ОГЛАВЛЕНИЕ

ГЛАВА 0

Логика и множества (факультативно)

Данная глава носит справочный характер и может быть пропущена при первом чтении конспекта. Тем не менее, настоятельно рекомендуется регулярно возвращаться к ней по мере освоения материала.

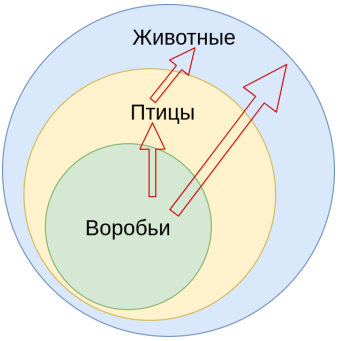
0.1 Суждения и силлогизмы

0.1.1 Конспект

1. Типовая конструкция суждения: ***Посылки*** $\vdash$ ***Вывод***.

2. Пример:

   (*Все птицы — животные*) и (*все воробьи — птицы*),
   вывод: (*все воробьи — животные*).
   Такой вывод является правильным независимо от того, правильные ли посылки.
   (*Все птицы — животные*) и (*все цветы — птицы*), вывод: (*все цветы — животные*).
   Это суждение истинно независимо от ложности посылок. Суждение показывает *только взаимосвязь* посылок и вывода. Принцип «чушь на входе — чушь на выходе».

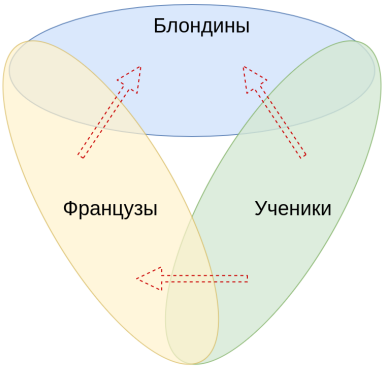


3. При построении суждения посылки могут быть ложными. Более того, в математической логике из ложной посылки следует все, что угодно. Например, *если снег черный, то лес зеленый*. Лес при этом может быть зеленым (летом) и не быть таковым (зимой), но суждение остается истинным, т.к. посылка про снег является ложной.

4. Сравните: если запись числа a оканчивается на 0, то оно кратно 5. Здесь мы ничего не знаем про число a, но если для него выполняется посылка, то выполняется и вывод. А если не выполняется, то истинность самого суждения при этом никак не страдает. Более того, мы знаем, что

на 5 также делятся и другие числа, и это значит, что путать местами посылки и вывод ни в коем случае нельзя! Ведь ***не всегда верно***, что если число делится на 5, то его запись заканчивается на 0.

5. Другой пример:



(*Некоторые французы — блондины*) и (*некоторые ученики — французы*), следовательно, (*некоторые ученики — блондины*). ***Такое суждение неверно***. Поскольку слово «некоторые» не гарантирует, что таковым признаком обладают все французы. А значит, из свойства «быть французом» не всегда следует «быть блондином».

6. Здесь обе посылки истинные, но вывод ложный. Хотя легко представить ситуацию, когда некоторые ученики действительно будут блондинами. Но это — лишь предположение, а не строгое рассуждение.

7. В этом примере нарушается именно связка между посылками и выводом, т.к. две посылки не склеиваются по общему признаку. В первой посылке стоит «некоторые французы», а во второй просто «французы», это разные ***множества***, а потому связать две посылки вместе мы не можем!

8. Для построения ***силлогизма*** принципиально, чтобы связующее звено было одинаковым:

$$\textbf{\textit{если}}\ (A \text{ есть } B) \text{ и } (B \text{ есть } C),\ \textbf{\textit{то}}\ (A \text{ есть } C)$$

здесь связывание посылок происходит по свойству B, и если в нем допустить какое-то искажение, то можно придти к неверным выводам!

0.1.2 Задачи

1. Постройте вывод из посылок: (Сократ человек) И (все люди смертны).

0.2 Высказывания и предикаты

0.2.1 Конспект

1. ***Высказывание*** — это любое утверждение на любом языке, которое может быть либо только истинным, либо только ложным.

2. Примеры высказываний: «*Шесть больше трех*», «*Дважды два — пять*», «$\sqrt{2}$ — *число иррациональное*», «*среди натуральных чисел существует наибольшее*», «*всякое четное число является суммой двух простых чисел*».

3. Все эти высказывания имеют либо истинное, либо ложное значение, хотя про последнее мы не знаем точный ответ. Но мы точно знаем, что их значения не могут быть переменными, т.е. зависеть от каких-то внешних факторов или других высказываний.

4. Из выше приведенных примеров: «*все птицы — животные*» и «*все воробьи — птицы*» есть истинные высказывания.

5. Но эти высказывания можно разобрать на составляющие. Для чего нам понадобятся предикаты.

6. ***Предикат*** — это суждение, зависящее от переменных, обозначающих объекты данного суждения.

7. Например, «x *есть воробей*», «x *есть птица*», «x *есть животное*». Каждое из них может быть истиным или ложным, смотря что подставить вместо x. При $x =$ «*рыба*» первые два будут ложными, а при $x =$ «*ромашка*» ложными будут все три предиката.

8. Аналогично, «x *есть ученик*», «x *есть француз*», «x *есть блондин*». Заметим, что если ранее мы оперировали ***свойствами*** (быть учеником, французом, блондином), то теперь перешли к оперированию ***объектом*** x, который может обладать тем или иным свойством.

9. Из предикатов можно построить новые предикаты, используя логические связки: И($\wedge$), ИЛИ($\vee$), НЕ($\neg$), СЛЕДУЕТ($\to$).

10. Например, «(x *есть воробей*)$\to$(x *есть птица*)», «(x *есть птица*)$\to$(x *есть животное*)»). Эти предикаты содержат переменную x, но они всегда истинны. Такие тождественно истинные предикаты называются ***тавтологиями***. Тавтологии отличаются от истинных высказываний тем, что содержат переменные, которые можно считать фиктивными. Чтобы тавтологию сделать высказыванием, достаточно перед ним сказать «*для любого* x», тогда x перестанет быть параметром, а выражение превратится в истинное высказывание:

$$\text{«(}\textit{для любого } x\text{) (}x \textit{ есть воробей}\text{)}\to\text{(}x \textit{ есть птица}\text{)»}$$

11. Это называется правилом введения ***квантора всеобщности***.

12. Далее, рассмотрим высказывание «*некоторые французы блондины*». Поступить аналогично предыдущему и заменить его на предикат «(x *есть*

француз)→(*x есть блондин*)» нельзя! Дело в том, что высказывание «*все воробьи — птицы*» говорит о вложении одного свойства в другое: быть воробьем означает также быть птицей. Но при слове «*некоторые*» мы понимаем, что речь идет не о свойстве «*быть французом*», а о том, что некоторые из французов обладают свойством «*быть блондином*». То есть, мы утверждаем, что существует хотя бы один такой объект x, который есть и француз и блондин одновременно!

13. Иначе говоря, мы имеем дело со связкой И:

$$(x \text{ есть француз}) \wedge (x \text{ есть блондин}),$$

данный предикат не всегда является истиной, его истинность зависит от конкретного x.

14. Тем не менее, и такой предикат можно превратить в высказывание, причем истинное. Для этого нужно слово «некоторые» превратить в «*существует x*», так что получится истинное высказывание

$$\text{«}(\text{существует } x)\ (x \text{ есть француз}) \wedge (x \text{ есть блондин})\text{»}$$

15. Это называется правилом введения ***квантора существования***.

16. Примеры перевода высказываний с языка свойств на язык объектов:

Все птицы — животные	(*для любого x*) (*x есть птица*)→(*x есть животное*)
Все воробьи — птицы	(*для любого x*) (*x есть воробей*)→(*x есть птица*)
Все воробьи — животные	(*для любого x*) (*x есть воробей*)→(*x есть животное*)
Если число заканчивается на 0, то оно кратно 5	(*для любого a*) (*a заканчивается на* 0)→(*a кратно* 5)
Некоторые французы — блондины	(*существует x*) (*x есть француз*)∧(*x есть блондин*)
Некоторые ученики — французы	(*существует x*) (*x есть ученик*)∧(*x есть француз*)
Некоторые ученики — блондины	(*существует x*) (*x есть ученик*)∧(*x есть блондин*)

17. Видим, что построить вывод можно только в том случае, когда две посылки склеиваются по общему предикату «*x есть птица*», при этом сами посылки являются импликациями (следование).

18. Можно комбинировать общие и частные суждения:

«(x *есть птица*)$\wedge$(*все птицы — животные*)»,

откуда следует вывод «(x *есть животное*)».

Здесь мы объединили в посылке предикат, что-то говорящий о свойстве объекта x, с высказыванием, которое что-то говорит о связи двух свойств, и нашли новое свойство объекта x. Это типичное рассуждение от общего к частному.

19. Построение выводов из заданных или полученных ранее истинных высказываний и предикатов называется ***дедукцией*** и является основным методом рассуждений при получении математических теорем.

20. Иногда для построения нужного вывода требуетя перебрать сотни комбинаций ранее доказанных посылок. Но часто для нащупывания правильной цепочки доказательства хватает вспомогательных иллюстраций или опыта исследователя, погруженного в данную тему.

21. Ранее мы отмечали, что рассуждения в обратную сторону — от вывода к посылкам — неверны. Однако очень часто это верно отчасти. Например, мы знаем дедуктивный вывод: если число оканчивается на 0, то оно делится на 5. На основе этого мы не можем доказать точно, но ***можем предположить***, что если число делится на 5, то оно, вероятно, может оканчиваться на 0. Как мы знаем, это верно примерно в половине случаев. Если бы такое *разворачивание импликации* было бы всегда абсолютно невозможным, то дедукция представляла бы собой простейший случай вывода, когда ложь влечет любое суждение. Для построения теорий это абсолютно бесполезно.

22. Метод *рассуждения назад*, к уже известной посылке, называется ***абдукцией***. Именно таким методом, как правило, пользовался Шерлок Холмс в своих умозаключениях. Именно поэтому его выводы всегда носят вероятностный характер и сопровождаются словами «вероятно», «скорее всего» и т.п. Искусство Шерлока Холмса заключается в том, чтобы из всех возможных посылок в данной конкретной ситуации выбрать наиболее вероятную.

23. Например, цитируем из рассказа «Этюд в багровых тонах» (Конан Дойль),

«Этот человек по типу — врач, но выправка у него военная. Значит, военный врач. Он только что приехал из тропиков — лицо у него смуглое, но это не природный оттенок его кожи, так как запястья у него гораздо белее. Лицо изможденное, — очевидно, немало натерпелся и перенес болезнь. Был ранен в левую руку — держит ее неподвижно и немножко неестественно. Где же под тропиками военный врач-англичанин мог натерпеться лишений и получить рану? Конечно же,

в Афганистане». Весь ход мыслей не занял и секунды. И вот я сказал, что вы приехали из Афганистана.

24. Рассмотрим только часть умозаключений Холмса и сравним их с арифметическим примером

Ватсон — военный врач с изможденным лицом и загорелый	Число 30 — делится на 5
Воевавшие в Афганистане — военные с изможденным лицом и загорелые	Оканчивающее на 0 число — делится на 5
Вывод: Ватсон прибыл из Афганистана	Вывод: 30 оканчивается на 0

25. Как видим, нам дано две посылки, в одной из которых дается некая связь между свойствами (воевавшие есть военные и т.д., а также оканчивающиеся на 0 делятся на 5), а в другой дается свойство конкретного объекта (Ватсон и число 30). Это свойство общее в обеих посылках, но по нему нельзя склеить их в силлогизм, т.к. свойство всегда стоит в конце посылки. Но Холмс знает, что практически все военные с изможденным лицом и загорелые — это воевавшие в Афганистане (хотя это и неверно на 100%), и на основании этого он предполагает(!), что и Ватсон такой же, раз он обладает таким же свойством.

26. На примере числа 30 это тоже сработало, однако стоит нам подставить 25 вместо 30, как вся цепочка рассуждений порушится! Поэтому абдуктивные умозаключения нельзя считать математическими, однако они могут навести на правильное дедуктивное умозаключение, в результате чего либо появляется теорема (*Все военные с изможденным лицом воевали в Афганистане*), либо обнаруживается контрпример (в нашем случае это число 25, которое опровергает предположение о том, что все делящиеся на 5 числа оканчаиваются на 0).

0.2.2 Задачи

1. Какое абдуктивное предположение можно сделать из следующих посылок: (Зимой выпадает снег) И (Сейчас есть снег) ?

0.3 Связь предикатов и множеств

0.3.1 Конспект

1. Выше мы оперировали такими понятиями как свойство и объект, обладающий свойством, на основе чего вводили различные высказывания и предикаты. Посмотрим, как они связаны с понятием ***множество***.

2. Пусть M — множество всех людей, живущих на планете. Тогда предикат $h(x)$ «x есть человек» можно переписать следующим способом: $h(x) = (x \in M)$. Это одновременно означает и то, что x находится в множестве M, и то, что x обладает свойством «быть человеком». Говорят также, что M есть область истинности предиката $h(x)$. Таким образом, множество олицетворяет собой свойство, а элементы множества — объекты, обладающие данным свойством.

