 - 4ac$. Способ нахождения *количества* решений кубического уравнения *без решения самого уравнения* легко вывести напрямую (задача 8.1.5 ниже). В частности, для решения следующих задач не требуется знать формулы для корней кубического уравнения; более того, решения, не использующие этих формул, *проще* вывода указанных формул. Ср. с задачами 8.1.7, 8.2.1 ниже.

8.1.2. Сколько (вещественных) решений имеет уравнение

(a) $x^3 + 2x + 7 = 0$; (b) $x^3 - 4x - 1 = 0$?

8.1.3.* **Теорема о промежуточном значении.** Для многочлена f и чисел $a < b$ если $f(a) > 0 > f(b)$, то существует такое $c \in (a, b)$, что $f(c) = 0$.

Этой теоремой можно пользоваться в дальнейшем без доказательства.

8.1.4. (a) Уравнение $x^3 + x + q = 0$ имеет ровно одно решение при любом q.

(b) При каком условии на p, q уравнение $x^3 + px + q = 0$ имеет ровно два решения?

(c) Выразите эти два решения через p, q.

8.1.5. (a) Для функции $f(x) = x^3 - 6x + 2$ найдите промежутки возрастания и убывания.

(b) Для той же функции найдите наибольшее и наименьшее значения на отрезке $[0, 3]$.

(c) При каких q уравнение $x^3 - x + q = 0$ имеет ровно одно решение?

Поэтому при любом q уравнение $x^3+x+q=0$ имеет *ровно одно* решение.

8.1.5. (d) *Ответ*: если $p=q=0$, то корень один; иначе обозначим $D := \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$; при $D>0$ корень один, при $D=0$ корней два, при $D<0$ корней три.

8.1.7. (b) *Ответ*: если $p=q=0$, то корень один; иначе обозначим $D := \left(\frac{p}{4}\right)^4 + \left(\frac{q}{3}\right)^3$; при $D>0$ корень один, при $D=0$ корней два, при $D<0$ корней три.

8.2 Элементы анализа для многочленов (2)

8.2.1. (a) **Правило знаков Декарта.** Число *положительных* решений уравнения $p_n x^n + \ldots + p_1 x + p_0 = 0$ не превосходит числа перемен знака в последовательности $p_0, \ldots, p_n$.

(b) Как аналогично правилу знаков Декарта оценить количество *отрицательных* корней данного многочлена?

(c)* Как аналогично правилу знаков Декарта оценить количество корней данного многочлена на данном промежутке $[a,b]$?

(d) **Неравенства Маклорена.** Для $x_1, \ldots, x_n > 0$ обозначим

$$M_k = \sqrt[k]{\frac{\sum\limits_{i_1<\ldots<i_k} x_{i_1}\cdot\ldots\cdot x_{i_k}}{\binom{n}{k}}}.$$

(Заметьте, что M_1 — это среднее арифметическое и M_n — среднее геометрическое.) Тогда $M_1 \geqslant \ldots \geqslant M_n$.

Для решения этих и многих других задач необходимо следующее понятие.

Производной f' многочлена f называется многочлен, полученный подстановкой $y=x$ в многочлен $\frac{f(y)-f(x)}{y-x}$ от двух переменных x, y. (Сообразите, почему это многочлен.)

Геометрический смысл: уравнение *касательной* к графику многочлена f в точке a есть $y = f'(a)(x-a)+f(a)$. (Формально, это можно воспринимать как определение касательной.)

8.5.8. (a) Минимальный модуль корня многочлена $\sum_{k=0}^{n} \frac{x^k}{k!}$ стремится к бесконечности при $n \to \infty$.

(b) При чётном n многочлен $\sum_{k=0}^{n} \frac{x^k}{k!}$ не имеет вещественных корней, а при нечётном n имеет ровно один вещественный корень.

Подсказки

8.5.1. См., например, [Zo].

8.5.3. Многие классические неравенства доказываются с помощью теоремы 8.5.2 (a). Об этом автор узнал от А. В. Зелевинского. Сейчас этот метод широко известен. Такое решение задачи 8.5.3 приведено после задачи 6.1.4. Неравенства о средних степенных 6.1.4 и Маклорена 8.2.1 (d) можно доказать аналогично.

8.5.4. (b) По п. (a) существует такое R, что $|P(z)| > |P(0)|$ при $|z| > R$. Тогда минимум на круге радиуса R равен глобальному минимуму.

8.5.6, **8.5.7.** Вышеприведённые классические теоремы Ролля, Лагранжа и Тейлора также вытекают из теоремы 8.5.2 (a).

8.6 Применения компактности (4*). *А. Я. Канель-Белов*

В этом пункте задачи посложнее и подсказок поменьше. Однако он будет интересен читателю, так как, насколько нам известно, такая подборка интересных задач по этой важной теме впервые публикуется в неспециальной литературе.

8.6.1. Близкая идея в конечном случае. Запись числа состоит из нулей и единиц. Любой фрагмент «10» числа заменяют на «0001». Докажите, что рано или поздно заменять будет нечего.

8.6.2. Идея компактности. (a) Известно, что человечество живёт вечно, а число людей в каждом поколении конечно. Докажите, что найдётся бесконечная мужская цепочка наследников.

(b) В бесконечном парламенте у каждого парламентария не более трёх врагов. Докажите, что парламент можно разбить на две палаты так, что у каждого парламентария будет не более одного врага в своей палате. (Для конечного парламента эта задача разбирается в задаче 20.5.7 пункта «Полуинварианты».)

(c) Известно, что любую *конечную* карту на плоскости можно правильно раскрасить в 4 цвета. Докажите, что тогда *произвольную* карту на плоскости также можно правильно раскрасить в 4 цвета. (Страны можно считать многоугольниками. Раскраска называется *правильной*, если любые две страны с общим участком границы раскрашены в разные цвета.)

(d) (Загадка.) Прочитайте п. 20.5 «Полуинварианты». Какие утверждения верны для бесконечных множеств, а какие нет?

8.6.3. Для любых M и k найдётся достаточно большое v с таким свойством: если все рёбра полного графа с v вершинами покрашены в M цветов, то найдётся полный подграф с k вершинами, все рёбра которого покрашены в один цвет.

8.6.4. Из любой бесконечной последовательности целых чисел можно выбрать подпоследовательность либо так, чтобы каждый её член делился на предыдущий, либо так, чтобы ни один член не делился на другой.

8.6.5. На плоскости отмечено бесконечное множество точек, никакие три из которых не лежат на одной прямой. Тогда найдётся выпуклая фигура, граница которой проходит через его бесконечное подмножество.

Идеи, с помощью которых доказываются остановки процессов, зачастую работают вместе с идеей компактности, с которой они являются своего рода родственниками.

8.6.6. Существует ли такое n, что любое рациональное число между 0 и 1 представимо в виде $\sum\limits_{i=1}^{n} \frac{1}{a_i}$, где $0 < a_i \in \mathbb{Z}$?

Глава 2

Геометрия

Как правило, параграфы и пункты этой главы можно изучать независимо друг от друга и от остальных частей книги. В тех случаях, когда для решения задач какого-нибудь пункта желательно знакомство с другими материалами, это указывается в начале пункта. Если задачу можно решать разными методами, она приводится в пункте, посвящённом одному из них, а о возможности других решений говорится в комментарии. Помимо обозначений, принятых во всей книге, в данной главе везде, где не оговорено обратное, используются принятые в геометрии обозначения элементов треугольника, описанные в начале параграфа «Треугольник».

9 Треугольник

Всюду в данной главе, кроме специально оговорённых случаев, используются следующие обозначения: ABC — данный треугольник, A_i, B_i, C_i, $i = 1, 2, \ldots,$ — точки на сторонах BC,CA и AB соответственно (или на продолжениях этих сторон, если это оговорено в условии задачи); ω — вписанная окружность, I — её центр, r — её радиус; Ω — описанная окружность, O — её центр, R — её радиус; G — точка пересечения медиан (центр тяжести, центроид), H — точка пересечения высот (ортоцентр). Проведём биссектрисы AI, BI, CI до пересечения с Ω в точках A', B', C' соответственно. Таким образом, A', B', C' — середины дуг AB, BC, CA. *Ортотреуголь-*

ник — треугольник с вершинами в основаниях высот, *серединный треугольник* — треугольник с вершинами в серединах сторон данного треугольника. Перпендикуляр, опущенный из точки A на BC, обозначается $h(A, BC)$.

Окружностью ABC называется окружность, описанная вокруг треугольника ABC.

9.1 Принцип Карно (1). *В. Ю. Протасов, А. А. Гаврилюк*

9.1.1. Теорема Карно. В точках A_1, B_1, C_1, лежащих на сторонах треугольника ABC или на их продолжениях, восставлены перпендикуляры к этим сторонам. Докажите, что они пересекаются в одной точке тогда и только тогда, когда

$$C_1A^2 - C_1B^2 + A_1B^2 - A_1C^2 + B_1C^2 - B_1A^2 = 0.$$

9.1.2. Сформулируйте и докажите обобщённую теорему Карно для произвольных точек плоскости A_1, B_1, C_1, не обязательно лежащих на прямых, содержащих стороны треугольника ABC.

9.1.3.° В каком из следующих случаев перпендикуляры, восставленные к сторонам треугольника в указанных точках, могут не пересекаться в одной точке:

1) A_1, B_1, C_1 — точки касания сторон с вписанной окружностью;

2) A_2, B_2, C_2 — точки касания сторон с соответствующими вневписанными окружностями;

3) A_3, B_3, C_3 — основания биссектрис треугольника?

9.1.4. Пусть вневписанная окружность треугольника касается его стороны AB в точке C_1 и касается продолжений двух других сторон. Аналогично определяются точки A_1 и B_1. Докажите, что перпендикуляры, восставленные к сторонам треугольника в точках A_1, B_1, C_1 пересекаются в одной точке.

9.1.5. На плоскости даны три пересекающиеся окружности. Докажите, что три их общие хорды пересекаются в одной точке.

Примечание. Это утверждение обычно доказывают, используя понятие степени точки (см. п. 10.4). Однако его легко вывести и из обобщённой теоремы Карно.

9.3.7. Все углы треугольника ABC меньше 120°, T — его *точка Торричелли* (т. е. точка, для которой выполнено равенство $\angle ATB = \angle BTC = \angle CTA = 120^\circ$).

(a) Докажите, что прямая Эйлера треугольника ATB параллельна прямой CT.

Указание. Можно воспользоваться задачей 9.3.3.

(b) Докажите, что прямые Эйлера треугольников ATB, BTC и CTA пересекаются в одной точке.

9.3.8. В вершинах остроугольного треугольника проведены касательные к его описанной окружности. Докажите, что центр описанной окружности треугольника, образованного этими тремя касательными, лежит на прямой Эйлера исходного треугольника.

Указания, ответы и решения

9.3.3. Угол C должен быть острым, так как в противном случае точки O и H лежат по разные стороны от AB. Так как расстояние от O до AB равно $R\cos C$, а высота, проведённая из вершины C, равна $AC\sin A = 2R\sin A\sin B$, параллельность прямой Эйлера и прямой AB равносильна равенству $3\cos C = 2\sin A\sin B$. Учитывая, что $\cos C = -\cos(A+B) = \sin A\sin B - \cos A\cos B$, получаем утверждение задачи.

9.3.6. Из условия следует, что степени точки O относительно этих окружностей равны R^2. Кроме того, если AA' и BB' — высоты треугольника, то четырёхугольник $ABA'B'$ вписанный, и, значит, $HA\cdot HA' = HB\cdot HB'$. Поэтому степени точки H относительно всех трёх окружностей также равны, т. е. прямая OH является их общей радикальной осью.

9.4 Формула Карно (2*). *А. Д. Блинков*

Формула Карно (по имени французского математика, физика и политического деятеля Лазаря Карно, 1753–1823) утверждает, что в остроугольном треугольнике сумма расстояний от центра описанной окружности до сторон треугольника равняется сумме радиусов

описанной и вписанной окружностей, т. е. $OM_1+OM_2+OM_3 = R+r$, где M_1, M_2, M_3 — середины BC, CA, AB соответственно. Её доказательство с помощью теоремы Птолемея приводится в п. 10.6 «Теоремы Птолемея и Кези». Здесь мы рассмотрим её применения и ещё один способ её доказательства, в процессе которого будут получены другие важные факты.

9.4.1. Пусть биссектриса угла A пересекает окружность, описанную около треугольника ABC, в точке W, а точка D диаметрально противоположна точке W. Докажите, что

(a) $M_1W = (r_a - r)/2$;

(b) $M_1D = (r_b + r_c)/2$, где r, r_a, r_b, r_c — радиусы вписанной и вневписанных окружностей.

9.4.2. Докажите формулу Карно.

Рассмотрим теперь несколько задач на применение формулы Карно. Если явно не оговорено обратное, то треугольник, заданный в условии, остроугольный.

9.4.3. Докажите, что сумма расстояний от вершин треугольника до ортоцентра равна сумме диаметров его вписанной и описанной окружностей.

9.4.4. Докажите, что в треугольнике ABC выполняются неравенства

(a) $AH + BH + CH \leqslant 3R$;

(b) $3OH \geqslant R - 2r$.

9.4.5. (a) Докажите, что $m_a + m_b + m_c \leqslant \frac{9}{2}R$, где m_a, m_b и m_c — длины медиан треугольника.

(b) Пусть в треугольнике ABC биссектрисы углов A, B и C пересекают описанную окружность в точках W_1, W_2 и W_3 соответственно. Докажите, что $AW_1 + BW_2 + CW_3 \leqslant 6{,}5R - r$.

9.4.6. (a) Докажите, что для углов треугольника выполняется неравенство

$$\frac{3r}{R} \leqslant \cos A + \cos B + \cos C \leqslant \frac{3}{2}.$$

(b) Пусть AH_1, BH_2 и CH_3 — высоты треугольника ABC. Выразите сумму диаметров окружностей, описанных около треугольников AH_2H_3, BH_1H_3 и CH_1H_2, через R и r.

9.4.7. В окружность радиуса R вписан треугольник, а в каждый сегмент, ограниченный стороной треугольника и меньшей из дуг окружности, вписана окружность наибольшего возможного радиуса. Найдите сумму диаметров трёх получившихся окружностей и радиуса окружности, вписанной в треугольник.

9.4.8. (a) Докажите, что в треугольнике ABC выполняется равенство

$$a(OM_2 + OM_3) + b(OM_1 + OM_3) + c(OM_1 + OM_2) = 2pR.$$

(b) **Неравенство Эрдёша.** Пусть h_a — наибольшая высота треугольника ABC. Докажите, что $h_a \geqslant R + r$.

9.4.9. (a) Выведите аналоги формулы Карно для прямоугольного и тупоугольного треугольников.

(b) Четырёхугольник $ABCD$ вписанный. Пусть r_1 и r_2 — радиусы окружностей, вписанных в треугольники ABC и ADC, а r_3 и r_4 — радиусы окружностей, вписанных в треугольники ABD и CBD. Докажите, что $r_1 + r_2 = r_3 + r_4$.

9.4.10. Пусть d, d_1, d_2 и d_3 — расстояния от центра O окружности, описанной около треугольника, до центров его вписанной и вневписанных окружностей. Докажите, что

$$R^2 = \frac{d^2 + d_1^2 + d_2^2 + d_3^2}{12}.$$

9.4.11. (a) Докажите, что если точка принадлежит отрезку, соединяющему основания двух биссектрис треугольника, то сумма расстояний от этой точки до двух сторон треугольника равна расстоянию от неё до третьей стороны.

(b) Пусть центр окружности, описанной около треугольника, лежит на отрезке, соединяющем основания двух биссектрис. Докажите, что расстояние от ортоцентра треугольника до одной из его вершин равно $R + r$.

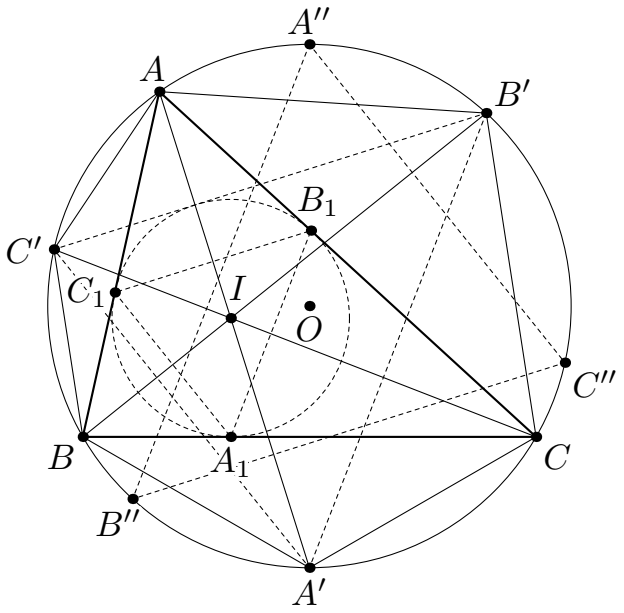

Рис. 2.4:

угольника $A_1B_1C_1$, следовательно, прямые Эйлера обязаны совпадать.

9.8 «Полувписанная» окружность (2*). *П. А. Кожевников*

Пусть A' и A'' — середины дуг BC описанной окружности Ω, соответственно не содержащей и содержащей точку A; B' и B'', C' и C'' определяются аналогично.

Рассмотрим окружность S_A (назовём её *полувписанной*), касающуюся сторон AB, AC и окружности Ω (внутренним образом). Основными в этой серии являются следующие факты:

— прямая, проходящая через точки касания полувписанной окружности со сторонами, содержит точку I;

— точка касания полувписанной окружности с окружностью Ω лежит на прямой $A''I$.

Основная серия-1

Докажите следующие утверждения.

9.8.1. Пусть перпендикуляр к биссектрисе AI, проведённый через точку I, пересекает AB и AC в точках K и L соответственно. Тогда окружности BKI, CLI и Ω пересекаются в одной точке T.

9.8.2. Точки T, I, A'' лежат на одной прямой.

9.8.3. Точки T, K, C' лежат на одной прямой.

9.8.4. Точки K, L и T являются точками касания окружности S_A с прямыми AB, AC и окружностью Ω.

9.8.5. (a) Прямая CC' касается окружности $TBKI$.

(b) Точка T — центр поворотной гомотетии, переводящей треугольник BKI в треугольник ILC.

Основная серия-2

9.8.6. Прямая AT проходит через центр гомотетии с положительным коэффициентом, переводящей окружность ω в Ω.

9.8.7. Пусть A_1 и A_2 — точки касания вписанной и вневписанной окружностей со стороной BC соответственно. Тогда

(a) AA' — биссектриса угла TAA_2;

(b) $\angle BTA_1 = \angle ABC$. (*Задача* 4.7.7 *из* [GZ].)

9.8.8. Пусть AT пересекает KL в точке Z. Тогда $\angle BZK = \angle CZL$. (*Задача* 4.7.5 *из* [GZ].)

9.8.9. Прямые KL, TA' и BC пересекаются в одной точке или параллельны. (*И. Шарыгин.*)

9.8.10. Точка пересечения Y_A из предыдущей задачи и точки Y_B, Y_C, определённые аналогичным образом, лежат на одной прямой.

Дополнительные задачи-1

9.8.11. Пусть P — произвольная точка на дуге $BA'C$.

(a) Пусть $P_b = BB' \cap PC'$, $P_c = CC' \cap PB'$. Тогда окружность PP_bP_c проходит через T. ([Za14], *задача* 8.8, 2013 *г.*)

(b) Пусть J_b и J_c — центры вписанных окружностей треугольников PAB и PAC. Тогда окружность PJ_bJ_c проходит через T. (*Задача* 4.7.9 *из* [GZ].)

(c) Пусть касательные к ω из точки P пересекают BC в точках U_1 и U_2. Тогда окружность PU_1U_2 проходит через T. (*Задача* 4.7.10 *из* [GZ].)

(d) Пусть прямые, проходящие через I параллельно биссектрисам углов между прямыми AP и BC пересекают прямую BC в точках V_1 и V_2 Тогда окружность PV_1V_2 проходит через T. (*См. частный случай задачи* 4.7.18 *из* [GZ].)

Дополнительные задачи-2

Следующие задачи — про «обобщённые полувписанные» окружности, т. е. окружности, касающиеся двух прямых и окружности.

9.8.12. Пусть D — точка на стороне AC треугольника ABC, и пусть S_1 — окружность, касающаяся окружности Ω внутренним образом в точке R, а также отрезков BD и AD в точках M и N соответственно.

(a) Докажите, что точки B, M, I, R лежат на одной окружности.

(b) **Лемма Саваямы.** Прямая MN проходит через центр I вписанной окружности ω треугольника ABC.

9.8.13. Пусть D — точка на отрезке AC треугольника ABC; S_1 — окружность, касающаяся отрезков BD и AD, а также окружности Ω внутренним образом; S_2 — окружность, касающаяся отрезков BD и CD, а также окружности Ω внутренним образом.

(a) **Теорема Тебо.** Линия центров окружностей S_1 и S_2 проходит через I.

(b) Докажите, что окружности S_1 и S_2 равны тогда и только тогда, когда $D = B_2$.

9.8.14. Найдите аналоги предложенных задач для «полувписанных» и «обобщённых полувписанных» окружностей, касающихся Ω внешним образом.

9.9 Обобщённая теорема Наполеона (2*). *П. А. Кожевников*

Классическая теорема Наполеона гласит, что центры правильных треугольников, построенных на сторонах произвольного треугольника вне его, являются вершинами равностороннего треугольника.

