Математическое Образование

Журнал Фонда математического образования и просвещения

Год четвертый

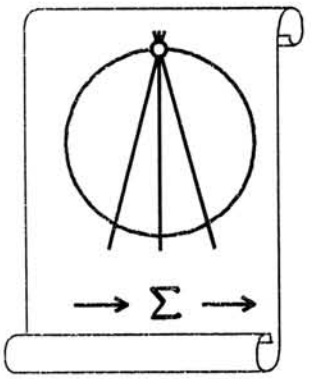
№ 4 (15)

Октябрь - декабрь 2000 г.

Москва

МАТЕМАТИЧЕСКОЕ ОБРАЗОВАНИЕ

Периодическое издание в области математического образования



Учредитель: Фонд математического образования и просвещения

N 4 (15), 2000 г.

Москва

Математическое образование

Журнал Фонда математического образования и просвещения

N 4 (15), октябрь – декабрь 2000 г.

Содержание

Фонд математического образования и просвещения, Москва, 2000 г.
"Математическое образование", периодическое издание.
Зарегистрировано в Роскомпечати РФ,
лицензия №015955 от 15.04.97.
Подписано к печати 12.03.2001.
Компьютерный набор и верстка, компьютерная графика: С. Кулешов.
Объем 6 п.л. Тираж 1000 экз. Цена свободная.

Тезисы по алгебре

А. Н. Земляков

Редакция начинает ряд публикаций учебных материалов одного из ведущих центров углубленной физико-математической подготовки старших школьников — легендарной "Колмогоровской" ФМШ N 18 при МГУ. В настоящем и следующих ближайших номерах публикуются учебные материалы по алгебре и геометрии для одногодичного потока. Автор материалов — выпускник ФМШ 1967 г., золотой медалист, преподаватель ФМШ в 1969 – 1984 гг. Александр Николаевич Земляков. Более 30 лет он занимается методическими и методологическими вопросами обучения математике, углубленным обучением математике в старших классах. Является автором нескольких методических пособий, в соавторстве изданы учебные, научно-методические и научно-популярные книги, опубликованы многочисленные методические и научно-популярные статьи в журналах "Математика в школе" и "Квант". Соросовский учитель с 1994 г.

Предисловие

«Рассмотрим некоторый, предикативно неограниченный и, следовательно, уникальный экземпляр *А.*»
(Роберт Орос ди Бартини)

Публикуемый учебный текст — «*тезисы*» — приводится точно в том виде, в каком он появился впервые, осенью 1975 года (исключая 2 поправки на современность: в тезисах 57 и 95 — *прим. ред.*). Эти материалы предназначались для учащихся одногодичного потока ФМШ *N*° 18 при МГУ, или, как тогда называлась физико-математическая школа-интернат при МГУ, «*СШИФМП N*° 18 *МОСГОРОНО*[1] *при МГУ им. М. В. Ломоносова*». Несколько слов об одногодичном потоке ФМШ — о тогдашних «*ЕЖах*», как назывались классы этого потока (по литерам «*Е*», «*Ж*», а иногда и «*И*», которыми традиционно обозначались классы[2]).

[1]Эта памятная аббревиатура означает: «*Специализированная школа-интернат физико-математического профиля Московского городского отдела народного образования*».

[2]С этим связана забавная история тех лет: А. Б. Сосинский, задерживаясь по дороге в ФМШ, позвонил в интернат по телефону-автомату и попросил позвать Землякова, который «*в аквариуме у ежей зачет принимает*»! (Аквариумами в интернате назывались большие застекленные аудитории на 2-м и 3-м этажах.) Сколь же были ошарашены услышавшие это граждане, ожидавшие своей очереди у телефонной будки ...

Одногодичный поток был организован в 1966 г. с тем, чтобы дать возможность получить продвинутое образование тем школьникам из российской и белорусской «глубинки», интерес которых к физике и (или!) математике проявился только к выпускному классу (а таких, как показал мой последующий педагогический опыт, довольно много). Как правило, после двух туров экзамена в ФМШ (письменного и устного), окончательный прием в ЕЖи происходил после трех-четырех недель интенсивного «образовательно-испытательного процесса» в ЛФМШ — в летней отборочной физико-математической школе. Сначала ЛФМШ работала в п. Красновидово, на Можайском море (напротив Бородинского поля!), а потом многие годы — в, говоря по-современному, наукограде Пущино-на-Оке (напротив знаменитого заповедника с бизонами!). В летней школе лекции по математике часто читал Андрей Николаевич Колмогоров, по физике — Борис Борисович Буховцев, устраивал музыкальные вечера Павел Сергеевич Александров ... А школьники должны были продемонстрировать не только (и даже не столько) свои способности в физике и математике, но и восприимчивость к обучению, *способность учиться*. Задачи, стоявшие перед перед поступившими после летней ФМШ в «зимнюю», а также, соответственно, и перед преподавателями одногодичного потока, были тоже не из простых. Всего за один год «ежам» предстояло освоиться с физикой–математикой настолько, чтобы понять свои интересы, сориентироваться в своем будущем, а с другой стороны — достаточно хорошо подготовиться к вступительным экзаменам.

По стечению обстоятельств летняя школа 1975 г. проводилась в Москве, в интернатских «трех кубиках»[3]. До речки — только на электричке, и ЛФМШ получилась очень «крутой». А осенью в ЕЖах появились новые преподаватели: к геометрии подключились выпускники ФМШ В. Дубровский (и сейчас работает в интернате — в СУНЦе) и А. Звонкин (ныне во Франции), а к алгебре — руководитель двухгодичного потока ФМШ 1965-67 гг. Алексей Брониславович Сосинский[4], с которым в паре я и работал[5]. Чему учить (чему *полезно учить*), мы с Сосинским, в общем-то, понимали; а вот *как* — в ФМШ всегда был широкий выбор. Вот тогда и появились «*Тезисы по алгебре*».

Это «жанр» *учебного текста* отнюдь не я придумал. Зимой 1965-66 гг. нашего первого лектора по физике, одного из троих главных инициаторов создания (в декабре 1963-го) московской ФМШ, академика Исаака Константиновича Кикоина[6] сменил один из молодых основоположников ФМШ, тогдашний завуч по физике Олег Николаевич Найда. Он излагал электростатику, дойдя и до электродинами-

---

[3] «*Твои три кубика,*
О, спецреспублика ... »
— Юлий Ким, из «*Гимна ФМШ*». Три кубика — три корпуса ФМШ.

[4] Единственный преподаватель математики в нашем выпуске (1967), которого полагалось называть по имени-отчеству; в ФМШ было заведено, что учителей математики из университета ученики звали по имени — Женя Гайдуков, Миша Козлов, Игорь Журбенко, Дима Гордеев, Саша Мищенко ..., — но, разумеется, на Вы.

[5] Автор данного текста начал работать в ЕЖах в 1971 г., и с того же времени, следуя своему замечательному учителю Игорю Константиновичу Сурину, «завел» в этих классах специальный предмет — «*Элементарную математику*», для подготовки к конкурсным экзаменам. В 1975–76 г. мы вели «элементарку» вместе с Сашей Звонкиным.

[6] Двое других: Андрей Николаевич Колмогоров и ректор МГУ Иван Георгиевич Петровский.

ки, в форме как раз *тезисов* — коротких полудогматических «сентенций», которые сначала объяснялись, а потом и записывались (под номерами!). Десять лет спустя мы с Сосинским и попробовали возродить такой *стиль*, но не в виде лекций — в ЕЖах было решено обойтись без лекций по алгебре, — а как «печатные материалы», предназначенные и для преподавателей (т. е. для нас самих! Замечу, что, как это нередко бывало в ФМШ, на уроках алгебры мы делили каждый класс на группы), и для школьников.

Тезисы суть как бы «порции» учебного материала, рассчитанные — каждый тезис — для «отдельного переваривания», не обязательно легкого. Тезисы, раз они тезисы, не обязаны быть рядоположными. На них легко ссылаться, почти любой тезис можно пропустить, почти на каждом можно закончить занятие. Но, конечно, каждое занятие («пара» по-вузовски, т. е. два урока, как ныне принято в старших классах многих школ) должно быть направлено на какую-то *идею*, быть каким-то ощутимым *продвижением* в освоении, и, в соответствии с этим, тезисы сгруппированы в разделы — по разделу на неделю, т. е. на занятие.

Не исключено, что на выбор жанра данного «учебного повествования» повлияли и весьма популярные в то время художественные эссе Валентина Катаева — от «Маленькой железной двери ... » до «Святого колодца» и «Травы забвения» («Алмазный мой венец» в 1975 г. был только начат). «Новый катаевский стиль» — сейчас причисляемый к авангарду и даже к «раннему постмодернизму» *мовизм* — привлекал и, отчасти, поражал (за недоступностью с 20-го года и, следовательно, неизвестностью произведений блестящего В. В. Розанова). В какой-то степени «Тезисы» можно отнести к «пронумерованному мовизму»! (Вообще-то я издавна считаю, что *учебная литература — это тоже литература*[7]; тем более, *учебный текст — это тоже текст*[8].)

Разделы-параграфы тезисов предваряются эпиграфами, сообразно тематике (и настроению момента!). Тезисы по алгебре охватывают первое полугодие; во втором полугодии, как обычно, основной акцент был перенесен на элементарную алгебру — на подготовку к вступительным экзаменам. Тем не менее, в рамках бывшей алгебры были пройдены две весьма поучительные темы: *аффинные геометрии* (в основном, конечные) и *элементы современной логики* (с доказательством теоремы Гёделя о неполноте). И тезисы продолжались, и эпиграфы ... Отрывком из последнего эпиграфа к «*Тезисам по логике*» А. Б. Сосинского я и закончу этот «мемуарно-методический» очерк:

«Радуйся, юноша, молодости своей,
И в дни юности твоей да будет сердцу благо ... »
(*Экклесиаст, 11:9* (*пер. С. Аверинцева*)).

Те времена — учебы у Сосинского, а потом — работы с ним, — были неповторимыми, *уникальными*; впрочем, как и многие другие времена ... Возможно, этим и объясняется появление первого эпиграфа к тезисам — первой фразы легендар-

[7] И учебник Андрея Петровича Киселева по геометрии — литература, причем близкая к science fiction! Глубоко символично, на мой взгляд, что А. П. Киселев похоронен на «Литераторских мостках» Волкова кладбища Санкт-Петербурга, почти рядом с Александром Блоком.

[8] *Текст* — наимоднейшее слово в «около-литературе» 90-х.

ной в то время (да и поныне) статьи в «Докладах Академии наук СССР» (1965; том 163, $N°\,4$) итальянского «красного барона» и советского авиаконструктора-«диссидента» Роберта Людвиговича (!) ди Бартини, представленной итальянцем же и знаменитым академиком АН СССР Бруно Понтекорво (эпиграф к данному очерку взят из более подробного варианта статьи, помещенного в сборнике «Проблемы теории гравитации и элементарных частиц»: М., Атомиздат, 1966!). Фантастически-выдающаяся личность Роберта Ороса ди Бартини (1897–1974), которого в 2000 г. назвали самым загадочным человеком столетия (и стали считать прообразом булгаковского Воланда!), конечно, требует отдельного внимания[9].

[9]Много чего о нем можно найти в Интернете.

ТЕЗИСЫ ПО АЛГЕБРЕ

А. Н. Земляков

Содержание.

Часть I (1-я четверть)
Кольца, арифметика, числа.

«Рассмотрим некоторый тотальный и, следовательно, уникальный экземпляр A.»
(Роберт Орос ди Бартини)

Глава I. Кольцо целых чисел и арифметика

«Бог создал натуральные числа,
все прочее — творение человека.»
(Леопольд Кронекер)

§ 1. Кольца и подкольца

«Алгебраист — это человек, имеющий дело с числами; действия, которые он имеет возможность выполнять над ними, бывают лишь четырех видов: $+$, $-$, $\times$, $:$.»
(Герман Вейль)

1. В математике (в арифметике и алгебре) часто приходится сталкиваться с системами объектов, над которыми можно производить некие операции, или «действия» — такие, как сложение, вычитание, умножение и т.д. Эти операции во многих случаях подчиняются общим законам — правилам, таким, как переместительный закон, сочетательный закон и т.д. Целесообразно отвлечься от конкретной природы объектов, над которыми производятся операции, и сформулировать «хорошие»свойства операций в абстрактной форме.

2. Определение. *Операцией $*$ на множестве M* называется закон, по которому каждым двум элементам x и y множества M ставится в соответствие вполне определенный третий элемент $z \in M$, обозначаемый $z = x*y$ (результат операции). Порядок x и y при этом существен — приведите соответствующий *пример операции*. Совсем абстрактно можно определить операцию $*$ на M как отображение $* : M \times M \longrightarrow M : (x, y) \mapsto x * y$; здесь $M \times M$ — множество всех упорядоченных пар $\{(x, y) | \, x \in M, \, y \in M\}$.

3. Примеры операций: а) «$+$», «$\times$», «$-$» на множестве $\mathbb{R}$ всех действительных чисел;

б) «$\circ$» — операция композиции на множестве всех отображений какого-то фиксированного множества $\mathcal{A}$ в себя, или на выделенном классе отображений (скажем, композиция перемещений плоскости).

4. Примеры не операций: а) деление «:»не является операцией на $\mathbb{R}$, ибо не определено число $x : 0$ (однако деление будет операцией на $\mathbb{R} \setminus \{0\}$);

б) вычитание «$-$»не есть операция на множестве $\mathbb{N}$ натуральных чисел: хотя мы знаем, что $2 - 5 = -3$, но $-3 \notin \mathbb{N}$ (напомним, что вычитание является операцией на более широком множестве $\mathbb{Z}$ всех целых чисел);

в) сложение не есть операция на множестве $2\mathbb{Z}+1$ всех чисел вида $2k+1$, $k \in \mathbb{Z}$ (т.е. на множестве всех нечетных чисел); объясните, почему?

5. Примеры «диких» операций. Можно положить:

а) $x * y = 5xy^{17}$ для $x, y \in \mathbb{R}$;

б) $m * n =$НОК(m, n) (для $m, n \in \mathbb{N}$).

Это будут операции (на $\mathbb{R}$ и $\mathbb{N}$ соответственно). Вообще на любом бесконечном множестве существует бесконечно много операций. Мы далее будем интересоваться только «хорошими» операциями, т.е. операциями, обладающими хорошими свойствами.

6. Операцию на конечном множестве $M = \{a_1, \ldots, a_n\}$ удобно задавать с помощью таблицы (поясните). *Вопрос:* Сколько всего операций существует на множестве из n элементов?

7. Основное определение 1. Множество R с заданными на нем операциями «$+$»и «$\cdot$», условно, называемыми сложением и умножением, называется *кольцом*, если операции «$+$»и «$\cdot$»удовлетворяют так называемым *аксиомам кольца:*

(К$+$) (коммутативность сложения) $\forall x, y \in R \;\; x + y = y + x$;

(А$+$) (ассоциативность сложения) $\forall x, y, z \in R \;\; (x + y) + z = x + (y + z)$;

(Н$+$) (существование нуля, или нейтрального по отношению к операции сложения элемента) $\exists 0 \in R : \; \forall x \in R \;\; x + 0 = x$;

(О$+$) (обратимость сложения, или существование противоположного элемента) $\forall x \in R \; \exists y \in R : \;\; x + y = 0$ (y обозначается «$-x$»);

(К$\cdot$) (коммутативность умножения) $\forall x, y \in R \;\; xy = yx$ (здесь $xy = x \cdot y$);

(А$\cdot$) (ассоциативность умножения) $\forall x, y, z \in R \;\; (xy)z = x(yz)$;

(Д$\cdot, +$) (дистрибутивность умножения по отношению к сложению) $\forall x, y, z \in R \;\; x(y + z) = xy + xz$.

8. Со всеми этими свойствами-аксиомами каждый встречался — например, в арифметике, как с правилами действий (вспомните названия этих свойств). Все они имеют место, скажем, когда $R = \mathbb{Z}$, а «$+$» и «$\cdot$» — обычные операции сложения и умножения. Таким образом, можно кратко сказать, что $(\mathbb{Z}, +, \cdot)$ — кольцо. Приведите еще примеры колец.

9. Аксиомы кольца — это самые нужные при вычислениях свойства операций. Заметим, что из аксиом (Н$+$) и (О$+$) вытекает возможность вычитания в произвольном кольце $(R, +, \cdot)$:

$$x - y = x + (-y).$$

Мы не требуем существования деления, потому что в простейшем важном кольце — в кольце целых чисел $\mathbb{Z}$ — деление осуществимо далеко не всегда.

10. Примеры колец. а) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ с обычными операциями «$+$» и «$\cdot$».

б) Множество четных чисел $2\mathbb{Z}$ с теми же операциями.

в) Множество всех функций $f : \mathbb{R} \longrightarrow \mathbb{R}$ с обычными операциями сложения и умножения функций: $(f_1 + f_2)(x) = f_1(x) + f_2(x)$, $(f_1 f_2)(x) = f_1(x) \cdot f_2(x)$.

Примеры не колец. а) $2\mathbb{Z} + 1$ (нет операции сложения!).

б) $(\mathbb{N}, +, \cdot)$ (не выполнены аксиомы — какие?).

В примерах не колец имеются в виду обычные операции сложения и умножения.

11. Если в кольце $R = (R, +, \cdot)$ выполнена дополнительная аксиома

(Н$\cdot$) (существование единицы, т.е. элемента, нейтрального по отношению к умножению) $\exists\, 1 \in R :\ \ 1 \cdot x = x$, — то говорят, что R — *кольцо с единицей.*

Примеры: $\mathbb{Z}$ — кольцо с единицей, $2\mathbb{Z}$ — кольцо *без единицы.*

12. Полное наименование определенных в т. 7 колец — ассоциативные коммутативные кольца (в общей алгебре рассматривают и другие кольца).

13. Основное наше кольцо — это $\mathbb{Z}$. Наука о строении кольца $\mathbb{Z}$ называется *арифметикой;* ею мы и займемся. Кое-какие другие примеры колец, и также некоторые общие свойства (всех) колец будут чуть дальше.

14. *Первый вопрос.* Какие подмножества $A \subset \mathbb{Z}$ сами по себе являются кольцами — с обычными операциями сложения и умножения? Пример: $A = 2\mathbb{Z}$.