3. Если множество X является частью множества Y, (например, множество всех женщин есть часть множества M), то мы пишем $X \subseteq Y$ (X *содержится в* Y, Y *включает* X). Важно не путать значки $\in$ и $\subseteq$, т.к. первй говорит о принадлежности объекта к свойству, а второй — о вложении свойств (о том, что одно свойство меньше или равно другому). Используется также символ строгого вложения $\subset$, означающий, что вложение имеется, но при этом множества не равны.

4. Вложение множеств выражается с помощью принадлежности:

$$X \subseteq Y \text{ эквивалентно } (\forall x)(x \in X) \to (x \in Y)$$

   По сути, это ровно то же самое, что мы ранее делали при переводе языка свойств на язык объектов: *все* X *есть* Y равносильно высказыванию (*для любого* x) (x *обладает свойством* X)$\to$(x *обладает свойством* Y).

5. Обозначим далее: $p(x)$ предикат «x *есть воробей*», $o(x)$ предикат «x *есть птица*», $a(x)$ предикат «x *есть животное*». Ранее мы получали следующий вывод:

$$(\forall x)(p(x) \to o(x)) \wedge (\forall x)(o(x) \to a(x)) \vdash (\forall x)(p(x) \to a(x))$$

6. Попробуем то же самое выразить множествами. Обозначим через P область истинности предиката $p(x)$, т.е. множество всех воробьев, O — множество всех птиц, A — множество всех животных. Тогда написанный выше с помощью предикатов вывод можно записать на языке множеств так:

$$(P \subseteq O \subseteq A) \vdash (P \subseteq A),$$

   поскольку все воробьи есть птицы, все птицы есть животные, а в итоге все воробьи есть животные.

7. На самом деле, существует намного более тесная связь между логическими связками и операциями над множествами. Вернемся снова к картинке про французов, блондинов и учеников. На ней есть три множества, обозначенные соответствующими овалами. Обозначим их следующим способом:

$$F = \{x \mid x \text{ — француз}\}, \quad B = \{x \mid x \text{ — блондин}\}, \quad E = \{x \mid x \text{ — ученик}\}$$

8. Здесь можно увидеть примеры ***пересечений*** множеств:

$$F \cap B = \{x \mid (x \text{ — француз}) \wedge (x \text{ — блондин})\},$$
$$F \cap E = \{x \mid (x \text{ — француз}) \wedge (x \text{ — ученик})\},$$
$$E \cap B = \{x \mid (x \text{ — ученик}) \wedge (x \text{ — блондин})\}.$$

   Видим, что они соответствуют логической связке И соответствующих предикатов, выражающих свойства.

9. На той же схеме мы можем усмотреть и такие теоретико-множественные конструкции, как:

$$F \setminus B = \{x \mid (x \text{ — француз}) \wedge \neg(x \text{ — блондин})\},$$

   т.е. множество французов, не являющихся блондинами. $F \setminus B$ есть операция ***вычитания*** множеств.

10. Наконец, множество

$$F \cup E = \{x \mid (x \text{ — француз}) \vee (x \text{ — ученик})\}$$

    представляет собой свойство быть французом ИЛИ учеником. Оно содержит в себе как всех французов, так и всех учеников, причем среди них есть как французы, не являющиеся учениками, так и французы, являющиеся учениками, а также ученики, не являющиеся французами. ***Объединение*** множеств соответствует логической связке ИЛИ.

11. Итак, мы можем легко оперировать предикатами, представляя, что они выражают свойство объекта принадлежать некоторому множеству, и наоборот, оперировать множествами, представляя, что оперируем предикатами, для которых эти множества суть область истинности. При этом И соответствует пересечению, ИЛИ — обединению множеств. Отрицание соответствует вычитанию множеств, причем разность $X \setminus Y$ можно рассматривать как пересечение $X \cap (\neg Y)$. Наконец, вложение множеств соответствует импликации предикатов.

0.3.2 Задачи

1. Выразить свойство «*быть учеником и блондином одновременно*» через множества E и B.

2. Написать множество, соответствующее всем «*птицам, не являющимся воробьями*» через множества O и P.

3. Какие элементы содержит множество $P \setminus A$, множество $M \cap F$, множество $(F \cup B) \setminus (F \cap B)$?

4. Что выражает высказывание $(M \setminus F) \subseteq (M \setminus B)$?

5. Докажите: $(E \subseteq F) \vdash (M \setminus F) \subseteq (M \setminus E)$ (от противного).

0.4 Построение множеств

0.4.1 Конспект

1. Построение множеств прямо наследует из их связи с предикатами. Тем не менее, важно знать язык, позволяющмй компактно и наглядно записывать конструктивные примеры построения множеств.

2. Конечное множество, элементами которого являются объекты $a, b, \ldots, z$ (их не обязательно 26, просто какой-то набор), обозначается

$$\{a, b, \ldots, z\},$$

при этом неважно, в каком порядке записаны элементы внутри скобок, и есть ли там дубликаты. Если в списке один и тот же элемент повторяется несколько раз, то его дубли можно спокойно выбрасывать.[1]

3. Примеры: $\{0\}$, $\{0, 1\}$, $\{0, 1, 2, 3\}$, $\{0, 0, 1, 1, 1\}$. Последнее множество равно множеству $\{0, 1\}$ (убрали кратные вхождения). Еще пример: $\{\}$ — ***пустое множество***, обозначаемое также символом $\emptyset$.

4. Как мы уже видели ранее, множество можно задать в ***предикативной форме***, общий вид которой такой:

$$\{x \mid \varphi(x)\}, \quad \{f(x) \mid \varphi(x)\},$$

где $\varphi(x)$ — это предикат, выражающий свойство объекта x, а $f(x)$ — некоторое преобразование объекта x (функция).

В первом случае даное множество является областью истинности предиката $\varphi(x)$ и содержит в себе все элементы, и только их, для которых $\varphi(x)$ истинно. Во втором случае множество содержит все значения функции $f(x)$, примененные к объектам из области истинности $\varphi(x)$. Очевидно, что

$$\{f(x) \mid \varphi(x)\} = \{y \mid (y = f(x)) \wedge \varphi(x)\}$$

[1] В математике существует понятие ***мультимножество***, в котором как раз количество дубликатов имеет значение и называется кратностью элемента. Мультимножество удобно, например, для записи разложения числа по степеням простых.

5. Конечное множество в предикативной форме записывается так:

$$\{a, b, \ldots, z\} = \{x \mid (x = a) \vee (x = b) \vee \cdots \vee (x = z)\},$$

где предикат $\varphi(x) = (x = a) \vee (x = b) \vee \cdots \vee (x = z)$ выражает свойство x входить в список объектов $a, b, \ldots, z$.

6. Объединение (или сумма) множеств:

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\},$$

например, $\{a, b\} \cup \{b, c\} = \{a, b, c\}$.

7. Пересечение множеств:

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\},$$

например, $\{a, b\} \cup \{b, c\} = \{b\}$.

8. Разность множеств:

$$A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\},$$

например, $\{a, b\} \setminus \{b, c\} = \{a\}$. Заметим, что $A \setminus B$ не всегда равно $B \setminus A$.

9. Если элементы множеств — это числа, то с ними можно производить арифметические операции:

$$A + B = \{x + y \mid (x \in A) \wedge (y \in B)\}, \quad kA = \{kx \mid x \in A\},$$

здесь первое множество — это сумма по Минковскому двух множеств, оно содержит все возможные суммы $x + y$, где первое слагаемое берется из первого множества, второе — из второго.

Легко видеть также, что $A + \emptyset = \emptyset$, т.к. предикат $y \in B$ в случае $B = \emptyset$ тождественно ложный.

Важно: не следует путать $A + A$ и $2A$! Например,

$$\{0, 1\} + \{0, 1\} = \{0, 1, 2\}, \text{ но } 2\{0, 1\} = \{0, 2\}.$$

10. Аналогично можно определить произведение множеств по Минковскому:

$$AB = \{xy \mid (x \in A) \wedge (y \in B)\},$$

откуда легко определяется степень множества A^k, а также его экспонента $\exp(A) = \sum_k (1/k!) A^k$.

Аналогично сумме видим, что $A\emptyset = \emptyset$.

0.4.2 Задачи

1. Найти объединение, пересечение и разность множеств $\{0, 1, 2, 3\}$ и $\{1, 2, 5\}$ (разность как в прямом, так и в обратном порядке).

2. Записать множество $\{0, 1, 2\}$ в предикативной форме.

3. Записать множество всех простых чисел в предикативной форме.

4. Доказать, что $A + \{0\} = A$, $A \cdot \{1\} = A$.

5. **Когда $A \setminus B = B \setminus A$?

6. ***Доказать, что $\max \exp(\{0, x\}) = e^x$.

ГЛАВА 1

Визуальная арифметика

1.1 Сложение и вычитание

1.1.1 Конспект

1. Берем произвольную прямую, и на ней будем откладывать отрезки — вправо и влево.

2. Откладывание вправо есть прибавление длины, а откладывание влево — вычитание (уменьшение) длины.

3. Можно откладывать ноль, т.е. ничего не делать. В этом случае все равно — прибавляем или вычитаем ноль.

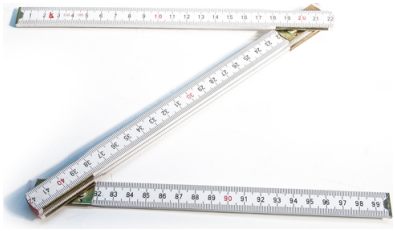
4. Мы можем комбинировать откладывание отрезков вправо и влево, т.е. производить серию последовательных откладываний отрезков (они могут быть разными по длине), на каждом шаге — от текущей точки положения.

5. Результат *серии откладываний* равносилен одному откладыванию отрезка, соединяющего стартовую и финишную точки, причем финишная точка:

   - может быть справа от стартовой (результатом является одно откладывание вправо, т.е. прибавление длины),
   - может совпадать с ней (результатом оказалось нулевое откладывание)
   - или быть слева от стартовой точки (результатом является одно откладывание влево, т.е. вычитание).

6. Откладывание *изотропно*, т.е. одинаковые серии откладываний, приложенные к разным стартовым точкам, приводят к одинаковым результирующим отрезкам, отложенным от этих стартовых точек. Иначе говоря, величина и направление откладывания не зависит от начального местоположения!

7. Серии откладываний можно проиллюстрировать складным метром. Раскладывание колена на 180^o означает прибавление его длины к общей серии откладываний, а складывание — вычитание его длины из общей серии откладываний. При этом от стартовой точки можно уйти как вправо, так и влево, или остаться на месте.



8. С помощью этой же линейки нетрудно продемонстрировать, что композиция откладываний ***ассоциативна*** и ***коммутативна***: можно сначала сложить/разложить одну линейку, затем вторую, затем приложить вторую к первой или первую ко второй — результат будет один и тот же!

9. Кроме того, очевидно, что у каждого откладывания существует обратное, приводящее в результате к нулевому откладыванию. Для этого нужно произвести ровно ту же самую серию откладываний, только поменять ось направления. Или, что то же самое. пройтись по линейке в обратную сторону.

10. Далее любое откладывание будем записывать буквами $a, b, c, \ldots$, имея ввиду под ними как прибавления, так и вычитания.

11. Откладывание, противоположное a, будем обозначать $-a$. При этом комбинация откладываний соединяется знаком '+', а если встречается комбинация $a + (-b)$, то пишем проще: $a - b$.

12. Обратные откладывания — это просто перевернутые в обратную сторону «линейки»!

13. Результат откладывания (конфигурацию линейки с учтом ее направления) будем называть ***вектором***. Если вектор смотрит влево (финишная точка левее стартовой), то вектор называется *отрицательным*, а если вправо — *положительным*. Нулевой вектор — когда финиш и старт совпадают.

14. Композицию откладываний будем называть ***суммой векторов*** или просто суммой, а процедуру откладывания — ***сложением***.

Свойства сложения:

SUM1 $(a + b) + c = a + (b + c)$ (ассоциативность);

SUM2 $a + b = b + a$ (коммутативность);

SUM3 $a + 0 = 0 + a = a$ (аддитивное свойство нуля);

SUM4 $a + (-a) = 0$ (обратный элемент);

SUM5 если $a + x = b + x$, то $a = b$ (правило сокращения);

SUM6 верно одно и только одно: либо $a = b$, либо $a = b + x$, либо $a = b - x$, где x — откладывание вправо (трихотомия)

1.1.2 Задачи

1. Вывести свойства сложения.

1.2 Сравнение

1.2.1 Конспект

1. Понятие отрицательного и положительного векторов позволяют ввести сравнение на векторах.
2. Для начала скажем, что положительный вектор больше нуля: $x > 0$.
3. Далее, если $b = a + x$, где $x > 0$, то пишем $a < b$.

Свойства сравнения (можно вывести из определения):

Ord1 не верно, что $x < x$ (антирефлексивность);

Ord2 если $a < b$ и $b < c$, то $a < c$ (транзитивность);

Ord3 верно одно и только одно: либо $a = b$, либо $a < b$, либо $b < a$ (трихотомия);

Ord4 $a < b \Leftrightarrow a + x < b + x$, где $x > 0$ (изотропность сравнения)

1.2.2 Задачи

1. Вывести свойства сравнения.

1.3 Умножение

1.3.1 Конспект

1. Строим две перпендикулярно направленные оси Ox и Oy. На каждой оси — свой собственный мир векторов и линеек.
2. Умножение — это площадь, построенная на перпендикулярных векторах. Картинка $2 \times 2 = 4$.