Теорема Наполеона является частным случаем утверждения задачи 13.1.7, п. «Комплексные числа и геометрия». В этом пункте мы докажем другое обобщение теоремы Наполеона.

Предлагаем для решения серию задач, внешне не имеющих никакой связи с теоремой Наполеона. Можно решать задачи любыми методами, а затем познакомиться с обобщением теоремы Наполеона и получить решения задач как следствия этого сильного факта.

Вводные задачи

9.9.1. Докажите, что центры квадратов, построенных на сторонах параллелограмма вне его, являются вершинами квадрата.

9.9.2. На боковых сторонах трапеции $ABCD$ построены треугольники ABE и CDF так, что $AE \parallel CF$ и $BE \parallel DF$. Докажите, что если E лежит на стороне CD, то F лежит на стороне AB.

9.9.3. (a) Две окружности пересекаются в точках A и B. Через точку A проведена прямая, вторично пересекающая первую окружность в точке C, а вторую — в точке D (можно считать, что точки C и D лежат по разные стороны от точки A). Пусть M и N — середины дуг BC и BD, не содержащих точку A, а K — середина отрезка CD. Докажите, что угол MKN прямой. (*Д. Терёшин. Всероссийская математическая олимпиада* 1997 *г.*)

(b) Круг поделили хордой AB на два круговых сегмента и один из них повернули вокруг точки A на некоторый угол. Пусть при этом повороте точка B перешла в точку D. Докажите, что отрезки, соединяющие середины дуг сегментов с серединой отрезка BD, перпендикулярны друг другу. (*З. Насыров*, [Kv92].)

9.9.4. Через вершину A треугольника ABC проведены прямые l_1 и l_2, симметричные относительно биссектрисы угла A. Докажите,

9.9.9.* Обобщённая теорема Наполеона. Пусть на сторонах треугольника ABC построены такие треугольники (возможно, вырожденные) BCA_1, CAB_1, ABC_1, что выполнены следующие условия:

1) $\angle(\overrightarrow{A_1B}, \overrightarrow{A_1C}) + \angle(\overrightarrow{B_1C}, \overrightarrow{B_1A}) + \angle(\overrightarrow{C_1A}, \overrightarrow{C_1B}) \equiv 0 \pmod{2\pi}$;

2) $AB_1 \cdot BC_1 \cdot CA_1 = BA_1 \cdot CB_1 \cdot AC_1$.

Тогда углы треугольника $A_1B_1C_1$ находятся из равенств

$$\angle(\overrightarrow{A_1C_1}, \overrightarrow{A_1B_1}) \equiv \angle(\overrightarrow{BC_1}, \overrightarrow{BA}) + \angle(\overrightarrow{CA}, \overrightarrow{CB_1}) \pmod{2\pi};$$
$$\angle(\overrightarrow{B_1A_1}, \overrightarrow{B_1C_1}) \equiv \angle(\overrightarrow{CA_1}, \overrightarrow{CB}) + \angle(\overrightarrow{AB}, \overrightarrow{AC_1}) \pmod{2\pi};$$
$$\angle(\overrightarrow{C_1B_1}, \overrightarrow{C_1A_1}) \equiv \angle(\overrightarrow{AB_1}, \overrightarrow{AC}) + \angle(\overrightarrow{BC}, \overrightarrow{BA_1}) \pmod{2\pi}.$$

Примечание. В теореме предполагается, что точка A_1 отлична от B, C, B_1, C_1 и т. д. Однако допускается, что вершины каких-то из треугольников BCA_1, CAB_1, ABC_1 и $A_1B_1C_1$ лежат на одной прямой. В этом случае говорят, что соответствующий треугольник является вырожденным, а его углы считают равными (с точностью до 2π) 0, 0 и π.

Таким образом, в теореме утверждается, что при выполнении условий 1 и 2 углы треугольника $A_1B_1C_1$ зависят лишь от углов треугольников, построенных на сторонах треугольника ABC, и не зависят от углов самого треугольника ABC. Условие теоремы может быть описано также таким изящным образом (см. [Bel]): пусть даны точки M, N, P, T и на сторонах треугольника ABC строятся треугольники ABC_1, BCA_1, CAB_1, подобные с сохранением ориентации соответственно треугольникам MNT, NPT, PMT. Действительно, выполнение условий 1 и 2 в этом случае проверяется непосредственно. С другой стороны, если треугольники ABC_1, BCA_1, CAB_1 удовлетворяют условиям теоремы, а треугольники MNT и NPT подобны соответственно треугольникам ABC_1 и BCA_1, то и треугольник PMT подобен CAB_1.

Конструкция из обобщённой теоремы Наполеона интересна, в ней можно обнаружить ещё несколько красивых фактов, например, окружности ABC_1, BCA_1, CAB_1 и $A_1B_1C_1$ имеют общую точку (отсюда можно понять, что на самом деле в этой конструкции треугольники ABC_1, BCA_1, CAB_1 и $A_1B_1C_1$ равноправны).

10.6 Теоремы Птолемея и Кези (3*). *А. Д. Блинков, А. А. Заславский*

10.6.1 Теорема Птолемея

10.6.1. (a) Докажите, что для любых четырёх различных точек A, B, C, D выполнено *неравенство Птолемея*

$$AB \cdot CD + AD \cdot BC \geqslant AC \cdot BD.$$

(b) **Теорема Птолемея.** Это неравенство обращается в равенство тогда и только тогда, когда $ABCD$ — вписанный четырёхугольник.

10.6.2. В остроугольном треугольнике ABC обозначим $|BC| = a$, $|AC| = b$. Найдите $|AB|$, если радиус окружности, описанной около $\triangle ABC$, равен R.

10.6.3. Биссектриса угла A треугольника ABC пересекает описанную около него окружность в точке W.

(a) Выразите отношение AW/IW, где I — центр окружности, вписанной в треугольник ABC, через длины сторон треугольника.

(b) Докажите, что $AW > \frac{AB+AC}{2}$.

10.6.4. На гипотенузе AB прямоугольного треугольника ABC во внешнюю сторону построен квадрат, O — его центр. Найдите $|OC|$, если a и b — катеты треугольника.

10.6.5. Дан правильный треугольник ABC и точка P.

(a) Докажите, что если точка P лежит на описанной около треугольника окружности, то расстояние от неё до одной из вершин треугольника равно сумме расстояний до двух других вершин.

(b) **Теорема Помпейю**. Для любой точки P, не лежащей на описанной окружности, из отрезков PA, PB, PC можно составить треугольник.

10.6.6. Сумма расстояний от точки X, выбранной вне квадрата, до двух его ближайших соседних вершин равна m. Найдите наибольшее значение суммы расстояний от X до двух других вершин квадрата.

10.6.7. Точки M и N — середины диагоналей AC и BD вписанного четырёхугольника $ABCD$. Известно, что $\angle ABD = \angle MBC$. Докажите, что $\angle BCA = \angle NCD$. (*Кубок Колмогорова*, 1999 *г.*)

10.6.8. (a) Точки A, B, C и D — четыре последовательные вершины правильного семиугольника. Докажите, что $\frac{1}{AB} = \frac{1}{AC} + \frac{1}{AD}$.

(b) Докажите, что $\frac{1}{\sin(\pi/7)} = \frac{1}{\sin(2\pi/7)} + \frac{1}{\sin(3\pi/7)}$.

10.6.9. В выпуклом шестиугольнике $ABCDEF$ известно, что $AB = BC = a$, $CD = DE = b$, $EF = FA = c$. Докажите, что $\frac{a}{BE} + \frac{b}{AD} + \frac{c}{CF} \geqslant \frac{3}{2}$.

10.6.10. Стороны вписанного четырёхугольника равны a, b, c, d. Найдите его диагонали.

10.6.11. Выведите из теоремы Птолемея формулу Карно (см. п. 9.4 «Формула Карно»).

10.6.2 Теорема Кези

10.6.12. Обобщённая теорема Птолемея, или теорема Кези. (a) Даны четыре непересекающихся круга, ограниченных окружностями α, β, γ, δ. Докажите, что окружность, касающаяся их внешним образом, или прямая, касающаяся их всех так, что круги лежат относительно неё в одной полуплоскости, существует тогда и только тогда, когда

$$l_{\alpha\beta}l_{\gamma\delta} + l_{\alpha\delta}l_{\beta\gamma} = l_{\alpha\gamma}l_{\beta\delta},$$

где $l_{\alpha\beta}$ — длина общей внешней касательной к окружностям α, β и т. д.

(b) Сформулируйте теорему Кези для случая, когда искомая окружность касается некоторых из данных окружностей внутренним образом.

10.6.13. Сформулируйте утверждение, аналогичное теореме Кези, для случая, когда

(a) одна;

(b) две из данных окружностей вырождаются в прямые;

(c) какие-то из данных окружностей вырождаются в точки.

10.6.14. Пусть на сторонах AC и BC треугольника ABC взяты такие точки X, Y, что $XY \parallel AB$. Докажите, что существует окружность, проходящая через X, Y и касающаяся одинаковым образом вневписанных окружностей треугольника, вписанных в углы A и B.

10.6.15. Докажите **теорему Фейербаха**: окружность, проходящая через середины сторон треугольника, касается его вписанной и вневписанных окружностей.

10.6.16. Докажите, что три окружности, каждая из которых касается внутренним образом одной из вневписанных окружностей треугольника и внешним образом двух других, пересекаются в одной точке.

10.6.17. Даны две окружности, лежащие одна вне другой. Произвольная окружность, касающаяся их одинаковым образом, пересекает одну из их общих внутренних касательных в точках A и A', а другую — в точках B и B'. Докажите, что среди прямых AB, AB', $A'B$, $A'B'$ найдутся две, параллельные общим внешним касательным к данным окружностям.

10.6.18. Даны две концентрические окружности a_1 и a_2. Каждая из окружностей b_1 и b_2 касается внешним образом окружности a_1 и внутренним — a_2, а каждая из окружностей c_1 и c_2 касается внутренним образом обеих окружностей a_1 и a_2. Оказалось, что окружности b_1, b_2 пересекают c_1, c_2 в восьми точках. Докажите, что эти точки лежат на двух окружностях или прямых, отличных от b_1, b_2, c_1, c_2. (*В. Протасов*, III *Олимпиада им. И. Ф. Шарыгина.*)

Указания, ответы и решения

10.6.1. Сделайте инверсию с центром A и воспользуйтесь утверждениями задач 11.10.2, 11.10.5. Заметим, что неравенство Птолемея верно даже для точек, не лежащих в одной плоскости.

10.6.2. *Ответ*: $\frac{a\sqrt{4R^2-b^2}+b\sqrt{4R^2-a^2}}{2R}$.

Проведите диаметр CD и примените к полученному четырёхугольнику теорему Птолемея.

11 Геометрические преобразования

В данном параграфе задачи расположены так, чтобы сначала новые понятия (геометрических преобразований) использовались для решения интересных задач, формулируемых без этих понятий, и только потом эти новые (но уже мотивированные) понятия изучались сами по себе.

Подробнее о геометрических преобразованиях см., например, [Za03] (теорема Шаля — § 1.2, подобие и гомотетия — § 1.3, аффинные преобразования — гл. 2, проективные преобразования — гл. 3, инверсия — гл. 4, комплексная интерпретация движений и подобий — § 6.1, комплексная интерпретация инверсии — § 6.2), [Pr95] и [Ya75].

11.1 Применения движений. (1) *А. Д. Блинков*

Поворотом вокруг точки O на угол φ называется преобразование плоскости, оставляющее точку O на месте и переводящее любую отличную от O точку X в такую точку X', что $|OX| = OX'$ и ориентированный угол между векторами $\overrightarrow{OX}$ и $\overrightarrow{OX'}$ равен φ. Поворот на 180° называется *центральной симметрией*.

Параллельным переносом на вектор $\overrightarrow{m}$ называется преобразование плоскости, переводящее любую точку X в такую точку X', что $\overrightarrow{XX'} = \overrightarrow{m}$.

Осевой симметрией относительно прямой l называется преобразование плоскости, переводящее любую точку X в такую точку X', что $XX' \perp l$ и точки X, X' лежат по разные стороны от прямой l и равноудалены от неё.

11.1.1.° Параллелограмм имеет ровно четыре оси симметрии. Какое из следующих утверждений верно?

1) это прямоугольник, отличный от квадрата;
2) это ромб, отличный от квадрата;
3) это квадрат;
4) такого параллелограмма не существует.

11.1.2.° Треугольник имеет центр симметрии. Какое из следующих утверждений верно?

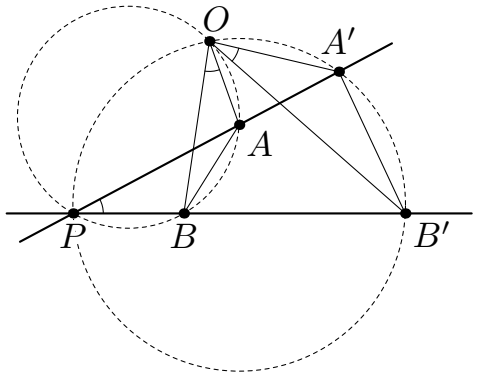

Рис. 2.41:

O под углом α. Следовательно, O лежит на дуге окружности, описанной около треугольника APB. Аналогично отрезок $A'B'$ должен быть «виден» из точки O под углом α, значит, точка O лежит на дуге окружности, описанной около треугольника $A'PB'$. Таким образом, O — вторая точка пересечения этих окружностей.

Если построенные окружности касаются, значит, обе точки проходят через P одновременно. В этом случае точка P сама будет искомой.

11.5 Поворотная гомотетия (2). *П. А. Кожевников*

11.5.1 Вводные задачи: немного о велосипедистах

11.5.1. По двум окружностям, пересекающимся в точках P и Q, одновременно начали движение из точки P по часовой стрелке с равными угловыми скоростями два велосипедиста A и B.

(a) Докажите, что прямая AB всё время проходит через Q.

(b) Докажите, что треугольники PAB всё время подобны друг другу и треугольнику PO_1O_2, где O_1 и O_2 — центры окружностей.

(c) Найдите ГМТ (траекторию движения) середин отрезков AB; центров вписанных окружностей треугольников PAB; любых соответственных точек подобных треугольников PAB.

(d) **Задача о велосипедистах.** Докажите, что A и B всё время равноудалены от фиксированной точки. (См. [VSh].)

11.5.2. По трём окружностям, имеющим общую точку O и попарно различные точки пересечения P, Q и R, одновременно начали

движение из точки O по часовой стрелке с равными угловыми скоростями три велосипедиста A, B и C.

(a) Докажите, что все треугольники ABC подобны между собой и треугольнику $O_1O_2O_3$, где O_1, O_2 и O_3 — центры окружностей.

(b) Какова траектория движения центра масс треугольника ABC?

11.5.3. Два велосипедиста P и Q едут равномерно по двум прямым, пересекающимся в точке O.

(a) Найдите траекторию середины отрезка PQ.

(b) Докажите, что если скорости велосипедистов равны, то середина дуги (одной из дуг) PQ окружности OPQ неподвижна.

(c) Докажите, что если велосипедисты проходят O не одновременно, то окружности OPQ имеют вторую общую точку, отличную от O.

11.5.4. Дан фиксированный треугольник ABC. По прямым BC, CA, AB едут соответственно велосипедисты P, Q, R так, что углы между RP и PQ, PQ и QR, QR и RP фиксированные.

(a) Докажите, что точка пересечения окружностей RAQ, RBP, PCQ неподвижна.

(b) Найдите ГМТ центров вписанных окружностей треугольников PQR.

11.5.2 Основные задачи

11.5.5. Три велосипедиста P, Q и R едут равномерно по трём прямым. Известно, что в некоторые два момента времени треугольник PQR был подобен с сохранением ориентации фиксированному треугольнику XYZ. Докажите, что это условие будет выполняться в любой момент времени.

11.5.6. В треугольник ABC вписан подобный ему треугольник PQR ($P \in BC$, $Q \in CA$, $R \in AB$, $\angle P = \angle A$, $\angle Q = \angle B$, $\angle R = \angle C$).

(a) Докажите, что центр описанной окружности треугольника ABC совпадает с ортоцентром треугольника PQR.

(b) Найдите максимальное значение выражения $\frac{S_{ABC}}{S_{PQR}}$.

(c) Докажите, что центр описанной окружности треугольника PQR равноудалён от центра описанной окружности и ортоцентра треугольника ABC.

11.5.7. Через вершины треугольника ABC проводятся три произвольные параллельные прямые d_a, d_b, d_c. Прямые d'_a, d'_b, d'_c, симметричные d_a, d_b, d_c относительно BC, CA, AB соответственно, образуют треугольник XYZ. Найдите геометрическое место центров вписанных окружностей таких треугольников.

11.5.8. Дан выпуклый четырёхугольник $ABCD$, стороны BC и AD которого равны, но не параллельны. Пусть E и F — внутренние точки отрезков BC и AD соответственно, удовлетворяющие условию $BE = DF$. Прямые AC и BD пересекаются в точке P, прямые BD и EF пересекаются в точке Q, прямые EF и AC пересекаются в точке R. Докажите, что для всевозможных способов выбора точек E, F окружности PQR имеют общую точку, отличную от P. (См. [IMO], 2005 г.)

11.5.9. Пусть O и I — центры описанной и вписанной окружностей треугольника ABC соответственно. Точки D, E и F выбраны на сторонах BC, CA и AB соответственно так, что $BD + BF = CA$ и $CD + CE = AB$. Описанные окружности треугольников BDF и CDE пересекаются в точках D и P. Докажите, что $OP = OI$. (См. [IMO], 2012 г.)

11.5.3 Дополнительные задачи

11.5.10. Впишите в данный остроугольный треугольник равносторонний треугольник с минимальной стороной.

11.5.11. На пол положили правильный треугольник ABC, выпиленный из фанеры. В пол вбили три гвоздя (по одному вплотную к каждой стороне треугольника) так, что треугольник невозможно повернуть, не отрывая от пола. Первый гвоздь делит сторону AB в отношении $1 : 3$, считая от вершины A, а второй делит сторону BC в отношении $2 : 1$, считая от вершины B. В каком отношении делит сторону AC третий гвоздь? (*Московская математическая олимпиада* 1998 *г.*)

11.5.12. Выпуклый многоугольник M можно поместить в треугольник T. Докажите, что это можно сделать так, чтобы одна из сторон многоугольника M лежала на стороне треугольника T.

Поворотной гомотетией называют преобразование $H_O^{k,\varphi} := H_O^k \circ R_O^\varphi$.

11.5.13. (a) Окружности α и β пересекаются в точках A и B. Пусть H — поворотная гомотетия с центром в точке A, переводящая α в β. Докажите, что для любой точки $X \in \alpha$ точка $H(X)$ получена пересечением прямой BX с окружностью β. (См. [Pr95, 19.27].)

(b) Окружности $S_1, \ldots, S_n$ проходят через точку O. Кузнечик из точки $X_i \in S_i$ прыгает в точку $X_{i+1} \in S_{i+1}$ так, что прямая X_iX_{i+1} проходит через вторую точку пересечения окружностей S_i и S_{i+1}. Докажите, что после n прыжков (с S_1 на $S_2, \ldots,$ с S_n на S_1) кузнечик вернётся в исходную точку. (См. [Pr95, 19.28].)

(c) Пусть концы отрезков AB и CD попарно различны, а P — точка пересечения прямых AB и CD. Центром поворотной гомотетии, переводящей AB в CD, является (отличная от P) точка пересечения описанных окружностей треугольников ACP и BDP. (См. [Pr95, 19.41 (б)].)

Указания, ответы и решения

11.5.1. (a) Из равенства угловых скоростей следует, что $\angle(PQ, QA) = \angle(PQ, QB)$.

(b) Угол $\angle(BA, AP) = \angle(QA, AP)$ постоянный и равен $\angle(O_2O_1, O_1P)$.

(c) Если M — середина AB, то $\angle(QM, MP)$ постоянный, поэтому M движется по окружности Γ, проходящей через P и Q.

Пусть N — любая точка треугольника PAB (в некоторый фиксированный момент). Рассмотрим поворотную гомотетию (см. определение перед задачей 11.5.13) с центром P, переводящую A в N. Она переводит траекторию точки A (окружность) в траекторию точки N.

(d) Серединные перпендикуляры к AB проходят через точку, диаметрально противоположную точке Q в окружности Γ (ГМТ середин отрезков AB из задачи (c)).

11.5.2. (a) Достаточно применить задачу 11.5.1 к парам окружностей.

12.3 Полярное соответствие (2). *А. А. Гаврилюк, П. А. Кожевников*

Традиционно при изучении полярного соответствия существенно используются свойства проективных преобразований. Мы же делаем попытку познакомиться с полярным соответствием и применением его свойств без привлечения проективной геометрии.

Введём нужные нам определения и обозначения. Пусть на плоскости фиксированы точка O и окружность ω радиуса R с центром в O.

Для каждой точки $X \neq O$ на луче OX строим такую точку X', что $OX \cdot OX' = R^2$. (Говорят, что X' и X *инверсны* относительно окружности ω.) Через точку X' проведём прямую x, перпендикулярную OX'. Прямая x называется *полярой* точки X, а точка X называется *полюсом* прямой x. Соответствие $X \leftrightarrow x$ является взаимно однозначным соответствием между точками, отличными от O, и прямыми, не проходящими через O. Это соответствие и называется *полярным соответствием*.

Ниже мы обозначаем точки, отличные от O (полюсы), большими латинскими буквами, а их поляры — соответствующими маленькими буквами: $A \leftrightarrow a$, $B \leftrightarrow b$, $C \leftrightarrow c$, ...