Начнем отвечать на этот вопрос. Конечно, прежде всего сложение и умножение должны быть операциями на A, т.е.

$$\forall x, y \in A \quad x + y \in A \ \text{ и } \ xy \in A.$$

Каким еще требованиям должны удовлетворять кольца $A \subset \mathbb{Z}$?

15. Основное определение 2. Подмножество $A \subset R$ кольца $(R, +, \cdot)$ называется *подкольцом* кольца R, если выполнены так называемые *аксиомы подкольца*:

(З+) (замкнутость по сложению) $\forall x, y \in A \quad x + y \in A$;

(З$-$) (замкнутость по отношению к взятию противоположного) $\forall x \in A \quad -x \in A$;

(З$\cdot$) (замкнутость по умножению) $\forall x, y \in A \quad xy \in A$.

16. Теорема. Если $A \subset R$ — подкольцо кольца $(R, +, \cdot)$, то на A определены операции «+» и «$\cdot$», причем $(A, +, \cdot)$ — кольцо (т.е. для A выполнены аксиомы кольца). Докажите эту теорему самостоятельно.

17. Примеры подколец. а) $\mathbb{Q}$ в $\mathbb{R}$, $\mathbb{Z}$ в $\mathbb{Q}$, $2\mathbb{Z}$ в $\mathbb{Z}$.

б) Множество всех многочленов $\mathbb{R}[x] = \{P_n(x)\}$ в кольце всех функций $f : \mathbb{R} \longrightarrow \mathbb{R}$.

18. *Задача.* Укажите, в каких случаях A — подкольцо кольца всех функций:

а) $A =$ четные функции,

б) $A =$ нечетные функции,

в) $A =$ линейные функции $y = ax + b$,

г) $A =$ периодические функции с данным периодом T,

д) $A =$ периодические функции со всевозможными периодами,

е) $A =$ функции $f : \mathbb{R} \longrightarrow \mathbb{R}$ такие, что 1) $f(0) = 0$, 2) $f(0) = 1$,

ж) $A =$ непрерывные функции,

з) $A =$ разрывные функции,

и) A = дифференцируемые функции.

19. *Задача.* Укажите, в каких случаях A — подкольцо кольца $\mathbb{R}$:
а) $A = \mathbb{Q} + \sqrt{2}\mathbb{Q} = \{a + b\sqrt{2} | \, a, b \in \mathbb{Q}\}$,
б) A = конечные десятичные дроби,
в) A = периодические (возможно, конечные) десятичные дроби,
г) $A = \mathbb{Q} + \sqrt[3]{2}\mathbb{Q} = \{a + b\sqrt[3]{2} | \, a, b \in \mathbb{Q}\}$.

20. Вернемся к вопросу 14. Теперь его можно сформулировать так: найти все подкольца кольца $\mathbb{Z}$. Один пример мы знаем: $A = 2\mathbb{Z}$. Нельзя ли его обобщить?! ... Все ли подкольца в $\mathbb{Z}$ теперь указаны??

21. К последнему вопросу из т. 20 мы еще вернемся. выясните пока, какие из указанных ниже подмножеств $A \subset \mathbb{Z}$ являются подкольцами в $\mathbb{Z}$:
а) $A = 2\mathbb{Z} \cap 3\mathbb{Z}$,
б) $A = 2\mathbb{Z} \cup 3\mathbb{Z}$,
в) $A = 2\mathbb{Z} + 3\mathbb{Z} = \{2x + 3y | \, x, y \in \mathbb{Z}\}$,
г) $A = 9\mathbb{Z} + 12\mathbb{Z}$.
(Всюду $a\mathbb{Z}$ — обозначение для $\{ax | \, x \in \mathbb{Z}\}$.

22. *Вопрос.* В каком случае подкольца $a\mathbb{Z}$ и $b\mathbb{Z}$ кольца $\mathbb{Z}$ вложены одно в другое, т.е. $a\mathbb{Z} \subset b\mathbb{Z}$? (Что в этом случае можно сказать про a и b? Верно ли обратное — если .... , то $a\mathbb{Z} \subset b\mathbb{Z}$.

23. Пусть A и B — подкольца кольца R. Докажите, что тогда их пересечение $C = A \cap B$ является подкольцом в R. Верно ли, что объединение $A \cup B$ подколец A и B тоже будет подкольцом?

24. Опишите все элементы подкольца $a\mathbb{Z} \cap b\mathbb{Z}$ кольца Z.

25. Докажите, что требования (З+) и (З−) в определении подкольца (т. 15) можно заменить одним требованием:
(З±) $\forall x, y \in A \quad x - y \in A$,
(т.е. докажите, что (З±) $\Leftrightarrow$ (З+) и (З−)).

Некоторые общие свойства колец

26. *Единственность нуля.* В рассмотренных примерах в каждом из колец имеется ровно один элемент 0. Выведите из аксиом кольца, что так будет всегда, т.е. в любом кольце только один 0.
(*Указание.* Рассмотрите сумму двух нулей $0_1 + 0_2 = ?$)

27. Заметим, что на самом деле утверждение т. 26 существенно для формулировки аксиомы (О+) — в ней имеется в виду тот единственный элемент 0, о существовании которого говорится в аксиоме (Н+).

Выведите из аксиом кольца единственность противоположного элемента: для любого $x \in R$ элемент $-x$ только один.

(*Указание.* Для двух противоположных элементов $(-x)_1$ и $(-x)_2$ рассмотрите сумму $(-x)_1 + x + (-x)_2 = ?$)

28. В рассмотренных примерах колец для любого $x \in R$ выполнено $x \cdot 0 = 0$. Докажите это свойство умножения на 0 в общем случае (выведите из аксиом кольца).

29. Докажите единственность единицы в кольце с единицей.

30. «Экзотический» пример. а) Пусть R — множество всех подмножеств плоскости. Для подмножеств A, B положим:

$$A + B = A \cup B, \qquad AB = A \cap B.$$

Выясните, какие из аксиом кольца выполнены, какие — нет.

б) Сделайте то же самое для «переставленных» операций:

$$A + B = A \cap B, \qquad AB = A \cup B.$$

§ 2. Делимость и подкольца кольца

«Кончай разговоры, пошли к лошадям.»
(Английская поговорка.)

31. Кольцо $\mathbb{Z}$ обладает одним крупным недостатком — не всегда одно целое число можно разделить на другое (и получить при этом целое число). Отсутствие операции деления в $\mathbb{Z}$ «компенсируется» наличием деления с остатком и понятия делимости.

32. Напомним, что для $a, b \in \mathbb{Z}$ *a делится на b*, $a \vdots b \iff \exists k \in \mathbb{Z} : \ a = bk$.

Далее, хорошо известно, как *разделить* одно целое число, $a \in \mathbb{Z}$, на другое целое число $d \neq 0$ *с остатком* — уголком. В результате получится неполное частное q и остаток r, причем, $0 \leqslant r < |d|$ и $a = qd + r$. Но вдруг при каком-нибудь другом способе деления a на d получится другое частное или другой остаток?! (Например, можно поделить уголком, но в другой — не десятичной — системе счисления!)

33. Теорема (о делении с остатком в кольце $\mathbb{Z}$). $\forall a \in \mathbb{Z}\ \forall d \in \mathbb{N}\ \exists!\, q, r \in \mathbb{Z}$ такие, что

(1) $a = qd + r$,
(2) $0 \leqslant r < d$.

($\exists!$ — сленговое сокращение для слов «существует единственный (-я, -ое)».)

34. Комментарий. *Существование* q и r можно усмотреть безотносительно к системам счисления — например, так: среди числе $0,\ d,\ 2d,\ 3d, \ldots, -d,\ -2d, \ldots$ найдется qd такое, что $qd \leqslant a < (q+1)d$. Если положить $r = a - qd$, то для q и r выполнены условия (1) и (2).

Докажите *единственность:* рассмотрите два представления,

$$a = q_1 d + r_1 = q_2 d + r_2, \quad 0 \leqslant r_1, r_2 < d,$$

и покажите, что $q_1 = q_2$, $r_1 = r_2$.

35. Теорема (о подкольцах Z). Любое подкольцо A кольца $\mathbb{Z}$ есть либо $\{0\}$ (оно состоит только из нуля), либо $a\mathbb{Z}$ — подкольцо чисел, делящихся на какое-то натуральное a : $A = \{0\}$ или $a\mathbb{Z}$, $a \in \mathbb{N}$.

(Как бы доказать эту теорему?)

36. Комментарий к теореме 35. Заметим, что если $A = a\mathbb{Z}$, то

$$A = \{0;\ a,\ 2a,\ 3a,\ \ldots;\ -a,\ -2a, \ldots\},$$

т.е. a — наименьший из положительных элементов подкольца A. Отсюда такая *схема доказательства.*

1) Пусть $A \subset \mathbb{Z}$ — подкольцо. Возьмем число $a = \min(A \cap \mathbb{N})$ (почему $A \cap \mathbb{N} \neq \emptyset$, и верно ли это?).

2) Докажем, что $\forall x \in A\ x \vdots a$. (Распространенный прием доказательства того, что $x \vdots a$ состоит в следующем. Разделим x на a с остатком, а затем докажем, что остаток r равен 0: $r = x - qa = 0$. Докажите это в рассматриваемом случае.) Отсюда $A \subset a\mathbb{Z}$.

3) Наконец, заметим, что, очевидно, $a\mathbb{Z} \subset A$ (поясните).

37. Итак, найдены все подкольца кольца $\mathbb{Z}$ — это подмножества вида $a\mathbb{Z}$, где $a \in \mathbb{N}$, и тривиальное подкольцо $\{0\}$.

Лемма (о вложенных подкольцах в $\mathbb{Z}$). $a\mathbb{Z} \subset c\mathbb{Z} \iff a \vdots c$. (Докажите.)

38. Из леммы 37 следует, что для подкольца $a\mathbb{Z} \subset \mathbb{Z}$ *содержащие его* подкольца $d\mathbb{Z}$ отвечают *делителям* d числа a ($a \vdots d$), а *содержащиеся в нем* (в $a\mathbb{Z}$) подкольца $k\mathbb{Z}$ отвечают *кратным* k числа a ($k \vdots a$). Следовательно, если рассмотреть сразу два подкольца $a\mathbb{Z}$ и $b\mathbb{Z}$, то «самое большое» подкольцо, содержащееся одновременно в $a\mathbb{Z}$ и в $b\mathbb{Z}$, которым, очевидно, будет пересечение $a\mathbb{Z} \cap b\mathbb{Z}$, отвечает НОК a и b.

$$a\mathbb{Z} \cup b\mathbb{Z} = k_0\mathbb{Z}, \quad \text{где} \quad k_0 = \text{НОК}(a, b).$$

С другой стороны, «наименьшее» подкольцо $A_{\min}$, содержащее одновременно $a\mathbb{Z}$ и $b\mathbb{Z}$, должно отвечать НОД(a, b) (обозначается просто (a, b)). Нетрудно понять, что раз $A_{\min} \supset a\mathbb{Z} \cup b\mathbb{Z}$, то $ax \in A_{\min}$, $ay \in A_{\min}$ и $ax + by \in A_{\min}$ при любых целых x и y, т.е. $A_{\min} \supset a\mathbb{Z} + b\mathbb{Z}$. Однако множество $A = a\mathbb{Z} + b\mathbb{Z}$ является подкольцом в $\mathbb{Z}$ (проверьте!), поэтому $A_{\min} = A$. Таким образом,

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}.$$

В частности, получаем, что раз $(a, b) \in a\mathbb{Z} + b\mathbb{Z}$, то НОД$(a, b)$ представим в виде

$$(a, b) = ax_0 + by_0, \qquad \text{где } x_0, y_0 \in \mathbb{Z}.$$

39. Рассуждения т. 38 *не строги,* ибо мы не придали точного смысла словам «самое большое» и «наименьшее» подкольцо. Дадим теперь независимую точную

формулировку этим рассуждениям. Напомним, что для двух чисел $a, b \in \mathbb{Z}$ их наибольшим общим делителем (НОД) называется число

$$(a,b) = \max\{d \in \mathbb{N} \mid a \vdots d,\ b \vdots d\}.$$

(Вопрос: почему множество общих делителей a и b не пусто?!)

40. Теорема (о представлении НОД). Наибольший общий делитель двух чисел $a, b \in \mathbb{Z} \setminus \{0\}$ делится на любой другой общий делитель a и b; более того, НОД(a,b) представляется в виде

$$(a,b) = ax_0 + by_0, \qquad \text{где } x_0, y_0 \in \mathbb{Z}.$$

(Проверьте это для $(a,b) = (2,3),\ (4,7),\ (6,16)$ — подберите соответствующие целые числа x_0 и y_0.)

Доказательство сформулированной теоремы проведем в несколько шагов — тезисы 42 и 42.

41. Рассмотрим множество $A = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$.

Лемма (о сумме подколец). $A = a\mathbb{Z} + b\mathbb{Z}$ — подкольцо кольца $\mathbb{Z}$. (Докажите.)

42. По теореме 35 (о подкольцах $\mathbb{Z}$) из леммы 41 выводим, что

$$a\mathbb{Z} + b\mathbb{Z} = d_0\mathbb{Z}.$$

Утверждения. а) d_0 — общий делитель a и b.

б) $d_0 = ax_0 + by_0$ для некоторых $x_0, y_0 \in \mathbb{Z}$.

в) d_0 делится на любой другой общий делитель a и b.

(Докажите эти утверждения.)

Отсюда следует, что $d_0 = (a,b)$, и теорема 40 доказана (поясните).

43. Теорема 40 имеет много приложений. К ней мы будем обращаться еще не один раз, и начнем с весьма важного утверждения.

44. Основная лемма арифметики. Если $ab \vdots c$, причем $(a,c) = 1$, то $b \vdots c$. (Докажите; воспользуйтесь теоремой 40.)

45. Теперь мы перечислим несколько следствий из О.Л.А. (т. 44).

Лемма. Если $(p,q) = 1$, то при любых $k, l \in \mathbb{N}$ выполнено и $(p^k, q^l) = 1$. (Докажите; сначала рассмотрите случай $l = 1$.)

46. Теорема Пифагора. Если число $a \in \mathbb{N}$ не является n-ой степенью никакого натурального числа, то число $\sqrt[n]{a}$ *иррационально* (т.е. не представимо в виде $\frac{p}{q}$, где $p \in \mathbb{Z}$, $q \in \mathbb{N}$; в этом случае коротко пишут $\sqrt[n]{a} \notin \mathbb{Q}$.)

(Докажите. *Указание:* используйте лемму 45 в рассуждении от противного.)

47. Теорему 46 можно переформулировать так:

если уравнение $x^n = a$, $a \in \mathbb{N}$, не имеет целых решений, то оно не имеет и рациональных решений. Обобщение:

Теорема (о целых корнях уравнений над $\mathbb{Z}$).

Если уравнение

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

с целыми коэффициентами имеет рациональный корень x_0 ($x_0 = \frac{p}{q} \in \mathbb{Q}$), то этот корень обязательно целый.

(Докажите.)

48. Теорема (о рациональных корнях уравнений над $\mathbb{Z}$).
Если несократимая дробь $\frac{p}{q} = x_0$ является корнем уравнения

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

с целыми коэффициентами, то p — делитель a_n.

(Докажите. Заметим, что теорема 47 — частный случай теоремы 48. Последняя применяется при отыскании рациональных корней уравнения с целыми коэффициентами.)

49. Следствие. $\sin 10^\circ \notin \mathbb{Q}$.

(Докажите. *Указание:* $\sin 30^\circ = \frac{1}{2} = \sin 3 \cdot 10^\circ$; воспользовавшись формулой синуса 3α: $\sin 3\alpha = 3\sin\alpha - 4\sin^3\alpha$, выпишите уравнение, которому удовлетворяет $x_0 = \sin 10^\circ$, а затем примените теорему 48.)

Замечание. Можно доказать, что если $A \in \mathbb{Q}$ и $0 < A < 90$, то $\sin A^\circ \notin \mathbb{Q}$, $\cos A^\circ \notin \mathbb{Q}$, за двумя исключениями: $\sin 30^\circ = \cos 60^\circ = \frac{1}{2}$.

50. Докажите, что если $m, n \in \mathbb{N} \setminus \{1\}$, $(m, n) = 1$, то $\log_m n \notin \mathbb{Q}$.

(*Указание:* воспользуйтесь леммой 45.)

Через некоторое время мы подробнее займемся вопросом о том, какие бывают иррациональные числа.

Замечание 1. В случае, когда $(a, b) = 1$, в арифметики принято говорить, что числа a и b *взаимно простые*.

Замечание 2. Когда мы говорим о делителях целого числа a, то имеем в виду только натуральные делители (то же относится к общим делителям).

§ 3. Простые числа

«... Инженер подозревает, что все нечетные числа простые. Во всяком случае, 1 можно рассматривать как простое число, — доказывает он. Затем идут 3, 5 и 7, все, несомненно простые. Затем идет 9 — досадный случай. 9, по-видимому, не является простым числом. Но 11 и 13, конечно, простые. Возвратимся к 9, — говорит он, — я заключаю, что 9 должно быть ошибкой эксперимента... »

(Дьердь Пойа)

51. Напомним, что число $p \in \mathbb{N}$ называется *простым*, если $p \geqslant 2$ и не имеет делителей, кроме 1 и p:

$$p \vdots d,\ d \in \mathbb{N} \implies d = 1,\ \vee\ d = p.$$

В противном случае число $p \neq 1$ называется *составным*.

52. Простейший способ составления таблицы всех простых числе — *решето Эратосфена:* выписав подряд все натуральные числа,

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ \ldots\ ,$$

мы зачеркиваем 1, затем все числа, кратные 2, кроме 2; затем числа, кратные 3, кроме 3, и так далее, переходя каждый раз к следующему невычеркнутому числу. В результате незачеркнутыми останутся только простые числа.

Вопрос. Вдруг, начиная с некоторого места, все числа окажутся зачеркнутыми? По-другому, конечно или бесконечно множество всех простых чисел?

53. Теорема Евклида. Множество $\mathbb{P}$ всех простых чисел бесконечно.

Доказательство 1. (Евклид.) Предположим противное, т.е. что множество $\mathbb{P}$ конечно, $\mathbb{P} = \{p_1, \ldots, p_k\}$. Придумайте теперь число, которое не делится ни на одно из чисел $p_1, \ldots, p_k$ (например, дает при делении на p_i остаток 1!). После этого останется заметить, что:

любое число либо само простое, либо имеет простой делитель. (Докажите последнее замечание — например, индукцией.)