3. Поскольку векторы у нас двух знаков, умножение также бывает двух знаков. Знак умножения определяется знаком (направлением) векторов и таблицей перемножения знаков:

	+	−
+	+	−
−	−	+

4. Понятие группы на данном примере. Элемент '+' является нейтральным элементом группы знаков. Многократные умножения знаков не выводят за пределы группы.
5. Умножение коммутативно и ассоциативно — можно продемонстрировать на картинках с квадратами и кубами.
6. Умножение на нулевой отрезок (мультипликативное свойство нуля) — очевидно из равенства и свойств сложения:

$$0 + a \times 0 = a \times 0 = a \times (0 + 0) = (a \times 0) + (a \times 0) \Rightarrow 0 = (a \times 0)$$

7. Дистрибутивный закон, в том числе при разнонаправленных векторах проверяется непосредственно на картинке: $a \times (b + c) = a \times b + a \times c$.
8. ***Единичный отрезок*** — способ свести многократное сложение одного вектора к умножению на сумму единичных отрезков! Прямоугольник единичной высоты и длины an перекладывается в прямоугольник $a \times n$, тем самым сложение превращается в умножение.
9. Умножение на единичный отрезок: $a \times 1 = a$.
10. Сложение отрезков — это также сложение прямоугольников единичной высоты.
11. Умножение отрезков — это не только площадь, но также и объем, который заметает вертикальный единичный отрезок на площади $a \times b$, поэтому $ab = a \times b \times 1$.
12. *Степень*: многократное умножение отрезка самого на себя. Иллюстрация — отрезок, квадрат, куб.
13. В дальнейшем умножение векторов в смысле нахождения площади/объема, т.е. $a \times b$, и умножение чисел как таковых, т.е. ab, будем считать одним и тем же понятием, так что $a \times b = ab$.

Свойства умножения:

Prod1 $(a \times b) \times c = a \times (b \times c)$ (ассоциативность);

Prod2 $a \times b = b \times a$ (коммутативность);

Prod3 $a \times 0 = 0 \times a = 0$ (мультипликативное свойство нуля);

Prod4 $a \times 1 = 1 \times a = a$ (нейтральный элемент по умножению);

Prod5 $a \times (b + c) = a \times b + a \times c$ (дистрибутивный закон);

Prod6 если $a \times b = 0$, то $a = 0$ или $b = 0$ (отсутствие делителей нуля);

Prod7 если $a \times c = b \times c$ и $c \neq 0$, то $a = b$ (правило сокращения);

Prod8 если $a \times c < b \times c$, то $a < b$ (монотонность);

Prod9 если $a < b$ и $c > 0$, то $a \times c < b \times c$.

1.3.2 Задачи

1. Вывести свойства умножения.

1.4 Натуральные числа

1.4.1 Конспект

1. Кратность операций сложения и умножения: $a+a+a+a+a+\ldots$, $aaa\ldots$ Натуральное число вводится для обозначения кратности одинаковых операций!
2. Нулевая кратность: в случае сложения ничего не складываем, остаемся на месте в начальной точке, поэтому
$$\underbrace{a + \cdots + a}_{0 \text{ раз}} = 0.$$
3. Нулевая степень: в случае умножения ничего не умножаем, от умножения остается только кратность 1, наследуемая от сложения, т.е. в произведении $1 \times a \times a \times \ldots$ выбрасываем все, остается только 1. Поэтому
$$\underbrace{a \times \cdots \times a}_{0 \text{ раз}} = 1,$$
кроме того, это согласуется с законом ассоциативности умножения. Многие правила в математике для крайних значений определяются с целью сохранить общий вид формул, если это не приводит к противоречию!
4. ***Натуральные числа*** — это показатели кратности операций (сложения и умножения).

5. С другой стороны, натуральные числа можно рассматривать как суммы единичных отрезков.
$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}}$$

6. Чудо, но это вполне согласуется с операциями сложения и умножения, сохраняет все законы арифметики: ассоциативность, коммутативность, дистрибутивность.

7. Поэтому натуральные числа, привязанные к единичным отрезкам, можно также считать мерой длины, площади, объема и т.д.

8. Ноль — натуральное число, поскольку мы рассматриваем нулевую кратность для однородности законов арифметики.

NotaBene Натуральные числа — это и кратности операций, и единицы измерения, т.е. числа.

9. Натуральные числа отвечают за соизмеримость и арифметическую кратность: a ***кратно*** b ($a \vdots b$), если $a = bn$ или $a = (-b)n$ при некотором натуральном n. Ноль кратен любому числу! Нулю кратен только ноль!

10. Если a кратно b, то говорят также, что b делит a, или что b является делителем a ($b|a$).

11. Если $a > 0$ кратно $b > 0$, то $a = kb = b + (k-1)b$, где $k > 0$. Здесь $x = (k-1)b$. Поэтому $a \geqslant b$. Так что для положительных векторов кратность означает превосходство в смысле сравнения. И наоборот, если b делит a, то $b \leqslant a$. Аналогичные неравенства можно получить и для отрицательных векторов.

1.4.2 Задачи

1. Доказать, что если $a|b$ и $b|c$, то $a|c$.

2. Доказать, что если $a|b$ и $b|a$, то $a = \pm b$ (a, b — натуральные).

1.5 Теорема Пифагора графически

1.5.1 Конспект

1. Строим квадрат $a + b \times a + b$ и внутри квадраты $a \times a$ и $b \times b$

2. Строим квдарат $a + b \times a + b$ и внутри квадрат $c \times c$

3. Делаем вывод, перекладывая треугольники

4. *Построение $\sqrt{2}$, $\sqrt{7}$ (используются признаки подобия треугольников, отношения строн)
5. Примеры пифагоровых троек (анонс теоремы!)

1.6 Бином Ньютона и другие формулы визуально

1.6.1 Конспект

1. Визуализация $(a-b)(a+b) = a^2 - b^2$.
2. Сумма подряд идущих чисел $1, 2, \ldots, n$ с помощью сложения прямоугольников.
3. Сумма подряд идущих нечетных чисел.
4. Вывод формулы $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
5. Разрезание сырного кубика на 8 частей тремя плоскостями.

1.6.2 Задачи

1. Вывести формулу квадрата суммы визуально.

1.7 Соизмеримость отрезков, алгоритм Евклида

1.7.1 Конспект

1. Два отрезка a и b, кузнечики прыгают, один на a и $-a$ сколько угодно раз, второй на b и $-b$ сколько угодно раз
2. Кузнечики стартуют в одной и той же точке (назовем ее O). Могут ли они попасть в одну точку, отличную от O, когда-нибудь?
3. Ответ — да, если есть такая точка A, что отрезок OA кратен и a, и b одновременно, т.е. при некотрых натуральных n, m, не равных нулю, будет верно равенство $an = bm$:

$$\underbrace{a + a + \cdots + a}_{n \text{ раз}} = \underbrace{b + b + \cdots + b}_{m \text{ раз}}$$

4. Отрезки, которые имеют общий кратный отрезок, называются ***соизмеримыми***
5. Иллюстрация: строим прямоугольник $a \times b$ ($a < b$), начинаем отсекать в нем квадраты: сначала отсекаем квадраты $a \times a$, пока можем, останется кусок $a \times b_1$ ($b_1 < a$), затем отсекаем квадраты $b_1 \times b_1$, пока можем, останется кусок $a_1 \times b_1$ ($a_1 < b_1$), и т.д.

6. Если исходные отрезки соизмеримы, то процесс остановится: исходный прямоугольник будет разбит на конечное число квадратиков.
7. Финальный квадратик будет иллюстрировать НОД отрезков a и b, т.к. это максимальный квадрат, которым можно замостить. прямоугольник $a \times b$.
8. Такой процесс называется ***алгоритмом Евклида***, к нему мы еще вернемся с более формальной точки зрения.
9. Заметим, что числа a и b при этом вовсе не обязан быть натуральными.
10. Несоизмеримость стороны квадрата и его диагонали: 1 и $\sqrt{2}$.
11. Алгоритм Евклида никогда не остановится. НОДом будет бесконечно малое число.

1.7.2 Задачи

1. Найти НОД(10,6) методом прямоугольников.
2. Сколько и каких шагов должен сделать кузнечик НОД(10,6), чтобы попасть в точку НОД(10,6)?

ГЛАВА 2

Движения на прямой

2.1 Сдвиг, композиция сдвигов

2.1.1 Конспект

1. Рассмотрим аффинную прямую, т.е. набор точек и векторов на прямой
2. Сумма точки и вектора есть точка, сумма векторов есть вектор, разность точек есть вектор
3. Команда «прибавить ко всем точкам вектор a» называется ***сдвигом*** прямой на вектор a
4. Сдвиг на a — это операция сложения с вектором без указания конкретной точки приложения, она применяется сразу ко всем точкам! В итоге вся прямая смещается как единое целое
5. Сдвиг является движением (не случайно это однокоренные слова!)
6. Вообще, ***движение — это преобразование, сохраняющее расстояния*** (размеры и форму): если между точками A и B было расстояние x, то после преобразования движения расстояние между точками A' и B', в которые перешли исходные точки, тоже будет x, и так для любой пары точек!
7. Математическое движение — это результат физического движения (есть только начальное и конечное состояние системы)
8. Сдвиг на вектор a будем обозначать T_a: $T_a(A)$ — это точка B такая, что AB есть вектор a (совпадает по направлению и длине)
9. Композиция сдвигов — это их последовательное применение:

$$(T_b \circ T_a)(A) = T_b(T_a(A))$$

10. Композиция сдвигов соответствует сумме векторов: $T_b \circ T_a = T_{a+b}$
11. Композиция сдвигов перестановочна в силу коммутативности сложения:

$$T_b \circ T_a = T_a \circ T_b$$

12. Кратность сдвига обозначается как степень

$$\underbrace{T_a \circ \cdots \circ T_a}_{n \text{ раз}} = T_a^n$$

и соответствует кратности сложения или умножению на степень кратности: $T_a^n = T_{an}$

13. Нулевой сдвиг $T_0 = \mathrm{id}$ — это ***тождественное преобразование***, которое ничего не меняет

14. Обратный сдвиг T_a^{-1} — это сдвиг на вектор $-a$, т.е. сдвиг в обратном направлении на ту же величину

15. Вообще, если есть какие-то два преобразования u и v и операция композиции $\circ$, то эти преобразования ***взаимно обратны***, если $u \circ v = \mathrm{id}$ и $v \circ u = \mathrm{id}$, т.е. последовательное применение этих преобразований является тождественным преобразованием

16. Очевидно, что всякий сдвиг имеет обратный, причем $T_a \circ T_a^{-1} = T_a^{-1} \circ T_a = \mathrm{id}$

17. Нулевой сдвиг сам себе обратен

18. Фиксируем понятие ***группы***. Это — множество с одной бинарной операцией, для которой выполняются законы:

    G1) Результат групповой операции снова лежит в этом же множестве (композиция сдвигов есть сдвиг).

    G2) Групповая операция ***ассоциативна*** (сочетательный закон):

    $$(T_a \circ T_b) \circ T_c = T_a \circ (T_b \circ T_c).$$

    G3) Групповая операция ***обратима***: для всякого сдвига T_a существует обратный ему $T_a^{-1} = T_{-a}$.

19. Мало того, группа сдвигов ***коммутативна*** (абелева), т.е. для ее операции выполняется переместительный закон:

    G4) $T_a \circ T_b = T_b \circ T_a$.

20. Кратность обратного сдвига: $T_a^{-n} \rightleftharpoons (T_a^{-1})^n = T_{-a}^n = T_{-an}$

21. На основе только одного сдвига T_a можно построить подгруппу сдвигов

$$\{T_a^n, T_a^{-n} \mid n = 0, 1, 2, \dots\}$$

22. Эта подгруппа — реализация целых чисел $\mathbb{Z}$, к которым мы еще вернемся позже.

23. Фиксируем понятие ***подгруппы***. Это — подмножество группы, на котором групповая операция удовлетворяет групповым законам, т.е. подгруппа сама является группой с той же операцией, которая задана в группе.
24. Каждый сдвиг T_a порождает (с помощью его многократного тиражирования) свою подгруппу в группе всех сдвигов.