Основные свойства и вводные задачи

Установите два основных *свойства полярного соответствия.*

П1. Двойственность. Включение $A \in b$ выполняется тогда и только тогда $B \in a$, т. е. поляра любой точки является геометрическим местом полюсов проходящих через неё прямых.

П2.* Пусть две прямые m и l, проходящие через произвольную точку $A \notin \omega$, пересекают ω в точках M_1, M_2 и L_1, L_2. Тогда $M_1L_1 \cap M_2L_2 \in a$ или $M_1L_1 \parallel M_2L_2 \parallel a$.

Докажите следующие факты.

В1. Если $A \in \omega$, то a — это касательная к ω, проведённая через A.

В2. Если точка A расположена вне окружности ω, то a проходит через точки касания с ω касательных, проведённых через A.

B3. Если O, A, B не лежат на одной прямой, то $a \cap b \leftrightarrow AB$.

B4. Точки A, B, C лежат на одной прямой тогда и только тогда, когда a, b, c проходят через одну точку или параллельны.

Основные задачи

12.3.1.° Даны окружность и её хорда AB. Где лежит точка пересечения поляр точек A и B?

1) внутри окружности; 2) вне окружности; 3) на окружности.

12.3.2.° Пусть C — середина хорды AB. Тогда поляра точки C

1) параллельна AB;
2) перпендикулярна AB;
3) касается окружности.

12.3.3.° При полярном соответствии относительно вписанной окружности треугольник переходит

1) в серединный треугольник;
2) в ортотреугольник;
3) в треугольник, образованный точками касания сторон с вписанной окружностью.

12.3.4. Даны окружность ω и прямая l, не имеющие общих точек. Из точки X, которая движется по прямой l, проводятся касательные XA, XB к ω. Докажите, что все хорды AB имеют общую точку.

12.3.5. Симметричная бабочка. (a) Дана точка A на диаметре BC полуокружности ω. Точки X, Y на ω таковы, что $\angle XAB = \angle YAC$. Докажите, что прямые XY проходят через одну точку или параллельны.

(b) Точки A и A' инверсны относительно окружности ω, причём точка A' расположена внутри ω. Через A' проводятся хорды XY. Докажите, что центры вписанной и одной из вневписанных окружностей треугольника AXY фиксированны. (*С. Маркелов, см.* [Sh97].)

12.3.6. Основное свойство симедианы. Касательные к описанной окружности треугольника ABC, проведённые через точки B

и C, пересекаются в точке P. Докажите, что AP — симедиана (т. е. прямая, симметричная медиане AM относительно биссектрисы угла A).

12.3.7. Гармонический четырёхугольник. Пусть четырёхугольник $ABCD$ вписан в окружность ω. Известно, что касательные к ω, проведённые в точках A и C, пересекаются на прямой BD или параллельны BD. Докажите, что касательные к ω, проведённые в точках B и D, пересекаются на прямой AC или параллельны AC.

В следующих трёх задачах дан четырёхугольник $ABCD$, у которого диагонали пересекаются в точке P, продолжения сторон AB и CD — в точке R, продолжения сторон BC и DA — в точке Q.

12.3.8. Вписанный четырёхугольник. Пусть четырёхугольник $ABCD$ вписан в окружность с центром O. Докажите, что четвёрка точек O, P, Q, R ортоцентрическая (т. е. каждая точка является ортоцентром треугольника с вершинами в оставшихся трёх точках).

12.3.9. Описанный четырёхугольник. Пусть четырёхугольник $ABCD$ описан около окружности; K, L, M, N — точки касания с окружностью сторон AB, BC, CD, DA соответственно; прямые KL и MN пересекаются в точке S, а прямые LM и NK — в точке T.

(a) Докажите, что точки Q, R, S, T лежат на одной прямой.

(b) Докажите, что KM и LN пересекаются в точке P.

12.3.10. Вписанно-описанный четырёхугольник. Четырёхугольник $ABCD$ описан около окружности ω с центром I и вписан в окружность Ω с центром O.

(a) Докажите, что O, I, P лежат на одной прямой.

(b) Зафиксируем ω и Ω и рассмотрим всевозможные четырёхугольники $ABCD$, описанные около окружности ω и вписанные в окружность Ω. Докажите, что для всех таких четырёхугольников точки P совпадают, а также что прямые QR совпадают.

Комментарий. Согласно теореме Понселе если существует хотя бы один четырёхугольник, описанный около окружности ω и вписанный в окружность Ω, то существует бесконечно много таких четырёхугольников.

13.1 Комплексные числа и элементарная геометрия.

Пусть на плоскости задана система координат. Тогда комплексному числу $z = x + yi$ соответствует точка плоскости Z с координатами (x, y). При этом модуль числа z равен расстоянию от Z до начала координат O, а аргумент равен ориентированному углу между положительным направлением оси Ox и вектором $\overrightarrow{OZ}$, т. е. углу, на который надо повернуть против часовой стрелки ось Ox, чтобы совместить её положительное направление с направлением вектора $\overrightarrow{OZ}$. Оси Ox и Oy называют *действительной* и *мнимой* осями.

13.1.1. (Загадка.) Выясните геометрический смысл сложения комплексных чисел.

13.1.2. (a) Каким геометрическим преобразованием комплексной плоскости получается число iz из числа z?

(b) (Загадка.) Обозначим $e^{i\varphi} := \cos\varphi + i\sin\varphi$. Каков геометрический смысл умножения на $e^{i\varphi}$? А на $re^{i\varphi}$, где r — вещественное число (см. определение тригонометрической формы комплексного числа в п. 4.5)?

(c) Выразите число w, полученное из числа z поворотом на угол φ против часовой стрелки относительно центра z_0, через z, z_0 и φ.

(d) Докажите, что композиция поворотов плоскости (с различными центрами) — поворот или параллельный перенос.

(e) Докажите, что точки z_1, z_2, z_3 лежат на одной прямой тогда и только тогда, когда отношение $(z_3 - z_1)/(z_2 - z_1)$ вещественно.

Комментарий. Задача 13.1.2 (b) легко решается с помощью тригонометрических формул сложения. Однако можно поступить наоборот: решить эту задачу геометрически, доказать, что при умножении комплексных чисел их модули перемножаются, а аргументы складываются, а затем, используя этот результат, получить доказательство формул сложения, не требующее перебора различных случаев.

13.1.3.$^\circ$ Какое преобразование плоскости задаётся формулой $z \mapsto 2z + 2$?

Теперь воспользуемся тем, что аффинное преобразование однозначно определяется образами трёх точек, не лежащих на одной прямой. Пусть точки 0, 1 и i переходят в z_0, z_1, z_2 соответственно. Тогда данное преобразование задаётся формулой требуемого вида, в которой $c = z_0$, $a = (z_1 + z_2 - 2z_0)/2$, $b = (z_1 - z_2)/2$. Из того, что z_0, z_1, z_2 не лежат на одной прямой, следует, что $|a| \neq |b|$.

13.1.7. Пусть $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Тогда точки $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ являются вершинами правильного n-угольника. Согласно предыдущей задаче можно считать, что вершинами данного многоугольника являются точки $a\varepsilon^k + b\varepsilon^{-k}, k = 0, 1, \ldots, n-1$. Значит, центр k-го правильного n-угольника z_k удовлетворяет равенству $a\varepsilon^{k+1} + b\varepsilon^{-k-1} - z_k = \varepsilon(a\varepsilon^k + b\varepsilon^{-k} - z_k)$. Отсюда легко получить, что z_k образуют геометрическую прогрессию с знаменателем ε, т. е. являются вершинами правильного n-угольника.

13.2 Комплексные числа и круговые преобразования.

Преобразование круговой плоскости, сохраняющее обобщённые окружности, называется *круговым*. Произвольное отличное от подобия круговое преобразование может быть представлено как композиция инверсии и движения.

13.2.1.° Четвёрка комплексных чисел z_1, z_2, z_3, z_4 удовлетворяет равенству $\frac{(z_1-z_3)(z_2-z_4)}{(z_1-z_4)(z_2-z_3)} = 2$. Что можно сказать о четвёрке точек плоскости, соответствующих числам z_1, z_2, z_3, z_4?

1) Они являются вершинами параллелограмма.

2) Они лежат на одной прямой или на одной окружности.

3) Площадь треугольника $0z_1z_2$ равна площади треугольника $0z_3z_4$ (точка 0 — начало координат).

13.2.2. Докажите, что преобразование комплексной плоскости является круговым тогда и только тогда, когда оно задаётся дробно-линейной функцией вида $f(z) = (az + b)/(cz + d)$ или $f(z) = (a\bar{z} + b)/(c\bar{z} + d)$, где $ad - bc \neq 0$.

13.2.3. Докажите, что для любых шести различных точек A, B, C, A', B', C' существует ровно два круговых преобразования, переводящих A в A', B в B', C в C'.

Двойным отношением четырёх комплексных чисел a, b, c, d, где $a \neq d$, $b \neq c$, называется комплексное число $(a, b, c, d) = \frac{(a-c)(b-d)}{(a-d)(b-c)}$.

13.2.4. Докажите, что для данных восьми различных точек A, B, C, D; A', B', C', D' круговое преобразование, переводящее A в A', B в B', C в C', D в D', существует тогда и только тогда, когда для соответствующих комплексных чисел выполняется равенство $(a, b, c, d) = (a', b', c', d')$ или $\overline{(a, b, c, d)} = (a', b', c', d')$.

13.2.5. Даны два треугольника ABC и $A'B'C'$. Докажите, что существует инверсия, переводящая треугольник ABC в треугольник, равный $A'B'C'$.

13.2.6. Дан четырёхугольник $ABCD$. Докажите, что существует инверсия, переводящая его вершины в вершины параллелограмма, причём все параллелограммы, полученные в результате таких инверсий, подобны.

См. также задачу 11.10.4 (c) п. «Инверсия».

Дополнительные задачи

13.2.7. (a) Пусть a, b, c — комплексные числа, соответствующие не лежащим на одной прямой точкам A, B, C; $f(z) = (z-a)(z-b)(z-c)$. Докажите, что две точки, соответствующие корням производной $f'(z)$, изогонально сопряжены относительно треугольника ABC.

(b)* *Эллипсом Штейнера* треугольника ABC называется эллипс наибольшей площади, лежащий внутри треугольника. Докажите, что фокусы эллипса Штейнера соответствуют корням производной $f'(z)$.

13.2.8. Пусть a, b, c — комплексные числа, соответствующие точкам A, B, C, причём $|a| = |b| = |c| = 1$. Докажите, что точки Z_1, Z_2 изогонально сопряжены относительно треугольника ABC тогда и только тогда, когда соответствующие комплексные числа удовлетворяют соотношению

$$z_1 + z_2 + abc\bar{z_1}\bar{z_2} = a + b + c.$$

сторонах четырёхугольника, проходящий через середины его диагоналей, за исключением концов.

Для параллелограмма ответ очевиден.

Пусть P и Q — середины диагоналей AC и BD данного четырёхугольника, отличного от параллелограмма (см. рис. 2.54 *б*). Тогда $S_{ABP} + S_{CDP} = S_{ABQ} + S_{CDQ} = S_{ABCD}/2$.

Если точка M лежит внутри $ABCD$ на PQ, то $S_{APM} = S_{CPM}$ (так как точки A и C равноудалены от PM) и $S_{BPM} = S_{DPM}$ (так как точки B и D равноудалены от PM). Таким образом, $S_{ABM} + S_{CDM} = S_{ABP} + S_{CDP} + S_{APM} + S_{BPM} - S_{CPM} - S_{DPM} = S_{ABP} + S_{CDP} = S_{ABCD}/2 = S_{ADM} + S_{BCM}$.

Если точка M не лежит на указанном отрезке, то, действуя аналогично, проверяем, что указанное в условии равенство не выполняется.

14.3 Построения. Ящик инструментов (2). *А. А. Гаврилюк*

При изучении материала этого раздела желательно знакомство с § 10 «Окружность» и рекомендованной в нем литературой.

14.3.1. Даны два отрезка с длинами x, y. С помощью циркуля и линейки постройте отрезок длины $\sqrt{3xy + y\sqrt[4]{xy^3}}$.

14.3.2. (a) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки разделите его пополам.

(b) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки удвойте его.

(c) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки разделите его на n равных частей.

Ср. с задачей 11.9.5 п. «Центральная проекция и проективные преобразования".

14.3.3. Даны окружность ω, её диаметр AB и точка X. С помощью одной линейки постройте перпендикуляр из точки X на AB, если точка X лежит

(a) не на окружности; (b) на окружности.

14.3.4. Даны окружность ω и точка X. С помощью одной линейки постройте (все возможные) касательные, проведённые из точки X к окружности, если точка X лежит

(a) вне окружности; (b) на окружности.

14.3.5. При помощи только циркуля постройте образ данной точки X при инверсии относительно данной окружности ω.

14.3.6. Дана окружность на плоскости. С помощью двусторонней линейки постройте её центр. (С помощью двусторонней линейки можно проводить прямую через две точки, проводить прямую, параллельную проведённой ранее прямой и отстоящую от неё на расстояние, равное ширине линейки, а также проводить через две точки, расстояние между которыми не меньше ширины линейки, две параллельные прямые, расстояние между которыми равно ширине линейки.)

14.3.7. Даны прямая l и отрезок OA, ей параллельный. С помощью двусторонней линейки постройте точки пересечения прямой l с окружностью радиуса OA и с центром в точке O.

14.3.8. При помощи только циркуля постройте окружность, проходящую через три данные точки.

14.3.9. Задача Аполлония. Постройте окружность, касающуюся трёх данных, при помощи циркуля и линейки.

В последующих задачах этого пункта *построением* будем называть некоторую последовательность следующих элементарных операций:

— с помощью линейки провести прямую через две данные или ранее построенные точки;

— с помощью циркуля построить окружность с центром A и радиусом BC, где A, B, C — данные или ранее построенные точки;

— найти точки пересечения двух данных или ранее построенных линий (прямых или окружностей).

В последующих теоремах никакие другие операции не разрешаются (в отличие от предыдущих задач, где разрешена, например, операция «взять произвольную точку уже построенного множества»). В частности, если изначально не даны хотя бы две точки, ничего построить нельзя.

14.3.10.* **Теорема.** С помощью циркуля и линейки можно осуществлять те и только те построения, которые «сводятся» к арифметическим операциям и операции извлечения квадратного корня, то есть если на плоскости фиксирована система координат, то координаты всех построимых точек выражаются через координаты исходных точек с помощью указанных операций.

Комментарий. Из этой теоремы, в частности, следует, что если дан отрезок длины 1, то для любых отрезков с длинами a, b можно построить отрезки с длинами $a+b$, $a-b$, ab, a/b, $\sqrt{a}$ и длина любого отрезка, который можно построить, выражается через a и b с помощью указанных операций (ср. с основной теоремой из п. 5.2.3).

14.3.11.* **Теорема** (Мор—Маскерони). Любое построение, осуществимое циркулем и линейкой, можно осуществить одним циркулем (прямая считается построенной, если построены две различные лежащие на ней точки, см. [Fu87]).

14.3.12.* **Теорема** (Штейнер). Любое построение, осуществимое циркулем и линейкой, можно осуществить одной линейкой, если начерчена одна окружность и отмечен её центр (окружность считается построенной, если построены её центр и лежащая на ней точка, см. [Smo]).

Следующая задача предназначена для закрепления материала.

14.3.13.° Пользуясь теоремами Мора—Маскерони и Штейнера, определите, какие инструменты необходимы для построения центра данной окружности.

1) циркуль и линейка; 2) только линейка; 3) только циркуль.

Указания, ответы и решения

14.3.1. Высота прямоугольного треугольника является средним геометрическим отрезков, на которые она делит гипотенузу. Поэтому если даны отрезки с длинами a, b, то, построив полуокружность с диаметром $a+b$ и найдя её пересечение с прямой, перпендикулярной диаметру и делящей его на отрезки длины a и b, получим отрезок длины $\sqrt{ab}$. Для решения данной задачи достаточно последовательно построить отрезки с длинами $z_1 = \sqrt{xy}$, $z_2 = \sqrt{yz_1}$, $z_3 = 3x + z_2$, $z = \sqrt{yz_3}$.

[fest] Шесть фестивалей (материалы Российских фестивалей юных математиков). Краснодар: ГИНМЦ, 1996.

[Fu87] *Фукс Д.* Построения одним циркулем // Квант. 1987. № 7. С. 34–37.

[Smo] *Смогоржевский А. С.* Линейка в геометрических построениях. М.: Гостехиздат, 1956.

15 Стереометрия

Чужбина так же сродственна отчизне,
Как тупику соседствует пространство.

И. Бродский.

15.1 Рисование (2). *А. Б. Скопенков*

15.1.1. Куб с ребром 3 разбит на 27 единичных кубиков. Нарисуйте

(a) ежа (объединение центрального кубика и имеющих с ним общую грань);

(b) то, что получается при выкидывании ежа из куба;

(c)* то, что получается при выкидывании угловых кубиков из куба.

15.1.2. Можно ли пространство заполнить непересекающимися ежами?

15.1.3. Правильные многоугольники с каким числом сторон могут получиться при пересечении куба плоскостью?

15.1.4. (a) Нарисуйте объединение куба $A \dots D_1$ с кубом, полученным из него поворотом на $\pi/3$ относительно большой диагонали.

(b) Нарисуйте объединение тетраэдра $ABCD$ с тетраэдром, полученным из него поворотом на $\pi/2$ относительно бимедианы, т. е. прямой, соединяющей середины противоположных рёбер.

15.1.5. На плоскости стоят куб и каркас треугольной пирамиды, высота которой больше высоты куба. Нарисуйте тень от каркаса пирамиды на кубе, если пучок света параллелен прямой, соединяющей вершину пирамиды с центром верхней грани куба.

15.2.20. (a), (b), (c), (d), (e*), (f*) Постройте биекцию, сохраняющую композицию, между каждым из найденных множеств самосовмещений из задачи 15.2.19 и некоторым множеством перестановок n-элементного множества.

15.2.21. (a) Укажите два вращения правильного додекаэдра, композициями которых можно получить любое другое.

(b) Постройте биекцию, сохраняющую композицию, между множеством вращений додекаэдра и множеством чётных перестановок пяти элементов.

15.3 Многомерье (4*). *А. Я. Канель-Белов*

15.3.1 Простейшие многогранники в многомерном пространстве. *Ю. М. Бурман, А. Я. Канель-Белов*

Хорошо известно, что точке плоскости можно сопоставить пару чисел — её декартовых координат (для этого нужно предварительно выбрать систему координат, то есть начало координат и оси). Тем самым плоскость можно понимать просто как множество всевозможных пар (x_1, x_2) действительных чисел. Аналогично трёхмерное пространство можно считать просто множеством всевозможных троек (x_1, x_2, x_3). Накладывая на числа различные ограничения, мы получим описание разнообразных подмножеств плоскости и пространства (плоских фигур и трёхмерных тел).

15.3.1.° Даны три набора условий на числа x_1, x_2, x_3:

1) $x_1 = x_2 = 2x_3$;

2) $x_1 + 2x_2 + 3x_3 = 0$, $3x_1 + 2x_2 + x_1 = 1$;

3) $x_1^2 + x_3^2 - 2x_3 = -1$.

Какие из них задают прямую в трёхмерном пространстве?

Когда измерений больше, чем три, координатный подход становится ведущим: удобно *определить*, скажем, четырёхмерное пространство как множество всевозможных наборов (x_1, x_2, x_3, x_4) из четырёх действительных чисел.

В этом пункте *отрезком* мы будем называть множество $[-1, 1] = \{x\colon |x| \leqslant 1\}$ чисел, по модулю не превосходящих 1; *квадратом* — множество $[-1, 1]^2 = \{(x_1, x_2)\colon |x_1|, |x_2| \leqslant 1\}$ пар чисел, каждое из

15.3.2 Многомерные объёмы

Объём n-мерного многогранника определяется аналогично площади фигуры на плоскости (см. п. 25.5 «Принцип Дирихле и его применения в геометрии»).

Объёмом n-мерных многогранников называется заданная на множестве многогранников неотрицательная функция V, удовлетворяющая следующим условиям:

— если многогранник M_1 можно движением перевести в многогранник M_2, то $V(M_1) = V(M_2)$;

— $V(M_1 \cup M_2) = V(M_1) + V(M_2) - V(M_1 \cap M_2)$;

— объём любого подмножества $(n-1)$-мерной гиперплоскости равен нулю;

— объём куба с ребром a равен a^n.

Используя эти свойства и при необходимости верхние и нижние оценки, можно найти объём любого многогранника. Например, объём n-мерной пирамиды задаётся формулой $V = \frac{1}{n}Sh$, где S — $(n-1)$-мерный объём основания пирамиды, а h — её высота. Можно также находить объёмы некоторых n-мерных тел (т. е. ограниченных подмножеств n-мерного пространства), не являющихся многогранниками.

15.3.25. У 100-мерного арбуза (шара) радиус равен 1 метру, а толщина корки — 1 см. Какой процент его объёма занимает мякоть?

15.3.26. Докажите, что в единичный куб достаточно большой размерности можно поместить здание МГУ, т. е. существует трёхмерная плоскость, в пересечение которой с кубом можно поместить это здание.

15.3.27. Укажите какое-нибудь такое n, что в n-мерный единичный куб можно поместить круг радиуса R.

15.3.28. Укажите какое-нибудь такое n, что в n-мерный единичный куб можно поместить шар радиуса R.

15.3.29. Укажите какое-нибудь такое n, что в n-мерный единичный куб можно поместить n-мерный шар радиуса R.

15.3.30. К чему стремится объём n-мерного шара радиуса 2015 при $n \to \infty$?