54. *Доказательство 2.*

Лемма. Для любого $n \in \mathbb{N}$, $n \geqslant 3$, существует простое число p такое, что $n < p < n!$.

(Докажите. *Указание:* на что не может делиться число $n! + 1$?!)

Очевидно, теорема 53 следует из леммы 54 (поясните).

55. *Доказательство 3.*

Определение. Числа вида $F_n = 2^{2^n} + 1$, где $n \geqslant 0$, называются *числами Ферма*.

Лемма. Если $m \neq n$, то $(F_m, F_n) = 1$.

(Докажите. *Указание:* разложите на множители число $F_m - 2 = 2^{2^m} - 1$.)

Теперь выведите из этой леммы теорему Евклида (т. 53).

Замечание. Как возникают в математике числа Ферма, мы увидим потом.

56. Итак, простых чисел бесконечно много. Отметим, однако, что нет хороших формул, задающих простые числа.

Пример. Формула $p = x^2 - x + 41$ дает простые числа при $x = 0,\ 1,\ \ldots,\ 40$, но, конечно, при $x = 41$ число p составное.

Теорема Эйлера. Любой многочлен $y = p_n(x)$ с целыми коэффициентами при целых x принимает бесконечно много различных составных значений.

(Докажите.)

По поводу формул, задающих простые числа, см. статью Ю. Матиясевича в «Кванте», 1975 год, № 5.

57. Конечно, составных чисел бесконечно много. Более того, для любого $n \in \mathbb{N}$ найдется n штук идущих подряд составных чисел (покажите).

Заметим, что все четные числа, кроме 2, являются составными, и поэтому простые числа, кроме 2 и 3, подряд идти не могут — самое меньшее, они идут через одно: $2k-1$ и $2k+1$. Подобные пары простых чисел называются *близнецами*. Примеры близнецов: 3 и 5, 5 и 7, 11 и 13, 17 и 19. И посейчас, в 2001 году(!) неизвестно, конечно или бесконечно число близнецов!

58. О распределении простых чисел в натуральном ряду вообще известно не так уж много. Приведем несколько утверждений на сей счет.

а) **Постулат Бертрана.** (или **теорема Чебышева**). Для любого $n \in \mathbb{N}$ существует простое p такое, что $n \leqslant p \leqslant 2n$.

б) **Теорема Римана.** Если π_n — число простых числе среди натуральных чисел от 1 до n, то $\pi_n \approx \ln n$. Точнее, $\lim\limits_{n\to\infty} \frac{\pi_n}{\ln n} = 1$, где

$$\ln M = \log_e M, \qquad e = \lim_{k\to\infty} \left(1 + \frac{1}{k}\right)^k = 2,7818281\ldots .$$

в) **Формула Серпинского.** Если p_n — n-е по счету простое число, то $p_n \approx n \ln n$ (в том смысле, что $\lim\limits_{k\to\infty} \frac{p_n}{n \ln n} = 1$.)

г) **Теорема Дирихле.** Существует простое число, десятичная запись которого кончается на любой наперед заданный набор цифр, лишь бы последняя цифра не была четной или пятеркой. (Более общим образом, если $(a, b) = 1$, то среди членов арифметической прогрессии $a_n = a + bn$, $n \in \mathbb{N}$, бесконечно много простых чисел.)

59. Лемма. Любое число $n \in \mathbb{N}$, $n \geqslant 2$, разлагается на простые сомножители. Дайте точное доказательство этого очевидного утверждения — индукцией по n.

60. Основная теорема арифметики. Любое число $n \in \mathbb{N}$, $n \geqslant 2$, имеет *единственное* разложение на простые множители: если

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

два таких разложения, то $k = l$, а простые числа $q_1, \ldots, q_l$ можно перенумеровать так, что $p_1 = q_1$, $p_2 = q_2$, и т.д.

61. Теорема 60 представляется очевидной: как же может быть иначе?! Так долго думали и математики, а первое доказательство этой теоремы было дано лишь в XIX веке — Гауссом. Мы, прежде чем доказывать теорему 60, покажем, почему единственность разложения чисел на простые множители отнюдь *не* очевидна.

62. Рассмотрим кольцо $R = 2\mathbb{Z}$ четных чисел. В нем можно определить понятие делимости: для $a, b \in R$ $a \vdots b$, если $\exists\, k \in R$ такое, что $a = bk$. (Например, $8 \vdots 4$, но 12 не делится на 4 в кольце R!) Аналогично определяются и четно-простые числа — такими будут 2, 6, 10, 14, 18, 22, ... , $2(2k+1)$ при произвольном натуральном k. Любое четное число разлагается на четно-простые множители; например, $4 = 2 \cdot 2$, $6 = 6$, $8 = 2 \cdot 2 \cdot 2$, $12 = 2 \cdot 6$. Продолжите этот список. Найдите число $n \in R$, имеющее два *разных* разложения на четно-простые множители! (*Указание:* дойдите до 40.)

63. Наше доказательство теоремы 60 опирается на следующее очевидное утверждение:

Лемма. Для простых p и q либо $p = q$, либо $(p, q) = 1$.

(Дайте доказательство.)

64. Докажите теперь теорему 60 индукцией по n, используя лемму 63 и Основную лемму арифметики (т. 44).

Другое доказательство этой теоремы, обходящее Основную лемму арифметики, см. в книге Куранта и Роббинса «Что такое математика», стр. 47-48.

65. В практических вопросах вместо Основной теоремы арифметики чаще используется Основная лемма. При разложении конкретных чисел на простые множители полезно следующее

Утверждение. Наибольший простой делитель составного числа $n \in \mathbb{N}$ не превосходит $\sqrt{n}$. (Докажите.)

Таким образом, чтобы установить, является ли число n простым или нет, достаточно перебрать все простые числа от 1 до $\sqrt{n}$ и выяснить, делят ли они число n. (При $n \leqslant 10\,000$ таких простых чисел не более 50.)

66. Примеры. а) Разложите на простые множители числа

$$111,\ 1111,\ 11111,\ 111111,\ 1111111.$$

б) Докажите, что следующие числа являются составными:

$$\underbrace{222\ldots21}_{\text{1969 двоек}}, \qquad 2^{\overbrace{55\ldots5}^{\text{1000 раз}}}+1, \qquad 2^{3^{1969}}+1, \qquad 2^{3^{1969}}-1.$$

67. Лемма. Если p — простое число, то при $1 \leqslant k \leqslant p-1$ число C_p^k делится на p. (Докажите.)

68. Следствие. При простом p для любых $a, b \in \mathbb{Z}$ число $(a+b)^p - a^p - b^p$ делится на p. (Докажите.)

69. Малая теорема Ферма. Если p — простое, то $\forall n \in \mathbb{Z}\ (n^p - n) \vdots p$.

Усмотрите справедливость этого факта для $p = 2$, $p = 3$. А как для $p = 5$?!

Докажите Малую теорему Ферма для произвольного простого p индукцией по n (конечно, можно рассматривать только $n \in \mathbb{N}$!), используя следствие 68.

Замечание. Общих утверждений о делимости, таких как тт. 68, 69, не так уж много в арифметике. Мы еще вернемся к Малой теореме Ферма и докажем некоторое ее обобщение.

70. Иногда разложение числа n на простые множители полезно записывать в виде

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s},$$

где $\alpha_i \geqslant 1$, а $p_1, \ldots, p_s$ — *различные* простые числа.

Задача. Пусть $\tau(n)$ — число всех делителей числа n (включая 1 и n). Как по разложению n на простые сомножители найти $\tau(n)$? (Начните с числа $n = p^\alpha$ и $n = p^\alpha q^\beta$.)

Глава II. Кольца и поля вычетов

§ 4. Уравнения в целых числах.

«Диофантовых уравнений анализ немало служит изощрению разума начинающих и большое проворство в исчислении приносит.»

(Леонард Эйлер)

71. Уравнения в целых числах (диофантовы уравнения) возникают в некоторых задачах математики, экономики и физики (целочисленные задачи связаны с квантовой физикой!).

Пример. Решить задачу об отыскании рациональных корней какого-то уравнения $f(x) = 0$ — все равно, что найти все целые решения (m, n) уравнения $f\left(\frac{m}{n}\right) = 0$.

72. Мы уже исследовали задачу об отыскании рациональных корней уравнения

$$P_k(x) = a_k x^k + \cdots + a_1 x + a_0 = 0, \quad \text{где все } a_i \in \mathbb{Z}.$$

Подставляя $x = \frac{m}{n}$ и умножая обе части на n^k, получим соответствующее диофантово уравнение, *однородное* по m и n:

$$a_k m^k + a_{k-1} m^{k-1} n + \cdots + a_1 m n^{k-1} + a_0 n^k = 0.$$

Очевидно, верно и обратное: однородные по m и n диофантовы уравнения сводятся к уравнениям вида $P_k\left(\frac{m}{n}\right) = 0$.

Чтобы решить последнее уравнение, достаточно найти все взаимно-простые решения, т.е. пары (m_0, n_0), для которых дробь $\frac{m_0}{n_0}$ несократима. Их можно найти перебором, исходя из теоремы 48 ($a_k \vdots n_0$, $a_0 \vdots m_0$); любое другое решение имеет вид (dm_0, dn_0), где $d \in \mathbb{Z}$ (поясните).

73. Займемся неоднородными уравнениями. Диофантовы уравнения с одним неизвестным произвольной степени,

$$P_k(n) = a_k n^k + \cdots + a_1 n + a_0 = 0,\ n \in \mathbb{Z},$$

опять-таки, решаются перебором, с помощью теоремы 47 ($a_k = 1$), или 48. Следующий случай — уравнения с двумя неизвестными, m и n.

74. Простейшее из таких уравнений — линейное:

$$am + bn = c, \quad \text{где } a, b, c \in \mathbb{Z}. \tag{$*$}$$

Лемма. Если (m_1, n_1) и (m_0, n_0) — решения уравнения $(*)$, то $(m, n) = (m_1 - m_0, n_1 - n_0)$ — решение соответствующего однородного уравнения

$$am + bn = 0. \tag{$**$}$$

(Докажите.)

75. Однородное уравнение $(**)$ мы умеем решать: $(**) \longrightarrow a\frac{m}{n} + b = 0$. И если $\frac{m_1}{n_1} = -\frac{b}{a}$ — несократимое решение последнего уравнения, то общее решение $(**)$ есть $(m, n) = (dm_1, dn_1)$, где $d \in \mathbb{Z}$.

76. Из леммы 74 следует, что общее решение неоднородного уравнения $(*)$ получается прибавлением к произвольному его частному решению (m_0, n_0) общего решения однородного уравнения (т. 75) (dm_1, dn_1):

$$(m, n) = (m_0, n_0) + (dm_1, dn_1) = (m_0 + dm_1, n_0 + dn_1),\ d \in \mathbb{Z}.$$

Примеры. Решите уравнения:

а) $2m + 3n = 1$, в) $4m + 7n = 1$, д) $4m + 6n = 3$.
б) $2m + 3n = 2$, г) $4m + 7n = 2$,

77. Итак, неоднородные линейные уравнения $am + bn = c$ над $\mathbb{Z}$ можно решать по следующей схеме.

(а) Находим (выписываем) общее решение однородного уравнения $am + bn = 0$.

(б) Отыскиваем частное решение (m_0, n_0) неоднородного уравнения.

(в) Выписываем общее решение неоднородного уравнения $(m_0 + dm_1, n_0 + dn_1)$.

(Заметим, что аналогично решаются и многие другие уравнения математики, например, неоднородные линейные дифференциальные уравнения.)

Возникают естественные вопросы:

А. Всегда ли неоднородное уравнение имеет хотя бы одно решение?

Б. Как отыскать частное решение неоднородного уравнения?

78. Теорема. А. Если НОД$(a,b) = d_0$ и c не делится на d_0, то уравнение $am + bn = c$ не имеет решений (в целых числах)!

Б. В противном случае обе части уравнения $am + bn = c$ можно сократить на d_0 — получится уравнение:

$$a_0m + b_0n = c_0, \qquad \text{где } (a_0, b_0) = 1.$$

Последнее уравнение всегда имеет решение. (Докажите.)

79. Теорема 78.Б вытекает из теоремы о представлении НОД (т. 40):

$$(a_0, b_0) = 1 = a_0m_0 + b_0n_0 \;\Leftrightarrow\; c_0 = a_0(c_0m_0) + b_0(c_0n_0).$$

Однако наше доказательство теоремы 40 не дает явного способа (алгоритма) отыскания чисел m_0 и n_0. При малых a_0 и b_0 часто решение (m_0, n_0) очевидно, но как быть при больших a_0 и b_0?!

Вернемся к НОД и укажем хороший способ его нахождения и, заодно, представления.

80. Итак, нужно найти $d_0 = (a,b)$, $a, b \in \mathbb{N}$. Изобразим числа a и b отрезками длин a и b; тогда d_0 — наибольший отрезок целой длины, целое число раз укладывающийся на отрезки a и b. Чтобы практически найти d_0, поступают так: меньший из отрезков a, b откладывают на бóльшем, пока это возможно, затем оставшийся от бóльшего отрезок r_0 откладывают на меньшем, получившийся остаток r_1 откладывают на r_0, и т.д. В итоге какой-то остаток r_k целое число раз уложится на предыдущем r_{k-1}. Ясно, это и есть d_0.

81. Формализуем описанную процедуру. *Алгоритм Евклида.* Запишем цепочку делений с остатком:

$$\begin{aligned}
b &= q_0a + r_0, && 0 < r_0 < a,\\
a &= q_1r_0 + r_1, && 0 < r_1 < r_0,\\
r_0 &= q_2r_1 + r_2, && 0 < r_2 < r_1,\\
&\dots && \dots\\
r_{i-1} &= q_{i+1}r_i + r_{i+1}, && 0 < r_{i+1} < r_i,\\
&\dots && \dots\\
r_{k-2} &= q_kr_{k-1} + r_k, && 0 < r_k < r_{k-1},\\
r_{k-1} &= q_{k+1}r_k, && r_{k+1} = 0.
\end{aligned}$$

Эта цепочка обязательно оборвется — на некотором шаге остаток r_{k+1} будет равен 0, ибо все $r_i \geqslant 0$ и $a > r_0 > r_1 > r_2 \cdots$.

Теорема Евклида. $r_k = d_0 = (a,b)$

Ее доказательство будет состоять из двух шагов (тт. 82, 83).

82. Лемма. a и b делятся на r_k.

(Докажите: покажите, что r_i делится на r_k при $i = k-1,\ k-2, \dots$.)

83. Лемма. r_k представляется в виде $r_k = am_0 + bn_0$, где m_0 и n_0 — целые.

(Докажите: покажите, что каждое из r_i представляется в таком виде при $i = 0, 1, 2, \ldots, k$.)

Следствие. Если $a, b \vdots d$, то $r_k \vdots d$ (поясните).

С учетом леммы 82 отсюда получаем, что $r_k = (a, b)$, и теорема 81 доказана.

84. При доказательство леммы 83 получен способ (алгоритм) отыскания целых m_0 и n_0 таких, что $d_0 = am_0 + bn_0$. Он дает возможность алгоритмически отыскивать частное решение уравнения вида $am + bn = c$.

Примеры. Проведите алгоритм Евклида для отыскания НОД (14,100) и (15,100) Укажите, при каких $c \in \mathbb{Z}$ уравнения

а) $14m + 100n = c$,

б) $15m + 100n = c$

имеют решения над $\mathbb{Z}$ и выпишите общий вид решений.

85. *Геометрический алгоритм Евклида* (т. 80) можно применить к любым двум отрезкам a и b (не обязательно целой длины). Если этот алгоритм на каком-то шаге обрывается, то последний полученный отрезок называется *общей мерой* отрезков a и b, а сами эти отрезки называются *соизмеримыми*.

Теорема. Отрезки длин a и b соизмеримы тогда и только тогда, когда отношение $\frac{b}{a} \in \mathbb{Q}$.

(Докажите.)

Таким образом, геометрический алгоритм Евклида может оказаться бесконечным — никогда не заканчивающимся.

86. Строчки алгоритма Евклида (т.81) можно переписать так:

$$\frac{b}{a} = q_0 + \frac{r_0}{a} = q_0 + \frac{1}{a/r_0}, \qquad 0 < \frac{r_0}{a} < 1,\ \frac{a}{r_0} > 1$$

$$\frac{a}{r_0} = q_1 + \frac{r_1}{r_0} = q_1 + \frac{1}{r_0/r_1}, \qquad 0 < \frac{r_1}{r_0} < 1,\ \frac{r_0}{r_1} > 1,$$

$$\frac{r_0}{r_1} = q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{r_1/r_2}, \qquad 0 < \frac{r_2}{r_1} < 1,\ \frac{r_1}{r_2} > 1,$$

и т.д.

Отсюда получается представление числа $\frac{b}{a}$ в виде так называемой *цепной дроби*:

$$\frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots}} \qquad \text{где все } q_i \in \mathbb{N}.$$

В таком виде можно записать любое число $\alpha \in \mathbb{R}$, $\alpha > 0$: $\alpha = \frac{\alpha}{1}$. Цепную дробь числа α кратко обозначают $[\alpha] = [q_0;\, q_1, q_2, q_3, \ldots]$.

Теорема. Цепная дробь числа $\alpha \in \mathbb{R}$ конечна $\Leftrightarrow$ $\alpha \in \mathbb{Q}$.

(Поясните.)

87. Примеры. Разложите в цепную дробь числа

а) $\alpha = \sqrt{2}$,

б) $\alpha = \sqrt{3}$,

в) $\pi = 3,14\ldots$ (напишите первые члены дроби).

88. Пример. Найдите число α, разложение которого в цепную дробь имеет вид:

$$[\alpha] = [1;\, 1, 1, 1, \ldots] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}}$$

(Здесь будет логическая тонкость.)

Несколько позже мы еще раз упомянем о цепных дробях. С ними связаны многие замечательные и удивительные факты и конструкции. Заметим, что в 1968 году цепные дроби были обнаружены (и переоткрыты!) физиками при решении задач космологии (общей теории относительности)!!

89. *Геометрическая интерпретация уравнения* $am + bn = c$. Точки (m, n) с целыми координатами образуют на координатной плоскости так называемую целочисленную решетку. Уравнение $ax + by = 0$ при $(a, b) \neq (0, 0)$ задает на плоскости прямую. Решить это уравнение в целых числах — значит найти все целочисленные точки на соответствующей прямой. Вспоминая схему 78 и схему 77, получаем:

(а) при целых a, b, c на «целочисленной» прямой $ax + by = c$ может не лежать ни одной целочисленной точки;

(б) но если на этой прямой $ax + by = c$ $(a, b, c \in \mathbb{Z})$ лежит хотя бы одна целочисленная точка, то на ней лежит бесконечно много таких точек, причем они идут через одинаковые промежутки вдоль этой прямой.