2.2 Отражение

2.2.1 Конспект

1. Еще один вид движений прямой — ***отражение***
2. Отражение связано с выделенной точкой — центром отражения, и все точки переводит в симметричные относительно данного центра. Взяли прямую и перевернули ее на 180^o, оставляя центр отраженя на месте
3. Отражение с центром O будем обозначать S_O
4. Композиция отражений:

$$S_O \circ S_C = T_{2CO}, \quad S_C \circ S_O = T_{2OC}$$

5. Видим, что композиция отражений является сдвигом и при этом не коммутативна!
6. Композиция отражения и сдвига:

$$S_O \circ T_a = S_{O-a/2}, \quad T_a \circ S_O = S_{O+a/2}$$

7. Такая композиция является отражением и при этом не коммутативна!
8. Кратность отражения S_O^n определяется четностью числа n. В случае четного n это id, в случае нечетного — исходное S_O
9. Отражение обратно самому себе: $S_O \circ S_O = \mathrm{id}$
10. Пара $\{\mathrm{id}, S_O\}$ образует самую маленькую нетривиальную группу движений, которая к тому же является абелевой и циклической (т.е. все ее элементы есть степени какого-то одного, а именно $S_O = S_O^1$, $\mathrm{id} = S_O^2$)

	id	S_O
id	id	S_O
S_O	S_O	id

11. Видим, что таблица полностью повторяет таблицу умножения знаков, причем id является нейтральным элементом

2.3 Таблица Кэли движений прямой

2.3.1 Конспект

1. Еще пример группы: рассмотрим класс всех сдвигов $\mathbb{T}$ и класс всех отражений $\mathbb{S}$
2. Мы можем определить композицию классов $\mathbb{T} \circ \mathbb{T}$, $\mathbb{T} \circ \mathbb{S}$, $\mathbb{S} \circ \mathbb{T}$ и $\mathbb{S} \circ \mathbb{S}$ как все возможные композиции движений из этих классов в указанном порядке. Иначе говоря, композиции классов — это их умножение по Минковскому:

$$\mathbb{T} \circ \mathbb{T} = \{t \circ t' \mid (t \in \mathbb{T}) \wedge (t' \in \mathbb{T})\}, \quad \mathbb{T} \circ \mathbb{S} = \{t \circ s \mid (t \in \mathbb{T}) \wedge (s \in \mathbb{S})\}$$

$$\mathbb{S} \circ \mathbb{T} = \{s \circ t \mid (s \in \mathbb{S}) \wedge (t \in \mathbb{T})\}, \quad \mathbb{S} \circ \mathbb{S} = \{s \circ s' \mid (s \in \mathbb{S}) \wedge (s' \in \mathbb{S})\}$$

3. Из произведенных выше вычислений легко видеть таблицу композиций этих классов:

	$\mathbb{T}$	$\mathbb{S}$
$\mathbb{T}$	$\mathbb{T}$	$\mathbb{S}$
$\mathbb{S}$	$\mathbb{S}$	$\mathbb{T}$

4. Видим полную аналогию с таблицей знаков и таблицей для id, S_O. Здесь класс $\mathbb{T}$ является нейтральным элементом
5. Если теперь собрать в одну кучу все сдвиги и отражения, то получим группу движений прямой
6. Наша цель — доказать, что других движений нет, т.е. что мнжество $\{T_a, S_O\}_{a,O}$ полностью исчерпывает все возможные движения прямой

2.4 Теоема о гвоздях, аналог теоремы Шаля

2.4.1 Конспект

1. Анализ движений проводится на основе наблюдений за количеством стационарных точек
2. Пусть движение M таково, что оно оставляет на месте две точки $A \neq B$.
3. $M(A) = A$ и $M(B) = B$. Пусть $C' = M(C)$. M сохраняет расстояния AC и BC, откуда $AC = AC'$ и $BC = BC'$, откуда $C = C'$. Т.е. $M(C) = C$ для любых точек C, т.е. $M = \mathrm{id}$
4. Пусть движение M оставляет на месте ровно одну точку O. В этом случае $A' = M(A)$ и $A \neq A'$ и $OA = OA'$, тогда A' — отражение A относительно O. Следовательно, $M = S_O$

5. Пусть движение M не оставляет на месте ни одной точки и пусть $B = M(A)$ ($B \neq A$). Обозначим $x = AB$. Тогда $T_x^{-1} \circ M(A) = A$, т.е. $T_x^{-1} \circ M$ оставляет на месте хотя бы одну точку. Если оно оставляет на месте ровно одну точку A, то это некоторая симметрия S_O, но тогда $M = T_x \circ S_O = S_{O+x/2}$. Получается, что M сохраняет точку $O + x/2$ на месте. Противоречие. Остается вариант, что $T_x^{-1} \circ M$ оставляет на месте две точки, но тогда $T_x^{-1} \circ M = \mathrm{id}$, откуда $M = T_x \circ \mathrm{id} = T_x$ — сдвиг.
6. Таким образом, все движения прямой — это либо сдвиги (в частности, id), либо отражения (теорема Шаля)
7. При этом, любое движение — это либо одна симметрия, либо композиция двух симметрий

2.4.2 Задачи

1. Построить сдвиг на 7 единиц вправо с помощью композиции двух симметрий.

2. Каким движением является следующая композиция?

$$S_{O+n} \circ S_{O+n-1} \circ \dots S_{O+1} \circ S_O$$

   Ответ получить в зависимости от четности n.

ГЛАВА 3

Вокруг окружности

3.1 Движения окружности

3.1.1 Конспект

1. Берем окружность (обруч). Какие у нее есть движения, переводящие его в самого себя?
2. Очевидно, вращение вокруг центра окружности, а также симметрии относительно прямых, проходящих через центр
3. Окружность — аналог прямой. Только эту прямую взяли за 2 конца и замкнули где-то на бесконечности
4. Поэтому вращение окружности соответствует сдвигу прямой, а симметрия окружности относительно прямой — отражению на прямой относительно точки (можно считать ее симметрией относительно перпендикулярной прямой)
5. Если представить, что на окружности большого радиуса живут маленькие одномерные математики, то для них окружность будет практически не отличима от прямой, и движения окружности они будут воспринимать именно как движения прямой
6. Поворот на угол α обозначим R_α (положительный — против часовой стрелки), симметрию относительно прямой, имеющей угол наклона φ, обозначим S_φ $(0 \leqslant \varphi < \pi)$
7. Вновь замечаем, что композиция поворотов есть поворот на суммарный угол: $R_\alpha \circ R_\beta = R_{\alpha+\beta}$
8. У каждого поворота есть обратный: $R_\alpha^{-1} = R_{-\alpha}$
9. Повороты коммутируют
10. Есть нейтральный поворот $\mathrm{id} = R_0$
11. Так что все повороты образуют группу относительно операции композиции
12. Тем не менее, есть одна особенность: поворот на угол $2\pi k$ — это тоже id

13. Вообще, повороты, заданные углами с шагом 2π, равны: $R_\alpha = R_{\alpha \pm 2\pi k}$, где k — натуральное число
14. Некоторые повороты дают id в некоторой кратности, например, $R^4_{90^o} = \mathrm{id}$, $R^6_{60^o} = \mathrm{id}$ и т.д.
15. Если угол, выраженный в градусах, соизмерим с величиной 360^o, то поворот на данный угол имеет положительную степень, в которой он обращается в id
16. Но есть угол, не обладающий таким свойством, это угол в 1 радиан. Если бы он был соизмерим с полным оборотом, то число π оказалось бы соизмеримым с 1, а это не так!
17. Поэтому некоторые вращения образуют конечные циклические подгруппы в группе движений, а некоторые — нет.

3.2 Группа движений окружности, теорема Шаля

3.2.1 Конспект

1. Композиция симметрий:

$$S_\psi \circ S_\varphi = R_{2(\psi-\varphi)}, \quad S_\varphi \circ S_\psi = R_{2(\varphi-\psi)}$$

2. Видим, что композиция симметрий является поворотом и при этом не коммутативна!
3. Композиция симметрии и поворота:

$$S_\varphi \circ R_\alpha = S_{\varphi-\alpha/2}, \quad R_\alpha \circ S_\varphi = S_{\varphi+\alpha/2}$$

4. Такая композиция является отражением и при этом не коммутативна!
5. По аналогии с прямой обозначим $\mathbb{T}$ класс всех вращений окружности, $\mathbb{S}$ — класс всех симметрий окружности
6. Получаем аналогичную таблицу композиций:

	$\mathbb{T}$	$\mathbb{S}$
$\mathbb{T}$	$\mathbb{T}$	$\mathbb{S}$
$\mathbb{S}$	$\mathbb{S}$	$\mathbb{T}$

   где $\mathbb{T}$ является нейтральным элементом
7. Снова наблюдаем все ту же группу умножения знаков!
8. Существуют ли другие движения окружности? Ответ — нет!

9. Если движение сохраняет на месте две точки окружности, не являющиеся диаметрально противоположными, то это id
10. Если движение сохраняет на месте ровно две диаметрально противоположные точки, то это симметрия
11. Если движение не имеет неподвижных точек, то это поворот на угол, не кратный 360^o
12. Всякое движение окружности — это либо поворот, либо симметрия (теорема Шаля)
13. Причем всякое движение окружности можно представить как симметрию или композицию симметрий

3.2.2 Задачи

1. Центральная симметрия — это какое движение?
2. Композицией каких симметрий можно выразить центральную симметрию?
3. С помощью симметрии относительно оси Ox и вращений выразить симметрию относительно оси Oy.

3.3 Наматывание прямой на окружность

3.3.1 Конспект

1. Совместим теперь окружность с прямой иным способом. Выделим на окружности точку O и начнем ее обход (вращение) в положительном направлении.
2. Выше мы видели, что углы поворота, кратные 360^o, т.е. полном обороту, соответствуют тождественному движению, т.е. приведут нас в точку отправления O.
3. Однако, если с точки зрения математического движения ничего не изменилось, физически мы проделали путь, равный длине окружности. Для удобства будем считать, что радиус окружности есть единичный вектор, так что ее длина равна 2π, и с каждым полным оборотом мы будем «наматывать» расстояние 2π.
4. Вообще, расстояние, пройденное по окружности единичного радиуса, когда этот радиус заметает угол α, равно $\alpha(2\pi/360^o)$. Чтобы каждый раз не переводить единицы измерения радиуса в градусы и наоборот, углы также приняют измерять в единицах длины — радианах. А именно,

угол в 1 *радиан соответствует повороту, при котором точка проделает по окружности путь, равный по длине радиусу данной окружности.* Нетрудно видеть, что в градусах 1 радиан будет иметь выражение $360^o/(2\pi)$ или $180^o/\pi$.

5. В дальнейшем условимся все углы измерять в радианах, если не потребуется иное.

6. Известно, что число π не соизмеримо с целыми числами, так что поворот R_1 на 1 радиан ни в какой положительной степени не приведет нас снова в точку исхода O.

7. Зато поворот $R_{2\pi}$ в точности возвращает нас в точку отправления O.

8. При каждом таком повороте мы проделываем путь, равный углу поворота, т.е. 2π (радиус равен 1).

9. Следовательно степени такого поворота $R^n_{2\pi}$ дадут прохождение пути длиной $2\pi n$.

10. Представим эту картину не с точки зрения жителей окружности, бегающих по замкнутой траектории, а с точки зрения жителей прямой, которая наматывается на окружность. С их точки зрения все выглядит несколько иначе и больше напоминает движение оклеса по дорожному полотну: окружность катится по прямой и через равные промежутки касается точкой O данной прямой.

11. Если при этом два друга — один из мира окружности, второй из мира прямой, — двигаются с одинаковой скоростью в одном направлении, то они могут синхронизироваться в точке касания окружности и прямой и разговаривать друг с другом.

12. Итак, колесо катится, два друга беседуют, точка O то и дело, а именно через каждые 2π метров соприкасается с прямой. Каждый раз, когда точка O касается прямой, наш ученый друг из мира прямой ставит на прямой отметину и считает их по порядку, т.е. приравнивает к степени совершенного поворота: в начальный момент времени это был 0, затем 1 оборот, затем 2 оборота, и т.д.

13. Что же мы видим на прямой? Мы видим не что иное как шкалу натуральных чисел, в точности соответствующую степеням вращений окружности.

14. Представим теперь, что в какой-то момент касания точки O с прямой физика мира изменилась, и вращение начало осуществляться в обратную сторону!

15. Наши друзья-ученые при этом продолжат совместное путешествие, но только назад. Они пойдут отсчитывать уже проставленные отметки на

прямой в убывающем порядке, пока не вренутся в точку 0. Но здесь состоится чудо, и движение продолжится дальше.

16. Как все это записать на языке вращений и сдвигов?

17. Предположим, что сначала окружность повернулась на n полных оборотов вперед, а затем на m полных оборотов назад.

18. Мы получаем итоговое вращение, записываемое как $R_{2\pi n} \circ R_{2\pi m}^{-1}$.

19. А что мы имеем с точки зрения движения на прямой?

20. Сначала был произведен сдвиг $T_{2\pi n}$, затем сдвиг $T_{-2\pi m}$.

21. И мы видим, что индекс, определяющий итоговое вращение и итоговый сдвиг, — один и тот же!

22. Причем, если $n > m$, то сдвиг будет вправо на расстояние $2\pi(n-m)$, а поворот будет положительным на угол $2\pi(n-m)$.

23. Если же $n < m$, то сдвиг будет влево на расстояние $2\pi(m-n)$, а поворот будет отрицательным (по часовой стрелке) на угол $2\pi(m-n)$.

24. Ранее мы уже договаривались, что перед векторами, направленными влево, будем ставить знак '-'. Так же будем поступать и с углами вращений в отрицательную сторону.

25. Соответственно, при $n < m$ мы будем иметь итоговый сдвиг $T_{-2\pi(m-n)}$ и итоговый поворот $R_{-2\pi(m-n)}$, которые также можно записать в виде степеней:

$$T_{-2\pi(m-n)} = T_{2\pi}^{-(m-n)} \text{ и } R_{-2\pi(m-n)} = R_{2\pi}^{-(m-n)}.$$

26. Осталось добавить маленький штрих к портрету, а именно: в случае $n < m$ под разностью $n - m$ будем понимать запись $-(m-n)$.

27. Тогда уже независимо от того, $n < m$, или $m < n$, или $n = m$, композиция поворотов и сдвигов сначала на n вправо и затем на m влево будет записываться одинаково:

$$T_{2\pi(n-m)} = T_{2\pi}^{n-m} \text{ и } R_{2\pi(n-m)} = R_{2\pi}^{n-m}.$$

28. В итоге мы приходим к тому, что называется ***целыми числами***, включающими натуральные числа и отрицательные натуральные числа (при этом $-0 = 0$).