Известно, что объём n-мерного шара радиуса R равен

$$B_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)},$$

где $\Gamma(z) = \int\limits_0^\infty y^z e^{-y} dy$, $z > 0$ — знаменитая *гамма-функция* Эйлера. Она доопределяет факториал на комплексную плоскость: $\Gamma(k) = (k+1)!$ при целом k и $\Gamma(z) = \Gamma(z-1)z$. Последнее равенство позволяет доопределить $\Gamma(z)$ также и при $\mathrm{Re}(z) < 0$. Известно, что $\Gamma(x)\Gamma(1-x) = \pi/\sin(\pi z)$, в частности $\Gamma(1/2) = \sqrt{\pi}/2$.

15.3.31. Найдите площадь поверхности n-мерного шара единичного объёма.

15.3.32. Найдите объём n-мерного симплекса с единичным ребром. Найдите ребро n-мерного симплекса с единичным объёмом. (Определения n-мерных симплекса и октаэдра приведены в п. 15.3.1 «Комбинаторная геометрия в многомерном пространстве».)

Диаметром ограниченного подмножества M n-мерного пространства называется $\sup\{|XY|, X, Y \in M\}$, где $\mathrm{dist}(X, Y)$ — расстояние между точками X и Y.

15.3.33. Найдите объём n-мерного октаэдра с единичным ребром. Найдите диаметр n-мерного симплекса с единичным объёмом.

15.3.3 Объёмы и сечения

Обозначим $x_+ = \max(x, 0) = \begin{cases} x & \text{при } x \geqslant 0, \\ 0 & \text{при } x \geqslant 0. \end{cases}$

Открытой полуплоскостью называется множество точек плоскости, лежащих строго по одну сторону от некоторой прямой. *Замкнутой полуплоскостью* называется объединение открытой полуплоскости и ее граничной прямой. Прямая, заданная уравнением $ax + by + c = 0$, разбивает плоскость на две полуплоскости (замкнутую и открытую), координаты точек которых удовлетворяют неравенствам $ax + by + c \geqslant 0$ и $ax + by + c < 0$. Аналогично определяются

Глава 3

Комбинаторика

17 Подсчеты в комбинаторике

Этот параграф посвящен в основном вопросу «Сколько существует объектов с данными свойствами?». В нем собраны материалы для самого первого знакомства с подсчетами в комбинаторике. Продолжить их изучение мы рекомендуем по главе 1 книги [GDI].

17.1 Подсчеты числа способов (1). *А. А. Гаврилюк, Д. А. Пермяков*

Этот пункт не требует никаких знаний и подходит для первого знакомства с комбинаторикой.

17.1.1. (a) Назовем натуральное число *симпатичным*, если в его записи встречаются только четные цифры. Выпишите все двузначные симпатичные числа и подсчитайте их количество.

(b) Сколько существует пятизначных симпатичных чисел?

(c) Сколько существует шестизначных чисел, в записи которых есть хотя бы одна четная цифра?

(d) Каких семизначных чисел больше: тех, в записи которых есть единица, или остальных?

17.1.2. Из двух математиков и десяти экономистов надо составить комиссию из восьми человек. Сколькими способами можно составить комиссию, если в нее должен входить хотя бы один математик?

17.1.3. (a) Найдите сумму всех семизначных чисел, которые можно получить всевозможными перестановками цифр $1, \ldots, 7$.

(b) Из цифр $1, 2, 3, \ldots, 9$ составлены все четырехзначные числа, не содержащие повторяющихся цифр. Найдите сумму этих чисел.

(c) Найдите сумму всех четырехзначных чисел, не содержащих повторяющихся цифр.

17.1.4. (a) На двух клетках шахматной доски стоят черный и белый короли. За один ход можно пойти любым королем (короли дружат, так что могут стоять в соседних клетках, но не в одной и той же). Могут ли в результате их передвижений встретиться все возможные варианты расположения этих королей, причем ровно по одному разу?

(b) Тот же вопрос, если короли разучились ходить по диагонали.

17.1.5. (a) Найдите сумму всех 6-значных чисел, получаемых при всех перестановках цифр $4, 5, 5, 6, 6, 6$.

(b) Найдите сумму всех 10-значных чисел, получаемых при всех перестановках цифр $4, 5, 5, 6, 6, 6, 7, 7, 7, 7$.

17.1.6. (a) Тому Сойеру поручили покрасить забор из 8 досок в белый цвет. В силу своей лени он покрасит не более 3 досок. Сколько у него способов это сделать?

(b) А сколько способов покрасить не более 5 досок?

(c) А сколько способов покрасить любое количество досок?

Указания, ответы и решения

17.1.1. *Ответы*: (b) 2500; (c) 884 375; (d) в которых есть единица.

(b) *Решение* (написано А. Колоченковым). Первой цифрой симпатичного числа может быть 2, 4, 6, или 8 — всего 4 варианта. Для каждой цифры со второй по пятую есть 5 вариантов: 0, 2, 4, 6, 8. Значит, всего симпатичных чисел $4 \cdot 5 \cdot 5 \cdot 5 \cdot 5 = 2500$.

Это рассуждение в комбинаторике называется *правилом произведения* и подробно обсуждается в статье [Vi71].

(c) *Решение* (написано А. Колоченковым). Вычтем из общего количества шестизначных чисел количество шестизначных чисел,

17.2.5. *Ответ*: да.

17.2.6. *Ответ*: да.

17.2.7. *Ответ*: $(N+1)!-1$.

17.3 Формула включений и исключений (2). *Д. А. Пермяков*

Этот пункт посвящен доказательству и использованию формулы включений и исключений. Она позволяет отвечать на вопрос «Сколько существует объектов с данными свойствами?» во многих непростых случаях. Потребуются базовые навыки решения задач по комбинаторике. В частности, нужно уметь приводить строгие доказательства с использованием взаимно однозначных соответствий, правил суммы и произведения. Например, полезно прорешать п. 17.1 «Подсчеты числа способов» или задачи из статьи [Vi71].

17.3.1. Сколькими способами можно переставить числа от 1 до n, чтобы

(a) и 1, и 2 не оказались на своем месте;

(b) ровно одно из чисел 1, 2 и 3 оказалось на своем месте;

(c) каждое из чисел 1, 2 и 3 оказалось не на своем месте;

(d) каждое из чисел 1, 2, 3 и 4 оказалось не на своем месте?

Обозначим через $\varphi(n)$ функцию Эйлера, т. е. количество чисел от 1 до n, взаимно простых с числом n.

17.3.2. (a) Найдите количество целых чисел от 1 до 1001, не делящихся ни на одно из чисел 7, 11, 13.

(b) Найдите $\varphi(1)$, $\varphi(p)$, $\varphi(p^2)$, $\varphi(p^\alpha)$, где p — простое число, $\alpha > 2$.

(c) Докажите, что $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)$, где $n = p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}$ — каноническое разложение числа n.

17.3.3. (a) На полу комнаты площадью 24 м^2 расположены три ковра (произвольной формы) площадью 12 м^2 каждый. Тогда площадь пересечения некоторых двух ковров не меньше 4 м^2.

(b) На кафтане расположено пять заплат (произвольной формы). Площадь каждой из них больше трех пятых площади кафтана. Тогда площадь общей части некоторых двух заплат больше одной пятой площади кафтана.

(c)* То же, что в п. (b), если площадь каждой заплаты больше *половины* площади кафтана.

В этом пункте предлагаются задачи следующего типа: даны конечное множество U и набор свойств (подмножеств) $A_k \subset U$, $k = 1, \ldots, n$. Требуется найти количество элементов, для которых выполнено хотя бы одно из свойств A_k (т. е. $|A_1 \cup \ldots \cup A_n|$), либо количество элементов, для которых не выполнено ни одно из свойств A_k (т. е. $|U - (A_1 \cup \ldots \cup A_n)|$). Для этого используются два варианта формулы включений и исключений (см. задачу 17.3.5 (b)). При этом если во всех пересечениях множеств набора число элементов зависит только от количества пересекаемых множеств, то формулу можно упростить (см. задачу 17.3.5 (a)).

17.3.4. Рассмотрим подмножества A_1, A_2, A_3, A_4 конечного множества U. Докажите равенства

(a) $A_1 \cup A_2 = (A_1 \backslash A_2) \sqcup (A_1 \cap A_2) \sqcup (A_2 \backslash A_1)$;

(b) $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$;

(c) $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.

(d) Количество элементов в U, не принадлежащих ни одному из подмножеств A_1, A_2, A_3, равно

$$|U| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_3| - |A_1 \cap A_2 \cap A_3|.$$

(e) Для $k = 1, 2, 3, 4$ обозначим

$$M_k := \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant 4} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|.$$

Докажите, что количество элементов в A, не принадлежащих ни одному из A_i, равно $|U| - M_1 + M_2 - M_3 + M_4$.

(f) В условиях п. (e) количество элементов, принадлежащих ровно одному из множеств A_i, равно $M_1 - 2M_2 + 3M_3 - 4M_4$.

17.3.5. Формула включений и исключений. Рассмотрим подмножества $A_1, \ldots, A_n$ конечного множества U. Положим по определению $\Big|\bigcap\limits_{j\in\varnothing} A_j\Big| := U$.

(a) Пусть число $\alpha_{|S|} := \Big|\bigcap\limits_{j\in S} A_j\Big|$ зависит только от размера $|S|$ набора $S \subset \{1, \ldots, n\}$ индексов, а не от самого набора. Тогда

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} \alpha_k,$$
$$|U - (A_1 \cup \ldots \cup A_n)| = \sum_{k=0}^{n} (-1)^{k} \binom{n}{k} \alpha_k.$$

(b) Обозначим $M_k := \sum\limits_{S\in\binom{n}{k}} \Big|\bigcap\limits_{j\in S} A_j\Big|$, где суммирование производится по всем k-элементным подмножествам множества $\{1, \ldots, n\}$. В частности, $M_0 := |U|$. Тогда

$$|A_1 \cup \ldots \cup A_n| = M_1 - M_2 + M_3 - \ldots + (-1)^{n+1} M_n,$$
$$|U - (A_1 \cup \ldots \cup A_n)| = M_0 - M_1 + M_2 + \ldots + (-1)^{n} M_n.$$

(c) **Неравенства Бонферрони.** Для любого $0 \leqslant s < n/2$ справедливы неравенства

$$M_1 - M_2 + M_3 - \ldots - M_{2s} \leqslant |A_1 \cup \ldots \cup A_n| \leqslant M_1 - M_2 + M_3 - \ldots + M_{2s+1},$$
$$M_0 - M_1 + M_2 - \ldots + M_{2s} \geqslant |U - (A_1 \cup \ldots \cup A_n)| \geqslant$$
$$\geqslant M_0 - M_1 + M_2 - \ldots - M_{2s+1}.$$

(d) Число элементов, принадлежащих ровно r из подмножеств $A_1, \ldots, A_n$, равно $\sum\limits_{k=r}^{n} (-1)^{k-r} \binom{k}{r} M_k$.

17.3.6. На полке стоят 10 различных книг.

(a) Сколькими способами их можно переставить так, чтобы ни одна книга не осталась на своем месте?

(b) Количество таких перестановок книг, при которых на месте остаётся ровно 4 книги, больше 50 000.

В следующей задаче в ответе можно использовать суммы (аналогично формуле включений и исключений).

17.3.7. (a) Сколькими способами можно расселить 20 туристов по 5 различным домикам, чтобы ни один домик не оказался пустым?

(b) Сколько существует различных сюръекций $f\colon \mathbb{Z}_k \to \mathbb{Z}_n$?

17.3.8. По кругу стоят числа $1, 2, \ldots, n$. Найдите число способов выбрать k из них, чтобы никакие два выбранных числа не стояли рядом.

(b) Найдите число способов рассадить n пар враждующих рыцарей за круглый стол с нумерованными местами, чтобы никакие два враждующих рыцаря не сидели рядом.

17.3.9. Куб с ребром длины 20 разбит на 8000 единичных кубиков, и в каждом кубике записано число. Известно, что в каждом столбике из 20 кубиков, параллельном ребру куба, сумма чисел равна 1 (рассматриваются столбики всех трех направлений). В некотором кубике записано число 10. Через этот кубик проходят три слоя $1 \times 20 \times 20$, параллельные граням куба. Найдите сумму всех чисел вне этих слоев.

17.3.10.* Сколько существует шестизначных трамвайных билетов, в которых нет двух семерок рядом и всего

(a) не более трех семерок;

(b) не более четырех семерок;

(c) сколько угодно семерок?

17.3.11.* Докажите следующую формулу:

$$n! \cdot x_1 x_2 \ldots x_n = (x_1 + x_2 + \ldots + x_n)^n - \\ - \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{n-1} \leqslant n} (x_{i_1} + x_{i_2} + \ldots + x_{i_{n-1}})^n + \\ + \sum_{1 \leqslant i_1 < i_2 < \ldots < i_{n-2} \leqslant n} (x_{i_1} + x_{i_2} + \ldots + x_{i_{n-2}})^n - \ldots + (-1)^{n-1} \sum_{i=1}^{n} x_i^n.$$

Литература

[GDI] *Глибичук А. А.*, *Дайняк А. Б.*, *Ильинский Д. Г.*, *Купавский А. Б.*, *Райгородский А. М.*, *Скопенков А. Б.*, *Чернов А. А.* Элементы дискретной математики в задачах. М.: МЦНМО, 2015;

`http://www.mccme.ru/circles/oim/discrbook.pdf`.

[Prob] Интернет-проект «Задачи» `http://problems.ru`.

[Kru] Р. Крутовский, О графах данного диаметра без малых циклов, препринт. `http://www.mccme.ru/circles/oim/mmks/works2013/krutowski2.pdf`.

20 Конструкции и инварианты

Эта тема доступна и для учеников 6—7 классов, но тогда нужно пользоваться не этим параграфом, а статьёй [LT] и соответствующим разделом книги [GIF].

20.1 Конструкции[7] (1). *А. В. Шаповалов*[8]

Если на вопрос «Может ли?» вы подозреваете ответ «Может», то стоит спросить себя: «Как такое может быть?». Уточните вопрос: «Какими свойствами эта конструкция должна обладать?». Дополнительное знание поможет сильно сузить круг поисков. Задавайте себе вопросы на протяжении всего построения. Вы с удивлением

[7] Эта подборка задач составлена по книгам [Shap14] и [Shap15].

[8] `http://www.ashap.info`.

увидите, как много конструкций окажутся логичными и единственно возможными.

Часто примеров много, а нужен только один. Избыток свободы может сбивать с толку: неясно, с чего начинать. Примените *здравый смысл*, *естественные соображения*. Они ограничивают поле для поиска примера, но зато поиск убыстряется и облегчается. Вообще, ваш опыт гораздо больше, чем вы думаете. Ответом может оказаться *хорошо знакомый объект*, просто надо посмотреть на него под нужным углом.

20.1.1. У двух треугольников равны по две стороны, а также равны высоты, проведённые к третьей стороне. Обязательно ли эти треугольники равны?

20.1.2. Верно ли, что в вершинах любого треугольника можно поставить по положительному числу так, чтобы длина каждой стороны была равна сумме чисел в её концах?

20.1.3. В кружке у каждого участника ровно по 6 друзей. Может ли у каждой пары участников быть ровно по два общих друга?

Конструкцию с большим числом деталей проще строить из одинаковых «кирпичей». Даже если все они одинаковыми быть не могут, попробуйте взять одинаковых побольше. Можно ещё выбрать два вида деталей и посчитать, сколько нужно тех и других.

Ну, а если детали «для сборки» заданы и они разные? Тогда стоит попытаться объединить эти части в *одинаковые блоки*, и строить из блоков.

20.1.4. Назовём неотрицательное целое число *зеброй*, если в его записи строго чередуются чётные и нечётные цифры и среди цифр есть не менее трёх различных. Может ли разность двух 100-значных зебр быть 100-значной зеброй?

20.1.5. Грани параллелепипеда со сторонами 3, 4 и 5 разбиты на единичные клетки. В каждую клетку вписали по натуральному числу. Рассмотрим всевозможные кольца шириной в одну клетку, параллельные какой-нибудь грани. Может ли сумма чисел в каждом таком кольце быть одной и той же?

В задачах, где требуются равные части, приходится выбирать форму частей. Тут может помочь такое соображение: части заведомо равны, если они получаются друг из друга симметрией, сдвигом или поворотами. Так, для квадрата популярны разрезания, переходящие в себя при повороте на 90°, а для правильного треугольника — при повороте на 120°. Для симметричных объектов поиск примера начинают с симметричных или «почти симметричных» конструкций. Симметрия и идея «расположить объекты по кругу» применима и в негеометрических задачах.

20.1.6. Можно ли рёбра куба занумеровать числами -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6 так, чтобы для каждой тройки рёбер, выходящих из одной вершины, сумма была одинакова?

20.1.7. Круг разрезали на несколько равных частей. Обязательно ли граница каждой части проходит через центр круга?

Если к конструкции предъявляются противоречивые требования, присмотритесь внимательнее. Часто эти противоречия мнимые. Так, *большой* периметр не противоречит *малой* площади. Вообще, словам «много», «мало», «сильно» нужно уметь придать в решении точный математический смысл с помощью уравнений и неравенств.

20.1.8.* В море плавает айсберг в форме выпуклого многогранника. Может ли случиться, что 90 % его объёма находится ниже уровня воды и при этом больше половины его поверхности находится выше уровня воды?

20.1.9. Есть три игральных кубика с нестандартными наборами чисел на гранях. Скажем, что кубик A *выигрывает* у кубика B, если при их одновременном бросании число на A будет больше числа на B с вероятностью *больше* 0,5. Может ли первый кубик выигрывать у второго, второй — у третьего, а третий — у первого?

(Приведём равносильную формулировку этой же задачи, не использующую понятие вероятности: для пары кубиков A и B составим 36 упорядоченных пар вида (грань A, грань B). Заменим в каждой паре грань на число, стоящее на грани. Кубик A *выигрывает* у B, если более чем в половине пар первое число больше второго.)

Помешать решить задачу могут невидимые барьеры в голове решателя. Если очевидного решения не видно, надо расширять список вариантов, по возможности до полного. *Инерция мышления* проявляется в том, что ключевой вариант пропускают либо не подозревают, что вариантов более одного. Примените «метод Шерлока Холмса»: отбросьте все невозможные случаи, тогда *последний вариант* окажется возможным, каким бы невероятным он ни казался.

Рис. 3.1:

20.1.10. На столе лежат 9 яблок, образуя 10 рядов по 3 яблока в каждом (см. рис. 3.1). Известно, что у девяти рядов веса одинаковы, а вес десятого ряда отличается. Есть электронные весы, на которых за рубль можно узнать вес любой группы яблок. Какое наименьшее число рублей надо заплатить, чтобы узнать, вес какого именно ряда отличается?

20.1.11. Может ли прямая разбить какой-нибудь шестиугольник на 4 равных треугольника?

Редукция — это сведе́ние сложной задачи к более простой. Так, если сложную конструкцию не удаётся сразу построить целиком, постройте её *необходимую часть*. Даже если эту часть не удастся потом достроить до целого, решение упрощённой задачи может послужить разминкой, после чего вы вернётесь к сложной задаче уже с накопленным опытом.

20.1.12. Барон Мюнхгаузен говорит, что у него есть многозначное число-*палиндром* (т. е. оно читается одинаково слева направо

и справа налево). Написав его на бумажной ленте, барон сделал несколько разрезов между цифрами. Лента распалась на N кусков. Переложив куски в другом порядке, барон увидел, что на кусках по разу записаны числа 1, 2, ..., N. Могут ли слова барона быть правдой?

При построении конструкции может мешать неоднозначность выбора. В *узком месте* всё однозначно или неопределённость минимальна, что сокращает перебор. Начав с узкого места, мы либо быстро придём к противоречию, либо построим большой кусок конструкции. Как искать узкие места? Присмотритесь: они служат препятствиями к построению конструкции или кажутся таковыми.

20.1.13. Записав числа 1, $\frac{1}{2}$, $\frac{1}{3}$, ..., $\frac{1}{10}$ в некотором порядке, соедините их знаками четырёх арифметических действий так, чтобы полученное выражение равнялось 0. (Скобки использовать нельзя.)

20.1.14. Существуют ли три равных семиугольника, все вершины которых совпадают, но никакие стороны не совпадают?

20.1.15. Можно ли разрезать какой-нибудь треугольник на четыре выпуклые фигуры: треугольник, четырёхугольник, пятиугольник и шестиугольник?

При *постепенном конструировании* к примеру идут через цепочку вспомогательных конструкций-*заготовок*. На каждом шаге очередная конструкция *улучшается* до следующей. В заготовке требования к окончательной конструкции выполнены лишь частично. Оставляем *принципиальные* условия, временно забываем или ослабляем *технические*.

20.1.16. Могут ли в остроугольном треугольнике все стороны и высоты измеряться целым числом сантиметров?

20.1.17. Докажите, что существует палиндром, делящийся на 6^{100}. (Напомним, что *палиндром* — это число, которое не меняется при записи его цифр в обратном порядке.)

Наконец, при *конструкции по индукции* результат получается постепенно, но уже за бесконечное число шагов. Таким конструкциям посвящён п. 18.5 «Конечное и счётное».

Продолжить знакомство с конструкциями можно по статье [GK] и книгам [Shap14, Shap15, Shap08].

Указания, ответы и решения

Решения задач и *пути к решению* тщательно разделены. Решение — это то, что решающий задачу в идеале должен написать. Путь к решению должен остаться в голове, здесь он поясняет, как это решение можно было придумать. В задачах на конструкцию решение и путь к решению обычно имеют мало общего.