90. Аналогичным образом (тт. 74-76) исследуются линейные уравнения с тремя неизвестными, $ax+by+cz = d$, и с большим числом неизвестных (прикиньте, как?).

91. Диофантовы уравнения решают с древнейших времен, но до сих пор диофантов анализ — одна из самых сложных и малоисследованных ветвей математики, в которой почти нет общих теорем и методов. Упомянем, что, кроме разобранных нами однородных и линейных уравнений, известны еще общие схемы решения квадратных уравнений, решение же уравнений степени 3 и выше остаются искусством.

92. Пример. Уравнение Пифагора $x^2 + y^2 = z^2$, $x, y, z \in \mathbb{Z}$.

Его решения (x, y, z) соответствуют прямоугольным треугольникам с длинами сторон $|x|$, $|y|$, $|z|$ (за исключением тривиальных решений: $(a, 0, a)$ и $(0, a, a)$) — так называемым пифагоровым треугольникам. Например, египетский треугольник дает решение $(3, 4, 5)$.

Вопрос. Сколько существует различных (не подобных друг другу) пифагоровых треугольников?

Ответ. Бесконечно много. Покажем, почему.

93. Уравнение Пифагора однородно, и его удобно записать в виде:

$$u^2 + v^2 = 1, \qquad u = \frac{x}{z},\ v = \frac{y}{z}.$$

Спрашивается, таким образом, сколько точек (u, v) с рациональными координатами лежит на единичной окружности $u^2 + v^2 = 1$?

94. Можно считать, что $(u, v) = (\cos\alpha, \sin\alpha)$. По известным формулам

$$\cos\alpha = \frac{1 - \operatorname{tg}^2\frac{\alpha}{2}}{1 + \operatorname{tg}^2\frac{\alpha}{2}}, \qquad \sin\alpha = \frac{2\operatorname{tg}\frac{\alpha}{2}}{1 + \operatorname{tg}^2\frac{\alpha}{2}},$$

поэтому для рациональности $\cos\alpha$ и $\sin\alpha$ достаточно, чтобы $\operatorname{tg}\frac{\alpha}{2} \in \mathbb{Q}$. В действительности это и необходимо, так как

$$\operatorname{tg}\frac{\alpha}{2} = \frac{\sin\alpha}{1 + \cos\alpha}.$$

(поясните).

Итак, общее решение уравнения $u^2 + v^2 = 1$ в рациональных числах имеет вид

$$(u, v) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right), \quad t \in \mathbb{Q}.$$

Взяв $t = \frac{m}{n}$, напишите формулы для общего решения исходного уравнения $x^2 + y^2 = z^2$.

95. Естественное обобщение уравнения Пифагора — уравнение $x^n + y^n = z^n$.

Большая (Великая) теорема Ферма. Для $n \in \mathbb{N}$, $n \geqslant 3$ уравнение

$$x^n + y^n = z^n, \qquad x, y, z \in \mathbb{Z},$$

не имеет нетривиальных решений (т.е. решений, отличных от $(a, 0, a)$, $(0, a, a)$.

Доказательство этой теоремы, сформулированной более 300 лет назад Пьером Ферма (на полях книги Диофанта «Арифметика»), было найдено только в 1995 году (американским математиком Эндрю Уайлсом в сотрудничестве с англичанином Робертом Тейлором).

Дополнительные задачи к уравнениям в целых числах

1. Решить в целых числах уравнение $x^3 + (x+1)^3 + (x+2)^3 = (x+3)^3$.

2. Доказать, что для любых натуральных m и n существуют целые a, b, c такие, что уравнение $ax + by = c$ имеет единственное решение в натуральных числах: $(x, y) = (m, n)$.

2 а. Верно ли аналогичное утверждение для двух пар: (m_1, n_1), (m_2, n_2)?

3. Доказать, что $\forall N \in \mathbb{N}$ существуют целые a, b, c такие, что уравнение $ax + by = c$ имеет в точности N решений в натуральных числах.

4. Решить в целых числах уравнение $2x^3 + xy - 7 = 0$.

4 а. Доказать, что это уравнение имеет бесконечно много решений в рациональных числах.

§ 5. Кольца вычетов $\mathbb{Z}_m$

«В мир согласный
Вечно-ясный,
Чет и нечет нас влечет.»
(К. Д. Бальмонт)

96. Общие задачи на делимость, вида

$$\text{«при каких } x \in \mathbb{Z} \;\; f(x) \vdots m?\text{»}$$

($f(x)$, или $f(x,y)$ — какое-то выражение), встречаются в математике довольно часто. Например, переписав линейное уравнение $mx + ny = k$ в виде $k - ny = mx$, мы сводим его к задаче на делимость:

$$\text{«при каких } y \in \mathbb{Z} \;\; (k - ny) \vdots m?\text{»}$$

(зная y, легко найти и x).

Очевидно обратное: условие делимости «$f(x) \vdots m$» — это уравнение в целых числах $f(x) = my$.

97. В таких задачах («$f(x) \vdots m$») чаще всего не существен конкретный вид целого числа x, а важно, какой остаток имеет x при делении на m.

Пример. Выясним при каких $x \in \mathbb{Z}$ $f(x) = x^2 + 2$ делится на 3.

Число x может иметь при делении на 3 остатки $\overline{x} = 0, 1, 2$. Соответственно этому, $x^2 + 2$ имеет остатки такие же, как $0^2 + 2$, т.е. 2; $1^2 + 2 = 3$, т.е. 0; $2^2 + 2 = 6$, т.е. 0. Нас интересует, когда остаток от деления $x^2 + 2$ на 3 равен 0, и мы получаем *ответ:* когда $\overline{x} = 1$ или 2, т.е. $x = 3k + 1$ или $3k + 2$. Доказано утверждение: если x не делится на 3, то $x^2 + 2$ делится на 3.

98. Зафиксируем $m \in \mathbb{N}$ и будем обозначать через $\overline{a}$ остаток от деления a на m (возможных значений $\overline{a}$, т.е. возможных остатков, всего m штук — от 0 до $m - 1$).

Лемма. Для любых x, x_0, y, y_0 если $\overline{x} = \overline{x_0}$, $\overline{y} = \overline{y_0}$, то $\overline{x + y} = \overline{x_0 + y_0}$, $\overline{xy} = \overline{x_0 y_0}$ (и $\overline{nx} = \overline{nx_0}$, $\overline{x^n} = \overline{x_0^n}$).

(Иными словами, если мы интересуемся остатками при делении на m, то вместо рассматриваемых чисел можно складывать и умножать их остатки или любые числа с такими же остатками. Докажите.)

Замечание. Обычно вместо $\overline{a} = \overline{b}$ пишут $a \equiv b \mod m$ (т.е. $(a - b) \vdots m$).

99. Леммы 98 достаточно для решения многих задач на делимость и остатки.

Пример. Найдем остаток от деления числа $A = 2^{1000}$ на 9. Имеем:

$$2^{1000} = 2^{3 \cdot 333 + 1} = 2 \cdot 8^{333} \;\Rightarrow\; \overline{2^{1000}} = \overline{2 \cdot 8^{333}} = \overline{2 \cdot (-1)^{333}} = \overline{-2} = 7.$$

Задачи. Найти остатки от деления чисел
$A = 13^{16} - 2^{25} \cdot 5^{15}$ на 3, на 4, на 5, на 6;
$B = 2^{60} + 6^{50}$ на 15, на 17.

100. Итак, при рассмотрении вопросов о делимости на фиксированное число m числа с одинаковыми остатками (при делении на m) можно считать как бы одинаковыми. Придадим этому утверждению точную (и весьма красивую) форму.

101. Определение. *Вычетами по модулю* $m \in \mathbb{N}$ называется m классов (множеств) чисел, имеющих при делении на m одинаковые остатки:

$$\begin{aligned}
&\widetilde{0} = \{0 + mk | \, k \in \mathbb{Z}\} = m\mathbb{Z},\\
&\widetilde{1} = \{1 + mk | \, k \in \mathbb{Z}\} = 1 + m\mathbb{Z},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\widetilde{m-1} = \{(m-1) + mk | \, k \in \mathbb{Z}\} = (m-1) + m\mathbb{Z}.
\end{aligned}$$

Через $\widetilde{r}$ обозначено множество $r + m\mathbb{Z}$ всех чисел вида $r + mk$, дающих при делении на m остаток r. Удобно для произвольного $x \in \mathbb{Z}$ через $\widetilde{x}$ обозначить тот вычет (класс чисел), которому принадлежит x. Рассматривая вычеты, мы как бы «склеиваем» в единый объект (вычет) все числа с одинаковыми остатками.

Пример. Пусть $m = 5$. Что такое $\widetilde{6}$, $\widetilde{10}$, $\widetilde{17}$, $\widetilde{-1}$, $\widetilde{-22}$?

Замечание. Очевидно, $\widetilde{x} = \widetilde{y} \iff \overline{x} = \overline{y}$.

102. Множество всех вычетов по модулю m обозначается через $\mathbb{Z}_m$

$$\mathbb{Z}_m = \{\widetilde{0}, \widetilde{1}, \widetilde{2}, \ldots, \widetilde{m-1}\}.$$

Определим на этом множестве операции сложения и умножения формулами

$$\widetilde{x} + \widetilde{y} = \widetilde{x+y},$$

$$\widetilde{x} \cdot \widetilde{y} = \widetilde{xy}.$$

Лемма. Определение операций $+$ и $\cdot$ на множестве $\mathbb{Z}_m$ *корректно*, т.е. если $\widetilde{x} = \widetilde{x}_1$ и $\widetilde{y} = \widetilde{y}_1$ — две разных записи одних и тех же вычетов, то $\widetilde{x} + \widetilde{y} = \widetilde{x}_1 + \widetilde{y}_1$ и $\widetilde{x}\widetilde{y} = \widetilde{x}_1\widetilde{y}_1$. (Поясните, почему.)

103. Теорема. $(\mathbb{Z}_m, +, \cdot)$ — кольцо с единицей.

(Докажите: проверьте аксиомы кольца. Отметим, что в этом кольце $0 = \widetilde{0}$, $1 = \widetilde{1}$, $-\widetilde{x} = \widetilde{-x}$.)

104. Итак, для любого $m \in \mathbb{N}$ мы определили конечное кольцо, состоящее из m элементов — *кольцо вычетов* $\mathbb{Z}_m$ *по модулю* m. Тот факт, что вычеты по данному модулю образуют кольцо, на практике означает, что с вычетами при сложении и умножении можно обращаться как с целыми числами (выполнены те же самые правила — аксиомы кольца).

105. Пример. Решим в целых числах уравнение $6x + 7y = 13$. Перейдем в кольцо вычетов $\mathbb{Z}_3$, там получим уравнение

$$\widetilde{7} \cdot \widetilde{y} = \widetilde{13} \;\Leftrightarrow\; \widetilde{1} \cdot \widetilde{y} = \widetilde{1} \;\Leftrightarrow\; \widetilde{y} = \widetilde{1} \;\Leftrightarrow\; y = 1 + 3k,\ k \in \mathbb{Z}.$$

Подставив y в исходное уравнение, находим x:

$$3x = 13 - 7y = 13 - 7(1 + 3k) = 6 - 7 \cdot 3k \;\Rightarrow\; x = 2 - 7k.$$

Ответ: $(x, y) = (2 - 7k, 1 + 3k)$, $k \in \mathbb{Z}$.

106. Примеры. Решите в целых числах уравнения (с помощью вычетов):

а) $4x + 7y = 13$,

б) $5x + 7y = 13$.

Общая схема решения линейного уравнения $mx + ny = k$.

В кольце $\mathbb{Z}_m$ имеем: $\widetilde{n}\widetilde{y} = \widetilde{k}$. Решаем это уравнение в $\mathbb{Z}_m$ (перебором), находим $\widetilde{y}$ и y. Подставляя y в исходное уравнение, находим соответствующие значения x.

107. Пример. Найти все целые n такие, что $f(n) = 5n^2 + 10n + 7$ делится

а) на 3, б) на 4.

(Задачи такого вида сводятся к квадратным уравнениям в кольцах вычетов, которые также решаются перебором. Потом мы поговорим чуть подробнее о квадратных уравнениях над кольцами вычетов.)

108. Самое важное из хороших свойств колец Z_m — их конечность; это дает возможность любое уравнение над $\mathbb{Z}_m$ решать *перебором*. Однако кольца $\mathbb{Z}_m$ по сравнению с $\mathbb{Z}$ обладают многими «плохими» и довольно досадными свойствами.

Список плохих свойств $\mathbb{Z}_m$. Пусть, например, $m = 10$.

а) Нет однозначности деления с остатком: $\widetilde{7} = \widetilde{1} \cdot \widetilde{5} + \widetilde{2} = \widetilde{3} \cdot \widetilde{5} + \widetilde{2}$.

б) Нет хорошего отношения неравенства: скажем, если считать, что $\widetilde{0} < \widetilde{1} < \widetilde{2} < \cdots < \widetilde{9}$, то $\widetilde{9} > \widetilde{0}$, $\widetilde{1} > \widetilde{0} \Rightarrow \widetilde{0} > \widetilde{0}$ (или $\widetilde{9} > \widetilde{3}$, $\widetilde{2} > \widetilde{0} \Rightarrow \widetilde{9} + \widetilde{2} = \widetilde{1} > \widetilde{3}$.

в) Нельзя сокращать: $\widetilde{1} \cdot \widetilde{5} = \widetilde{3} \cdot \widetilde{5}$, но $\widetilde{1} \neq \widetilde{3}$.

г) $\widetilde{4} \neq \widetilde{0}$, $\widetilde{5} \neq \widetilde{0}$, но $\widetilde{4} \cdot \widetilde{5} = \widetilde{0}$!

Теперь мы проанализируем эти свойства и выясним, как их нужно «обходить».

109. Определение. В произвольном кольце R элемент $a \in R$, $a \neq 0$ называется *делителем нуля*, если существует $b \in R$ такой, что $b \neq 0$ и $ab = 0$.

Пример. $\widetilde{4}$ и $\widetilde{5}$ — делители нуля в $\mathbb{Z}_{10}$. В кольце $\mathbb{Z}$ нет делителей нуля.

Задача. Перечислите все делители нуля в кольцах $\mathbb{Z}_{10}$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$. Ответьте на вопрос: при каком условии $\widetilde{r}$ является делителем нуля в $\mathbb{Z}_m$?

110. Теорема. Если $(r, m) > 1$ и $\widetilde{r} \neq \widetilde{0}$, то $\widetilde{r}$ — делитель нуля в $\mathbb{Z}_m$.

(Докажите.)

111. Обратимся к вопросу о сокращении. В произвольном кольце R

$$ax = ay \iff ax - ay = 0 \iff a(x - y) = 0,$$

и если a — не делитель нуля в R, то $x - y = 0$, т.е. $x = y$ (поясните). Значит в кольце R можно сокращать на элементы, не являющиеся делителями нуля, а на делители нуля (и сам 0) сокращать нельзя (объясните).

Теорема. Если $\widetilde{r} \neq \widetilde{0}$ — делитель нуля в $\mathbb{Z}_m$, то $(r, m) > 1$.

(Докажите.)

Вопрос: при каких m в кольце $\mathbb{Z}_m$ можно сокращать на любой $\widetilde{r} \neq \widetilde{0}$?

112. Опишите все делители нуля в кольцах

а) всех функций $f : \mathbb{R} \longrightarrow \mathbb{R}$,

б) непрерывных функций $f : \mathbb{R} \longrightarrow \mathbb{R}$,

в) в кольце $\mathbb{Z}^2 = \{(m,n) | \, m,n \in \mathbb{Z}\}$ с покоординатными операциями сложения и умножения: $(m,n)+(m',n') = (m+m', n+n')$, $(m,n)\cdot(m',n') = (mm', nn')$.

113. *Применения вычетов.* Докажите следующие утверждения:
а) $m^2+n^2 \vdots 3 \;\Rightarrow\; m \vdots 3$ и $n \vdots 3$,
б) $m^2+n^2 \vdots 7 \;\Rightarrow\; m \vdots 7$ и $n \vdots 7$,
в) $m+n+k \vdots 6 \;\Rightarrow\; m^3+n^3+k^3 \vdots 6$.

114. *Применения вычетов.* Докажите, что следующие уравнения не имеют решений в целых числах:

а) $15x^2 - 7y^2 = 9$,
б) $5x^3 - 7y = 3$,
в) $x^2 - 2y^2 + 8z = 3$,
г) $12x + 5 = y^2$,
д) $x^2+y^2+z^2 = 1967$,
е) $x^{1972} + 1973x^{1917} - 144x + 137 = 0$,
ж) $x^3 + 3x^2y^2 + y^3 = 0$, кроме $(x,y) = (0,0)$,
з) $x^2+y^2 = 1967(u^2+v^2)$, кроме $(x,y,u,v) = (0,0,0,0)$.

Общее указание. Подберите такое m, чтобы соответствующее уравнение в $\mathbb{Z}_m$ не имело бы решений. (Почему отсюда следует, что это уравнение не имеет решений над $\mathbb{Z}$?)

115. *Применения вычетов.* Отыскание признаков делимости.

Признаки делимости на 2 и на 5 тривиальны, поэтому мы займемся признаком делимости на число $m \in \mathbb{N}$, взаимно простое с 10. Признак делимости на m в десятичной системе счисления — это способ по десятичной записи данного числа A находить остаток от деления A на m.

Итак, пусть $(m,10) = 1$. Рассмотрим в кольце $\mathbb{Z}_m$ вычеты $\widetilde{1}$, $\widetilde{10}$, $\widetilde{10^2}$, $\widetilde{10^3}$,.... Поскольку в $\mathbb{Z}_m$ ровно $m-1$ ненулевых вычетов, среди выписанных найдутся равные: пусть, скажем,

$$\widetilde{10^{k+r}} = \widetilde{10^k}.$$

Сократив на $\widetilde{10^k}$ (почему можно сокращать?!), получим: $\widetilde{10^r} = \widetilde{1}$. Отсюда такой *признак делимости* на m: если разбить десятичную запись числа A на группы, справа налево по r цифр в каждой, т.е. записать $A = A_0 + A_1\cdot 10^r + A_2\cdot 10^{2r} + \cdots$, где A_i — r-значные числа, то остаток от деления A на m равен остатку от деления на m суммы $A_0 + A_1 + A_2 + \cdots$: $\widetilde{A} = \widetilde{A_0} + \widetilde{A_1} + \widetilde{A_2} + \cdots$ (объясните).