29. Сколько бы мы ни вращали окружность на 2π в ту или иную сторону с помощью поворота $R_{2\pi}$, мы совершаем поворот на целую степень полного оборота. При этом как бы мы ни катали окружность по прямой, точка O будет ставить отметки в точках $2\pi k$, где k — целое число.

30. Последнее замечание про отрицательные числа:

$$T_{2\pi}^{-k} = S_0 \circ T_{2\pi}^{k} \text{ и } R_{2\pi}^{-k} = S_O \circ R_{2\pi}^{k}.$$

31. То есть отрицательные повороты и сдвиги — это всего лишь отражение положительных (в случае прямой центром отражения будет точка, помеченная как 0, а в случае окружности — прямая, проходящая через точку O и центр окружности)

ГЛАВА 4

Целые числа и ОТА

4.1 Целые числа. Кольцо

4.1.1 Конспект

1. Итак, совмещение вращений со сдвигами дает нам полную свободу перемещений в положительном и отрицательном направлении. При этом, с точки зрения окружности ничего не меняется — происходит итоговое движение id, а с точки зрения прямой — происходит разметка точек с равным шагом. Ясно, что сам шаг при этом не имеет значения. Мы могли бы взять окружность радиуса R, и тогда шаг был бы равен $2\pi R$. В частности, можно взять радиус $R = 1/2\pi$, и тогда точки на прямой расположатся с шагом 1.
2. Такую же картину можно получить, если взять все точки, получаемые из выделенной точки 0 степенями сдвига на единичный вектор, используя положительные и отрицательные, т.е. целые, степени.
3. Как видим, целые числа, как и натуральные, можно интерпретировать и как степени движений (и вообще любых преобразований, имеющих обратные), и как векторы сдвигов на прямой, а значит, к ним применимы определенные ранее операции сложения, вычитания и умножения. При этом результат умножения получает такой знак, который определяется из таблицы умножения знаков.
4. Множество всех целых чисел принято обозначать $\mathbb{Z}$. Вместе с операциями сложения (вычитания) и умножения структура $(\mathbb{Z}, +, \cdot)$ называется ***кольцом целых чисел***. Кольцо — это структура, где можно складывать, вычитать и умножать.
5. Понятие кольцо является расширением понятия группы, т.к. добавляется операция умножения.
6. Ранее мы уже видели такие группы, как группа движений прямой, группа умножения знаков, группа композиций классов сдвигов и симметрий, группа вращений окружности. Все они обладали одной операцией — композицией, которая соответствовала сложению параметров сдвигов и вращений.

7. Кроме того, мы ввели такое понятие как кратность, заменяя тем самым многократное сложение умножением на целое число.

8. Кратность операций нельзя рассматривать как умножение сдвигов или вращений, поскольку это сущности разного рода. Поэтому движения в общем случае образуют только лишь группу.

9. Однако, уже сами кратности, как самостоятельные сущности, можно и складывать, и умножать. Например, если мы рассмотрим сдвиг T_1 и композицию его кратностей $T_1^n \circ T_1^m$, то получим тот же сдвиг но в суммарной кратности T_1^{n+m}, где $n, m \in \mathbb{Z}$. Но ничто не мешает нам рассмотреть кратность m сдвига T_1^n, т.е. сдвиг $(T_1^n)^m$, а это уже будет не что иное, как сдвиг кратности nm, т.е. T_1^{nm}.

10. Иначе говоря, умножение на целых числах можно представить как кратности кратностей сдвигов!

11. Целые числа, если их рассматривать как счетчик витков по окружности, образуют так называемую ***фундаментальную группу*** окружности, которая является важным топологическим свойством окружности и ей подобным (в топологии) фигурам. Зная фундаментальную группу, можно определить, насколько схожи фигуры в топологическим смысле — можно ли из одной получить другую путем деформации без разрывов и склеиваний.

12. Фиксируем понятие ***кольцо***. Это — множество K с двумя бинарными операциями $+$ (плюс) и $\cdot$ (точка), которые подчинены следующим законам:

    R1) $a, b \in K \Rightarrow a + b \in K, a \cdot b \in K$ (замкнутость операций);

    R2) $a, b, c \in K \Rightarrow (a+b)+c = a+(b+c), (a\cdot b)\cdot c = a\cdot(b\cdot c)$ (ассоциативность операций);

    R3) существует элемент $0 \in K$ такой, что $a + 0 = 0 + a = a$ для всех $a \in K$ (аксиома нуля);

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

    R5) для всех $a, b, c \in K$ имеем $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$ (правая и левая дистрибутивность);

    R6) для всех $a, b \in K$ имеем $a + b = b + a$ (коммутативность сложения).

    Обычно изучаются ***кольца с единицей***, т.е. такие кольца, для которых

    R7) существует элемент $1 \in K$ такой, что $a \cdot 1 = 1 \cdot a = a$ для всех $a \in K$ (аксиома единицы),

а также ***коммутативные кольца***, т.е. такие кольца, для которых

R8) для всех $a, b \in K$ имеем $a \cdot b = b \cdot a$ (коммутативность умножения).

Иначе говоря, в коммутативном кольце с единицей можно складывать, вычитать и умножать по обычным правилам.

4.1.2 Задачи

1. Докажите, что $m\mathbb{Z}$ — подкольцо кольца $\mathbb{Z}$, т.е. в нем также можно складывать, вычитать и умножать. m — положительное целое число.

4.2 Кузнечик НОД и алгоритм Евклида

4.2.1 Конспект

1. Поработаем теперь непосредственно с целыми числами. Пусть у нас есть кузнечик, стоящий в точке 0, который умеет прыгать с шагом a и с шагом b в любую сторону. Числа a, b — натуральные.

2. Ясно, что он может попасть в любую точку вида $ka + mb$, где кратности k, m — целые. Как понять, в какие точки он может попасть, а в какие — нет?

3. Пусть d — наименьшее положительное число, в которое кузнечик может попасть, т.е. оно имеет вид $d = ka + mb$ при некоторых k, m. Тогда он может попасть и в любое число вида nd, поскольку $nd = (nk)a + (nm)b$, где $n \in \mathbb{Z}$. Следовательно, кузнечик может попасть во все целые числа, кратные d (множество $d\mathbb{Z}$).

4. Но в любые другие целые числа он не сможет попасть. Действительно, если он попадает в какое-то число x, лежащее между двумя соседними кратностями d, т.е. в число $x = nd + y$, где $0 < y < d$, то тогда он моможет попасть в число y, т.е. остаток от деления x на d. Но $y < d$ и притом положительное, а это противоречит выбору числа d. Таким образом, кузнечик попадает во все точки $d\mathbb{Z}$, и только в эти точки!

5. Что такое d на самом деле?

6. Для ответа на этот вопрос вспомним про алгоритм Евклида (с отсечениями квадратов). Пусть $a < b$. Вычтем из b столько a, сколько сможем: $b = k_0 a + r_1$, где $0 \leqslant r_1 < a$. Далее, из a вычитаем столько r_1, сколько сможем, если $r_1 > 0$. Получим $a = k_1 r_1 + r_2$, где $0 \leqslant r_2 < r_1$. Снова, если $r_2 > 0$, вычитаем из r_1 столько r_2, сколько можем: $r_1 = k_2 r_2 + r_3$, где $0 \leqslant r_3 < r_2$. И так далее.

7. Видим, что всякий раз, если $r_i > 0$, то мы приходим к $r_{i+1} < r_i$. Проблема в том, что это не может продолжаться бесконечно долго, т.к. от всякого натурального числа в сторону нуля можно спуститься за конечное число шагов (а ведь остатки у нас все положительные!). Так что рано или поздно случится $r_{n+1} = 0$, и на этом алгоритм Евклида остановится! Это значит, что прямоугольник $a \times b$ можно сложить квадратами $r_n \times r_n$.
8. Если теперь раскрутить равенства $r_{i-1} = k_i r_i + r_{i+1}$ в обратную сторону, то мы получим, во-первых, что a и b кратны r_n, и во-вторых, что $r_n = Ka + Mb$ при некоторых целых K, M. То есть, r_n есть общий делитель исходных чисел a и b, и наш кузнечик способен попасть в точку r_n (а значит, и во все точки, ему кратные, т.е. в $r_n\mathbb{Z}$).
9. С другой стороны, если какое-то q является общим делителем a и b, то q делит $r_1 = b - k_0 a$, делит $r_2 = a - k_1 r_1$, делит $r_3 = r_1 - k_2 r_2$, и т.д., и, наконец, делит r_n. Стало быть, $q \leqslant r_n$, и r_n — наибольшой общий делитель a и b.
10. Итак, кузнечик способен попасть в НОД(a, b), следовательно, $d \leqslant$ НОД(a, b). С другой стороны, выбор d таков, что $d = ka + mb$ при некоторых целых k, m, но тогда всякий делитель a и b является и делителем d, в частности НОД(a, b) делит d, откуда НОД$(a, b) \leqslant d$. Таким образом, минимальный шаг, на который способен сдвинуться кузнечик, — это наибольший общий делитель чисел a и b. Поэтому кузнечика с ногами a и b можно назвать НОД(a, b). Он способен прыгнуть (в несколько прыжков) во ВСЕ точки, кратные НОД(a, b), и ТОЛЬКО в эти точки!

4.2.2 Задачи

1. С помощью алгоритма Евклида найти НОД$(2020, 555)$.

4.3 Простые числа и ОТА

4.3.1 Конспект

1. У кузнечика НОД может получиться уникальная ситуация, когда при достаточно больших числах a и b он способен прыгнуть в любое целое число! Это верно в том и только том случае, когда НОД(a, b)=1. При этом говорят, что a и b взаимно просты. Например, 125 и 63 взаимно просты.
2. Взаимная простота также обеспечивается, если одно из чисел само по себе ***простое***, т.е. не делится ни на что, кроме 1 и самого себя. Например, 101 — простое, так что в паре с любым другим числом (кроме

кратного 101) оно будет взаимно просто, и наш кузнечик сможет прыгнуть в любую целую точку! Например, он умеет прыгать на 101 и 62, значит, он умеет прыгать в любое целое число!

3. Любое число можно представить как произведение степеней простых. Действительно, 1 есть произведение нулевых степеней простых чисел, например, 2^0. Предположим, что для всех чисел от 1 до n утверждение о разложимости справедливо (внимание! индукция!) и рассмотрим число $n+1$. Оно либо уже простое, либо делится на число меньше n, отличное от 1. Тогда $n+1 = mk$, причем $m, k \leqslant n$, а они есть произведение степеней простых по предположению индукции, но тогда и $n+1$ есть произведение степеней простых!

4. Простых чисел бесконечно много. Предположим, что это не так, и пронумеруем все простые числа:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \ldots,\ p_n$$

Далее рассмотрим число $m = p_1 p_2 \ldots p_n + 1$. Оно не кратно никакому простому числу из ряда $p_1, \ldots, p_n$, иначе бы 1 также было бы кратно этому простому. Следовательно, оно простое, но не входит в данный ряд. Противоречие.

5. Если простое число p делит произведение чисел ab, то оно по крайней мере делит одно из них. Доказательство: допустим, что p не делит a, тогда НОД$(p, a) = 1$, но тогда, как мы уже видели выше, $1 = kp + ma$ при некоторых целых k, m. Умножим это равенство на b: $b = kpb + mab$. Справа оба слагаемых делятся на p, значит, и b делится на p.

6. Из этого свойства легко получить ***основную теорему арифметики***: каждое натуральное число единственным образом представляется в виде произведения степеней простых чисел:

$$n = p_1^{k_1} p_2^{k_2} \ldots$$

Набор степеней $k_1, k_2, \ldots$ уникален для каждого числа n. Действительно, если бы было два разложения, то после сокращения на одинаковые сомножители мы бы получили равенство

$$p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m} = q_1^{s_1} q_2^{s_2} \ldots q_t^{s_t}$$

Но каждое простое слве делит все число справа, значит, делит один из его множителей, а значит, совпадает с одним из q_i, что по предположению невозможно. Противоречие! Следовательно, разложение по степеням простых единственно.

7. Здесь еще нужно сделать оговорку про $\mathbb{Z}$. Любое целое число также единственным образом раскладывается по степеням порстых, но с точностью до знака $\pm$ перед этим разложением.

Основную теорему арифметики можно доказать разными способами. Покажем еще один способ, который использует множества и операции Минковского с этими множествами.

T1 Пусть $P, Q \subseteq \mathbb{Z}$. Суммой и разностью по Минковскому называются, соответственно, множества:

$$P \oplus Q = \{x + y \mid x \in P, y \in Q\}, \quad P \ominus Q = \{x - y \mid x \in P, y \in Q\}.$$

T2 Множества вида $a\mathbb{Z}$ замкнуты относительно операций сложения и умножения (являются подкольцами кольца $\mathbb{Z}$), поэтому для любых $P, Q \subseteq a\mathbb{Z}$ и любых $k, n \in \mathbb{Z}$ имеет место вложение:

$$kP \oplus nQ \subseteq a\mathbb{Z}.$$

T3 $a|b$ тогда и только тогда, когда $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Действительно, если $a|b$, то $b = ka$. Если $x \in b\mathbb{Z}$, то $x = by = aky \in a\mathbb{Z}$.