Решение в задаче на конструкцию состоит из двух частей: *примера*, то есть описания конструкции, и *доказательства* того, что она удовлетворяет условию задачи. Для наших задач вторая часть не представляет труда и обычно опускается. Но иногда из многих возможных примеров нужно ещё выбрать тот, для которого доказательство проще.

20.1.1. *Ответ*: не обязательно.

Решение. Рассмотрим равнобедренный треугольник ACD и точку B на продолжении основания DC. У треугольников ABC и ABD сторона AB и высота AH общие, стороны AC и AD равны. Однако эти треугольники не равны: один — часть другого.

Путь к решению. Попробуем *построить* треугольник по двум сторонам b, c и высоте h, проведённой к третьей стороне. Для этого проведём прямую l (на ней будет лежать третья сторона) и построим вершину A на расстоянии h от l. Две другие вершины треугольника должны лежать на этой прямой на расстояниях b и c от точки A. Проведя окружности указанных радиусов с центром в точке A, получим (при $b > h$ и $c > h$) по две точки пересечения каждой из окружностей с l. Видим, что с точностью до симметрии есть два принципиально разных треугольника: когда вершины выбираются по одну сторону от ближайшей к A точки прямой и по разные стороны от неё.

20.1.2. *Ответ*: верно.

Решение. Впишем окружность в треугольник. Из каждой вершины к окружности проведено два равных отрезка касательных.

Если слово «инвариант» означает «неизменный», то «полуинвариант» — неизменный наполовину.

Бывает так, что мы меняем конструкцию, а какая-то связанная с этой конструкцией величина может меняться только в одну сторону, то есть либо только увеличиваться, либо только уменьшаться. Ещё возможно, что мы делаем ходы и в одну сторону меняется величина, связанная с позицией. Например, при игре в крестики-нолики число заполненных клеток с каждым ходом увеличивается. На ограниченной доске из этого следует, что рано или поздно игра закончится. При игре на бесконечной доске игра может не закончиться никогда, но зато мы можем гарантировать, что позиция не повторится, — ведь число заполненных клеток каждый раз новое!

Чуть более формально: пусть мы меняем конструкции (или позиции) с помощью *разрешённых операций* (или *ходов*) и нам удалось связать с каждой конструкцией/позицией *величину*, значение которой при любом разрешённом преобразовании либо не меняется, либо меняется всегда в одну и ту же сторону. Тогда эта величина называется *полуинвариантом*[14]. Если полуинвариант меняется при каждой операции/ходе, он называет *строгим*, иначе — *нестрогим*.

В типовых задачах «на полуинвариант» доказывают невозможность а) повторения позиций; б) бесконечного числа ходов; в) построения конструкций. Для последнего находят полуинвариант и проверяют, что для получения искомой конструкции из исходной полуинвариант должен был бы *меняться не в ту сторону*.

Но как найти полуинвариант? Начните с проверки типовых величин: сумм, произведений, площадей, периметров и их комбинаций. Если конструкция зависит от целых чисел, то полуинвариантом может быть НОД или НОК.

В следующих двух задачах важно, что полуинвариант целочисленный и не может быть больше определённого числа.

20.5.1. На шахматной доске 100×100 королю разрешено ходить вправо, вверх или вправо-вверх по диагонали. Какое наибольшее число ходов он может сделать?

[14] Эта фраза не является формальным определеним полуинварианта. Но для решения задач формальное определение этого понятия не нужно.

20.5.2. В клетках таблицы 99×99 расставлены целые числа. Если в каком-то ряду (строке или столбце) сумма отрицательна, разрешается в этом ряду поменять знаки всех чисел на противоположные. Докажите, что в итоге можно сделать лишь конечное число таких операций.

Если полуинвариант не целочисленный, то его ограниченность ещё не гарантирует окончания процесса (например, убывающий положительный полуинвариант мог бы бесконечно долго принимать значения $1, 1/2, 1/3, 1/4, \ldots, 1/n, \ldots$). В этих случаях прекращение ходов гарантируется конечным числом позиций.

20.5.3. Дано 10 чисел. За одну операцию можно два неравных числа заменить на два равных с той же суммой. Может ли этот процесс для какого-то исходного набора чисел

(a) продолжаться бесконечно долго;

(b) зациклиться (то есть может ли один и тот же набор чисел возникнуть дважды)?

20.5.4. По кругу выписано несколько чисел. Если для некоторых четырёх идущих подряд чисел a, b, c, d оказывается, что $(a-d)(b-c) < 0$, то числа b и c можно поменять местами. Докажите, что такую операцию можно проделать лишь конечное число раз.

Очень часто положение, в котором нет разрешённых операций, и является искомым.

20.5.5. В клетки прямоугольной таблицы вписаны числа. Разрешается одновременно менять знак у всех чисел некоторого столбца или некоторой строки. Докажите, что многократным повторением этой операции можно превратить данную таблицу в такую, у которой суммы чисел в любой строке или любом столбце неотрицательны.

В комбинаторных задачах полуинвариантом часто служит число комбинаций, например пар, троек, подмножеств или перестановок какого-то вида.

20.5.6. В тридевятом царстве все города подняли над ратушами флаги — голубые либо оранжевые. Каждый день жители узнают

цвета флагов у соседей в радиусе 100 км. Один из городов, где у большинства соседей флаги другого цвета, меняет свой флаг на этот другой цвет. Докажите, что со временем смены цвета флагов прекратятся.

Некоторые конструкции создаются «методом последовательного улучшения». Мы берём несовершенную конструкцию и начинаем её преобразовывать. Полуинвариант гарантирует завершение процесса и достижение нужного эффекта в конце.

20.5.7. В парламенте каждый депутат имеет не более трёх врагов. Докажите, что парламент можно так разбить на две палаты, что у каждого депутата в его палате будет не более одного врага.

20.5.8. На плоскости дано 100 красных и 100 синих точек, никакие три из которых не лежат на одной прямой. Докажите, что можно провести 100 непересекающихся отрезков с концами разных цветов.

Полуинвариант может быть и *нестрогим*, т. е. не меняться при некоторых ходах. Тогда полезно найти ещё один полуинвариант, который строго меняется как раз тогда, когда первый остаётся неизменным.

20.5.9. На шахматной доске 100×100 королю разрешено ходить вправо, вверх, вправо-вверх или вправо-вниз по диагонали. Докажите, что он может сделать лишь конечное число ходов.

Если и второй полуинвариант оказывается нестрогим, то приходится рассматривать и третий, и четвёртый и т. д. В этом случае естественно рассматривать наборы значений полуинвариантов как строки, упорядоченные *лексикографически* (как слова в словаре: сравниваются первые элементы, при равенстве — вторые и т. д. и так до первого несовпадения).

20.5.10. В колоде часть карт лежит рубашкой вниз. Время от времени Петя вынимает из колоды пачку из нескольких подряд идущих карт, в которой верхняя и нижняя карты лежат рубашкой вниз (в частности, может вынуть просто одну карту рубашкой вниз), переворачивает эту пачку как одно целое и вставляет в то же место колоды. Докажите, что независимо от того, как Петя выбирает пачки, в конце концов все карты лягут рубашкой вверх.

21 Алгоритмы

21.1 Игры (1)[15]. *Д. А. Пермяков, М. Б. Скопенков, А. В. Шаповалов*

На конкретных примерах мы познакомимся с некоторыми красивыми идеями теории игр. Общие методические указания по теме «Игры» можно найти в соответствующем разделе книги [GIF].

Симметричная стратегия

Самая распространённая стратегия в играх — *симметричная* (а также её обобщение — *дополняющая*). Для решения последующих задач полезно знакомство с п. 20.2 «Инварианты I», поскольку многие стратегии в играх основаны на инвариантах (пример инварианта — симметричность позиции).

21.1.1. (a) Двое по очереди выкладывают доминошки на шахматную доску. Каждая доминошка покрывает ровно две клетки доски, каждая клетка может быть покрыта не более чем одной доминошкой. Проигрывает тот игрок, который не может положить очередную доминошку. Кто выигрывает при правильной игре? Как он должен для этого играть?

(b) То же для доски 8×9.

Вот что означают вопросы этой задачи. В ответе на первый вопрос нужно назвать игрока, который выигрывает при *любой* игре своего противника. В ответе на второй вопрос нужно привести *алгоритм* действий этого игрока, который гарантирует выигрыш (*выигрышную стратегию*). Важно чётко отделять *сам* алгоритм от *доказательства* того, что алгоритм приводит к желаемому результату.

Второй пункт этой задачи показывает, что не всегда симметричность позиции гарантирует, что симметричная стратегия работает.

[15]Подпункты «Симметричная стратегия», «Выращивание дерева позиций», «Передача хода» написаны Д. А. Пермяковым и М. Б. Скопенковым, «Игры-шутки», «Игра на опережение», «Накопление преимущества» — А. В. Шаповаловым, «Смесь» — всеми тремя авторами.

21.1.2.° (Загадка.) К какому результату приведёт попытка чёрных зеркально-симметрично копировать ходы противника в обычных шахматах при правильной игре белых? Выберите верный вариант ответа:

1) к ничьей; 2) к выигрышу белых; 3) к выигрышу чёрных.

Ключевой идеей является не столько симметрия, сколько разбиение всех возможных позиций на пары. *Дополняющая стратегия* состоит в том, чтобы на ход противника отвечать ходом во вторую позицию соответствующей пары.

21.1.3. На шахматной доске стоит король. Двое по очереди ходят им. Проигрывает игрок, после хода которого король оказывается в клетке, в которой побывал ранее. Кто выигрывает при правильной игре и как он должен для этого играть?

Игра на опережение

Игра на опережение — распространённый приём в нематематических играх. Но и в математических играх бывает, что выигрыш достаётся тому, кто первый сумеет занять ключевое положение. После этого, как правило, работает дополняющая стратегия.

21.1.4. Есть 9 запечатанных прозрачных коробок соответственно с $1, 2, 3, \ldots, 9$ фишками. Двое играющих по очереди берут по одной фишке из любой коробки, распечатывая, если необходимо, коробку. Проигрывает тот, кто последним распечатает коробку. Кто из них может всегда выиграть независимо от игры противника?

21.1.5. В одном из углов шахматной доски лежит плоский картонный квадрат 2×2, а в противоположном — квадрат 1×1. Двое играющих по очереди перекатывают каждый свой квадрат через сторону: Боря — большой квадрат, а Миша — маленький. Боря выигрывает, если не позднее 100-го хода Мишин квадрат окажется на клетке, накрытой Бориным квадратом. Может ли Боря выиграть независимо от игры Миши, если

(a) первым ходит Боря;

(b) первым ходит Миша?

Накопление преимущества

Накопление преимущества — тоже весьма распространённый приём в нематематических играх. В математических играх накопление обычно связано с каким-нибудь полуинвариантом. Поэтому для изучения таких игр полезно знакомство с п. 20.5 «Полуинварианты». При этом надо придумать алгоритм, ведущий к накоплению независимо от сопротивления соперника.

21.1.6. Миша стоит в центре круглой лужайки радиуса 100 метров. Каждую минуту он делает шаг длиной 1 метр. Перед каждым шагом он объявляет направление, в котором хочет шагнуть. Катя имеет право заставить его сменить направление на противоположное. Может ли Миша действовать так, чтобы в какой-то момент обязательно выйти с лужайки, или Катя всегда сможет ему помешать?

21.1.7. На клетчатой доске $1 \times 100\,000$ (вначале пустой) двое ходят по очереди. Первый может за ход выставить два крестика в любые два свободных поля доски. Второй может стереть любое количество крестиков, идущих подряд — без пустых клеток между ними. Если после хода первого образуется 13 или более крестиков подряд, он выиграл. Может ли первый игрок выиграть при правильной игре обеих сторон?

21.1.8. Двое играющих по очереди ломают палку: первый на две части, затем второй ломает любой из кусков на две части, затем первый — любой из кусков на две части и т. д. Один из игроков выигрывает, если сможет после какого-то из своих ходов сложить из 6 кусков два равных треугольника. Может ли другой ему помешать?

Игры-шутки

В *играх-шутках* побеждает всегда одна из сторон независимо от её желания.

21.1.9. (а) На столе лежат 2015 кучек по одному ореху. За один ход разрешается объединить две кучки в одну. Двое играющих делают

ходы по очереди, кто не сможет сделать ход, тот проигрывает. Кто выиграет?

(b) То же, но разрешается объединять кучки только с одинаковым числом орехов.

21.1.10. Дана клетчатая полоса $1 \times N$. Двое играют в следующую игру. На очередном ходу первый игрок ставит в одну из свободных клеток крестик, а второй — нолик. Не разрешается ставить в соседние клетки два крестика или два нолика. Проигрывает тот, кто не может сделать ход. Кто из игроков выигрывает при правильной игре? Как он должен для этого играть?

Кроме игр-шуток бывают и *почти шутки*, где выигрышная стратегия такова: если есть выигрыш в один ход, его надо сделать, иначе можно делать любой ход. Или, наоборот: делать любой ход, кроме тех, которые проигрывают в один ход. В таких играх важно догадаться, кому обязательно представится возможность сделать выигрышный ход или кто будет вынужден сделать проигрывающий ход, — и доказать это. Кроме того, выигрышная стратегия может состоять в достижении позиции, после которой игра превращается в игру-шутку с нужным исходом.

21.1.11. В десяти корзинах лежат яблоки: 1, 3, 5, ..., 19 яблок. Сначала берёт одно яблоко из любой корзины Вася, потом — Гена, потом Лёва, потом опять Вася и т. д. по кругу. Проигрывает тот, после чьего хода в каких-то корзинах станет яблок поровну. Кто из них не может избежать проигрыша?

21.1.12. Из спичек сложен клетчатый квадрат 9×9, сторона каждой клетки — одна спичка. Петя и Вася по очереди убирают по спичке, начинает Петя. Выиграет тот, после чьего хода не останется целых квадратиков 1×1. Кто может действовать так, чтобы обеспечить себе победу, как бы ни играл его соперник?

Выращивание дерева позиций

Один из универсальных способов анализа игры — *выращивание дерева позиций*.

21.1.13. *Ферзя — в угол, или «цзяньшицзы».* Ферзь стоит на d1. Двое по очереди ходят им по направлению вверх, вправо или вправо-вверх. Выигрывает тот, кто поставит его на h8. Кто выигрывает при правильной игре и как он должен для этого играть?

Если не получается, подумайте сначала над следующим вопросом.

21.1.14.° Кто выигрывает в игре из предыдущей задачи, если в начальный момент ферзь стоит на клетке f4? Выберите верный вариант ответа:

1) первый игрок; 2) второй игрок.

Выращивание дерева позиций означает полный анализ игры. Перейдём теперь к более сложной идее *передачи хода*, которая помогает даже тогда, когда для полного анализа нет никакой возможности.

Передача хода

21.1.15. В *двухходовых* шахматах фигуры ходят по обычным правилам, только за каждый ход разрешается сделать ровно два хода одной фигурой. Цель игры — съесть короля соперника. Правила троекратного повторения позиции и 50 ходов не действуют[16]. Докажите, что белые в двухходовых шахматах могут играть так, что заведомо не проиграют (т. е. либо выиграют, либо сыграют вничью).

21.1.16.° Правила *шахмат без цугцванга*[17] отличаются от правил обычных шахмат только добавлением возможности пропустить свой ход для каждого из игроков. Могут ли чёрные выиграть при правильной игре белых? Выберите верный вариант ответа:

1) могут; 2) не могут.

[16] Если не знаете, что это за правила, игнорируйте это предложение.

[17] *Цугцвангом* в шахматах называется такая позиция для игрока, в которой любой его ход эту позицию ухудшает.

[BL] *Барг А.*, *Лицын С.* Что есть фортуна? // Квант. 1990. № 9. С. 8–16.

[Ka] *Карпов Я.* Оптимальная кодировка почтового индекса // Квант. 1987. № 11. С. 19–20.

[Bu] *Бугаенко В. О.* Турниры им. Ломоносова. Конкурсы по математике. М.: МЦНМО-ЧеРо. 1998. См. также `\http://turlom.olimpiada.ru`.

Выразимость для функций алгебры логики

[BMS] *Белов А.*, *Митрофанов И.*, *Скопенков А.*, *Чиликов А.*, *Шапошников С.* 13-я проблема Гильберта о суперпозициях функций; `http://www.turgor.ru/lktg/2016/5/index.htm`

22 Вероятность[19]. *А. А. Заславский*

Данный параграф посвящён простейшим понятиям и применениям теории вероятности. Для его изучения необходимо знакомство с основами комбинаторики, например с п. 17.1 «Подсчёт числа способов» и 17.3 «Формула включений и исключений» данной книги. Кроме того, знакомство с теорией вероятностей полезно начинать на «физическом» уровне строгости, как в книгах [Shen], [Kolm]. Здесь же мы сразу даём «математические» определения. Однако мы приводим многие задачи на «практическом» языке и показываем на примерах, как их формализовать. Формализацию остальных задач оставляем читателю. Такая формализация является первым шагом решения, от которого может зависеть ответ. См., например, задачи 22.2.5 (b, c).

[19] Автор благодарен Ю. Н. Тюрину за полезное обсуждение.

22.1 Классическое определение вероятности (1).

Рассмотрим эксперимент, имеющий m равновозможных исходов, например бросание игральной кости, вытаскивание карты из колоды и т. д. Если интересующее нас событие (например, выпадение шестёрки, вытаскивание туза и т. д.) происходит в a из этих исходов, то *вероятность* события считают равной $p = a/m$.

Это пояснение полезно для начинающего, но не является математическим определением. Вот математическое определение.

Вероятностью подмножества A конечного множества M называется число

$$P(A) = P_M(A) := |A|/|M|.$$

Далее, если не оговорено противное, множество M фиксировано и пропускается из обозначений. Тогда вероятность определена для всех его подмножеств. Их часто называют *событиями*.

22.1.1. Из колоды в 52 карты вытаскивается одна карта. Найдите вероятность того, что она окажется

(a) чёрной масти; (b) тузом; (c) картинкой;

(d) дамой пик; (e) королём или бубной.

Например, в задаче 22.1.1 (c) множество M («всех возможных исходов») совпадает с множеством карт в колоде, а множество A («исходов, в которых происходит рассматриваемое событие») — с множеством картинок. Так эта и многие другие вероятностные задачи могут быть строго сформулированы на комбинаторном языке.

22.1.2. Монета бросается 3 раза. Найдите вероятность выпадения

(a) трёх орлов; (b) двух орлов и решки.

22.1.3. Найдите вероятность того, что при бросании двух игральных костей

(a) на первой выпадет больше очков, чем на второй;

(b) сумма выпавших очков составит $2, 3, \ldots, 12$.

22.1.4. Найдите вероятность того, что случайное целое число от 1 до 105

(a) делится на 5; (b) делится на 7; (c) делится на 35.

(a′, b′, c′) То же для случайного целого числа от 1 до 100.

22.1.5. Федя знает ответы на 10 вопросов из 30. Билет состоит из двух вопросов. С какой вероятностью Федя ответит на оба вопроса?

Для решения некоторых из вышеприведённых задач полезны следующие.

22.1.6. (a) **Правило сложения.** Пусть $A \cap B = \emptyset$. Выразите $P(A \cup B)$ через $P(A)$ и $P(B)$.

(b) Выразите вероятность $P(A \cup B)$ через $P(A)$, $P(B)$ и $P(A \cap B)$.

(c) **Правило умножения.** Выразите вероятность $P_{M \times N}(A \times B)$ через $P_M(A)$ и $P_N(B)$.

Комментарий: $P_M(A) = P_{M \times N}(A \times N)$ и $P_N(B) = P_{M \times N}(M \times B)$.

22.1.7. (a) В ящике лежат красные и чёрные носки. Какое минимальное количество носков может быть в ящике, если вероятность того, что два случайно вытянутых носка красные, равна $1/2$?

(b) То же, если дополнительно известно, что число чёрных носков чётно.

22.1.8.* (a) С какой вероятностью треугольник, образованный тремя случайными вершинами правильного $2n$-угольника, будет прямоугольным; остроугольным; тупоугольным?

(Если эта задача не получается, то см. следующий пункт.)

(b) Найдите пределы полученных вероятностей при $n \to \infty$. (Подумайте о смысле полученных результатов. Ср. с задачей 22.2.5 (c).)

Указания, ответы и решения

22.1.4. *Ответы*: (a) 0,2; (b) $\frac{1}{7}$; (c) $\frac{1}{35}$; (a′) 0,2; (b′) 0,14; (c′) 0,05.

(a) *Решение* (написано Е. Павловым). Пусть $M = \{1, 2, \ldots, 105\}$ — множество всех возможных исходов, $A = \{5, 10, \ldots, 105\} = \{x \in M : 5 \mid x\}$ — множество благоприятных исходов. Тогда по определению вероятность множества A равна $P(A) = \frac{|A|}{|M|} = \frac{\lfloor \frac{105}{5} \rfloor}{105} = 0{,}2$.

22.1.5. *Ответ*: $\frac{3}{29}$. *Решение* (написано П. Белопашенцевой). Обозначим через M множество всех неупорядоченных пар различных

22.2 Более общее определение вероятности (1)

22.2.1. (a) Один стрелок попадает в цель с вероятностью 0,8, другой — 0,7. Найдите вероятность поражения цели, если оба стреляют одновременно.

(В этой и некоторых других задачах этого пункта формализация приводится после условий.)

(b) Рабочий обслуживает три станка. Вероятности их остановки равны соответственно 0,1; 0,2; 0,15. Найдите вероятность безотказной работы всех станков.