Пример. Хорошо известные признаки делимости на 3 и на 9 — частные случаи выведенного признака ($r = 1$).

Задача. Найдите r для $m = 11,\ 37$. Опишите соответствующие признаки.

Замечание. Аналогично строится признак делимости по соотношению $\widetilde{10^r} = -\widetilde{1}$ в кольце $\mathbb{Z}_m$. Опишите, как именно. Укажите такие признаки делимости на 11 и на 101.

§ 6. Обратимые вычеты и поля вычетов

«О поле, поле ...»
(А. С. Пушкин, «Руслан и Людмила»)

116. Сокращение в кольце действительных чисел

$$ax = ay \;\Rightarrow\; x = y \qquad \text{при } a \neq 0$$

можно понимать и как деление на a, т.е. умножение на число a^{-1}.

Определение. Элемент a произвольного кольца R с единицей 1 называется *обратимым*, если $\exists\, b \in R$ такой, что $ab = 1$ (этот элемент b обозначается a^{-1} и называется *обратным* к a). Множество всех обратимых элементов кольца R обозначается R^*.

Примеры. В кольце $\mathbb{Z}$ имеется только два обратимых элемента — это 1 и -1, а в кольцах $\mathbb{Q}$ и $\mathbb{R}$ любой элемент, отличный от нуля, обратим:

$$\mathbb{Z}^* = \{1, -1\}, \quad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}.$$

Обратимые элементы колец хороши и тем, что для $a \in R^*$ уравнение

$$ax = c$$

в кольце R можно решать не перебором, а умножением обеих частей уравнения на обратный элемент a^{-1} : $\quad x = a^{-1}c$.

Замечание. Если $a \in R^*$, то у A есть *ровно один* обратный элемент. Покажите, что если b_1 и b_2 — обратные к a, то $b_1 = b_2$. (*Указание.* Рассмотрите произведение b_1ab_2.) Отметим также, что обратимые элементы кольца не являются делителями нуля (докажите).

118. Лемма. Если $a \in R^*$ и $b \in R^*$, то $ab \in R^*$ и $a^{-1} \in R^*$. (По-другому говорят, что $(R^*, \cdot)$ — мультипликативная подгруппа кольца R.)
(Докажите.)

119. Вернемся к кольцам вычетов. Заметим, что если $\widetilde{n} \in \mathbb{Z}_m^*$, то это означает, что для некоторого $\widetilde{x} \in \mathbb{Z}_m$ $\widetilde{n}\widetilde{x} = \widetilde{1}$, т.е. $\widetilde{nx - 1} = \widetilde{0}$ или $nx - 1 = my$.

Теорема. $\widetilde{n} \in \mathbb{Z}_m^* \;\Leftrightarrow\; (n, m) = 1$.
(Докажите.)

120. Итак, в кольце $\mathbb{Z}_m$ обратимые вычеты $\widetilde{r}$ соответствуют остаткам $r = 1,\ 2,\ \ldots,\ m-1$, взаимно простым с m.

Следствие. Если $m = p$ — простое число, что $\mathbb{Z}_m^* = \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\widetilde{0}\}$ (иными словами, все ненулевые вычеты по простому модулю обратимы).

Замечание. Если m составное, то $\mathbb{Z}_m^* \neq \mathbb{Z}_m \setminus \{\widetilde{0}\}$ — существуют ненулевые необратимые вычеты (например, таковы делители нуля в $\mathbb{Z}_m$).

121. Обозначим число элементов в $\mathbb{Z}_m^*$ через $\varphi(m)$. По-другому, $\varphi(m)$ — количество натуральных чисел, меньших m и взаимно простых с m. Функция $m \mapsto \varphi(m)$ называется *функцией Эйлера.*

Примеры. $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$; $\varphi(6) = ?$, $\varphi(7) = ?$, $\varphi(8) = ?$, $\varphi(9) = ?$, $\varphi(10) = ?$

122. Выпишем все $\varphi(m)$ элементов множества $\mathbb{Z}_m^*$ в одну строчку и умножим затем каждый элемент этой строчки на какой-нибудь фиксированный элемент $x \in \mathbb{Z}_m^*$:

$$\mathbb{Z}_m^* = \{x_1,\ x_2,\ x_3, \dots, x_{\varphi(m)}\},$$
$$x\mathbb{Z}_m^* = \{xx_1,\ xx_2,\ xx_3, \dots, xx_{\varphi(m)}\}.$$

Лемма. $x\mathbb{Z}_m^* = \mathbb{Z}_m^*$, т.е. во второй строчке находятся обратимые элементы кольца $\mathbb{Z}_m$, причем каждый обратимый элемент x_i встречается во второй строчке ровно один раз. (Докажите.)

123. Из леммы 122 следует, что произведения по отдельности в строчках $\mathbb{Z}_m^*$ и $x\mathbb{Z}_m^*$ равны:

$$x_1x_2x_3\cdots x_{\varphi(m)} = (xx_1)(xx_2)(xx_3)\cdots(xx_{\varphi(m)}) = x^{\varphi(m)}\cdot(x_1x_2x_3\cdots x_{\varphi(m)}).$$

После сокращения (почему можно сокращать?) получим: для $x \in \mathbb{Z}_m^*$

$$x^{\varphi(m)} = 1.$$

Этим самым доказана

Теорема Ферма – Эйлера: $\forall m \in \mathbb{N}\ \forall n \in \mathbb{Z}\ (n,m) = 1 \implies n^{\varphi(m)} - 1 \vdots m$ (Поясните.)

124. Примеры. а) $\varphi(8) = 4$, поэтому $(n,8) = 1 \implies n^4 - 1 \vdots 8$;

б) $\varphi(9) = 6$, поэтому $(n,9) = 1 \implies n^6 - 1 \vdots 9$;

в) если $m = p$ простое, то $\varphi(p) = p - 1$, а условие $(n,p) = 1$ означает, что n не делится на p; в этом случае получаем: $n^{p-1} - 1 \vdots p$. Домножив $n^{p-1} - 1$ на n, узнаём старую Малую теорему Ферма (см. т. 69):

$$\forall n \in \mathbb{Z}\ \ n^p - n \vdots p.$$

125. Обратная теорема Ферма – Эйлера: $n^{\varphi m} - 1 \vdots m \implies (n,m) = 1$. (Докажите.)

126. В лемме 122 мы воспользовались свойством $x, y \in R^* \ \Rightarrow\ xy \in R^*$ из леммы 118. По той же лемме 118 $\forall x \in R^*\ \ x^{-1} \in R^*$. Следовательно, для каждого элемента $x_i \in \mathbb{Z}_m^*$ найдется $x_k \in \mathbb{Z}_m^*$ т.ч. $x_k = x_i^{-1}$, и поэтому при перемножении всех элементов $x_1,\ x_2,\ \dots,\ x_{\varphi(m)}$ получится 1:

$$x_1 \cdot x_2 \cdots x_{\varphi(m)} = 1.$$

Нет ли ошибки в этом рассуждении?!

127. Рассуждения т. 126 неверны: может оказаться, что некоторый элемент $x \in \mathbb{Z}_m^*$ является обратным к себе самому, т.е. $x^{-1} = x$. В этом случае $x^2 = \widetilde{1}$ или $x^2 - \widetilde{1} = 0$, т.е. $(x - \widetilde{1})(x + \widetilde{1}) = 0$. При любом m этому уравнению удовлетворяют вычеты $x = \widetilde{1}$ и $x = \widetilde{-1}$. Если m составное, то могут существовать и другие решения — например, в кольце $\mathbb{Z}_8$ таковы $x = \widetilde{3}$ и $x = \widetilde{5}$ (проверьте!). В случае простого $m = p$ других элементов, кроме $x = \widetilde{1}$ и $x = \widetilde{-1}$ обратных к самим себе нет — докажите. Исправляя рассуждения т. 126, получаем:

$$\widetilde{1} \cdot \widetilde{2} \cdot \widetilde{3} \cdots \widetilde{(p-2)} \cdot \widetilde{(p-1)} = \widetilde{1} \cdot \widetilde{(p-1)} = \widetilde{-1}, \quad \text{т.е. } \widetilde{(p-1)!} = \widetilde{-1},\ \widetilde{(p-1)! + 1} = \widetilde{0}.$$

Тем самым доказана **Теорема Вильсона:** если p простое, то $(p-1)! + 1 \vdots p$.

Докажите **обратную теорему Вильсона:** если $(m-1)!+1 \vdots m$, то m — простое. Иначе говоря, докажите, что при составном m число $(m-1)! + 1$ не делится на m.

128. Итак, мы выяснили, что кольца $\mathbb{Z}_m$ «особенно хороши» в том случае, когда $m = p$ — простое число.

Определение. Кольцо R с единицей 1 (т.ч. $1 \neq 0$) называется *полем*, если $R^* = R \setminus \{0\}$. Другими словами, кольцо с единицей — поле, если выполнена, в дополнение ко всем аксиомам кольца с 1, аксиома *обратимости умножения:*

$(\mathrm{O}\cdot)\ \forall a \in R\ a \neq 0 \ \Rightarrow\ \exists b \in R:\ ab = 1\ (b = a^{-1})$.

Примеры. *Поля:* $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$ при простом p.

Кольца, но не поля: $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}_m$ при составном m.

129. Таким образом, поля — это специальный класс «хороших» колец: таких, в которых осуществимо деление на любой отличный от 0 элемент. В любом поле F линейные уравнения $ax = c$ решают, как обычные линейные уравнения над полем $\mathbb{R}$:

$$ax = c \iff x = ca^{-1} \qquad (\text{при } a \neq 0).$$

В следующих тезисах (130–131) обсуждается еще одно свойство, отличающее поля от колец.

130. *Квадратные уравнения.* Простейшее из квадратных уравнений имеет вид $x^2 = a$. Как хорошо известно, в действительных числах (говорят, над полем действительных чисел) такое уравнение имеет не более двух корней. Это же уравнение можно рассматривать над произвольным кольцом: взять $a \in R$ и отыскать корни $x \in R$ уравнения $x^2 = a$. Из сказанного следует, что уравнение $x^2 = a$ имеет не более двух корней и над полем $\mathbb{Q} \subset \mathbb{R}$ и над кольцом $\mathbb{Z} \subset \mathbb{Q}$.

Пример. Составим таблицу квадратов в кольце вычетов $\mathbb{Z}_8$:

x	$=$	$\widetilde{1}$	$\widetilde{2}$	$\widetilde{3}$	$\widetilde{4}$	$\widetilde{5}$	$\widetilde{6}$	$\widetilde{7}$	$\widetilde{0}$
x^2	$=$	$\widetilde{1}$	$\widetilde{4}$	$\widetilde{1}$	$\widetilde{0}$	$\widetilde{1}$	$\widetilde{4}$	$\widetilde{1}$	$\widetilde{0}$

Мы видим отсюда, что уравнение $x^2 = \widetilde{1}$ над кольцом $\mathbb{Z}_8$ имеет 4 корня.

131. Теорема. Квадратное уравнение $x^2 = a$ над произвольным полем (в том числе и над $\mathbb{Z}_p$) имеет не более двух решений.

(Докажите. *Указание:* допустив, что уравнение $x^2 = a$ имеет корень x_0, т.е. $x_0^2 = a$, запишите уравнение в виде $x^2 - x_0^2 = 0$ и разложите левую часть на множители.)

132. Пока что мы не знаем никаких других полей, кроме $\mathbb{Z}_p$, $\mathbb{Q}$ и $\mathbb{R}$. Прежде чем приступить к изучению (и примерам) новых полей, мы должны проанализировать свойства рациональных и действительных чисел. К этому мы и приступим.

133. Теорема. Над полем $\mathbb{Z}_p$ при любых a и b выполнено равенство:

$$(a+b)^p = a^p + b^p.$$

(Докажите.)

134. Выведем формулу для функции Эйлера $\varphi(m)$ (впоследствии она пригодится!).

Лемма 1. Если $m = p^\alpha$, где p простое, то

$$\varphi(m) = \varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha - p^{\alpha-1}.$$

(Докажите.)

135. Лемма 2. Если $(m,n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$.

Докажите эту лемму в три шага по следующей схеме.

Подлемма А. $(r, mn) = 1 \Leftrightarrow (r,m) = 1$ и $(r,n) = 1$. (Докажите.)

Второй шаг. Мы рассматриваем, таким образом, количество чисел взаимно простых с m и n, среди чисел от 1 до mn. Расположим их в таблицу:

$$\begin{array}{ccccc} 1 & 2 & 3 & \dots & m \\ m+1 & m+2 & m+3 & \dots & 2m \\ 2m+1 & 2m+2 & 2m+3 & \dots & 3m \\ \dots & \dots & \dots & \dots & \dots \\ (n-1)m+1 & \dots & \dots & \dots & nm \end{array}$$

Очевидно, $(rm + k, m) = 1 \Leftrightarrow (k,m) = 1$, поэтому числа, взаимно простые с m заполняют в точности $\varphi(m)$ столбцов этой таблицы (это числа, стоящие в столбцах с номером k таким, что $(k,m) = 1$).

Подлемма Б. Числа, стоящие в каждом из столбцов таблицы, имеют разные остатки при делении на n. (Докажите.)

Контрольный вопрос. Где использовано, что $(m,n) = 1$?

Следовательно, в каждом из $\varphi(m)$ выделенных на втором шаге столбцов (из чисел, взаимно простых с m) ровно $\varphi(n)$ чисел будут взаимно простыми с числом n (объясните!). Требуемое доказано:

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Следствие. Если разложение числа m на простые сомножители имеет вид:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

то

$$\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

Глава III. Теория чисел

§ 7. Иррациональные и алгебраические числа

«... У алгебраиста не было бы оснований выходить за пределы этой области, если бы требования геометрии и физики не вынудили математиков заняться ужасным делом анализа непрерывности и не заставили их погрузить рациональные числа в континуум всех действительных чисел.»
(Герман Вейль)

136. Напомним, что *рациональные числа* — это дроби вида $\frac{m}{n}$, где $m \in \mathbb{Z}$, $n \in \mathbb{N}$, действия с которыми производятся по обычным правилам; таким образом, имея кольцо целых чисел $\mathbb{Z}$, $\mathbb{Z} \supset \mathbb{N}$, мы можем его расширить — построить поле рациональных чисел

$$\mathbb{Q} = \left\{ \frac{m}{n} | \, m \in \mathbb{Z},\ n \in \mathbb{N} \right\}, \quad \text{где } \frac{m}{n} = \frac{m'}{n'} \iff mn' = nm'.$$

137. С другой стороны, *действительные числа,* по определению, суть всевозможные бесконечные десятичные дроби:

$$\mathbb{R} \ni x = a_0, a_1 a_2 a_3 \dots a_n \dots, \quad a_0 \in \mathbb{Z},\ a_i \in \mathcal{Z} = \{0,\ 1,\ 2,\ \dots,\ 9\},$$

причем, если, начиная с некоторого места, в дроби идут подряд девятки, все их можно заменить на нули, прибавив единицу к предыдущему разряду:

$$a_0, a_1 a_2 \dots a_k 999 \dots 9 \dots = a_0, a_1 a_2 \dots (a_k + 1)000 \dots 0 \dots .$$

Все остальные дроби считаются различными, если они отличаются хотя бы в одном разряде.

Для дробей — двух действительных чисел $x, y \in \mathbb{R}$, — как обычно, можно определить, которое(-ая) из них меньше другого: $x < y$ или $y < x$.

138. *Десятично-рациональные числа.* Пусть $\mathbb{Q}_{(10)}$ — множество всех конечных десятичных дробей:

$$\alpha = a_), a_1 a_2 \dots a_m 000 \dots = a_0, a_1 a_2 \dots a_m.$$

Эти дроби можно отождествить с рациональными числами:

$$\alpha = a_0 + \frac{a_1 a_2 \dots a_m}{10^m} \in \mathbb{Q},$$

и, тем самым, вложить $\mathbb{Q}_{(10)}$ в $\mathbb{Q}$, т.е. считать, что $\mathbb{Q}_{(10)} \subset \mathbb{Q}$.

Лемма. $\mathbb{Q}_{(10)}$ — подполе поля $\mathbb{Q}$ (это означает, что если $\alpha, \beta \in \mathbb{Q}_{(10)}$, то и $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ принадлежать $\mathbb{Q}_{(10)}$. (Поясните.)

139. *Операции над действительными числами.* Для $x = a_0, a_1 a_2 a_3 \ldots \in \mathbb{R}$ положим:

$$x_n = a_0, a_1 a_2 \ldots a_n \in \mathbb{Q}_{(10)}, \quad x'_n = x_n + 10^{-n} \in \mathbb{Q}_{(10)} \ (n \in \mathbb{N}).$$

Тогда, очевидно, $x_n \leqslant x < x'_n$ при любом $n \in \mathbb{N}$. Поскольку десятично-рациональные числа мы умеем складывать, естественно дать следующее

Определение. Для $x, y \in \mathbb{R}$ их *суммой*

$$x + y = z$$

называется такое действительное число, что при любом $n \in \mathbb{N}$ справедливо

$$x_n + y_n \leqslant z < x'_n + y'_n.$$

Лемма (без доказательства). Число z с указанным выше свойством существует, притом только одно.

Аналогичным образом, только с учетом знаков чисел x и y, определяется *произведение* xy.

Теорема (без доказательства). $(\mathbb{R}, +, \cdot)$ — поле.

140. Конечно, $\mathbb{Q}_{(10)}$ является подкольцом поля $\mathbb{R}$. Хорошо известная процедура разложения обыкновенной дроби $\frac{m}{n} \in \mathbb{Q}$ в десятичную дробь $x = x\left(\frac{m}{n}\right)$ дает инъективное отображение всего поля $\mathbb{Q}$ рациональных чисел в поле действительных чисел, причем если $\frac{m}{n} \mapsto x$ и $\frac{m'}{n'} \mapsto x'$, то $\frac{m}{n} + \frac{m'}{n'} \mapsto x + x'$ и $\frac{m}{n} \cdot \frac{m'}{n'} \mapsto xx'$ (это — не совсем очевидная *теорема*, доказательство которой мы не приводим). Таким образом, можно считать, что $\mathbb{Q} \subset \mathbb{R}$ и $\mathbb{Q}$ — подполе $\mathbb{R}$.