Пусть $b\mathbb{Z} \subseteq a\mathbb{Z}$, тогда $b \in b\mathbb{Z}$ и, следовательно, $b \in a\mathbb{Z}$, т.е. $b = ka$ при некотором целом k, тогда $a|b$.

T4 Решим неравенство $P \ominus P \subseteq P$, где $P \subseteq \mathbb{Z}$.

1) Пустое множество удовлетворяет этому неравенству.

2) Множество $P = \{0\}$ также удовлетворяет данному неравенству.

3) Пусть $c \in P$ и $c \neq 0$. В этом случае ясно, что в P есть положительные числа ($0 = c - c$, а значит, есть c и $-c$). Пусть $a = \min\{x \mid (x \in P) \wedge (x > 0)\}$. Легко видеть, что $a\mathbb{Z} \subseteq P \ominus P \subseteq P$. Но если $P \setminus a\mathbb{Z}$ не пусто, то существует $x \in P \setminus a\mathbb{Z}$, причем $x = ka + d$, где $0 < d < a$. Но $d = x - ka \in P \ominus P$, т.е. $d \in P$, что противоречит выбору a. Следовательно, $P = a\mathbb{Z}$.

Таким образом, если $P \ominus P \subseteq P$, то либо $P = \emptyset$, либо $P = a\mathbb{Z}$ при некотором целом a.

T5 $a\mathbb{Z} \oplus b\mathbb{Z} = \text{НОД}(a, b)\mathbb{Z}$.

Действительно, $P = a\mathbb{Z} \oplus b\mathbb{Z}$ удовлетворяет неравенству $P \ominus P \subseteq P$, и значит, по свойству T4 $a\mathbb{Z} \oplus b\mathbb{Z}$ совпадает с множеством $c\mathbb{Z}$ при некотором c (причем, если $a, b > 0$, то и $c > 0$), т.е.

$$a\mathbb{Z} \oplus b\mathbb{Z} = c\mathbb{Z}.$$

Отсюда, с одной стороны, следует, что $a\mathbb{Z}, b\mathbb{Z} \subseteq c\mathbb{Z}$, откуда (свойство T3) $c|a$ и $c|b$. С другой стороны, если $d|a$ и $d|b$, то $a\mathbb{Z}, b\mathbb{Z} \subseteq d\mathbb{Z}$, откуда (свойство T2) $c\mathbb{Z} \subseteq d\mathbb{Z}$, откуда (свойство T3) $d|c$. То есть, любой делитель a и b не превосходит c, а c также является делителем a и b. Следовательно, $c = \text{НОД}(a, b)$.

T6 Если простое p делит произведение ab, то или $p|a$, или $p|b$.

Предположим, что $p \not| a$, тогда $\text{НОД}(p, a) = 1$ и (по свойству T5) $p\mathbb{Z} \oplus a\mathbb{Z} = \mathbb{Z}$. Откуда $1 = kp + ma$ при некоторых целых k, m. Тогда $b = kbp + mab$, откуда следует, что $p|b$.

Если предположить, что $p \not| b$, то аналогично выводим соотношение $p|a$.

T7 Отсюда, как уже отмечалось выше, легко выводится Основная теорема арифметики.

4.3.2 Задачи

1. Докажите, что если $P \ominus P \subseteq P$, то выполняется равенство $P \ominus P = P$.

2. Докажите, что неравенство $P \ominus P \subseteq P$ определяет все подгруппы $\mathbb{Z}$ по сложению.

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

ГЛАВА 5

Симметрии фигур

5.1 Симметрии правильного треугольника

5.1.1 Конспект

1. Вернемся на окружность и рассмотрим на ней вращение $R_{2\pi/3}$, т.е. на 120^o.

2. Множество вращений $R^3 = \{R_{2\pi/3}, R^2_{2\pi/3}, R^3_{2\pi/3}\}$ образует циклическую группу. Видим, что
$$R^3 = \{\mathrm{id}, R_{2\pi/3}, R_{4\pi/3}\}.$$

3. Зафиксируем точку A на окружности и найдем ее образы при действии этой группы: $B = R_{2\pi/3}(A)$, $C = R_{4\pi/3}(A)$. Набор точек $\{A, B, C\}$ образует орбиту точки A при действии группы R^3.

4. Посмотрим теперь на треугольник ABC. Какие движения переводят его в себя? Очевидно, вращения из группы R^3, но также есть и симметрии $S^3 = \{S_A, S_B, S_C\}$ относительно осей, проходящих через центр окружности и вершины треугольника.

5. Можем проверить, что объединение $R^3 \cup S^3$, состоящее из трех вращений и трех симметрий, образует группу относительно операции композиции движений.

6. Выпишем полную таблицу Кэли для этой группы:

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

7. На примере этой группы мы можем заметить, во-первых, что в группе можно выделить подгруппу вращений (верхний левый квадрат 3×3),

во-вторых, что группа движений треугольника конечна и некоммутативна, поскольку ее таблица умножения несимметрична. Кроме того, в полном сооветствии с таблицей умножения классов $\mathbb{R}$ и $\mathbb{S}$ видим, что композиция вращений есть вращение, композиция вращения и симметрии есть симметрия, композиций двух симметрий есть вращение.

8. В группе симметрий треугольника можно выделить базовые элементы: либо пара $(R_{2\pi/3}, S_A)$, либо пара (S_A, S_C). Понятно, что здесь можно заменить поворот и симметрии на другие.

9. Вопрос: есть ли еще какие-то движения окружности, переводящие правильный треугольник в себя?

10. Заметим, что при движении, переводящем треугольник в себя, вершины обязательно переходят в вершины. Если бы это было не так, то какая-то вершина перешла бы в точку на стороне треугольника, но тогда преобразование не сохранило бы угол при этой вершине. Таким образом, преобразований треугольника не может быть больше, чем всех возможных перестановок трех вершин:

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Нетрудно видеть, что эти перестановки в точности соответствуют преобразованиям $\mathrm{id}, R_{2\pi/3}, R_{4\pi/3}, S_A, S_B, S_C$. Так что данными преобразованиями исчерпываются все возможные движения, переводящие правильный треугольник в себя.

5.1.2 Задачи

1. Выписать все перестановки на 4 символах A, B, C, D.

5.2 Симметрии правильного многоугольника

5.2.1 Конспект

1. Рассмотрим еще один случай преобразований фигуры в себя. Пусть имеется правильный n-угольник. Тогда очевидными преобразованиями, сохраняющими форму и размеры фигуры, будут:

$$R_{2\pi k/n}, \quad S_k, \quad k = \overline{1, n}$$

2. В случае четного n в многоугольнике все вершины разбиваются на пары противоположных, лежащих на общей оси симметрии, поэтому имеется $n/2$ осей симметрии, проходящих через вершины, и $n/2$ осей, проходящих через середины строн. В случае нечетного n на каждую вершину приходится своя ось симметрии.

3. Как и в случае треугольника, несложно показать, что этими $2n$ преобразованиями исчерпываются все преобразования правильного многоугольника в себя, что, как видим, сильно меньше общего числа перестановок вершин, которое равно $n!$ (совпадение получается только при $n = 3$).

4. Однако и в этом случае в качестве базисных можно выбрать всего два преобразования: $R_{2\pi/n}$ и S_1, либо две симетрии, оси которых являются соседними.

5.2.2 Задачи

1. Составить полную таблицу Кэли для группы движений правильного 4-угольника.

2. Выразить поворот на 90 градусов с помощью двух симметрий.

5.3 Подгруппы движений окружности

5.3.1 Конспект

1. Правильные n-угольники дают приблизительное представление о подгруппах движений окружности. Приблизительное — именно в том смысле, что движения n-угольников с любой наперед заданной точностью (при достаточно большом n) будут представлять движения окружности.

2. Вопрос: все ли конечные подгруппы движений окружности задаются движениями правильных n-угольников?

3. Ответ: да, но с оговоркой. Некоторые конечные подгруппы совпадаются с некоторой группой движений n-угольника, другие же являются ее собственной подгруппой.

4. Действительно, пусть G — некоторая подгруппа движений окружности, причем конечная, т.е.

$$G = \{g_1, g_2, \ldots, g_m\}.$$

5. Возьмем произвольный элемент g_k и рассмотрим множество всех его целых степеней:
$$\langle g_k \rangle = \{\dots, g_k^{-1}, g_k^0, g_k, g_k^2, \dots\}$$

6. Данное множество, очевидно, является подгруппой группы G, а значит, конечно. Но тогда среди степеней g_k точно есть два совпадающих значения: $g_k^s = g_k^t$ при $t \neq s$. Пусть для определенности $t > s$. Тогда, умножая равенство на g_k^{-s}, получаем $g_k^{t-s} = g_k^0 = \mathrm{id}$. Иначе говоря, g_k в некоторой положительной степени превращается в id.

7. ***Порядком элемента*** $g \in G$ называется минимальное натуральное число s такое, что $g^s = \mathrm{id}$. Как видим, для всякого $g_k \in G$ такой порядок существует.

8. При этом, как мы установили ранее, g_k — это либо поворот окружности, либо отражение относительно оси, проходящей через ее центр. Во втором случае, очевидно, что степень g_k равна 2, т.к. отражение само себе обратно.

9. Если g_k — поворот, то это поворот на угол $2\pi/s$, где s — порядок g_k.

10. Порядок элемента является одновременно и порядком подгруппы $\langle g_k \rangle$. Действительно, если s — порядок элемента g_k, то все g_k в степенях меньше s различны (иначе порядок оказался бы меньше s), а все бОльшие степени сводятся к меньшим сокращением на g_k^s. Так что в подгруппе $\langle g_k \rangle$ ровно s элементов!

11. Конечная группа $\langle g_k \rangle$ называется ***циклической***. Это название вполне соответствует тому, что все элементы группы в нашем случае есть повороты окружности на определенный угол, нацело делящий 2π.

12. Итак, мы видим, что в G есть подгруппы вида $\langle g_k \rangle$, которые либо соответствуют вращениям многоугольников (если g_k — поворот), либо отражениям. Наша задача состоит в том, чтобы показать, что все эти подгруппы есть подгруппы движений какого-то одного n-угольника.

13. Пусть $G' = \{g \in G \mid g \text{ — поворот}\}$. Ясно, что G' — подгруппа группы G. Предположим далее, что $G' \neq G$, т.е. в группе G существует хотя бы одно отражение h. В этом случае, как мы видели ранее, все элементы произведения Минковского hG' также являются отражениями. Предположим, что существует отражение $h' \in G \setminus (hG' \cup G')$. Но ранее мы установили, что hh' есть поворот, причем $hh' = g \in G'$, т.к. $hh' \in G$. Но тогда $h' = h^{-1}g = hg \in hG'$ (отражение обладает свойством $h = h^{-1}$), а это противоречит выбору h'

14. Итак, если в группе G есть отражения, то все они находятся в одном классе hG', причем этот класс не зависит от выбора отражения h. Иначе

говоря, все отражения порождены каким-то одним отражением и всеми поворотами.

15. Осталось разобраться с подгруппой G' всех поворотов.

16. Возьмем из G' самый маленький поворот g_0, т.е. такой, у которого порядок наибольший. Угол поворота g_0 обозначим через x_0, а порядок g_0 — через s_0. Так что $x_0 s_0 = 2\pi$.

17. Пусть g — произвольный поворот из G' и его угол поворота равен x. Если x не делится нацело на x_0, то имеет место представление

$$x = kx_0 + y,$$

где $0 < y < x_0$. Кроме того, углу y соответствует поворот $g' = g(g_0)^{-k}$, который, очевидно, принадлежит группе G', а значит, имеет конечный порядок.

18. Каков порядок этого поворота? Ясно, что $s_0 y < s_0 x_0 = 2\pi$, следовательно, порядок поворота g' должен быть больше s_0. Но s_0 — наибольшоий порядок среди всех поворотов группы G'. Противоречие! Значит, $y = 0$, т.е. x нацело делится на x_0: $x = kx_0$ при некотором целом положительном k.

19. Таким образом, подгруппа G' группы G состоит из поворотов, являющихся степенями поворота g_0 — самого маленького поворота! В частности, отсюда следует и то, что порядок самой группы G' равен порядку этого поворота g_0.

20. Итак, произвольная конечная группа движений окружности:

    a) либо является циклической группой поворотов $\langle g_0 \rangle$, совпадающей с группой поворотов правильного n-угольника, где n — порядок этой группы,

    b) либо есть объединение $\langle g_0 \rangle \cup h\langle g_0 \rangle$, где h — некоторое отражение того же самого правильного n-угольника.

21. Снова видим, что конечная группа движений порождается парой базовых движений: одного поворота и однго отражения. Как и прежде, поворот можно заменить композицией двух отражений, и эти два отражения рассматривать как базовые элементы группы.

5.3.2 Задачи

1. Доказать, что $\langle g_0 \rangle \cap h\langle g_0 \rangle = \emptyset$, т.е. группа движений распадается на два равномощных класса. один из которых получается применением отражения ко второму.

2. Пусть G — коммутативная группа, $g \in G$ и H — подгруппа группы G. Доказать, что множество gH равномощно множеству H.

3. Вывести из предыдущего ***теорему Лагранжа***: порядок подгруппы делит порядок группы.

4. Обобщить результат на некоммутативные группы.