Для формализации вышеприведённых задач необходимо следующее более общее определение. Пусть задано множество M и каждому $m \in M$ поставлено в соответствие неотрицательное число $P(m)$, причём сумма всех этих чисел равна 1. Тогда *вероятностью* события A называется сумма чисел $P(m)$ по всем $m \in A$.

Например, в вышеприведённой задаче разумно считать, что множество M состоит из четырёх элементов: оба стрелка попали, первый попал и второй промахнулся, первый промахнулся и второй попал, оба промахнулись.

22.2.2. Сформулируйте и докажите аналоги правил суммы и произведения для вышеприведённого обобщения.

Приведённое определение можно обобщить на случай бесконечного множества M. (В этом случае для всех $m \in M$, кроме счётного числа, $P(m) = 0$.) Ещё более интересно следующее обобщение.

22.2.3. Найдите вероятность того, что случайная точка правильного треугольника лежит

(a) в треугольнике, образованном средними линиями;

(b) во вписанном круге.

Пусть $A \subset M$ — подмножества прямой (или плоскости, или пространства), имеющие длину. Не все подмножества имеют длину (или площадь или объём), см. замечание в п. 25.5 «принцип Дирихле и его применения в геометрии». Тогда *вероятностью* подмножества A в M называется число

$$P(A) = P_M(A) := L(A)/L(M),$$

где $L(A), L(M)$ — длины подмножеств.

Пусть $A \subset M$ — подмножества плоскости (или пространства), имеющие площадь. Тогда *вероятностью* подмножества A в M называется

$$P(A) = P_M(A) := S(A)/S(M),$$

где $S(A), S(M)$ — площади подмножеств. Аналогично определяется вероятность для подмножеств $A \subset M$ пространства, имеющих объёмы.

Как и в дискретном случае, когда множество M фиксировано, его подмножества, имеющие длину (площадь, объём), часто называются *событиями*.

22.2.4.* Сформулируйте и докажите аналоги правил суммы и произведения для вышеопределенных «геометрических» вероятностей.

22.2.5.* (a) Дуэли в городе Осторожности редко кончаются печальным исходом. Дело в том, что каждый дуэлянт прибывает на место встречи в случайный момент времени между 5 и 6 часами утра и, прождав соперника 5 минут, удаляется. В случае же прибытия последнего в эти 5 минут дуэль состоится. Какая часть дуэлей действительно заканчивается поединком?

(b) Стержень случайным образом ломают на три части. С какой вероятностью из этих частей можно составить треугольник?

(c) Найдите вероятность того, что случайный треугольник является остроугольным.

В задаче 22.2.5 (b) за M можно принять равносторонний треугольник с высотой, равной длине стержня. Так как для каждой точки внутри треугольника сумма расстояний от неё до сторон равна высоте, эти расстояния можно считать равными длинам получившихся при разломе частей стержня. Парадоксально, что у этой задачи (и у других, например, 22.2.5 (c)) имеются другие естественные формализации, дающие другой ответ!

Указания, ответы и решения

22.2.1. (a) *Ответ*: $1 - (1 - 0{,}7)(1 - 0{,}8) = 0{,}94$.

22.3 Независимость и условная вероятность (1)

Следующее определение обобщает ситуацию правила умножения 22.1.6(c). Подмножества (т. е. события) A и $B \neq \emptyset$ конечного множества M *независимы*, если доля (т. е. вероятность) множества $A \cap B$ в B равна доле (т. е. вероятности) множества A в M. Приведём симметричную переформулировку, которая работает и для $B = \emptyset$. Подмножества A и B конечного множества M называются *независимыми*, если

$$|A \cap B| \cdot |M| = |A| \cdot |B|.$$

Основной пример независимых подмножеств — в множестве всех клеток шахматной доски подмножество клеток в первых трёх её строках и подмножество клеток в последних четырёх её столбцах, или, более строго, $A \times N$ и $M \times B$ в $M \times N$.

22.3.1. Зависимы ли следующие подмножества? (Мы называем *зависимыми* подмножества, не являющиеся независимыми.)

(a) Подмножества $\{1, 2\} \subset \{1, 2, 3, 4\}$ и $\{1, 3\} \subset \{1, 2, 3, 4\}$.

(b) Подмножества $\{1, 2\} \subset \{1, 2, 3, 4, 5, 6\}$ и $\{1, 3\} \subset \{1, 2, 3, 4, 5, 6\}$.

22.3.2. Зависимы ли следующие подмножества множества целых чисел от 1 до 105?

(a) Подмножество чисел, делящихся на 5, и подмножество чисел, делящихся на 7.

(b) Подмножество чисел, делящихся на 15, и подмножество чисел, делящихся на 21.

(c) Подмножество чисел, делящихся на 15, и подмножество чисел, делящихся на 5.

(d) Подмножество чисел, делящихся на 10, и подмножество чисел, делящихся на 7.

Следующая переформулировка работает и для более общего определения вероятности, когда не все числа $P(m)$ равны.

Подмножества A и B множества M называются независимыми, если $P(A \cap B) = P(A) \cdot P(B)$.

22.3.3. Подмножества A и B конечного множества независимы тогда и только тогда, когда B и A независимы.

22.3.4. Два дворянина из свиты короля в ожидании выхода его Величества решили сыграть в кости. Они сделали одинаковые ставки и договорились, что тот, кто первым выиграет 10 партий, получает все деньги. При счёте 9:8 появился король и игру пришлось закончить. Как следует поделить деньги?

Это одна из задач, положивших начало теории вероятностей. (Решить её вам будет проще после задачи 22.3.12.) В XVII в. её предложил великому французскому математику Блезу Паскалю его знакомый — один из тех дворян, о которых говорится в задаче. Паскаль понял, что следует поделить деньги пропорционально шансам, которые имели игроки на окончательную победу в момент остановки игры. Он нашёл способ вычисления этих шансов (для любого счёта). Другой метод решения задачи, приводящий к тому же результату, нашёл другой великий математик XVII в. Пьер Ферма. Их методы основаны на следующем понятии.

Условной вероятностью подмножества A при условии подмножества B, для которого $P(B) \neq 0$, называется отношение

$$P(A|B) = P(A \cap B)/P(B).$$

Ясно, что независимость подмножеств A и B равносильна тому, что $P(A|B) = P(A)$.

22.3.5. (a) Известно, что при броске игральной кости выпало чётное число. Найдите вероятность того, что оно меньше 5.

(b) В семье два ребёнка. Известно, что один из них мальчик. Найдите вероятность того, что второй ребёнок тоже мальчик. (Мы предполагаем, что вероятности рождения мальчика и девочки равны половине и что пол второго ребёнка не зависит от пола первого.)

22.3.6. Лампочки выпускаются двумя заводами, причём первый из них производит 70 % всей продукции. Лампочки, произведённые первым заводом, горят с вероятностью 0,98, вторым — 0,95. Найдите вероятность того, что купленная лампочка горит.

Решение этой задачи обобщает следующий факт.

22.3.7. Формула полной вероятности. Если $M = B_1 \sqcup \ldots \sqcup B_n$ и $P(B_j) \neq 0$ (говорят, что $B_1, \ldots, B_n$ — *полная система событий*), то

$$P(A) = P(A|B_1)P(B_1) + \ldots + P(A|B_n)P(B_n).$$

22.3.8. Победитель в поединке двух боксёров определяется большинством голосов трёх судей. Двое судей выносят верное решение с вероятностью p, а третий голосует, бросая монету. Найдите вероятность принятия судьями верного решения.

22.3.9. Отец, мать и сын увлекаются шахматами. Отец обещает сыну приз, если он выиграет две партии подряд из трёх, сыгранных поочерёдно с отцом и матерью. Сын знает, что отец играет лучше матери. С кем ему выгоднее играть первую партию?

22.3.10.* Правила распространённой в ряде стран игры следующие: игрок бросает две кости. Он выигрывает, если сумма выпавших очков равна 7 или 11, и проигрывает, если она равна 2, 3 или 12. Во всех остальных случаях он бросает кости до тех пор, пока не выиграет, выбросив первоначальную сумму, или не проиграет, выбросив 7. Найти вероятность выигрыша.

22.3.11. Лампочки выпускаются двумя заводами, причём первый из них производит 70 % всей продукции. Лампочки, произведённые первым заводом, горят с вероятностью 0,98, вторым — 0,95. Купленная лампочка оказалась бракованной. Найдите вероятность того, что она выпущена первым заводом.

Решение этой задачи обобщает следующий факт.

22.3.12. Формула Байеса. Справедливо равенство $P(B|A) = P(A|B)P(B)$

Часто применяется следствие формул 22.3.7 и 22.3.12:

$$P(X|A) = \frac{P(A|X)P(X)}{P(A|B_1)P(B_1) + \ldots + P(A|B_n)P(B_n)}.$$

22.3.13. Вероятность того, что изделие бракованное, равна 0,04. Если изделие бракованное, то оно пройдёт тест с вероятностью 0,05,

С вероятностью $\frac{2^{n-1}}{2^n-1}$ близнецы оказываются в разных половинах турнирной сетки и могут встретиться только в финале. Отсюда по индукции получаем, что вероятность встречи равна $\frac{1}{2^{n-1}}$. Подробнее см. задачу 16 из книги [Mo].

22.3.15. (a) Пусть k-й жених лучше всех предыдущих. Тогда вероятность того, что он лучший из всех женихов, равна $\frac{k}{n}$, т. е. является возрастающей функцией от k. С другой стороны, очевидно, что вероятность выбрать наилучшего жениха, отвергнув k-го, является убывающей функцией от k. Поэтому пока первая вероятность меньше второй, женихов надо отвергать, а когда первая вероятность станет больше, надо принять предложение первого жениха, превосходящего всех предыдущих.

(b) Если невеста действует по описанной стратегии, то она получает лучшего жениха при выполнении следующих двух условий: номер k этого жениха больше $s = s(n)$ и лучший из первых $k-1$ женихов попадает в число первых s. Вероятность этого равна $\frac{1}{n}\left(1 + \frac{s}{s+1} + \ldots + \frac{s}{n-1}\right)$, что примерно равно $\frac{s}{n}\ln(n/s)$. Потому оптимальное значение s примерно равно $\frac{n}{e}$. При этом вероятность выбрать лучшего жениха при больших n примерно равна $\frac{1}{e}$ (см.[Mo], задача 47, [GZ]).

22.4 Случайные величины (3)

Пусть дано конечное или счётное множество M и для каждого элемента $m \in M$ задано число (вероятность) $P(m) \geqslant 0$, $\sum\limits_{m\in M} P(m) = 1$. Числовая функция X, заданная на M, называется *случайной величиной*. Множество пар $(x_i, p_i), i = 1, 2, \ldots$, где $\{x_1, x_2, \ldots\}$ — множество возможных значений случайной величины X, а $p_i = P(\{m \in M\colon X(m) = x_i\})$, $i = 1, 2, \ldots,$ — соответствующие им вероятности, называется *распределением* случайной величины X.

Комментарий. Как правило, при изучении случайной величины X не требуется знать, на каком множестве она определена. Достаточно знать только её распределение.

Событие $\{m \in M\colon X(m) = x_i\}$ в дальнейшем сокращённо обозначается $X = x_i$.

22.4.1. Монета подбрасывается 5 раз. Найдите распределение числа выпавших орлов.

22.4.2. (a) Вам предлагается такая игра. Вы платите 2 конфеты, затем бросается игральная кость, и вы получаете столько конфет, сколько очков выпадает. Выгодна ли вам эта игра?

(b) Правила те же, только в случае выпадения 1 очка вы платите 100 конфет. (У вас достаточно конфет, чтобы заплатить.) Выгодна ли вам эта игра?

(c) Банк предлагает вам стабильный доход совершенно бесплатно. Вы кладете в банк 8 конфет, после чего бросается игральная кость. Если выпадает 2, 3 или 4 очка, то вы получаете назад свой вклад плюс еще 1 конфету вдобавок. Если выпадает 5 или 6 очков ("рост рынка"), то вы получите даже плюс 2 конфеты вдобавок. А если выпадет 1 очко, то это "кризис", и вы теряете весь свой вклад. Выгодна ли вам эта игра?

Математическим ожиданием или *средним значением* случайной величины X называется сумма

$$E(X) = \sum x_i p_i = x_1 P(X = x_1) + x_2 P(X = x_2) + \dots.$$

Комментарий. Если множество значений случайной величины бесконечно, то это определение нуждается в уточнении. Сумма ряда в правой части называется *математическим ожиданием*, только когда этот ряд сходится абсолютно. В противном случае говорят, что у величины X *не существует математического ожидания.* Например, пусть случайная величина X принимает значение $n \in \mathbb{N}$ с вероятностью $p_n = \frac{1}{n(n+1)}$. Тогда ряд $\sum np_n = \sum \frac{1}{n+1}$ расходится, т. е. $E(X)$ не существует. В дальнейшем мы предполагаем, что для всех рассматриваемых случайных величин математические ожидания существуют, т. е. ряд $\sum x_i P(X = x_i)$ сходится абсолютно.

22.4.3. a) Докажите, что математическое ожидание случайной величины X, заданной на множестве M, равно $\sum\limits_{m \in M} X(m)P(m)$.

b) Докажите, что если $E(X) \leqslant x$, то существует $m \in M\colon X(m) \leqslant x$.

c) Пусть случайная величина X при всех $m \in M$ принимает одно и то же значение μ: $X(m) = \mu$. Найдите $E(X)$.

(d) Выразите $E(aX + bY)$, где a, b — вещественные числа, а X, Y — случайные величины, через a, b $E(X)$, $E(Y)$.

(e) Можно ли выразить $E(XY)$ через $E(X)$ и $E(Y)$?

Случайные величины X и Y называются *независимыми*, если события $X = x_i$ и $Y = y_j$ независимы при любых x_i, y_j, т. е.

$$P(\{m \in M\colon X(m) = x_i \text{ и } Y(m) = y_j\}) = P(X = x_i)P(Y = y_i).$$

Неформально независимость означает, что значения одной из случайных величин не влияют на распределение другой.

22.4.4. Докажите, что если случайные величины X и Y независимы, то математическое ожидание их произведения равно произведению их математических ожиданий: $E(XY) = E(X)E(Y)$.

Дисперсией случайной величины X называется число $D(X) = E\big((X - E(X))^2\big)$.

Комментарий. Если множество значений случайной величины бесконечно, то дисперсия может не существовать. В дальнейшем предполагается, что для всех рассматриваемых случайных величин дисперсия существует.

22.4.5. Докажите, что $D(X) = E(X^2) - E(X)^2$.

22.4.6. Докажите, что если X и Y независимы, то $D(X + Y) = D(X) + D(Y)$.

22.4.7. Неравенство Чебышёва. Докажите, что для любой случайной величины X и любого $\varepsilon > 0$ выполняется неравенство

$$P(|X - E(X)| \geqslant \varepsilon) \leqslant D(X)/\varepsilon^2.$$

22.4.8. Федя знает ответы на 20 из 30 вопросов. В билет входят 3 вопроса. Найдите распределение числа вопросов, на которые Федя сможет ответить.

22.4.9. Две одинаковые колоды карт перетасовываются, и карты последовательно парами выкладываются на стол. Найдите среднее значение числа пар, карты в которых совпадают.

22.4.10. В городе N предприниматели обязаны предоставлять всем рабочим выходной, если хотя бы у одного из них день рождения. Остальные дни являются рабочими. Сколько человек следует принять на работу, чтобы среднее значение числа рабочих человекодней было максимальным?

22.4.11. В задаче 22.4.8 найдите среднее значение Фединой оценки (если Федя ответит на 3 вопроса, он получит 5, на $2-4$ и т. д.).

22.4.12. В распространённой азартной игре игрок может делать ставку на один из номеров от 1 до 6. Бросаются 3 кости, и если выбранный номер выпал хотя бы на одной, то игрок получает свою ставку плюс столько же за каждое появление выбранного номера. Выгодна ли игра для игрока?

22.4.13. (Загадка.) Площадка имеет форму квадрата со стороной 350 м. При измерении стороны вероятность ошибки ± 10 м равна 0,16, ± 20 м — 0,08, ± 30 м — 0,05. Найдите среднее значение измеренной площади.

Комментарий. На самом деле ответ на этот вопрос зависит от того, как формализовано понятие измерения площади. Если независимо измерить каждую из сторон квадрата и перемножить полученные значения, то по задаче 22.4.4 среднее значение будет равно 350^2 м^2. Если же измерить только одну сторону и возвести результат в квадрат, то ответ будет другим.

22.4.14. В ряд в случайном порядке выписаны m единиц и n нулей. Найдите среднее число серий из k одинаковых цифр подряд.

22.4.15. Из колоды в 52 карты вынимаются карты до первого туза. Сколько карт в среднем будет вынуто?

22.4.16. По узкой дороге в одном направлении едут n машин. Вначале скорости всех машин различны. Каждая машина едет с постоянной скоростью, пока не догонит едущую впереди, после чего

едет со скоростью передней машины. В результате через достаточно большое время машины разбиваются на несколько групп. Найдите среднее значение числа групп.

Указания, ответы и решения

22.4.9. *Ответ*: 1.

22.4.10. *Ответ*: 364 или 365.

Вероятность того, что в данный день ни у одного из n рабочих не будет дня рождения, равна $(364/365)^n$. Следовательно, среднее число рабочих человеко-дней равно $365n(364/365)^n$. Это выражение достигает максимального значения при n, равном 364 или 365 (см. задачу 34 из книги [Mo]).

22.4.14. Вероятность того, что данная серия из k подряд идущих цифр состоит из одинаковых цифр, равна

$$\frac{m(m-1)\dots(m-k+1)+n(n-1)\dots(n-k+1)}{(m+n)(m+n-1)\dots(m+n-k+1)}.$$

Умножив её на общее число серий, равное $m+n-k+1$, получим искомое среднее.

22.4.15. Четыре туза делят колоду на пять кусков. Так как средние длины этих кусков равны, до первого туза лежит в среднем $48/5$ карт (см. задачу 40 из книги [Mo]).

22.4.16. k-я машина является головной машиной группы тогда и только тогда, когда её начальная скорость меньше, чем у всех передних машин, вероятность чего равна $1/k$. Поэтому искомое среднее равно $1+1/2+\ldots+1/n$, что при больших n примерно равно $\ln n$.

22.5 Испытания Бернулли (3)

Испытаниями Бернулли называется последовательность n независимых случайных величин, каждая из которых принимает два

значения: 1 с вероятностью p и 0 с вероятностью $q = 1 - p$. Обычно появление 1 называют *успехом*, а 0 — *неудачей*.

Приведём другое определение испытаний Бернулли. Пусть M — множество n-мерных векторов, все координаты которых равны 0 или 1, и для каждого $x \in M$ задана вероятность $P(x) = \Pi_{i=1}^{n} p_i$, где $p_i = p$, если $x_i = 1$, и $p_i = q = 1 - p$, если $x_i = 0$. Элементы множества M тоже назовём *испытаниями Бернулли*.

Комментарий. Оба определения являются эквивалентными в следующем смысле. Очевидно, что определённые на множестве M случайные величины x_i независимы и каждая из них принимает значение 1 с вероятностью p и 0 с вероятностью q. Поэтому каждый вектор $x \in M$ можно рассматривать как набор значений n независимых случайных величин x_i.

Случайная величина $X = \sum x_i$ называется *числом успехов*.

22.5.1. В n испытаниях Бернулли с вероятностью успеха p найдите

а) вероятность ровно k успехов;

б) среднее значение числа успехов;

в) дисперсию числа успехов;

г) наиболее вероятное значение числа успехов.

22.5.2. Закон больших чисел. Пусть X — число успехов в n испытаниях Бернулли с вероятностью успеха p. Пусть $t > 0$. Докажите, что

$$P\left(\left|\frac{X}{n} - p\right| \geqslant t\sqrt{\frac{pq}{n}}\right) \leqslant \frac{1}{t^2}$$

Указание. Примените неравенство Чебышёва.

Закон больших чисел означает, что при большом числе испытаний вероятность того, что частота успеха сильно отличается от его вероятности, мала. На самом деле этот закон справедлив не только для испытаний Бернулли: если наблюдать много независимых реализаций произвольной случайной величины, то их среднее с большой вероятностью будет мало отличаться от её математического ожидания. Этот закон позволяет, например, проводить социологические исследования, в которых на основе опроса некоторого количества случайно выбранных людей (достаточно большого,

но составляющего малую часть всего населения) делаются выводы о распространённости в обществе тех или иных мнений и предпочтений.

22.5.3. Пассажиру купейного вагона удобно, если все его попутчики одного с ним пола. Какая часть пассажиров испытывает удобства?

22.5.4. Вероятность рождения мальчика равна 0,515. Найдите вероятность того, что среди 6 детей не более 2 девочек.

22.5.5. Кооператив отгружает железные балки. Средняя длина балки 3 м, дисперсия 0,09 м^2. Сколько балок надо заказать, чтобы с вероятностью, не меньшей чем 0,999, хотя бы 1000 из них имели длину не менее 2 м?

22.5.6. Найдите среднее число испытаний до первого успеха, если вероятность успеха равна p.

22.5.7. Проводятся независимые испытания с вероятностью успеха 0,8. Испытания проводятся до первого успеха, но не более четырёх раз. Найдите среднее число испытаний.

22.5.8. (Загадка.) Старик ловил неводом рыбу ровно тридцать лет и три года. Каждый день он ловил ровно 7 рыб, которых как раз хватало на ужин. Живущий у старухи кот-долгожитель ест только макрель, которая ловится вдвое реже остальных рыб. В результате он 700 раз оставался голодным. Плавает ли макрель в море косяками или поодиночке?