Теорема. Дробь $x \in \mathbb{R}$ принадлежит $\mathbb{Q} \Leftrightarrow$ дробь x периодична.

Поясните доказательство этой теоремы.

141. Конструкции и утверждения тт. 137-140 по сути относятся к анализу. Теперь же мы займемся вопросами, относящимися скорее к алгебре.

142. *Существование иррациональных чисел.*

Утверждение. $\mathbb{R} \setminus \mathbb{Q} \neq \varnothing$.

I способ доказательства — теорема 140 (поясните).

II способ — теорема Пифагора (т.46) или теорема 48 (см. также тт. 49 и 50.

Замечание. При втором способе доказательства мы пользуемся следующим относящимся к анализу свойством поля $\mathbb{R}$:

Теорема. (Существование корня n-ой степени) $\forall a \in \mathbb{R}\ a \geqslant 0 \ \Rightarrow \ \exists x \in \mathbb{R}$ такое что $x^n = a$.

143. Иррациональности вида $\sqrt{2}$, $\sqrt[3]{2}$ и прочие такого же вида «предпочтительнее», чем иррациональные числа типа 0,1010010001... — например, тем, что не нужно ставить «...».

Определение. Числа, получающиеся из рациональных чисел применением конечного числа *алгебраических операций*, т.е. $+$, $\cdot$, $-$, $:$, $\sqrt[n]{\cdot}$, называются *радикальными*.

Теорема. Множество всех радикальных чисел $\mathcal{R}$ является подполем $\mathbb{R}$.

(Поясните.)

144. Конечно, $\mathbb{Q} \subset \mathcal{R}$ (объясните). Заметим, что наличие в радикальном числе $x \in \mathcal{R}$ «якобы несокращающихся» радикалов не означает, что $x \notin \mathbb{Q}$.

Пример. Число

$$x = \sqrt[3]{1 + \sqrt{\frac{28}{27}}} + \sqrt[3]{1 - \sqrt{\frac{28}{27}}}$$

в действительности равно 1! Докажите это. (*Указание:* $x = u + v$, $x^3 = \ldots$?)

Вопрос. Может быть, *любые* действительные числа являются радикальными? Иными словами, верно ли, что $\mathcal{R} = \mathbb{R}$, или нет?

Ответить на этот вопрос не так просто. Понятие радикальных чисел весьма прозрачно, но малоудобно в работе, поэтому мы прежде всего введем еще одно понятие.

Определение. Число $\alpha \in \mathbb{R}$ называется *алгебраическим*, если существует многочлен $P(x) = a_n x^n + \cdots + a_0$ с рациональными коэффициентами (для краткости будем писать $P(x) \in \mathbb{Q}[x]$) такой, что $P(\alpha) = 0$.

Пример. Докажите, что указанные ниже числа x являются алгебраическими, если $\alpha, \beta \in \mathbb{Q}$:

а) $x = \sqrt{\alpha} + \beta$, б) $x = \sqrt{\alpha} + \sqrt{\beta}$,

в) $x = \sqrt[3]{\alpha} + \sqrt[3]{\beta}$, г) $x = \sqrt{\alpha + \sqrt{\beta}}$,

д) $x = \sqrt[3]{\alpha} + \sqrt{\beta}$.

147. Проводя выкладки для примеров из т. 146, легко понять, что в действительности справедлива следующая

Теорема. $\mathcal{R} \subset \mathbb{A}$, где $\mathbb{A}$ — множество всех алгебраических чисел.

Доказывать ее мы не будем (попробуйте!)

148. Теперь мы уже имеем цепочку включений

$$\mathbb{Q} \subset \mathcal{R} \subset \mathbb{A} \subset \mathbb{R},$$

возникают вопросы: верно ли, что

(а) $\mathcal{R} = \mathbb{A}$? (б) $\mathbb{A} = \mathbb{R}$?

149. Ответ на вопрос 148 (а) отрицательный (!!): $\mathbb{A} \setminus \mathcal{R} \neq \emptyset$. Этот факт — одно из следствий т.н. *теории Галуа – Абеля*, о которой мы поговорим позже. (Грубо говоря, основная теорема этой теории гласит, что в общем случае уравнения вида $P(x) = 0$, где $P(x)$ — многочлен, не разрешимы в радикалах!)

Мы же обратимся к вопросу 148 (б): верно ли, что любое действительное число является алгебраическим?

150. *Алгебраические свойства алгебраических чисел.*

(1) $\alpha \in \mathbb{A} \implies -\alpha \in \mathbb{A}$,
(2) $\alpha \in \mathbb{A} \implies \frac{1}{\alpha} \in \mathbb{A}$,
(3) $\alpha \in \mathbb{A}\ , a \in \mathbb{Q} \implies a\alpha \in \mathbb{A}$,
(4) $\alpha \in \mathbb{A}\ , a \in \mathbb{Q} \implies a + \alpha \in \mathbb{A}$,
(5) $\alpha \in \mathbb{A} \implies \sqrt[n]{\alpha} \in \mathbb{A}\ (\forall n \in \mathbb{N})$,
(6) $\alpha \in \mathbb{A}\ , a \in \mathbb{Q} \implies \alpha^2 \in \mathbb{A}$
(Докажите.)

151. На самом деле можно доказать, что
(а) $\alpha, \beta \in \mathbb{A} \implies \alpha + \beta \in \mathbb{A}$,
(б) $\alpha, \beta \in \mathbb{A} \implies \alpha\beta \in \mathbb{A}$.
Это довольно сложные утверждения, но из них легко вывести такой факт.
Теорема. $\mathbb{A}$ — подполе поля $\mathbb{R}$.
(Поясните вывод этой теоремы. Заметим, что она, конечно, не противоречит тому, чтобы было $\mathbb{A} \neq \mathbb{R}$!)

152. Выведите из теоремы 151 теорему 147.

153. Итак, $\mathbb{Q}$, $\mathcal{R}$, $\mathbb{A}$ — подполя поля $\mathbb{R}$.
Вопрос. Являются ли подполями поля $\mathbb{R}$ подмножества $\mathbb{R} \setminus \mathbb{Q}$, $\mathbb{R} \setminus \mathcal{R}$, $\mathbb{R} \setminus \mathbb{A}$?
(*Ответ:* НЕТ. Это нужно твердо усвоить. Скажем, сумма и произведение иррациональных чисел НЕ ОБЯЗАНЫ быть иррациональными — приведите примеры.)

154. Собственно к вопросу 148 (б) (верно ли, что $\mathbb{R} \setminus \mathbb{A} = \emptyset$, или нет?) мы возвратимся чуть-чуть дальше, продемонстрировав весьма красивый прием доказательства некоторых математических теорем: в заключение упомянем еще о кое-каких фактах.

155. Определение. Множество $M \subset \mathbb{R}$ называется *всюду плотным* в $\mathbb{R}$, если

$$\forall (\alpha, \beta) \subset \mathbb{R} \quad M \cap (\alpha, \beta) \neq \emptyset,$$

(т.е. в *каждом* интервале числовой оси найдется хотя бы одна точка множества M.)

Утверждение. а) $\mathbb{Q}$ всюду плотно в $\mathbb{R}$.
б) $\mathbb{R} \setminus \mathbb{Q}$ тоже всюду плотно в $\mathbb{R}$.

(Докажите.)

§ 8. Эквивалентность и счетность

«— «Вопрос мой прост и краток, —
Промолвил Носорог, —
Что лучше — сорок пяток
Или пяток сорок?»
Увы, никто на это
Ответа
Дать не мог.»

(А. Милн)

156. Понятно, что для того, чтобы выяснить, в котором из двух конечных множеств A и B больше элементов, можно подсчитать число элементов $[A]$ и $[B]$ в каждом из них, а затем сравнить эти числа. Однако для больших множеств такой способ сравнения малопрактичен.

157. Пример. Пусть A — множество всех счастливых 6-значных билетов «по-московски» (сумма первых 3-х цифр равна сумме последних 3-х), а B — количество всех счастливых (6-значных) билетов «по-ленинградски» (сумма цифр на четных местах равна сумме цифр на нечетных). *Вопрос:* в каком из этих множеств больше билетов?

158. Решение предыдущей и аналогичных задач может быть основано на следующем утверждении.

Теорема Дирихле. Для конечных множеств A и B

$$[A] = [B] \;\Leftrightarrow\; \text{существует биекция } f : A \longrightarrow B.$$

(Часто употребляется вариант этой теоремы:

Принцип Дирихле. Если $[A] > [B]$, то любое отображение $f : A \longrightarrow B$ не инъективно: существуют $x_1, x_2 \in A$ такие, что $f(x_1) = f(x_2)$.)

159. Сила тривиальной теоремы 158 в том, что о биекциях можно рассуждать и в случае бесконечных множеств.

Определение 1. Два множества A и B (возможно, бесконечные) называются *эквивалентными* (или «равномощными»), если существует биекция $f : A \longrightarrow B$. В этом случае пишут $A \sim B$.

Определение 2. Для двух множеств A и B говорят, что B *мощнее* A, если

1) существует инъективное отображение $f : A \longrightarrow B$,

2) A не эквивалентно B, т.е. не существует биективного отображения $A \longrightarrow B$.

В этом случае пишут $A \prec B$.

160. Примеры. Покажите, что

а) $\mathbb{N} \sim 2\mathbb{N}$,

б) $\mathbb{N} \sim \mathbb{Z}$,

в) любые два отрезка эквивалентны,

г) интервал эквивалентен всей прямой.

161. Замечания. а) Если $A \sim B$, то $B \sim A$.
б) Если $A \sim B$ и $B \sim C$, то $A \sim C$.

(Докажите.)

162. Примеры. Докажите, что
а) $[0,1) \sim [0,1]$,
б) $(0,1) \sim [0,1)$,
в) отрезок $[0,1]$ эквивалентен квадрату $K = \{(x,y) \in \mathbb{R}^2 | \, 0 \leqslant x, y \leqslant 1\}$.

163. Не можете ли вы указать два не эквивалентных друг другу бесконечных множества?!
Кандидаты: а) $\mathbb{N}$ и $\mathbb{Q}$,
б) $\mathbb{N}$ и $\mathbb{R}$.
Разберемся с ними по очереди.

164. Удобно ввести следующее понятие.
Определение 3. Множество A называется *счетным*, если $A \sim \mathbb{N}$.
Иначе говоря, A счетно, если его элементы можно занумеровать всеми натуральными числами:

$$A = \{x_1,\ x_2,\ x_3,\ \ldots,\ x_n,\ \ldots\}$$

(отображение $n \mapsto x_n$ и есть биекция $\mathbb{N} \longrightarrow A$).

165. Примеры счетных множеств — $\mathbb{N}$, $2\mathbb{N}$, $\mathbb{Z}$ (поясните).
(Еще два примера: $\mathbb{N}^2$ и $\mathbb{Z}^2$ — множества пар (m,n), где m и n натуральные и целые, соответственно. Докажите, что множества $\mathbb{N}^2$ и $\mathbb{Z}^2$ счетны, изобразив их на координатной плоскости.)

166. *Свойства счетных множеств.* (Докажите.)
(А) Если A счетно, а $B \subset A$, то множество B либо конечно, либо счетно.
(Б) Если A и B счетны, то $A \cup B$ счетно (при доказательстве рассмотрите случаи $A \cap B = \varnothing$, $A \cap B$ конечно, $A \cap B$ бесконечно).
(В) Если $A = \{a_1, a_2, \ldots\}$ и $B = \{b_1, b_2, \ldots\}$ — счетные множества, то их прямое произведение

$$A \times B = \{(a_k, b_l) | \, a_k \in A,\ b_l \in B\}$$

является счетным. (Дайте наглядную интерпретацию множества $A \times B$!)

167. Вернемся к вопросу 163.
Первая теорема Кантора. Множество $\mathbb{Q}$ рациональных чисел счетно.
Доказательства.
I способ. $\mathbb{Q}$ можно отождествить с подмножеством несократимых дробей множества всех дробей $\frac{m}{n}$, где $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Осталось заметить, что дроби можно интерпретировать как пары (m,n), поэтому последнее множество есть $\mathbb{Z} \times \mathbb{N}$ — прямое произведение счетных.
II способ. Рациональные числа, принадлежащие отрезку $[0,1]$, легко перенумеровать — выписать их в последовательность:

$$0,\ 1,\ \frac{1}{2},\ \frac{1}{3},\ \frac{2}{3},\ \frac{1}{4},\ \frac{3}{4},\ \frac{1}{5},\ \frac{2}{5},\ \frac{3}{5},\ \ldots$$

Модифицировав эту нумерацию, можно перенумеровать и все рациональные числа.

168. Итак, доказан потрясающий факт — всех рациональных чисел, оказывается, ровно столько же, сколько натуральных чисел! Может быть, и всех действительных чисел столько же?!

Вторая теорема Кантора. Множество $\mathbb{R}$ всех действительных чисел несчетно (и $\mathbb{R}$ мощнее $\mathbb{N}$).

169. *I доказательство 2-ой теоремы Кантора.*

Допустим противное: все действительные числа, т.е. бесконечные десятичные дроби можно занумеровать —

$$\begin{aligned}
X_1 &= a_{10}, a_{11}a_{12}a_{13}\ldots a_{1n}\ldots\ ;\\
X_2 &= a_{20}, a_{21}a_{22}a_{23}\ldots a_{2n}\ldots\ ;\\
X_3 &= a_{30}, a_{31}a_{32}a_{33}\ldots a_{3n}\ldots\ ;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X_n &= a_{n0}, a_{n1}a_{n2}a_{n3}\ldots a_{nn}\ldots\ ;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Укажите теперь такую десятичную дробь, которая была бы отлична от каждой из дробей выписанного списка (хотя бы в одном разряде !!). (Это и будет противоречие!)

170. *II доказательство 2-ой теоремы Кантора.*

Опять допустим противное. Тогда и множество точек отрезка $\Delta_0 = [0,1]$ можно занумеровать:

$$\Delta_0 = \{x_1,\ x_2,\ x_3,\ \ldots,\ x_n,\ \ldots\}.$$

Разделим Δ_0 на три равные части и выберем ту из них — отрезок Δ_1, — которая не содержит точку x_1 : $\Delta_1 \not\ni x_1$ (поясните). Затем разделим отрезок Δ_1 на три равных отрезка и выберем тот из них, Δ_2, который не содержит x_2 : $\Delta_2 \not\ni x_2$, — и так далее.

Мы получим *последовательность стягивающихся отрезков:*

$$\Delta_0 \supset \Delta_1 \supset \Delta_2 \cdots \supset \Delta_n \supset \cdots \ (\text{длина } \Delta_n \text{ равна } \frac{1}{3^n}),$$

— причем $\forall n \in \mathbb{N}\ \ \Delta_n \not\ni x_n$, откуда следует, что $\forall k \leqslant n\ \ \Delta_n \not\ni x_k$. Рассмотрим число $x_0 = \bigcap\limits_{n=1}^{\infty} \Delta_n \in \Delta_0$ (мы применили так называемую «лемму о стягивающихся отрезках» из анализа). Вопрос: какой номер имеет x_0?! (Противоречие.)

171. *III доказательство 2-ой теоремы Кантора.*

Пусть $A \subset [0,1]$, $A = \{x_1,\ x_2,\ \ldots\}$ — счетное множество. Для каждого номера n рассмотрим интервал

$$\Sigma_n = \left(x_n - \frac{\varepsilon}{2^{n+1}}, x_n + \frac{\varepsilon}{2^{n+1}}\right)$$

длины $\frac{\varepsilon}{2^n}$, окружающий точку $x_n \in A$.

Лемма. Объединение интервалов Σ_n, т.е. множество $\Sigma = \bigcup_{n=1}^{\infty} \Sigma_n$, не содержит отрезок $[0,1]$ («целиком»), если $\varepsilon < 1$.

Доказательство. Сумма длин всех интервалов равна ε (объясните и выведите отсюда утверждение леммы).

Следствие. Отрезок $[0,1]$ несчетен (счетное множество не может совпадать со всем отрезком $[0,1]$).

(Поясните. Очевидно, отсюда следует 2-я теорема Кантора.)

Замечание. Утверждение леммы (выше) особенно эффективно для счетных подмножеств A, всюду плотных на отрезке $[0,1]$ — например, для множества $A = \mathbb{Q} \cap [0,1]$ (см. т. 155). Вдумайтесь!

172. Revenons à nos moutons[1].

Третья теорема Кантора. Множество $\mathbb{A}$ всех алгебраических чисел счетно.

Ее доказательство разобьем на 3 этапа.

(1) Множество $\mathcal{P}_n$ всех многочленов $P(x) \in \mathbb{Q}[x]$ данной степени n счетно.

(2) Множество $\mathbb{Q}[x]$ всех многочленов с рациональными коэффициентами счетно.

(3) Множество всех корней этих многочленов счетно.

Докажите утверждения (1)–(3). Выведите из (3) счетность множества $\mathbb{A}$. (Для доказательства (3) вам потребуется следующее почти очевидное утверждение: *любой ненулевой многочлен имеет конечное число корней.* Его мы обсудим потом.)

173. Следствие. $\mathbb{R} \setminus \mathbb{A} \neq \emptyset$. (Поясните.)

Заметим, что в действительности $\mathbb{R} \setminus \mathbb{A}$ несчетно (объясните, почему?). Числа $\alpha \in \mathbb{R} \setminus \mathbb{A}$ называются *трансцендентными* («запредельными»). Наше замечание показывает, что трансцендентных чисел «гораздо больше», чем не трансцендентных, т.е. алгебраических.

174. Следствие 173 — это теорема существования трансцендентных чисел. Она утверждает, что такие числа существуют, но не дает способа указать хотя бы одно из них! (Подобные теоремы существования иногда называют «чистыми».)

Исторически теорема существования трансцендентных чисел сначала была доказана *конструктивно*: Лиувилль указал (построил) число, не являющееся алгебраическим. Вот оно:

$$\lambda = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \frac{1}{10^{120}} + \cdots + \frac{1}{10^{n!}} + \cdots .$$

Доказательство трансцендентности числа λ совсем не сложно — трудно до него догадаться! (По этому поводу см. книгу Куранта и Роббинса.) Гораздо труднее было установить, что знаменитые числа

$$\pi = \frac{l}{d}, \quad \text{где } l \text{ и } d \text{ — длина и диаметр произвольной окружности, и}$$

$$e = \lim_{k \to \infty} \left(1 + \frac{1}{k}\right)^k = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots$$

являются также трансцендентными. Позднее мы еще вернемся к этому.