5.4 Симметрии ромба, группа Клейна

5.4.1 Конспект

1. Рассматриваем ромб, не являющийся квадратом.
2. Движения ромба состоят из:
   a) двух симметрий: относительно его диагоналей, обозначим эти симметрии S_1 и S_2;
   b) одного вращения: на угол π, обозначим это вращение R;
   c) тождественного преобразования id.
3. Других движений ромба не существует. Докажем это.

   Пронумеруем вершины ромба цифрами 1,2,3,4 (1 и 3 противоположны). Предположим, что при некотором преобразовании 1 переходит в 1. В этом случае 3 не может перейти ни в 1, ни в 2 или 4, иначе произойдет потеря инцидентности — вершина 3 либо совпадет с 1, либо будет соседней. Стало быть, 3 также останется на месте. Но тогда остается ровно два преобразования: id и симметрия относительно оси 13 (обозначим ее S_1).

   Очевидно также, что 1 не может перейти в 2 или 4, т.к. в противном случае расстояние 1–3 перейдет в расстояние 2–4, а это невозможно для ромба с различными диагоналями. Остается вариант перехода 1 в 3, который дает два оставшихся преобразования: поворот на 180^o и симметрию относительно диагонали 24 (обозначим ее S_2).

   Если провести аналогичный анализ для остальных вершин, то мы получим те же самые преобразования.
4. Таблица Кэли группы движений ромба:
5. Отличие данной группы от группы движений правильного n-угольника состоит в том, что группа ромба является коммутативной (абелевой).
6. Эта группа нам еще встретится позднее под именем «четвернаяя группа Клейна», когда мы будем говорить об арифметике остатков.

id	R	S_1	S_2
R	id	S_2	S_1
S_1	S_2	id	R
S_2	S_1	R	id

ГЛАВА 6

Движения плоскости и пространства

6.1 Виды движений плоскости. Теорема Шаля

6.1.1 Конспект

1. Разбираем движения, попутно доказывая лемму «о гвоздях».
2. Пусть на плоскости три точки, не лежащие на одной прямой, остаются неподвижными при движении. Вывод: это id.
3. Пусть на плоскости неподвижны 2 точки и вся прямая, проходящая через них, остальные точки подвижны. Тогда это симметрия относительно данной прямой.
4. Пусть неподвижна лишь одна точка. Такое возможно лишь при вращении вокруг этой точки на угол, не кратный полному обороту.
5. Пусть вообще нет неподвижных точек. Берем любую точку, смотрим, куда она переходит, применяем сдвиг (параллельный перенос). Оставшееся преобразование имеет как минимум 1 неподвижную точку, а значит, является либо id, либо симметрией, либо поворотом. Интересно, что поворот в данном случае можно исключить, т.к. композиция сдвига и поворота есть просто поворот, а значит, в исходном преобразовании была как минимум одна неподвижная точка. Следовательно, исходное движение есть либо сдвиг, либо смещенная симметрия (композиция сдвига и симметрии).
6. Таким образом, движение плоскости можно рассматривать как комбинацию параллельного переноса (в частности, на нулевой вектор), поворота (в частности, на нулевой угол) и симметрии относительно произвольной прямой.
7. ***Теорема Шаля***. Произвольное движение (без разложения его на компоненты) есть движение одного из следующих классов:

   а) класс параллельных переносов (на произвольный вектор), который мы обозначим $\rightrightarrows$;

b) класс поворотов относительно произвольного центра, который мы обозначим ↻;

c) класс ***скользящих симметрий*** (сдвиг на произвольный вектор с последующей симметрией относительно оси данного вектора), который мы обозначим ⟝⟞.

8. Таблица композиций для таких классов выглядит следующим образом:

	⇉	↻	⟝⟞
⇉	⇉	↻	⟝⟞
↻	↻	⇉ или ↻	⟝⟞
⟝⟞	⟝⟞	⟝⟞	⇉ или ↻

9. Аналогично одномерным случаям (прямая и окружность) можно выбирать различные базовые преобразования для построения с их помощью всех движений.

10. Всякое движение есть композиция не более трех симметрий (относительно разных и, вообще говоря, не обязательно параллельных осей).

11. Сдвиг можно представить как композицию двух симметрий (относительно параллельных осей).

12. Поворот можно представить как композицию двух симметрий (относительно пересекающихся осей).

13. Скользящую симметрию можно представить как композицию трех симметрий (две на сдвиг и одна собственно симметрия).

6.1.2 Задачи

1. Показать, что композиция поворотов (относительно разных центров) есть либо сдвиг, либо поворот (вычислить его центр).

2. Показать, что композиция сдвига и поворота есть поворот.

6.2 Сравнение движений прямой, окружности и плоскости

6.2.1 Конспект

1. Отметим несколько общих свойств рассмотренных нами движений прямой, окружности и плоскости.

2. Во-первых, их всех можно свести к композиции симметрий. Для одномерных объектов (прямая и окружность) — не более двух, для двумерных — не более трех.

3. Во-вторых, все движения можно разделить на два класса: сохраняющие и меняющие ***ориентацию***. Те движения, которые сводятся к композиции четного числа симметрий, сохраняют ориентацию фигур, а те, которые сводятся к композиции нечетного числа симметрий, — меняют ориентацию фигур. Изменение ориентации означает, что право и лево меняются местами, т.е. мы как бы переходим в зазеркалье.

4. При этом нужно отметить, что преобразования, меняющие ориентацию, обязательно требуют выхода в пространство, если мы хотим осуществить их непрерывным движением.

5. В-третьих, есть и более глубинная связь движений прямой, окружности и плоскости. Мы уже отмечали, что окружность можно рассматривать как прямую, у которой склеили противоположные концы (где-то на бесконечности). И с этой точки зрения сдвиг на прямой является прямой аналогией вращения окружности. Особенно, если величина сдвига сильно меньше радиуса.

6. А симметрия прямой при этом естественным образом превращается в симметрию окружности. Только ось симметрии должна проходить через место склейки двух бесконечностей. Остальные же симметрии можно получить дополнительным сдвигом, т.е. вращением.

7. Далее, окружность находится на плоскости. И поэтому вращение окружности полностью аналогично вращению плоскости, если при этом совместить их центры.

8. Еще проще увидеть совпадения понятий сдвига на прямой и плоскости. В обоих случаях мы просто смещаем все точки на какой-то вектор.

9. Тем не менее, на плоскости появляется новый вид движения, который комбинирует в себе сдвиг и отражение относительно оси сдвига. Это — скользящая симметрия, т.е. симметрия с последующим применением сдвига вдоль оси симметрии. На одномерных объектах такое движение в принципе невозможно. На прямой симметрия относительно этой же прямой ничего не дает, т.е. является id, а на окружности симметрия относительно самой окружности вообще требует специального построения в геометрии плоскости.

6.3 Векторно-числовое представление движений плоскости

6.3.1 Конспект

1. ***Аффинное пространство*** — множество точек и векторов. В аффинном пространстве мы работаем сразу с двумя сортами объектов — точками и векторами, на которых заданы операции сложения и вычитания. При этом в сумме $a+b$ и разности $a-b$ могут быть такие комбинации:

   1) a — точка, b — вектор, результатом $a+b$ будет точка, соответствующая концу вектора b, когда он отложен от точки a, результатом $a-b$ будет точка c такая, что $c+b=a$;

   2) a и b — векторы, результатом $a+b$ будет вектор, построенный по правилу параллелограмма, результатом $a-b$ будет вектор c такой, что $c+b=a$;

   3) a и b — точки, результатом $a-b$ будет вектор с началом в точке b и концом в точке a.

2. Движения — это преобразования точек. Параметром движения может быть вектор и/или угол (число).

3. Сдвиг на плоскости на вектор a обозначим T_a. Операция T_a осуществляет прибавление вектора a к точкам плоскости. Композиция сдвигов соответствует сумме векторов сдвига: $T_a \circ T_b = T_{b+a}$.

4. Поворот вокруг нуля мы ранее обозначали R_α, где α — угол в радианах.

5. Поворот на угол α относительно произвольной точки M можно выразить так:
$$R_{M,\alpha} = T_{O+M} \circ R_\alpha \circ T_{O-M},$$
т.е. сначала сдвигаем точку M в центр вращения, отмеченный точкой O, затем производим вращение, затем возвращаем точку M на место обратным сдвигом.

6. Наконец, у нас остается такой вид движения, который осуществляет отражение относительно произвольной прямой на плоскости. Обозначим его S_l.

7. Предположим, что на плоскости помимо точки O мы также зафиксировали некоторую прямую, проходящую через O с выделенным направлением OA (A лежит на этой прямой и не совпадает с O). Зафиксируем отражение S_{OA} относительно данной выбранной оси OA. Отметим, что $S_{OA} = S_{AO}$, т.е. отражение не зависит от направления оси отражения.

8. Выразим произвольное отражение через базовое отражение S_{OA} и другие движения. Для этого обозначим через M произвольную точку прямой l, через α — угол наклона прямой l относительно направления OA. Тогда
$$S_l = T_{O+M} \circ R_\alpha \circ S_{OA} \circ R_{-\alpha} \circ T_{O-M},$$
т.е. сначала мы сдвигаем плоскость так, чтобы точка M оказалась в точке O, затем выполняем поворот на угол $-\alpha$, далее выполняем стандартное отражение, а затем производим обратные операции, которые возвращают прямую l на место.

9. Соответственно, скользящая симметрия, при которой выполняется отражение относительно оси l и сдвиг на вектор MM' ($M, M' \in l$), записывается так:
$$S_l = T_{O+M} \circ R_\alpha \circ S_{OA} \circ R_{-\alpha} \circ T_{O-M} \circ T_{M'-M},$$

10. В терминах движений T, R, S можно записать все возможные виды движений плоскости, т.е. сдвиг на произвольный вектор, поворот на произвольный угол относительно произвоьлной точки, скользящую симметрию относительно произвольной прямой l со сдвигом на произвольный вектор, лежащий на этой прямой.

11. Если мы вернемся на окружность, то нам потребуется исключить сдвиги, оставив только вращения и симметрии.

6.4 Пара слов о движениях сферы

6.4.1 Конспект

1. Имея опыт перехода от прямой к окружности, мы можем легко найти движения сферы, отправляясь от движений плоскости.

2. Представим себе сферу как плоскость, у которой бесконечно удаленный край был стянут в точку (метод «хинкали»).

3. Во что превращаются при этом движения плоскости?

4. Сдвиг, он же параллельный перенос, превращается в такое движение, при котором все точки движутся по параллельным траекториям. С точки зрения географии это есть движение вдоль широтных линий. Да, проходят они при этом разное расстояние! Из-за чего, кстати, и появляются силы Кориолиса, создающие океанические течения вроде Гольфстрима. Но собственные расстояния между точками сохраняются, и это, несомненно, движение.

5. Вращение, которое, как мы помним, на окружности соответствует сдвигу на прямой, в случае сферы в прямом смысле слова совпадает со сдвигом! Дело в том, что вращение сферы вокруг оси, — это вращение вокруг полюса, при котором угол поворота измеряется меридианом. Но ведь то же самое движение около экватора есть то, что мы только что отнесли к сдвигам вдоль широтных линий.

6. Таким образом, сдвиг прямой и вращение окружности в случае сферы чудесным образом объединяются в один вид движений — осевое вращение. И это делает движения сферы чуть проще, чем движения плоскости, где сдвиг можно представить лишь как композицию двух вращений.

7. Далее, симметрия плоскости относительно прямой естественным образом переходит в отражение сферы относительно центральной секущей плоскости или, иначе говоря, относительно окружности большого круга. При такой симметрии полюса сферы меняются местами (полюса определются пересечением со сферой прямой, пересекающей плоскость отражения в центре сферы и перпендикулярной ей), а плоскость отражения остается на месте.

8. Наконец, скользящая симметрия плоскости есть композиция сдвига и осевой симметрии, и ей на сфере соответствует ***зеркальное вращение***, т.е. композиция отражения и вращения параллельно плоскости отражения.

9. Таким образом, все движения сферы распадаются на два класса: вращения и зеркальные вращения. При этом, все движения есть композиция не более чем трех отражений.

10. Этот аналог теоремы Шаля для сферы можно доказать, используя очередную лемму о гвоздях, предполагая неподвижность пары противоположых точек (случай одной точки на плоскости), неподвижность целой окружности большого круга (случай двух точек на плоскости), отсутствие неподвижных точек.

6.4.2 Задачи

1. Построить таблицу движений сферы аналогично таблице движений плоскости (символику придумайте сами).

2. **Доказать, что других движений на сфере не существует (лемма о гвоздях).

6.5 Пара слов о движениях пространства

6.5.1 Конспект

1. Наконец, мы можем от сферы перейти к пространству. На самом деле, переход в пространство сопровождается лишь добавлением сдвига в пространстве. Т.е. любое движение сферы можно рассматривать как движение пространства с одной неподвижной точкой — центром сферы. После чего можно применить сдвиг этого центра, и получить новые движения. Понятно, что никаких других движений тут быть не может.

2. Тем не менее, классификация движений пространства становится сложнее примерно так же, как классификация движений плоскости превосходит классификацию движений окружности. А именно, в пространстве появляется ***винтовое движение*** как композиция осевого вращения и сдвига вдоль оси вращения. Это — обобщение скользящей симметрии на плоскости (если винт осуществляет поворот на 180^0, мы как раз получаем скользящую симметрию).

3. Есть также и собственно ***скользящая симметрия пространства***. Это — отражение относительно плоскости с последующим сдвигом вдоль направления, параллельного данной плоскости. Такое движение также является обобщением скользящей симметрии на плоскости.