Комментарий. Конечно, точно ответить на поставленный вопрос невозможно. Однако можно оценить, какая из двух гипотез лучше согласуется с данными.

Указания, ответы и решения

22.5.1. *Ответы*: а) $\binom{n}{k}p^k q^{n-k}$;

б) np;

в) npq;

г) $\lfloor np \rfloor$, если $\{np\} \leqslant q$, и $\lfloor np \rfloor + 1$, если $\{np\} \geqslant q$ (при равенстве соответствующие вероятности совпадают). *Указание.* Найдите отношение вероятностей ровно k успехов и ровно $k+1$ успехов.

преобразования», § 5 «Разрешимость в радикалах», § 24 «Группы» и статьи [Sk15].

23.1 Порядок, тип, сопряжённость (1)

23.1.1. Пятнадцать школьников сидят на пятнадцати пронумерованных стульях. Каждую минуту добрый преподаватель пересаживает их по следующей схеме:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 5 & 10 & 8 & 11 & 14 & 15 & 6 & 13 & 1 & 4 & 9 & 7 & 2 & 12 \end{pmatrix}.$$

Через сколько минут все школьники впервые окажутся на своих первоначальных местах?

Перестановка множества — запись элементов этого множества в некотором порядке. Если говорить более строго, *перестановкой* множества называется взаимно однозначное отображение этого множества на себя (т. е. биекция). (Перестановку f удобно изображать в виде *ориентированного графа*, вершины которого — элементы множества, а рёбра идут из вершины a_k в вершину $f(a_k)$.) Перестановка множества $\{a_1, a_2, \dots, a_n\}$, переводящая a_k в $f(a_k)$, записывается в виде

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix};$$

обычно $a_k = k$ для всех $k = 1, \dots, n$.

Обратной к f перестановкой называется перестановка f^{-1}, определённая формулой $f(f^{-1}(x)) = x$. Она записывается в виде

$$\begin{pmatrix} f(a_1) & f(a_2) & \dots & f(a_n) \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Композицией перестановок f и g называется перестановка $f \circ g$, определённая формулой $(f \circ g)(x) := f(g(x))$.

23.1.2. Найдите композиции

(a) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Циклом $(a_1, a_2, \ldots, a_n)$ называется перестановка

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \\ a_2 & a_3 & \ldots & a_n & a_1 \end{pmatrix}$$

множества, содержащего элементы $a_1, a_2, \ldots, a_n$, которая переводит a_n в a_1 и a_i в a_{i+1} для любого $i < n$, а каждый из остальных элементов переводит в себя.

На этом языке результаты задачи 23.1.2 можно коротко выразить так: $(12) \circ (132) = (13)$ и $(123) \circ (132) = (1)$.

23.1.3. Найдите композиции (перестановок на множестве цифр)
(a) $(12) \circ (23)$; (b) $(23) \circ (12)$; (c) $(12) \circ (13) \circ (12)$;
(d) $(12345) \circ (12)$; (e) $(12345) \circ (56789)$.
Ответ дайте в виде композиции непересекающихся циклов. Например, $(123) \circ (234) = (12) \circ (34)$.

Далее знак композиции опускается.

23.1.4. Для любой перестановки f существует $n > 0$, для которого $f^n = \mathrm{id}$ (т. е. после n-кратного применения перестановки f каждый элемент перейдёт в себя).

Порядком $\operatorname{ord} f$ перестановки f называется наименьшее целое положительное число n, для которого $f^n = \mathrm{id}$.

23.1.5. Существуют ли перестановки 9-элементного множества порядков 7; 10; 12; 11?

23.1.6. Чему равен порядок композиции непересекающихся циклов из $n_1, \ldots, n_k$ элементов соответственно?

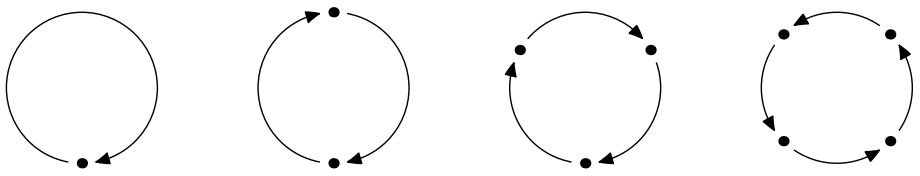

Рис. 3.21: Перестановка типа $\langle 1, 2, 3, 4 \rangle$

Перестановки $(n_1 + \ldots + n_k)$-элементного множества из задачи 23.1.6 называются перестановками *типа* $\langle n_1, \ldots, n_k \rangle$. Например, перестановки $(14)(253)$, $(15)(432)$ типа $\langle 2, 3 \rangle$, а перестановка $(1)(3)(245)$ — другого типа $\langle 1, 1, 3 \rangle$.

23.1.7. Найдите число перестановок типа
(a) $\langle 2,3\rangle$; (b) $\langle 3,3\rangle$; (c) $\langle 1,2,3,4\rangle$.

Перестановки a и b называются *сопряжёнными*, если $a = xbx^{-1}$ для некоторой перестановки x.

23.1.8. (a) Перестановки a и b сопряжены тогда и только тогда, когда их типы одинаковы.

(b) Пусть a и x — произвольные перестановки n-элементного множества. Тогда

$$xax^{-1} = \begin{pmatrix} x(1) & x(2) & \dots & x(n) \\ x(a(1)) & x(a(2)) & \dots & x(a(n)) \end{pmatrix}.$$

Иными словами, циклическое разложение перестановки xax^{-1} получается из циклического разложения перестановки a заменой каждого элемента на его x-образ: если $a = \prod\limits_{j=1}^{q} (i_{j,1}, i_{j,2}, \dots, i_{j,s_j})$, то

$$xax^{-1} = \prod_{j=1}^{q} (x(i_{j,1}), x(i_{j,2}), \dots, x(i_{j,s_j})).$$

(c) Найдите $gf^{-1}g^{-1}f$ для $f := (1,2,\dots,N)$ и $g := (N, N+1, \dots, L)$.

(d) Вращения куба вокруг больших диагоналей порождают сопряжённые перестановки множества его вершин.

23.1.9. Любая перестановка представляется в виде композиции
(a) непересекающихся циклов;
(b) *транспозиций*, т. е. перестановок, каждая из которых меняет местами некоторые два элемента, а остальные оставляет на месте (иными словами, циклов длины 2);
(c) транспозиций $(1i)$, $i = 2, 3, \dots, n$.

23.1.10. Найдите *две* перестановки, композициями которых можно получить любую перестановку n-элементного множества.

Подсказки

23.1.1. *Ответ*: через 105 минут.

Подсказки

23.2.1. *Ответы*: (a) нет; (b) нет; (c) нет.

23.2.2. *Ответ*: цикл длины n чётен при нечётном n и нечётен при чётном n.

23.2.3. (b) Просуммируйте чётности сомножителей по модулю 2.

23.2.5. *Ответы*: (a) поровну при $n > 1$; (b) $n - k$.

23.2.6. См. [Gr].

23.3 Комбинаторика классов эквивалентности (2)

Этот пункт посвящён подсчёту числа классов эквивалентости (т. е. раскрасок и т. д.). Такой подсчёт подводит читателя к важному понятию *группы преобразований* и к элементарной формулировке *леммы Бёрнсайда*. Формулировка и доказательство этого и других результатов на языке абстрактной теории групп делает их менее доступными. Ср. § 28.

Не требуется, чтобы в раскраске присутствовали все данные цвета. Раскраски, совмещающиеся вращением пространства (т. е. движением пространства, сохраняющим ориентацию и имеющим неподвижную точку), считаются одинаковыми (кроме задачи 23.3.1 (c)).

Следующие определения используются только в задачах 23.3.1.(b), 23.3.6.(e), 23.3.11 (и потому могут быть пропущены при решения остальных задач).

Изоморфизм между графами— такая биекция между множествами их вершин, что для любых двух вершин эти вершины соединены ребром тогда и только тогда, когда их образы при биекции соединены ребром. *Автоморфизм* графа— его изоморфизм на себя.

23.3.1. Сколько существует

(a) раскрасок граней куба в красный и серый цвета;

(b) различных (т. е. неизоморфных) неориентированных графов с 4 вершинами;

(c) раскрасок в r цветов вершин правильного тетраэдра?
Здесь раскраски, совмещающиеся движением пространства (не обязательно сохраняющим ориентацию), считаются одинаковыми.

23.3.2. Для простого p найдите количество замкнутых ориентированных связных p-звенных ломаных (возможно, самопересекающихся), проходящих через все вершины данного правильного p-угольника.

Здесь ломаные, совмещающиеся поворотом, неотличимы.

Задачи 23.3.1 и 23.3.2 простые, их можно решить без идей, приводящих к лемме Бёрнсайда.

23.3.3. Найдите количество раскрасок карусели из n незанумерованных вагончиков в r цветов (т. е. количество раскрасок вершин правильного n-угольника в r цветов, если раскраски, совмещающиеся поворотом, неотличимы) для
(a) $n = 5$; (b) $n = 4$; (c) $n = 6$.

Задачу 23.3.3 для произвольного n можно решить способом, аналогичным придуманному вами для малых n. Однако решение будет громоздким. Приведём более простой (для «очень непростых» n) способ на примере решения задачи 23.3.3 (c).

Назовём (*раскрашенным*) *поездом* раскраску карусели из *занумерованных* вагончиков в r цветов. Тогда всего имеется r^6 поездов из 6 вагончиков.

Распределим поезда по вокзалам так, чтобы на каждом вокзале находились все поезда, полученные из некоторой одной раскраски карусели всевозможными разрубаниями, т. е. искомое количество Z раскрасок равно количеству вокзалов.

Назовем *периодом* $T(\alpha)$ поезда α наименьшую положительную величину циклического сдвига, переводящего поезд α в себя.

23.3.4. Количество поездов на вокзале равно периоду каждого из поездов, стоящих на этом вокзале. В частности, периоды поездов, стоящих на одном вокзале, равны.

На каждом вокзале выберем один поезд. Посадим в него 6 пассажиров и выдадим им билеты с числами 0, 1, 2, 3, 4, 5. Тогда нужно найти общее число $6Z$ пассажиров.

По команде каждый пассажир переходит в (раскрашенный) поезд, полученный из выбранного поезда циклическим сдвигом на число, указанное в билете пассажира. Ясно, что каждый пассажир остается на прежнем вокзале.

23.3.5. (a) В выбранном поезде α останется $6/T(\alpha)$ пассажиров. Более формально, количество тех $s \in \{0,1,2,3,4,5\}$, для которых циклический сдвиг на s переводит поезд α в себя, равно $6/T(\alpha)$.

(b) В каждом поезде α окажется $6/T(\alpha)$ пассажиров.

Значит, общее число $6Z$ пассажиров равно количеству всех пар (α, s), в которых $s \in \{0,1,2,3,4,5\}$ и α — поезд, переходящий в себя при циклическом сдвиге на s вагончиков. Циклический сдвиг на s переводит в себя ровно $r^{\gcd(s,6)}$ поездов. Поэтому

$$6Z = r^6 + r + r^2 + r^3 + r^2 + r.$$

Приведенный план решения можно представить в виде формулы

$$6Z = \sum_x T(x) \cdot \frac{6}{T(x)} = \sum_\alpha \frac{6}{T(\alpha)} = r^6 + r + r^2 + r^3 + r^2 + r.$$

Здесь первое суммирование происходит по всем по всем раскраскам x каруселей, а второе — по всем поездам α.

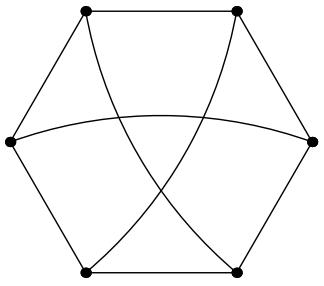

Рис. 3.22: Граф $K_{3,3}$

23.3.6. Найдите количество

(a) раскрасок карусели из n вагончиков в r цветов (см. формализацию и другое решение в [GDI, § 1.5]);

(b) r-цветных ожерелий из $n = 2k+1$ бусин (ожерелья считаются одинаковыми, если они совмещаются либо поворотом вокруг центра ожерелья, либо осевой симметрией ожерелья);

(c) раскрасок незанумерованных граней куба в r цветов;

(d) раскрасок незанумерованных вершин куба в r цветов;

(e) раскрасок незанумерованных вершин графа $K_{3,3}$ (рис. 3.22) в r цветов (раскраски считаются одинаковыми, если они совмещаются автоморфизмом этого графа).

23.3.7. Перечислите все вращения куба (т. е. вращения пространства, переводящие куб в себя). (Эта задача разбита на шаги в п. 15.2.2 «Самосовмещения».)

Приведем план решения задачи 23.3.6 (c). (Пункты (b)–(e) решаются аналогично. Пункт (b) решается и без этого указания.)

Назовём *(раскрашенной) коробкой* (или *замороженной раскраской*) раскраску занумерованых граней куба в r цветов. Тогда всего имеется r^6 коробок.

Распределим коробки по комнатам так, чтобы в каждой комнате находились все коробки, полученные из некоторой одной коробки всевозможными вращениями, т. е. искомое количество Z раскрасок равно количеству комнат.

В каждой комнате выберем одну коробку. Посадим в нее 24 таракана, соответствующих вращениям куба. Тогда нужно найти общее число тараканов $24Z$.

По команде каждый таракан переползает в коробку, полученную из выбранной тем вращением, которое соответствует этому таракану. Ясно, что каждый таракан остается в прежней комнате. Число тараканов, оставшихся в выбранной коробке, равно количеству вращений куба, переводящих эту коробку в себя. Обозначим через $\mathrm{st}\alpha$ количество вращений куба, переводящих (раскрашенную) коробку (т. е. замороженную раскраску) α в себя.

23.3.8. (a) Число тараканов, оказавшихся в коробке α, равно $\mathrm{st}\alpha$. Более формально, если существует вращение, переводящее замороженную раскраску α в замороженную раскраску α', то количество таких вращений равно $\mathrm{st}\alpha$.

(b) В любой другой коробке из выбранной комнаты окажется столько же тараканов, сколько в выбранной коробке. Более формально, для любых двух замороженных раскрасок α и α', переходящих друг в друга при некотором вращении, выполняется равенство $\mathrm{st}\alpha = \mathrm{st}\alpha'$. (Эти равные числа обозначаются $\mathrm{st}x$, где x — соответствующая раскраска незанумерованных граней куба.)

Поэтому общее число тараканов равно количеству всех пар (α, s), в которых s — вращение куба и α — коробка, переходящая в себя при вращении s. Поэтому осталось решить следующую задачу.

23.3.9. Для каждого вращения куба s найдите количество $\mathrm{fix}s$ коробок (т. е. замороженных раскрасок), переходящих в себя при вращении s.

Обозначим через N_x количество замороженных раскрасок, отвечающих раскраске x. Тогда для любой раскраски x число $\mathrm{st}x \cdot N_x$ равно количеству вращений куба, т. е. 24. Поэтому приведенный план решения можно представить в виде формулы

$$24Z = \sum_x \mathrm{st}x \cdot N_x = \sum_\alpha \mathrm{st}\alpha = \sum_s \mathrm{fix}s.$$

Здесь первое суммирование происходит по всем раскраскам x незанумерованных граней, второе — по всем замороженным раскраскам α, а третье — по всем вращениям куба s.

Как сформулировать общий результат, который можно было применять вместо повторения намеченных решений задач 23.3.6 (a), (c)?

23.3.10. Лемма Бёрнсайда. Пусть заданы конечное множество M и семейство $\{g_1, g_2, \ldots, g_n\}$ преобразований этого множества, замкнутое относительно взятия композиции и взятия обратного элемента. Назовём элементы множества M *эквивалентными*, если один из них можно перевести в другой одним из данных преобразований. Тогда количество классов эквивалентности равно $\frac{1}{n}\sum\limits_{k=1}^{n} \mathrm{fix}(g_k)$, где $\mathrm{fix}(g_k)$ — количество элементов множества M, которые преобразование g_k переводит в себя.

24.1 Зачем, для кого и как устроен этот параграф

Мы хотели бы привлечь внимание к теории групп широкого круга людей, интересующихся математикой и программированием: учителей, руководителей кружков, студентов и старшеклассников. В этой теории есть доступные и интересные им результаты-жемчужины. Формулировки таких результатов кратки и используют лишь простейшие определения; доказательства красивы и похожи на решения сложных олимпиадных задач. Именно с таких жемчужин полезно начинать изучение теории, на примере их доказательства показывая, как появляются её основные понятия. К сожалению, в бóльшей части существующей литературы эти жемчужины погребены под огромным количеством немотивированного материала, что делает их неинтересными и недоступными.

Основной вопрос. *Дано семейство G из n перестановок некоторого множества, замкнутое относительно композиции и взятия обратной перестановки. Для каких n обязательно найдётся такая перестановка $g \in G$, что $G = \{g, g^2, \dots, g^n\}$?*

Этот параграф предназначен для тех, кому понятна и интересна формулировка этого вопроса, ср. конец п. 24.2.1. На примере исследования этого просто формулируемого вопроса мы покажем, как *появляются* некоторые основные понятия теории групп. Ср. § 27 «Начинать с языка или содержания?». Мы дадим простое доказательство теоремы, отвечающей на этот вопрос. Оно не претендует на новизну, хотя мы не видели такого доказательства в литературе. (Ввиду элементарности вопроса выяснить новизну не представляется возможным.)

Этот параграф может быть интересен читателю, не знакомому с основами абстрактной теории групп, но изучавшему перестановки и основы теории чисел, например, по § 2, 3, 23. В частности, этот параграф не должен быть единственным и даже первым шагом в теорию групп. Он может быть интересен и читателю, знакомому с этими основами, ибо ответ на сформулированный вопрос нетривиален. Такому читателю может быть достаточно прочитать п. 24.3.

В п. 24.2 проиллюстрировано в задачах, как придумать ответ

и доказательство. Хотя придумать их непросто, *изложить* их можно коротко. В п. 24.3 приведено доказательство, формально независимое от п. 24.2. Освобождение доказательства от деталей, возникших при его придумывании, но не нужных для него самого, — важная часть его проверки.

Для понимания доказательства необходим опыт работы с перестановками и числами, включая теорему Ферма—Эйлера (задачи 3.1.1 и 3.1.5). Знаний по теории групп и опыта работы с определением абстрактной группы не требуется[23]. Небольшое количество необходимых понятий вводятся (и могут быть освоены читателем) в процессе доказательства. Конечно, читателю, не знакомому с основами теории групп, нужно будет самостоятельно доказывать некоторые факты. Хотя эти факты просты, они могут касаться новых для читателя объектов, и тогда ему нужно будет потрудиться. Такие упражнения — важная часть изучения этих понятий. Выполнять их интереснее ради красивых результатов, формулировки которых ясны и доступны неспециалисту (в частности, не используют этих понятий), но в доказательствах которых эти понятия возникают. Это предпочтительнее долгого немотивированного изучения теории. Этот параграф будет особенно интересен читателю, предпочитающему изучить доказательство красивого результата на несколько страниц, самостоятельно разбираясь в деталях, чем прочитать сотню страниц более лёгкого материала, не мотивированных таким результатом. Подробнее см. п. 1.2 «Изучение путём решения и обсуждения задач» и § 28 «О необходимости мотивировок».

Опыт работы с абстрактными группами как раз появится при изучении данного параграфа, хотя в нём формально не используется это понятие. Читатель увидит, что помимо всех рассматриваемых объектов есть ещё одно множество (на котором действуют перестановки). Странным образом оно так никогда и не выходит из тени. В результате естественно возникает общее понятие *группы*. Итак,

[23] В частности, наше доказательство не привлекает явно понятия факторгруппы, в отличие от более традиционных доказательств, см., например, [Br]. Конструкция факторгруппы — одна из простейших конструкций, которая всё-таки уже настолько сложна, что для неё удобнее общее понятие группы вместо группы преобразований. Мы также не используем теорем Силова, хотя наш разбор второго случая похож на их доказательство.

этот параграф посвящён мотивировке важного общего понятия группы (здесь оно не используется, но его и основы соответствующей теории можно найти в [Al, KaSu]). Хороший опыт в работе с основными понятиями теории групп получит и тот, кто не дойдёт до полного доказательства основного результата.

24.2 Как придумать

24.2.1 Постановка задачи (2)

24.2.1. Дано семейство G из 11 перестановок некоторого множества, замкнутое относительно композиции и взятия обратной перестановки (т. е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$). Тогда найдётся перестановка $g \in G$, для которой $G = \{g, g^2, \dots, g^{11}\}$.

24.2.2. Верен ли аналог предыдущего утверждения для аналогичного семейства G из n перестановок при $n = 2$; 3; 4; 5; 6; 7; 8; 9; 10; 12; 15; 21; 1001? (Ответ может быть разным для разных n.)

Группой преобразований называется непустое семейство G преобразований (т. е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т. е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$). Мы будем опускать слово «преобразований» (поскольку это определение «равносильно» обычному определению *группы* ввиду *теоремы Кэли*; ср. с цитатой из книги В. И. Арнольда в п. 28.1).

Если в конечной группе G найдётся перестановка g, из всех возможных степеней которой состоит G (т. е. $G = \{g, g^2, \dots, g^n, \dots\}$), то эта группа называется *циклической*. Примеры циклических и нециклических групп вы привели при решении задачи 24.2.2.

На этом языке основной вопрос из п. 24.1 формулируется так: *для каких n любая группа из n элементов циклическая?*

24.2.3. Для любого n имеется циклическая группа из n элементов.