[1] Вернемся к нашим баранам (фр.).

Итог

«Рассказ наш близится к концу. Как мы уже не раз предупреждали, наши сведения об этом конце отрывочны и носят характер скорее саги, нежели исторического отчета. Нам приходится, однако, этим довольствоваться.»
(Герман Гессе, «Игра в бисер»)

175. Итак, система (поле) действительных чисел $\mathbb{R}$ устроена весьма сложно:

$$\mathbb{R} \supsetneq \mathbb{A} \supsetneq \mathbb{Q}.$$

Далее мы увидим, что поле $\mathbb{R}$ не такое уж и хорошее с точки зрения алгебры.

С алгебраическими и трансцендентными числами связано очень много проблем, решаемых и по сей день. Кое о чем рассказано в дополнениях к тезисам.

На этом мы закончим наш экскурс в арифметику и теорию чисел и обратимся (возвратимся) к *теории уравнений.*

Александр Николаевич Земляков,
кандидат педагогических наук,
ведущий научный сотрудник
лаборатории дифференциации образования
Института общего среднего образования
Российской академии образования (ИОСО РАО).

E-mail: zemmm@yandex.ru

Об определениях длины окружности и площади круга

А. В. Гладкий

В учебнике геометрии А.П.Киселева [1] наряду с обычными определениями длины окружности и площади круга с помощью пределов имеется краткое изложение другого способа введения этих понятий, основанного на принципе непрерывности.[1] Широкого распространения в преподавании этот способ не получил. Между тем при тщательной разработке он может, по нашему убеждению, позволить соединить строгость с доступностью и наглядностью в большей мере, чем какой-либо другой. Цель настоящей статьи — дать более развернутое и более современное изложение этого способа.

I. Некоторые свойства вписанных и описанных многоугольников

Теорема 1. Если многоугольники M и M' вписаны в одну и ту же окружность и множество вершин многоугольника M есть истинная часть множества вершин многоугольника M', то: а) периметр M меньше периметра M'; б) площадь M меньше площади M'.

Доказательство. Рассмотрим сначала случай, когда множество вершин M' получается из множества вершин M добавлением одной вершины — скажем, F. Тогда сам многоугольник M' получается из многоугольника M добавлением треугольника ABF, где A и B — некоторые соседние вершины M (рис.1). Отсюда немедленно следует, что площадь M' больше площади M. Чтобы получить периметр M', нужно из периметра M вычесть AB и прибавить $AF + FB$; но сумма двух сторон треугольника больше его третьей стороны, и потому периметр M' больше периметра M.

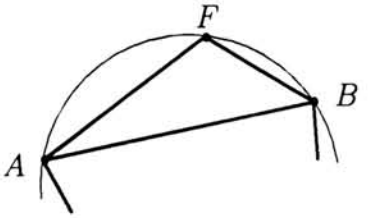


Рис. 1

[1] В сокращенном варианте книги [1], использовавшемся в 30^{x}–60^{x} гг. в качестве стабильного учебника, этот раздел опущен.

Перейдем теперь к общему случаю. Пусть множество вершин M' получается из множества вершин M добавлением вершин $C_1, C_2, \ldots, C_k$. Обозначим через M_1 многоугольник, множество вершин которого получается из множества вершин M добавлением вершины C_1, через M_2 — многоугольник, множество вершин которого получается из множества вершин M_1 добавлением вершины C_2, и т. д. В последовательности многоугольников $M, M_1, M_2, \ldots, M_k = M'$ по уже доказанному периметр и площадь каждого следующего многоугольника соответственно больше периметра и площади предыдущего. Это завершает доказательство.

Теорема 2. Если многоугольники M и M' описаны около одной и той же окружности и множество точек касания сторон многоугольника M с окружностью есть истинная часть соответствующего множества для M', то: а) периметр M больше периметра M'; б) площадь M больше площади M'.

Доказательство. Начнем с частного случая, когда множество точек касания M' с окружностью получается из соответствующего множества для M добавлением одной точки — скажем, G. Тогда сам многоугольник M' получается из многоугольника M «отрезанием» треугольника BHK, где B — общая вершина двух соседних сторон AB и BC многоугольника M, а H и K — точки, лежащие соответственно на AB и на BC (рис. 2). Отсюда сразу следует, что площадь M' меньше площади M.

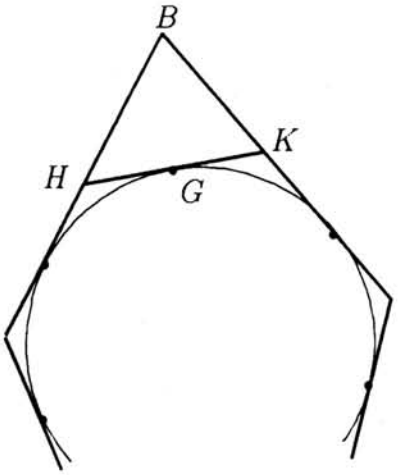


Рис. 2

Чтобы получить периметр M', нужно из периметра M вычесть $HB + BK$ и прибавить HK; поэтому периметр M' меньше периметра M.

Общий случай сводится к рассмотренному частному так же, как в доказательстве теоремы 1.

Теорема 3. Периметр и площадь всякого многоугольника, вписанного в окружность, соответственно меньше периметра и площади всякого многоугольника, описанного около той же окружности.

Доказательство. Утверждение о площадях очевидно. Чтобы доказать утверждение о периметрах, рассмотрим сначала частный случай, когда множество вершин вписанного многоугольника совпадает с множеством точек касания сторон

описанного многоугольника с окружностью. Пусть $A_1, A_2 \ldots, A_n$ — вписанный многоугольник, $B_1, B_2, \ldots, B_n$ — описанный, и стороны $B_1B_2, B_2B_3, \ldots, B_nB_1$ касаются окружности в точках $A_1, A_2, \ldots, A_n$ (см. рис. 3, где $n = 5$). Тогда

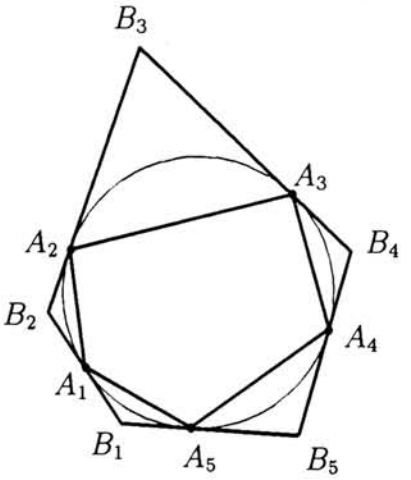


Рис. 3

$A_1A_2 + A_2A_3 + \ldots + A_nA_1 < (A_1B_2 + B_2A_2) + (A_2B_3 + B_3A_3) + \ldots$
$+(A_nB_1 + B_1A_1) = B_1B_2 + B_2B_3 + \ldots + B_nB_1.$

Теперь легко доказать утверждение для общего случая. Пусть M_1 — произвольный многоугольник, вписанный в окружность, и M_2 — произвольный многоугольник, описанный около той же окружности. Обозначим через E_1 множество вершин многоугольника M_1 и через E_2 — множество точек касания сторон многоугольника M_2 с окружностью. Положим $E = E_1 \cup E_2$ и рассмотрим вписанный многоугольник M_1' с множеством вершин E и описанный многоугольник M_2', для которого E является множеством точек касания его сторон с окружностью. Обозначим периметры многоугольников M_1, M_2, M_1', M_2' через p_1, p_2, p_1', p_2' соответственно. Ввиду теоремы 1 имеем $p_1 \leq p_1'$, ввиду теоремы 2 имеем $p_2' \leq p_2$. Поэтому $p_1 < p_2$.

Основная лемма. (а) Разность между периметрами двух правильных n-угольников, один из которых описан около окружности, а другой вписан в нее, при неограниченном возрастании числа n становится меньше любого наперед заданного положительного числа. (б) Аналогичное утверждение справедливо для разностей площадей.

Доказательство. Возьмем окружность с центром O и радиусом R и расположим вписанный в нее и описанный около нее правильные n-угольники таким образом, чтобы вершины вписанного n-угольника совпадали с точками касания с окружностью сторон описанного. Обозначим периметры вписанного и описанного n-угольников соответственно через p_n и P_n, площади через s_n и S_n.

Рассмотрим сектор нашей окружности, высекаемый радиусами, проведенными в соседние вершины A и B вписанного n-угольника (рис. 4). Пусть C — вершина

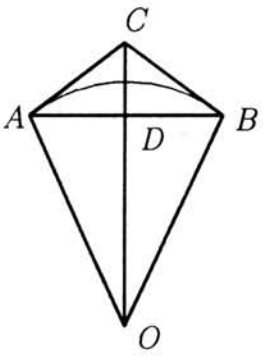


Рис. 4

описанного многоугольника, являющаяся точкой пересечения касательных, проведенных из A и B, и D — точка пересечения отрезков AB и OC. Легко видеть, что: (1) $AC = CB = \frac{1}{2n} \cdot P_n$; (2) $AD = DB = \frac{1}{2n} \cdot p_n$; (3) $OC \perp AB$; (4) треугольники OAC и ADC подобны; (5) $OD \geq \frac{1}{2}R$.

Далее, нетрудно доказать, что существует такое постоянное для данной окружности число T, не зависящее от n, что (6) $CD < \frac{T}{n^2}$. В самом деле, из (4) следует $\frac{CD}{AD} = \frac{AD}{OD}$, так что $CD = \frac{AD^2}{OD}$, откуда, используя (2) и (5), получаем $CD = \frac{p_n^2}{4n^2 \cdot OD} \leq \frac{p_n^2}{2n^2 R}$. Обозначив через P периметр какого-нибудь фиксированного многоугольника, описанного около данной окружности, и положив $T = \frac{P^2}{2R}$, имеем по теореме 3 $p_n < P$, откуда $CD < \frac{P^2}{2n^2 R} = \frac{T}{n^2}$, что и требовалось доказать.

Теперь утверждение (а) непосредственно следует из того, что

$$P_n - p_n = (AC + CB - AB) \cdot n = ((AC - AD) + (CB - BD)) \cdot n < 2CD \cdot n < \frac{2T}{n},$$

а утверждение (б) — из того, что

$$S_n' - s_n = \frac{1}{2} AB \cdot CD \cdot n = \frac{1}{2} p_n \cdot CD < \frac{1}{2} \cdot \frac{PT}{n^2}.$$

II. Принцип непрерывности

Далее мы будем пользоваться принципом непрерывности Дедекинда. Приведем определения, необходимые, чтобы его сформулировать.

Говорят, что множества $A, B \subset \Re$ ($\Re$ — множество всех действительных чисел) образуют **сечение**, если выполнены два условия:

D1. Множества A и B не пусты и их объединение совпадает с $\Re$ (т. е. всякое действительное число входит либо в A, либо в B).

D2. Всякое число из A меньше всякого числа из B.

Множество A называется **нижним классом** сечения, множество B — его **верхним классом**.

Примеры сечений:

1) Нижний класс — множество, состоящее из всех отрицательных чисел и нуля, верхний — множество всех положительных чисел.

2) Нижний класс — множество всех отрицательных чисел, верхний — множество всех неотрицательных чисел.

3) Нижний класс — множество всех чисел, меньших или равных единице, верхний — множество всех чисел, бóльших единицы.

4) Нижний класс — множество всех чисел, меньших единицы, верхний — множество всех чисел, бóльших или равных единице.

Легко заметить, что в сечении примера 1 в нижнем классе есть наибольшее число (им является 0), в то время как в верхнем классе наименьшего числа нет (в самом деле, какое бы положительное число α мы ни взяли, число $\frac{\alpha}{2}$ тоже положительно и меньше α, так что α не может быть наименьшим из положительных чисел). В сечении примера 2, наоборот, в верхнем классе есть наименьшее число (это тоже 0), а в нижнем нет наибольшего (если α — произвольное отрицательное число, то $\frac{\alpha}{2} > \alpha$, и $\frac{\alpha}{2}$ также отрицательно, так что α не может быть наибольшим из отрицательных чисел). Точно так же ясно, что в сечении примера 3 в нижнем классе есть наибольшее число, а в верхнем нет наименьшего, в то время как в сечении примера 4 в верхнем классе есть наименьшее число, а в нижнем нет наибольшего.

Может ли случиться так, что в нижнем классе какого-либо сечения есть наибольшее число и в то же время в верхнем есть наименьшее? Легко показать, что не может. В самом деле, пусть множества A и B образуют сечение, a_0 — наибольшее число из A и b_0 — наименьшее число из B. Тогда $a_0 < \frac{a_0+b_0}{2} < b_0$ (рис. 5). Поэтому число $\frac{a_0+b_0}{2}$ не может принадлежать A, т. к. оно больше наибольшего элемента A, и не может принадлежать B, т. к. оно меньше наименьшего элемента B. Но это противоречит определению сечения, согласно которому всякое действительное число должно входить либо в A, либо в B.

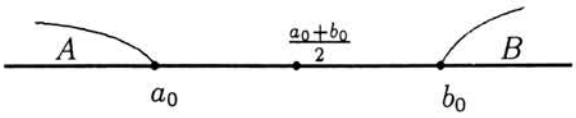


Рис. 5

Случай, когда в нижнем классе нет наибольшего числа и в верхнем нет наименьшего, также невозможен. В этом и состоит

Принцип непрерывности. Каково бы ни было сечение, либо в его нижнем классе есть наибольшее число, либо в верхнем есть наименьшее.

Наглядный смысл этого утверждения очевиден: оно означает, что прямая, служащая геометрическим образом множества всех действительных чисел $\mathfrak{R}$, «сплошь заполнена» точками, в ней нет «щелей» , «пустых мест». Его строгое обоснование в задачи нашей статьи не входит.[2]

Число, существование которого утверждается принципом непрерывности, мы будем называть **граничным числом сечения**.

[2]Такое обоснование можно найти, например, в книге [2].

III. Длина окружности

Теорема 4. Для любой окружности существует число, и притом только одно, которое больше периметра всякого многоугольника, вписанного в эту окружность, и меньше периметра всякого многоугольника, описанного около нее.

Доказательство. Пусть нам дана некоторая окружность. Многоугольники, вписанные в нее и описанные около нее, мы будем для краткости называть просто вписанными и описанными многоугольниками.

Чтобы облегчить усвоение доказательства, приведем его план. Оно будет состоять из четырех частей. Прежде всего (1) мы определим некоторые множества A и B и докажем, что они образуют сечение, в котором A является нижним классом, а B — верхним. Затем (2) докажем, что в множестве B нет наименьшего числа, откуда в силу принципа непрерывности будет следовать, что в множестве A есть наибольшее число. После этого (3) убедимся, что это число больше периметров всех вписанных многоугольников и меньше периметров всех описанных. И, наконец, (4) покажем, что число с таким свойством существует только одно.

Перейдем теперь к самому доказательству.

(1) Обозначим через A множество всех тех действительных чисел, которые меньше периметров всех описанных многоугольников, и через B — множество, состоящее из всех остальных действительных чисел. (Таким образом, объединение A и B совпадает с $\mathfrak{R}$.) Иными словами: число a принадлежит A тогда и только тогда, когда периметр всякого описанного многоугольника больше a; число b принадлежит B тогда и только тогда, когда не у всякого описанного многоугольника периметр больше b, т. е. когда существует описанный многоугольник, периметр которого меньше или равен b.

Ясно, что множества A и B не пусты: множеству A принадлежат, в частности, все отрицательные числа и нуль; множеству B принадлежат все числа, равные периметрам описанных многоугольников. В то же время, как мы уже заметили, объединение A и B совпадает с $\mathfrak{R}$. Таким образом, для множеств A и B выполняется условие D1 из определения сечения. Но и условие D2 также выполняется; если $A \in A$, $b \in B$, то существует описанный многоугольник, периметр которого P меньше или равен b; из $a \in A$ следует $a < P$; поэтому $a < b$.

(2) Итак, множества A и B образуют сечение. В силу принципа непрерывности должно существовать число l, являющееся **либо наибольшим в A, либо наименьшим в B**. Можно показать, однако, что в B нет наименьшего числа. Докажем это от противного. Допустим, что l — наименьшее число в множестве B. Тогда, поскольку $l \in B$, существует описанный многоугольник M', периметр которого P' меньше или равен l. Но по теореме 2 мы можем построить другой описанный многоугольник M'', периметр которого меньше периметра M'. Обозначая периметр M'' через P'', имеем $P'' < P' \leq l$. Но всякое число, равное периметру какого-нибудь описанного многоугольника, принадлежит B. Мы нашли, следовательно, число P'', такое, что $P'' \in B$ и в то же время $P'' < l$. А это противоречит тому, что l — наименьшее число в B.

Из только что доказанного следует, что число l принадлежит множеству A и является в нем наибольшим.

(3) Докажем теперь, что l и есть то самое число, которое нам нужно, т. е. что оно больше периметра всякого вписанного многоугольника и меньше периметра всякого описанного.

Тот факт, что l меньше периметра всякого описанного многоугольника, немедленно следует из того, что $l \in A$. Остается доказать, что периметр всякого вписанного многоугольника меньше l. Это мы докажем от противного. Допустим, что существует вписанный многоугольник m', периметр которого p' больше или равен l. По теореме 1 мы можем построить другой вписанный многоугольник m'', периметр которого больше периметра m'. Обозначая периметр m'' через p'', имеем $p'' > p' \geq l$. Но по теореме 3 периметр всякого вписанного многоугольника меньше периметра всякого описанного; поэтому $p'' \in A$. Мы нашли, следовательно, число p'', такое, что $p'' \in A$ и в то же время $p'' > l$; а это противоречит тому, что l — наибольшее число в A.

(4) Мы доказали, что существует число, которое больше периметров всех вписанных многоугольников и меньше периметров всех описанных. Нам осталось установить, что такое число имеется только одно.

Допустим противное: пусть существуют два различных числа, каждое из которых больше периметра всякого вписанного многоугольника и меньше периметра всякого описанного. Меньшее из этих двух чисел обозначим l_1, большее — l_2. Пусть теперь p_n есть периметр правильного вписанного n-угольника и P_n — периметр правильного описанного n-угольника. (Здесь n — любое натуральное число ≥ 3.) Имеем, очевидно, $p_n < l_1 < l_2 < P_n$, откуда

$P_n - p_n > l_2 - l_1$.