4. Заметим, что более сложное движение винт включает в себя более простые. Так, если винт имеет нулевой сдвиг, то он доставляет осевое вращение, а если винт имеет нулевой поворот, то он доставляет сдвиг. Понятно, что в случае полного зануления параметров винта мы получим id.

5. Точно так же, ***зеркальное вращение***, как и в случае сферы, при нулевом повороте доставляет просто симметрию.

6. Наконец, скользящая симметрия своим частным случаем имеет просто симметрию относительно плоскости.

7. Таким образом, классификация движений пространства включает следующие виды движений:

   a) винт (в частности, сдвиг, осевое вращение, id);

   b) зеркальное вращение (в частности, отражение);

   c) скользящая симметрия (в частности, отражение).

6.5.2 Задачи

1. Построить таблицу движений пространства аналогично таблице движений плоскости (символику придумайте сами).

2. *Показать, что центральная симметрия пространства — это зеркальное вращение.

3. **Доказать, что других движений в пространстве не существует (лемма о гвоздях).

Таблица 6.1: Сравнение движений.

	Собственные движения (не меняют ориентацию)			**Несобственные движения (меняют ориентацию)**		
	Перенос	Поворот	Смещение поворота	Симметрия	Смещенная симметрия	
Прямая	сдвиг на число			относительно точки		
Окружность	вращение			осевая симметрия		
Плоскость	параллельный перенос	относительно точки		осевая симметрия	скользящая симметрия (перенос+ симметрия)	
Сфера	вращение вблизи экватора	вращение вблизи полюса		отражение относительно плоскости	зеркальное вращение (вращение+симметрия)	
Пространство	параллельный перенос	осевое вращение	винт (перенос + вращение)	отражение относительно плоскости	скользящая симметрия (перенос+ симметрия)	зеркальное вращение (вращение+ симметрия)

ГЛАВА 7

Исчисление остатков

7.1 Арифметика остатков

7.1.1 Конспект

1. Рассмотрим бытовую задачу. Вам нужно выключить печку через 40 минут, но у вас нет таймера, зато есть будильник, на котором можно выставить время звонка. Сейчас 12:30, на какое время требуется поставить будильник? Ответ: 13:10. Почему так? Дело в том, что в часе 60 минут, и если к 30 минутам прибавить 40, получается 70 минут, что больше часа. Поэотму добавляем 1 час и остаток — 10 минут.

2. Еще пример: сколько часов будет через 20 часов, если сейчас 8 утра? Можно решать аналогично: $8 + 20 = 28$, затем убираем полные сутки, т.е. 24 часа, остается 4 часа утра.

3. Можно решать иначе. 20 часов — это -4 часа от суток. Следовательно, нужно просот вычесть из 8 утра 4 часа и получим те же 4 часа утра.

4. Во всех случаях мы решаем задачу нахождения остатка от деления на некоторое число. В случае минут это 60, в случае часов это 24.

5. Ранее мы уже пользовались представлением числа в виде $a = km + b$, где k — неполное частное от деления a на m, b — остаток от деления, который находится в промежутке от 0 (включая) до m (не включая).

6. Когда вас просят отметить в анкете количество полных лет, то вам по сути нужно найти неполное частное от деления вашего возраста на 1 год. Конечно, в данном случае нам это просто сделать, т.к. каждый год мы запоминаем именно количество прожитых лет, а не дней или недель.

7. Но, например, во многих сферах деятельности планирование календаря происходит неделями (и даже у себя в компьютере в настройках календаря вы можете вывести номер текущей недели в году). А сколько недель в году? Для этого нужно найти неполное частное от деления 365 (или 366) на 7, оно составляет 52.

8. Остаток от деления на неделю есть число от 0 до 6, которое определяет сдвиг вперед относительно текущего дня недели. Например, если

сегодня четверг, то какой день недели будет через 30 дней? Мы выбрасываем из 30 4 полных недели, что составляет 28 дней, и находим остаток, который равен 2. Это значит, что через 30 дней будет четверг плюс 2 дня, т.е. суббота.

9. Точно так же можно легко заметить, что каждый год происходит смещение дат на 1 или два дня вперед относительно дней недели. Так, если в этом году 1 января было субботой, то в следующем оно будет или воскресеньем (если мы не переходим через 29 февраля), или понедельником (если текущий год — високосный, т.е. содержит 366 дней).

10. Каждые 28 лет (а 28 — это наименьшее общее кратное 7 и 4) соответствие дат и дней недели повторяется.

11. При расчетах на более длительные периоды, а именно, при переходе через 1900 год или 2100 год, нужно учитывать также, что 3 раза за 400 лет не происходит добавление лишнего дня (29 февраля) для более точного соответствия календаря астрономическому году, т.е. 1900, 1800, 1700 годы не являются високосными, как и 2100, 2200 и 2300.

12. Тем не менее, часто в жизни встречается задача вычисления дня недели, и здесь нам на помощь приходит исчисление остатков по модулю 7. Например, сегодня 21 марта 2020 суббота, а нам нужно знать, какой день недели будет 31 августа 2020. Сначала мы находим день недели 21 августа, т.к. до этой даты целое число месяцев. При этом мы 3 раза переходим через 31 число (март, май, июль) и 2 раза — не переходим (апрель, июнь). Следовательно, 3 раза прибавляется остаток 3, и 2 раза — остаток 2, итого сумма остатков составляет 13. Но это больше 7, причем очень близко к 14, поэтому сумму остатков мы запишем как -1. Наконец, остается добавить 10 дней (от 21 августа до 31 августа). Итого получается 9, а по модулю 7 — всего 2. Таким образом, 31 августа 2020 года есть понедельник!

13. Равенство $a = km + b$ при исчислении остатков принято записывать так:

$$a \equiv b \pmod{m},$$

причем, если модуль m известен из контекста и не меняется при вычислениях, то его можно опускать, записывая просто $a \equiv b$.

14. Например, $365 \equiv 1 \pmod{7}$. Такая запись никак не информирует нас о коэффициенте k, т.е. о неполном частном.

15. Таблицы сложения остатков по модулю 7 и 8:

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Таблица сложения получается последовательными циклическими сдвигами верхней строки влево.

16. Таблица умножения остатков по модулю 7:

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Таблица умножения (за исключением нулевых строки и столбца) центрально симметрична.

17. Отметим еще одно свойство таблицы умножения: строка или столбец, номер которого НЕ взаимно прост с модулем, содержит нули. Это легко доказать. Пусть номер строки k и $s = \text{НОД}(k, m) > 1$. При этом ясно, что $s < m$, т.е. s является делителем m. Пусть также $t = m/s$. Рассмотрим тогда строку k и столбец t. Произведение их номеров равно $kt = km/s$. Поскольку k/s также целое, получаем, что kt кратно m, а значит, $kt \equiv 0 \pmod m$. Отметим, что $s = 1$ здесь не проходит ровно потому, что в этом случае t не будет номером столбца таблицы умножения.

18. На самом деле, верно и обратное: если строка таблицы умножения содержит нули, то номер строки не взаимно прост с модулем. Для этого мы докажем эквивалентное утверждение

Теорема . *Пусть $k > 0$ и $k \perp m$, тогда все остатки*

$$k, \quad 2k, \quad 3k, \quad \ldots, \quad (m-1)k \pmod m$$

попарно различны и отличны от нуля.

Доказательство. Предположим, что один из остатков равен нулю: $kl \equiv 0 \pmod{m}$, где $l \in \{1, 2, \ldots, m-1\}$. Тогда $kl = mt$ при некотором t. Но поскольку $k \perp m$, в силу ОТА число k делит t, а значит, $k \leqslant t$. Однако $l < m$, следовательно, $kl < mt$. Противоречие.

Далее, если среди остатков есть равные, например, $kl \equiv kt$, то здесь же найдется и остаток $k(l-t)$ (или $k(t-l)$, если $t > l$), который равен 0. А это невозможно по доказанному.

Таким образом, эти остатки все различны и положительны, а значит, являются перестановкой множества $\{1, 2, , \ldots, m-1\}$. □

19. Множество $\{0, 1, 2, \ldots, m-1\}$ с операциями сложения и умножения по модулю m называется ***кольцом вычетов*** по модулю m и обозначается $\mathbb{Z}/m\mathbb{Z}$ или, проще, $\mathbb{Z}_m$.

20. Множество $\mathbb{Z}_m^*$, состоящее только из чисел, взаимно простых с модулем m элементов $\mathbb{Z}_m$, образует группу по умножению остатков. Это легко увидеть из таблиц умножения, если исключить в них строки и столбцы, содержащие нули. Например, таблицей умножения для группы $\mathbb{Z}_8^*$ будет

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

7.1.2 Задачи

1. Построить таблицы сложения и умножения для остатков: 2,3,4,5,6.

2. Сравнить таблицу сложения остатков по модулю 2 с таблицами умножения классов сдвигов $\mathbb{T}$ и симметрий $\mathbb{S}$ для прямой и окружности.

3. Сравнить таблицу симметрий ромба с таблицей умножения группы $\mathbb{Z}_8^*$.

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

5. Проверить, что $\mathbb{Z}_m$ удовлетворяет аксиомам кольца.

7.1.3 Свойства арифметики остатков

1. Свойства сравнений таковы:

   M1. $a \equiv b \pmod m$ тогда и только тогда, когда $a - b$ кратно m;

   M2. если $a \equiv b$, $c \equiv d$, то $a + c \equiv b + d$, $a - c \equiv b - d$ и $ac \equiv bd$;

   M3. для $n \geqslant 0$ если $a \equiv b$, то $a^n \equiv b^n$;

   M4. признаки делимости на 3 и на 9: $a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n \equiv a_0 + \cdots + a_n$ по модулю 3 и по модулю 9;

   M5. если $m > 0$ и $d \perp m$, то

   $$ad \equiv bd \pmod m \iff a \equiv b \pmod m$$

   M6. если $m, d > 0$, то

   $$ad \equiv bd \pmod{md} \iff a \equiv b \pmod m$$

   M7. если $m > 0$, то для любого d

   $$ad \equiv bd \pmod m \iff a \equiv b \pmod{m/\text{НОД}(m,d)}$$

   M8. если $m, d > 0$, $a \equiv b \pmod{md}$, то $a \equiv b \pmod m$

   M9. если $m, n > 0$, то

   $$a \equiv b \pmod m,\quad a \equiv b \pmod n \iff a \equiv b \pmod{\text{НОК}(m,n)}$$

   M10. если $m, n > 0$ и $m \perp n$, то

   $$a \equiv b \pmod m,\quad a \equiv b \pmod n \iff a \equiv b \pmod{mn}$$

   M11. пусть m_p — степень простого числа p в разложении m по степеням простых (ОТА), тогда

   $$a \equiv b \pmod m \iff \forall p \quad a \equiv b \pmod{p^{m_p}} \quad (p \text{ — простое})$$

2. ***Китайская теорема об остатках***. Пусть числа $m_1, \ldots, m_k > 0$ попарно взаимно просты, $m = m_1 \ldots m_k$. Тогда

   $$a \equiv b \pmod m \iff a \equiv b \pmod{m_j},\quad j = 1, \ldots, k$$

3. ***Малая теорема Ферма***: $n^{p-1} \equiv 1 \pmod p$, где p — простое и $p \nmid m$.

4. Малая теорема Ферма обеспечивает существование обратных элементов в группе по умножени остатков $\mathbb{Z}_p^*$. Достаточно n умножить на n^{p-2}, и мы получим 1.

5. Отсюда следует, что $\mathbb{Z}_p$ при простом p является ***полем***.

6. Поле — это кольцо, в котором все ненулевые элементы обратимы. Кольцо целых чисел не является полем. Рассмотренные нами ранее группы движений также нельзя назвать полем, т.к. в них всего одно операция. Первое поле, которое мы встречаем в курсе — это $\mathbb{Z}_p$, поле вычетов по простому модулю.

7.1.4 Задачи

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

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

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

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

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

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

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

4. Докажите, что $\text{НОД}(n,m)\text{НОК}(n,m) = nm$.

5. Докажите, что

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

7.2 Многочлены

7.2.1 Конспект

1.

2.

3.

4.

5.
6.
7.
8.
9.
10.

7.2.2 Задачи

ГЛАВА 8

Основная теорема арифметики и ее следствия

8.1 Корни и разрешимость уравнений

8.1.1 Конспект

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

8.1.2 Задачи

8.2 Рациональные дроби

8.2.1 Конспект

1.
2.
3.
4.
5.
6.

7.
8.
9.
10.

8.2.2 Задачи

8.3 Цепные дроби

8.3.1 Конспект

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

8.3.2 Задачи

8.4 Расширение поля рациональных чисел

8.4.1 Конспект

1.
2.
3.
4.
5.
6.
7.
8.

9.

10.

8.4.2 Задачи

ГЛАВА 9

Комплексные числа и Гаусс

9.1 Комплексные числа

9.1.1 Конспект

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

9.1.2 Задачи

9.2 Реализация движений с помощью комплексных чисел

9.2.1 Конспект

1.
2.
3.
4.
5.
6.

7.
8.
9.
10.

9.2.2 Задачи

9.3 Гомотетии прямой и плоскости

9.3.1 Конспект

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

9.3.2 Задачи

9.4 Числа Гаусса

9.4.1 Конспект

1.
2.
3.
4.
5.
6.
7.
8.

9.

10.

9.4.2 Задачи