Почему основной вопрос так интересен?

[24] Операция умножения на множестве ненулевых вычетов по простому модулю имеет общее обобщение с операцией композиции перестановок. Но для исследовании основного вопроса не нужно понимать этого.

(d) Если в конечной группе есть перестановка порядка 3, то число перестановок в группе делится на 3.

(e) **Теорема Лагранжа.** Число перестановок конечной группы делится на порядок любой её перестановки.

(Это «некоммутативная версия» теоремы Ферма—Эйлера, см. задачи 3.1.1 и 3.1.5, а также подсказку к задаче 24.2.7.)

24.2.10. (a) Если число n чётное составное, то существует группа из n перестановок, не являющаяся циклической.

(b) Если число n делится на квадрат простого числа, то существует группа из n перестановок, не являющаяся циклической.

Группа G называется *коммутативной*, если $xy = yx$ для любых $x, y \in G$.

24.2.11. (a) Любая циклическая группа является коммутативной.

(b) Верно ли обратное?

24.2.12. (a) Любая коммутативная группа из 10 перестановок является циклической.

(b) То же для 21 перестановки.

(c) То же для 1001 перестановки.

(d) Для каких n любая коммутативная группа из n перестановок является циклической?

24.2.13. Могут ли в коммутативной группе из 10 перестановок быть две различные перестановки порядка 2?

(Это подсказка к задаче 24.2.12 (a).)

24.2.14.* Для каких n любая группа из n элементов является коммутативной? (Решение этой непростой задачи лучше отложить до разрешения основного вопроса.)

Подгруппой группы G называется подмножество группы G, также являющееся группой.

24.2.15. Теорема Лагранжа. Число перестановок в конечной группе делится на число перестановок в любой её подгруппе.

(Это подсказка к задаче 24.2.13.)

попавшим на эту прямую. Известно, что для любой прямой приращение вдоль неё равно 0. Докажите, что все записанные числа равны 0.

25.7.11. Известно, что для всех вещественных чисел x выполнено неравенство $a_1 \cos x + a_2 \cos 2x + \ldots + a_k \cos kx \geqslant -1$. Докажите, что $a_1 + a_2 + \ldots + a_k \leqslant k$.

25.7.12. На складе лежат 300 сапогов: 100 резиновых, 100 кирзовых, 100 яловых. Среди них поровну левых и правых. Докажите, что из имеющихся сапогов можно составить 50 правильных пар (т. е. в которых правый и левый сапог из одного материала).

В заключение предлагаем вам подумать над задачами 25.8.9 и 25.8.10 из п. 25.8 «Собери квадрат» и вот такой сложной задачей.

25.7.13.* На плоскости даны $n > 2$ непараллельных прямых, не все из которых проходят через одну точку. Докажите, что среди многоугольников, на которые они разбивают плоскость, можно найти $n - 2$ (пустых) треугольника.

Указания, ответы и решения

25.7.2, 25.7.13. Эти задачи подробно разбираются в статье [KK92].

25.8 Собери квадрат (3*). *М. Б. Скопенков, О. А. Малиновская, С. А. Дориченко, Ф. А. Шаров*

Этот пункт посвящён решению такой задачи (для некоторых частных случаев).

Задача. Когда из прямоугольников, подобных данному, можно составить квадрат?

В процессе решения мы познакомимся с красивыми применениями алгебры в комбинаторной геометрии, а именно — систем линейных уравнений и многочленов с целыми коэффициентами. Для

решения задач необходимо первоначальное знакомство с этими темами. Желательно также первоначальное знакомство с задачами на разрезание, см., например, [Sa97].

Наш подход к решению развивает идеи книги [Ya68].

Другой подход к решению — это физическая интерпретация, использующая электрические цепи (хотя без неё решать проще). Познакомиться с этой физической интерпретацией и её применением к решению поставленной задачи можно в статьях [SPD, SMD]. Увлекательный рассказ об истории её возникновения можно прочитать в книге [Ga99].

Наводящие вопросы

— У меня есть мысль! — сказал удав, открывая глаза. — Мысль. И я её думаю.
— Какая мысль? — спросила мартышка.
— Так сразу не скажешь...
— Ух ты! — подпрыгнула мартышка. — Ох, какая хорошая мысль. А можно я её тоже немножко подумаю?

Г. Остёр. Бабушка удава

25.8.1.° Верно ли, что при любых натуральных m и n из нескольких прямоугольников $m \times n$ можно сложить квадрат? Выберите верный вариант ответа:

1) верно; 2) неверно.

25.8.2. Дизайнеру заказали рамы для квадратного окна. На проектах (рис. 3.35 A, B) показано, как должны примыкать стёкла друг к другу и как они должны быть ориентированы (короткой или длинной стороной вверх). Можно ли сделать все стёкла в каждой раме подобными прямоугольниками?

25.8.3. Можно ли разрезать квадрат на три подобных, но неравных прямоугольника?

25.8.4. Можно ли разрезать квадрат на 5 квадратов?

25.8.5. Все полки у шкафа на рис. 3.36 C, как и все лоскутки, из которых сшито одеяло на рис. 3.36 D — квадратные. Являются ли квадратными сами шкаф и одеяло?

A B

Рис. 3.35: Проекты оконных рам; см. задачу 25.8.2

25.8.6. Можно ли замостить всю плоскость попарно различными квадратами, длины сторон которых — целые числа?

25.8.7. Можно ли разрезать квадрат на прямоугольники с отношением сторон $2+\sqrt{2}$? То же для $2-\sqrt{2}$, для $3+2\sqrt{2}$ и для $3-2\sqrt{2}$.

25.8.8. Является ли $1+\sqrt{2}$ суммой квадратов чисел вида $a+b\sqrt{2}$, где a и b рациональны?

Определение. Пусть на прямоугольном листе бумаги нарисовано разбиение на прямоугольники. Разрешается разрезать лист вдоль любого отрезка на два прямоугольника, потом произвести такие операции по отдельности с каждой из получившихся частей и так далее. Если таким образом можно реализовать исходное разбиение, то назовём его *тривиальным*. Например, разбиения на рис. 3.35 тривиальные, а на рис. 3.36 нетривиальные.

Следующие 4 задачи предлагается сначала решить для тривиальных разбиений, а уже потом подумать над произвольными разбиениями. В последующих подпунктах будут даны подсказки к решению этих трудных задач.

25.8.9. Какие прямоугольники можно (тривиально) разрезать на прямоугольники со стороной 1?

C

D

Рис. 3.36: Шкаф и одеяло; см. задачу 25.8.5

25.8.10. Какие прямоугольники можно (тривиально) разрезать на квадраты?

25.8.11. Можно ли квадрат (тривиально) разрезать на прямоугольники с отношением сторон $\sqrt{2}$? То же для $1+\sqrt{2}$.

Все числа, которые можно представить в виде $x = a + b\sqrt{2}$ с рациональными a и b, назовём *хорошими*.

25.8.12. (Основная задача.) При каких хороших x квадрат можно (тривиально) разрезать на прямоугольники с отношением сторон x?

Прямоугольник из квадратов.

Ты, дорога, иду по тебе и гляжу, но мне думается,
Мне думается, в тебе много такого, чего не увидишь глазами.
Уолт Уитмен. Песня большой дороги

В этом подпункте мы наметим новый вариант элементарного решения задач 25.8.10 и 25.8.12. В этом подпункте латинские буквы

a, b, c, d и эти же буквы с индексами обозначают *рациональные* числа.

25.8.13. Можно ли прямоугольник $1 \times \sqrt{2}$ разрезать на квадраты с рациональными сторонами? А со сторонами, которые либо рациональны, либо имеют вид $b\sqrt{2}$? А со сторонами, которые являются произвольными хорошими числами? Те же вопросы для прямоугольников $1 \times (1+\sqrt{2}\,)$ и $1 \times (2+\sqrt{2}\,)$.

Для доказательства невозможности разрезаний естественно использовать площадь и её *аддитивность*: площадь целого равна сумме площадей частей. Вряд ли получится ответить на вопросы задачи 25.8.13 для прямоугольника $1 \times (2+\sqrt{2}\,)$ без следующего обобщения понятия площади (мы обобщаем понятие площади так, чтобы площадь этого прямоугольника стала отрицательной, а площади квадратов оставались неотрицательными).

Определение. Пусть x — действительное число. Назовём *x-площадью* (или *площадью Гамеля*) прямоугольника $(a+b\sqrt{2}\,)\times(c+d\sqrt{2}\,)$ число $(a+bx)(c+dx)$. Число $\bar{s} := a - b\sqrt{2}$ назовём *сопряжённым* к числу $s = a + b\sqrt{2}$.

25.8.14. Обычная площадь прямоугольника $(a+b\sqrt{2}\,)\times(c+d\sqrt{2}\,)$ и сопряжённое к ней число — это одни из его x-площадей. Чему равно x в каждом из случаев?

25.8.15. Найдите все прямоугольники вида $(a+b\sqrt{2}\,)\times(c+d\sqrt{2}\,)$, x-площади которых неотрицательны при всех x.

25.8.16. Аддитивность x-площади. Если прямоугольник разрезан на конечное число прямоугольников, стороны которых — хорошие числа, то для любого $x \in \mathbb{R}$ x-площадь разрезаемого прямоугольника равна сумме x-площадей прямоугольников, на которые он разрезан.

Указание. Начните со случая разрезания на 2 прямоугольника.

25.8.17. Решите задачи 25.8.10 и 25.8.12 для частного случая, когда стороны всех квадратов и всех прямоугольников, участвующих в разрезании, — хорошие числа (разрезание не обязательно тривиально).

В следующих трёх задачах мы считаем, что прямоугольник $s_0 \times t_0$ разрезан на прямоугольники $s_1 \times t_1$, $s_2 \times t_2$, …, $s_N \times t_N$, причем s_0 и t_0 несоизмеримы.

25.8.18. Обозначим

$$P = \{s_0, t_0, s_1, t_1, \ldots, s_N, t_N\}.$$

Тогда можно выбрать такие числа $e_1, e_2, \ldots, e_n \in P$, чтобы любое число $p \in P$ единственным образом представлялось в виде

$$p = as_0 + bt_0 + a_1e_1 + a_2e_2 + \ldots + a_ne_n.$$

Указание. Начните с примера, изображённого на рис. 3.37.

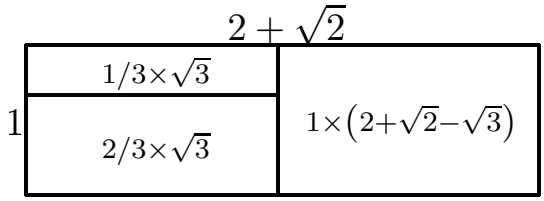

Рис. 3.37: К построению базиса

Зафиксируем набор чисел s_0, t_0, e_1, e_2, …, e_n из задачи 25.8.18. Он называется *базисом*.

Определение. Пусть y — действительное число. Назовём *y-площадью* прямоугольника со сторонами

$as_0 + bt_0 + a_1e_1 + a_2e_2 + \ldots + a_ne_n$ и $cs_0 + dt_0 + c_1e_1 + c_2e_2 + \ldots + c_ne_n$

число $(a + by)(c + dy)$.

Обратите внимание на то, что при $y = x$ и хороших несоизмеримых s_0, t_0 это определение не всегда эквивалентно определению x-площади выше!

25.8.19. Вычислите y-площадь разрезаемого прямоугольника $s_0 \times t_0$. Является ли она неотрицательной при всех y?

25.8.20. Докажите, что для любого y y-площадь разрезаемого прямоугольника $s_0 \times t_0$ равна сумме y-площадей прямоугольников, на которые он разрезан.

Глава 4

О преподавании

А. Б. Скопенков

Редакторы считают важным обсуждение вопросов и идей, затронутых в следующих статьях. При этом мнение авторов статей может не совпадать с мнением редакторов.

26 Олимпиады и математика

To him a thinking man's job was not to deny one reality
at the expense of the other, but to include and to connect
U. K. Le Guin. The Dispossessed[1]

Перед школьниками, их учителями и руководителями кружков встаёт вопрос: готовиться к олимпиадам или к «серьёзной» математике? Некоторые думают, что для первого надо прорешивать задачи последних олимпиад, для второго надо читать вузовские учебники, и что ввиду принципиальной разницы первого и второго бессмысленно пытаться достичь и того, и другого. Я придерживаюсь распространённого мнения о том, что эти подходы недостаточно эффективны и приводят к вредным «побочным эффектам»: школьни-

[1] Для него работой мыслителя было не отрицание одной реальности за счёт другой, а взаимовключение и взаимосвязь. *У. К. Ле Гуин*, «Обделённые» (пер. автора).

ки либо чрезмерно увлекаются *спортивным* элементом в решении задач, либо изучают *язык* математики вместо её содержания[2].

По моему мнению, основу математического образования должно составлять *решение и обсуждение интересных ученику задач, в процессе которых он знакомится с важными математическими идеями и теориями.* Это одновременно подготовит школьника и к математической науке, и к олимпиадам и не нанесёт вред его развитию в целом. Это будет более эффективно и для достижения успеха только в олимпиадах или только в науке (если не учитывать большого количества других факторов, кроме разумной организации занятий).

Как и при естественном развитии самой математики, каждая следующая задача должна быть мотивирована либо практикой, либо уже решёнными задачами (см. подробнее § 27 «Начинать с языка или содержания?» и 28 «О необходимости мотивировок»). Ученик, занимающийся «мотивированной для него» математикой (обычно более элементарной, но содержательной и потому сложной) вместо «немотивированной для него» математики (обычно менее элементарной, но языковой и потому тривиальной), имеет преимущество в дальнейшей учёбе и научной работе. А. Н. Колмогоров говорил, что до тридцати лет математику разумнее всего заниматься решением конкретно поставленных задач. А значит, умение решать сложные задачи является одним из важнейших для молодого математика.

Олимпиадных задач очень много; большинство из них интересны школьнику, и среди них много математически содержательных. Такие задачи могут составить основу изучаемого материала. Однако решение олимпиадных задач без изучения математических идей и теорий недостаточно эффективно для подготовки к олимпиадам (на долгих — год и более — промежутках времени, как и вообще ре-

[2]Имеется обширная литература, в которой в первую очередь излагается содержание, а язык появляется по ходу дела. Однако часто такая *популярная* литература недооценивается ввиду её «недостаточной серьёзности» по сравнению с учебниками *для университета*. Подробнее см. § 27 «Начинать с языка или содержания?».

Кроме того, даже чтение хороших книг без решения задач, как правило, неэффективно.

шение сиюминутных задач без фундаментального развития). А решение олимпиадных задач *вместе* с изучением стоящих за ними математических идей и теорий более эффективно. Это также позволит по-настоящему разобраться в идеях и теориях.

Кроме того, большинству людей легче достичь успеха на олимпиадах в том случае, когда они не считают успех главной целью. Задачу легче решить, если спокойно думать о самой задаче, а не о награде, которая последует за её решением. Поэтому школьник, мотивированный более высокой целью, чем успех на олимпиаде, имеет на этой олимпиаде психологическое преимущество.

См. также п. 1.2 «Изучение путём решения и обсуждения задач».

27 Начинать с языка или содержания?

По моему мнению, именно с *новых идей*, изложенных на уже имеющемся языке, а не с *введения нового языка*, полезно *начинать* изучение любой теории. Удачно представлять основные идеи на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей. Как правило, такие идеи наиболее ярко выражаются доказательствами, подобными приведённым в § 5, 24 и других частях этой книги. Имеется много других ярких примеров, упомянем только фейнмановские лекции по физике (там приводятся физические рассуждения, а не доказательства).

«*Мы стараемся свести к минимуму число понятий, откладывая определения до момента, когда они напрашиваются сами собой, и избегая задач на понимание и применение формальных определений (типа „является ли множество целых чисел группой по сложению?“)*»[Shen].

«*При изложении материала нужно ориентироваться на объекты, которые основательнее всего укореняются в человеческой памяти. Это — отнюдь не системы аксиом и не логические приёмы в доказательстве теорем. Изящное решение красивой задачи, формулировка которой ясна и доступна, имеет больше шансов удержаться в памяти студента, нежели абстрактная теория. Скажем больше, именно по такому решению, при наличии некото-*

рой математической культуры, студент впоследствии сможет восстановить теоретический материал. Обратное же, как показывает опыт, практически невозможно» [Kol, предисловие].

Такой стиль изложения не только делает материал более доступным, но позволяет сильным ученикам (для которых доступно даже абстрактное изложение) приобрести математический вкус и стиль. Это означает разумный выбор проблем для исследования и их мотивировки. Например, математик, понимающий, что теория Галуа мотивируется более важными и более сложными проблемами, чем построимость правильных многоугольников и разрешимость алгебраических уравнений в радикалах, вряд ли станет мотивировать созданную им теорию приложениями, которые можно получить и без его теории. Вкус и стиль означают также ясное изложение собственных открытий, не скрывающее ошибку или известность полученного результата за чрезмерным формализмом. К сожалению, такое — обычно непреднамеренное — сокрытие ошибки часто происходит с математиками, воспитанными на чрезмерно формальных курсах. Происходило это и с автором этих строк; к счастью, все мои серьёзные ошибки исправлялись *перед* публикациями.

Мода на искусственно формализованное изложение привела к следующему парадоксу. По данному *известному понятию* высшей математики зачастую непросто восстановить *конкретный красивый результат*, для которого это понятие действительно необходимо (и при получении которого это понятие возникло).

Доказательство с использованием некоторого нового термина имеют свои преимущества: оно подготавливает читателя к доказательству тех теорем, которые уже трудно или невозможно доказать без этого термина. Однако такие доказательства, как правило, не должны быть *первыми* доказательствами данного результата (легко себе представить результат *первого* знакомства с теоремой Пифагора на основе понятий векторного пространства и скалярного умножения). Кроме того, при приведении «терминологического» доказательства полезно оговорить его мотивированность не доказываемым результатом, а обучением полезному новому методу. Ну и, конечно, важно соблюсти баланс между доказываемым результатом и уровнем предлагаемой абстракции. Вот пример.

Необходимость мотивировок выглядит банальностью. Однако на практике в большинстве курсов и учебников по математике «университетского» уровня либо мотивировок нет, либо приводятся общие слова без ссылок на чёткие формулировки результатов, доступные ученику или неспециалисту, а не скрытые под толщей обозначений и терминов. В тех ситуациях, когда эти общие слова удаётся проверить, они иногда оказываются неадекватными, см. п. 28.2. Для разных людей мотивировки разные: для одних новое определение само по себе интересно, а для других необходима его полезность для уже имеющейся математики и её приложений. Подробнее о «естественно-научном» и «философском» аспектах математики см. в [PS15, конец § 2].

О необходимости мотивировок высказываются открыто, а желание их пропустить не осознают или не афишируют. Судить о том, почему мотивированное изложение не принимается, приходится его сторонникам.

«*Часто имеются непреодолимые трудности к мотивированности определений в курсе. Такое изложение требует высокого уровня общематематической подготовки и мотивированности его слушателей (а обычно большая часть слушателей хочет выучить и сдать). Преподавателю часто жалко времени на мотивировку определений...*» (И. С. Рубанов, из письма).

Думаю, большинство математиков согласны с необходимостью мотивировок. Однако трудно понимать, какие утверждения ученику неизвестны, когда преподавателю известно больше. Ещё труднее понимать, какие вещи для ученика не мотивированы его знаниями, когда знаниями преподавателя мотивировано гораздо больше. Тем более что ученик мотивирован не только знаниями, но доверием преподавателю, оценкой, etc. Может быть не только трудно, но даже неприятно посмотреть на материал с точки зрения неспециалиста и осознать немотивированность изложения, особенно привычного, своего или уважаемого автора. Знаю это по собственному опыту. Поэтому часто необходимость мотивировок *вообще* признаётся, но *в данном конкретном случае* находятся причины неприятия мотивированного изложения. Эти причины не продумываются, поскольку продумывание может привести к неприятному осозна-

29 Кружки и олимпиады как путь в математику и как спорт. *А. Я. Канель-Белов, А. И. Буфетов*

29.1 Введение

Внешкольные занятия математикой, которым посвящена находящаяся в руках у читателя книга, играют в математическом образовании в нашей стране важнейшую роль, которую трудно переоценить. При этом значительное число занятий так или иначе оказываются связанными с олимпиадами. Школьников и их учителей часто сводят вместе математические олимпиады (например, в 1993 году А. Я. был членом жюри московской олимпиады, а девятиклассник А. И. участником — так мы и познакомились).

Многие школьники, особенно на периферии, получают математическое образование, нацеленное в первую очередь на подготовку к олимпиадам. С этим необходимо считаться научным руководителям и организаторам учебного процесса. Даже те, кто не занимается подготовкой к олимпиадам в тренерском смысле этого слова, активно используют идеи и задачный материал олимпиад.

У истоков олимпиадного движения стояли великие ученые, однако позже олимпиадный мир стал жить собственной жизнью. По всему миру проводятся математические конкурсы и олимпиады. Появились специалисты по их проведению, возникла олимпиадная математика со своей методикой работы и своей литературой. С некоторой долей условности можно сказать, что в олимпиадном мире сложились две ценностные ориентации: «научная» и «спортивная». Эти различные взгляды на олимпиады проявляются в подборе задач, выработке критериев оценок, в кадровых вопросах, в организации математических лагерей.

В нашей заметке мы кратко противопоставляем эти подходы.

29.2 Спортивный подход

Несколько сгущая краски, попробуем передать спортивный подход фразой: «олимпиада — это спорт по решению головоломок». Такая ориентация влечет за собой многое: усиливается тренерство,