Но по основной лемме разность $P_n - p_n$ при неограниченном возрастании числа n становится меньше любого наперед заданного положительного числа; в частности, при достаточно больших значениях n будем иметь

$P_n - p_n < l_2 - l_1$.

Полученное противоречие завершает доказательство.

Доказанная теорема дает нам право сформулировать

Определение. То единственное число, которое больше периметров всех многоугольников, вписанных в окружность, и меньше периметров всех многоугольников, описанных около нее, называется **длиной окружности.**

Теорема 5. Отношение длины окружности к ее диаметру есть постоянное число, одно и то же для всех окружностей.

Доказательство. Пусть O и O' — две произвольные окружности, радиусы и длины которых равны R, R', l и l' соответственно. Нам нужно доказать, что $\frac{l}{2R} = \frac{l'}{2R'}$.

Допустим противное: пусть $\frac{l}{2R} \neq \frac{l'}{2R'}$, или, что то же самое, $\frac{l}{R} \neq \frac{l'}{R'}$. Пусть для определенности $\frac{l}{R} < \frac{l'}{R'}$. Постараемся вывести из этого неравенства противоречие.

Обозначим через p_n, P_n, p'_n и P'_n $(n = 3, 4, 5, \ldots)$ соответственно периметры правильных n-угольников m_n, M_n, m'_n, и M'_n, первый из которых вписан в окружность O, второй описан около O, третий вписан в O' и четвертый описан около O'. В силу определения длины окружности для любого n выполняются неравенства:

(1) $p_n < l < P_n$,

(1′) $p'_n < l' < P'_n$.

Деля почленно неравенство (1) на R и неравенство (1′) на R', получаем:

(2) $\frac{p_n}{R} < \frac{l}{R} < \frac{P_n}{R}$,

(2′) $\frac{p'_n}{R'} < \frac{l'}{R'} < \frac{P'_n}{R'}$.

Вспомним теперь, что периметры одноименных правильных n-угольников относятся как их радиусы или апофемы. Поэтому

$\frac{p_n}{p'_n} = \frac{P_n}{P'_n} = \frac{R}{R'}$

(поскольку для вписанных многоугольников m_n и m'_n числа R и R' являются радиусами, а для описанных многоугольников M_n и M'_n — апофемами).

Умножив равенство $\frac{p_n}{p'_n} = \frac{R}{R'}$ почленно на $\frac{p'_n}{R}$, а равенство $\frac{P_n}{P'_n} = \frac{R}{R'}$ на $\frac{P'_n}{R}$, получим:

(3) $\frac{p_n}{R} = \frac{p'_n}{R'}$; $\frac{P_n}{R} = \frac{P'_n}{R'}$.

А теперь из неравенств (2′) и равенств (3) получаем:

(4) $\frac{p_n}{R} < \frac{l'}{R'} < \frac{P_n}{R}$.

Неравенства (2) и (4) вместе с нашим допущением, что $\frac{l}{R} < \frac{l'}{R'}$, дают:

$\frac{p_n}{R} < \frac{l}{R} < \frac{l'}{R'} < \frac{P_n}{R}$,

причем это должно быть верно для любого $n = 3, 4, 5, \ldots$. Следовательно, для любого $n = 3, 4, 5, \ldots$ будет справедливо неравенство

$\frac{P_n}{R} - \frac{p_n}{R} > \frac{l'}{R'} - \frac{l}{R}$,

откуда

$P_n - p_n > \left(\frac{l'}{R'} - \frac{l}{R}\right) \cdot R$.

Но это противоречит основной лемме, в силу которой разность $P_n - p_n$ при достаточно больших n становится меньше любого наперед заданного положительного числа.

Отношение длины окружности к ее диаметру — одинаковое, как только что доказано, для всех окружностей — принято обозначать греческой буквой π (от слова $\pi\varepsilon\rho\iota\varphi\acute{\varepsilon}\rho\varepsilon\iota\alpha$ — окружность). Таким образом, длина окружности радиуса R равна $2\pi R$.

IV. Площадь круга

Теорема 6. Для любой окружности существует число, и притом только одно, которое больше площади всякого многоугольника, вписанного в эту окружность, и меньше площади всякого многоугольника, описанного около нее.

Доказательство этой теоремы совершенно аналогично доказательству теоремы 4. Сначала (1) нужно, обозначив, скажем, через A множество всех тех действительных чисел, которые меньше площадей всех описанных многоугольников, и через B — множество всех действительных чисел, не вошедших в A, доказать, что множества A и B образуют сечение. Затем (2) нужно доказать, что в B нет наименьшего числа, откуда в силу принципа непрерывности будет следовать, что в A есть наибольшее число. Потом (3) следует убедиться, что это число больше площадей всех вписанных многоугольников и меньше площадей всех описанных. Наконец, (4) нужно показать, что существует только одно число с таким свойством. На каждом из этих этапов можно повторить слово в слово соответствующие

рассуждения из доказательства теоремы 4 с той только разницей, что периметры всюду заменяются площадями.

Теорема 6 позволяет нам сформулировать

Определение. То единственное число, которое больше площадей всех многоугольников, вписанных в окружность, и меньше площадей всех многоугольников, описанных около нее, называется площадью круга, ограниченного данной окружностью.

Теорема 7. Площадь круга равна половине произведения его радиуса на длину ограничивающей его окружности.

Доказательство. Пусть R есть радиус круга, S — его площадь, l — длина ограничивающей его окружности. Нам нужно доказать, что $S = \frac{1}{2}Rl$. Для этого, очевидно, достаточно установить, что число $\frac{1}{2}Rl$ больше площадей всех вписанных в данную окружность многоугольников и меньше площадей всех описанных. Покажем, что это действительно так.

Рассмотрим произвольный вписанный многоугольник. Разобьем его на треугольники, каждый из которых ограничен одной из сторон многоугольника и отрезками, соединяющими концы этой стороны с центром окружности. Площадь каждого такого треугольника (рис. 6) равна половине произведения соответствующей стороны многоугольника на длину перпендикуляра, опущенного на нее из центра; а поскольку этот перпендикуляр, очевидно, короче радиуса, площадь нашего многоугольника меньше $\frac{1}{2}R \cdot a$, где a — длина рассматриваемой стороны многоугольника; поэтому площадь многоугольника меньше $\frac{1}{2}Rp$, где p — периметр многоугольника, и тем более меньше $\frac{1}{2}Rl$, т.к. $p < l$ (по определению длины окружности).

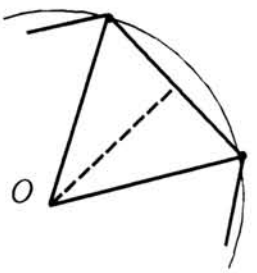


Рис. 6

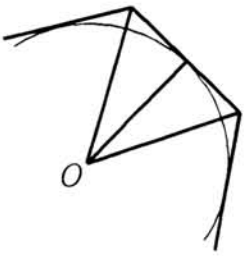


Рис. 7

Точно так же поступим с произвольным описанным многоугольником: разобьем его на треугольники, каждый из которых ограничен одной из сторон многоугольника и отрезками, соединяющими концы этой стороны с центром окружности. Площадь каждого такого треугольника (рис. 7) равна половине произведения соответствующей стороны многоугольника на длину перпендикуляра, опущенного на нее из центра, т. е. на радиус; поэтому площадь многоугольника равна $\frac{1}{2}RP$, где P — периметр многоугольника; но $\frac{1}{2}RP > \frac{1}{2}Rl$, поскольку $P > l$. Итак, мы доказали, что число $\frac{1}{2}Rl$ больше площадей всех вписанных многоугольников и меньше площадей всех описанных. Поэтому $S = \frac{1}{2}Rl = \pi R^2$.

Литература

1. *Киселев А. П.* Элементарная геометрия. М.: Госиздат, 1931. Переиздания: М.: Просвещение, 1980. М.: Просвещение, 1996.

2. *Гладкий А. В.* Числа: натуральные, рациональные, действительные, комплексные. М: Вербум-М, 2000.

Максимальная площадь веера

Виктор Оксман

Виктор Оксман — преподаватель математики Колледжа Западной Галилеи (Израиль). В заметке рассматривается экстремальная динамическая геометрическая задача, которую удается исследовать методами, доступными школьникам старших классов с углубленным изучением математики.

Рассмотрим три стержня (отрезка) OA, OB, OC заданных длин a, b, c $(a, b, c > 0)$, которые могут вращаться вокруг общего конца O. Каждому положению стержней соответствует треугольник ABC (веер), имеющий площадь S_{ABC} (рис. 1). Интуитивно ясно, что при некотором положении стержней $S_{\triangle ABC}$ достигает максимального значения. Так ли это? Если да, то чем характеризуется это положение и единственно ли оно? Ответы на эти вопросы даются ниже.

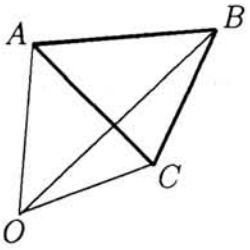


Рис. 1

Теорема 1. Среди треугольников ABC, образованных концами отрезков OA, OB, OC, существует треугольник максимальной площади.

Доказательство. Рассмотрим все треугольники ABC с фиксированным углом $\angle BOC = \alpha$. Площадь S_{ABC} будет максимальной, если точка A максимально удалена от прямой BC. Это достигается, когда $OA \perp BC$ и O — внутренняя точка отрезка AM (M — точка пересечения прямых OA и BC — рис. 2). Таким образом, для каждого фиксированного α $(0 \leq \alpha \leq 2\pi)$ существует и притом единственный треугольник ABC максимальной площади. Обозначим эту площадь через S. Мы получаем функцию $S(\alpha)$, определенную в замкнутом промежутке $[0, 2\pi]$. Легко доказать, что $S(\alpha)$ непрерывна в этом промежутке. Поэтому по теореме Вейерштрасса $S(\alpha)$ достигает в промежутке $[0, 2\pi]$ своего максимального значения (пока что не утверждается, что это происходит в единственной точке α — это будет доказано позже). Обозначим это значение через S_α.

Итак, S_α — максимальное значение площади треугольников ABC, образованных стержнями OA, OB, OC.

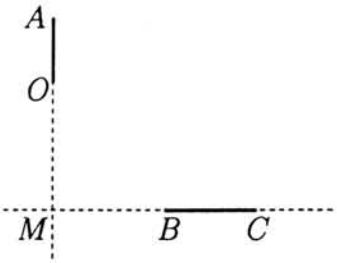


Рис. 2

Теорема 2. В треугольнике ABC максимальной площади точка O является его ортоцентром.

Доказательство. Мы уже видели в предыдущем доказательстве, что в треугольнике ABC максимальной площади $OA \perp BC$. Если аналогично зафиксировать $\angle AOC = \beta$ и $\angle AOB = \gamma$, то получим функции $S(\beta)$ и $S(\gamma)$, также достигающие своих максимальных значений S_β и S_γ в промежутке $[0, 2\pi]$. При этом $OB \perp AC$ и $OC \perp AB$. Но $S_\alpha = S_\beta = S_\gamma = S_{\max}$, где $S_{\max}$ — максимальная площадь треугольников ABC.

Итак, во всех случаях когда достигается $S_{\max}$ имеем:

$$OA \perp BC, \quad OB \perp AC, \quad OC \perp AB,$$

т.е. точка O — ортоцентр треугольника ABC.

Теорема 3. Треугольник ABC максимальной площади остроугольный.

Доказательство. Предположим, что $\angle ABC \geq 90°$. Если $\angle ABC = 90°$, то точка O (ортоцентр) совпадает с точкой B и длина стержня OB равна 0, что по условию невозможно.

Пусть угол $\angle ABC$ тупой. Тогда точка O лежит вне треугольника ABC. Повернув отрезок OB вокруг точки O на 180°, получим точку D, причем B — внутренняя точка треугольника ADC (рис. 3). Поэтому $S_{ABC} < S_{ADC}$ и, следовательно, $S_{\triangle ABC}$ не может быть максимальной.

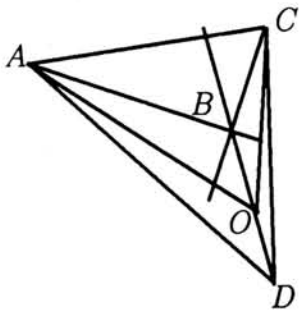


Рис. 3

Итак, треугольник максимальной площади обладает теми свойствами, что он остроугольный и точка O — его ортоцентр. Чтобы установить его единственность, докажем следующую лемму.

Лемма. Пусть $\triangle ABC$ и $\triangle A_1B_1C_1$ — треугольники одного типа (т.е. оба остроугольные, или оба прямоугольные, или оба тупоугольные); O и O_1 — их ортоцентры; $OA = O_1A_1$, $OB = O_1B_1$, $OC = O_1C_1$. Тогда эти треугольники равны.

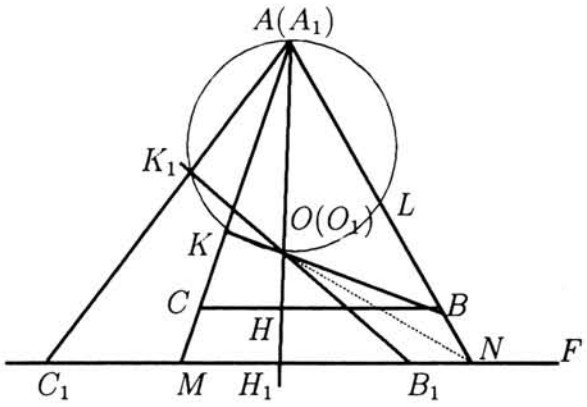


Рис. 4

Доказательство. Пусть оба данных треугольника остроугольные. Совместим равные отрезки OA и O_1A_1 так, чтобы точки B и B_1 расположились в одной полуплоскости относительно прямой OA (рис. 4). Докажем, что основание высоты AH треугольника ABC совпадает с основанием высоты A_1H_1 треугольника $A_1B_1C_1$, т.е. $AH = A_1H_1$.

Пусть $AH < A_1H_1$. Обозначим точки пересечения прямых AC и AB с прямой C_1B_1 соответственно через M и N. Тогда $\angle OBN > \angle CBN > 90°$. Поэтому $ON > OB$.

Пусть $\angle ANF$ — внешний угол треугольника MAN. Тогда $\angle ONF > \angle ANF > 90°$.

Поскольку $OB_1 = OB < ON$, точка B_1 — внутренняя точка отрезка H_1N. Аналогично точка C_1 — внутренняя точка отрезка MH_1.

Точки K, L (основания высот BK и CL треугольника CAB), O и A лежат на общей окружности с диаметром AO. Ясно, что $\angle B_1OH_1 < \angle BOH_1$ и $\angle B_1K_1A = \angle BKA = 90°$. Поэтому $\angle C_1AO > \angle MAO$. Но это противоречит тому, что точка C_1 — внутренняя точка отрезка MH_1.

Итак, $AH = A_1H_1$. Но тогда $OH = OH_1$, $CH = C_1H_1$, $BH = B_1H_1$ и $CB = C_1B_1$.

Аналогично получим, что $AB = A_1B_1$ и $AC = A_1C_1$.

Доказательство равенства тупоугольных треугольников аналогично приведенному выше. Случай прямоугольных треугольников тривиален.

Из доказанной леммы немедленно следует единственность треугольника максимальной площади с заданными длинами $OA = a$, $OB = b$, $OC = c$. Это остроугольный треугольник, имеющий своим ортоцентром точку O.

Естественно поставить вопрос о практическом построении такого треугольника.

Обозначив углы треугольника ABC соответственно через x, y, z, получим:

$$b\cos x = a\cos y, \quad c\cos x = a\cos z = -a\cos(x+y).$$

Отсюда

$$\cos x = \frac{n}{m}(\cos^2 x - (1-\cos^2 x)^{\frac{1}{2}}(m^2 - \cos^2 x)^{\frac{1}{2}})$$

или

$$n(1-\cos^2 x)^{\frac{1}{2}}(m^2-\cos^2 x)^{\frac{1}{2}} = \cos x(n\cos x - m),$$

где $m = \frac{a}{b}$, $n = -\frac{a}{c}$.

Обозначив $\cos x = t$ $(0 < t < 1)$, получим:

$$(1-t^2)^{\frac{1}{2}}(m^2-t^2)^{\frac{1}{2}} = t(t-\frac{m}{n}).$$

Это уравнение может иметь решение при условии, что $m > t$ и $t > \frac{m}{n}$, что равносильно $m > t$ (т.к. $n < 0$). Т.е. полученное значение $\cos x$ должно удовлетворять условию $\frac{a}{b} > \cos x$.

Возведя обе части данного уравнения в квадрат, получим:

$$2mnt^3 - (m^2+n^2+m^2n^2)t^2 + m^2n^2 = 0.$$

Таким образом, для практического построения треугольника максимальной площади достаточно одним из численных методов решить приближенно полученное уравнение, выбрав решение, удовлетворяющее условиям $0 < t < 1$ и $t < \frac{a}{b}$. То, что такое решение всегда существует и притом единственно, следует из доказанных выше теорем. Например, для случая $a = b = c$, получим интуитивно ожидаемый результат $x = 60°$, т.е. равносторонний треугольник.

В рассмотренной выше конструкции веер определялся как треугольник, образованный свободными концами стержней. При таком подходе в случае n стержней может получиться самопересекающийся n-угольник, что потребует специального уточнения, о какой площади идет речь. Поэтому в общем случае удобнее рассматривать суммарную площадь S треугольников, образованных соседними стержнями, и поставить вопрос о том, при каких положениях стержней достигается ее максимум. Например, для случая четырех стержней, изображенных на рис. 5,

$$S = S_{\triangle OBD} + S_{\triangle ODA} + S_{\triangle OAC} + S_{\triangle OBC}.$$

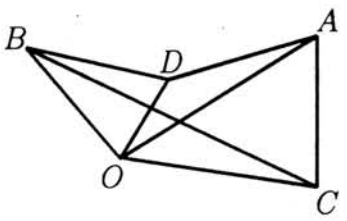


Рис. 5

Очевидно, что при таком подходе в случае трех стержней существуют 4 положения, в которых достигается $S_{\max}$. Одно из них соответствует установленному выше остроугольному треугольнику, имеющему точку O своим ортоцентром, а три других получаются из него поворотом каждого из стержней на 180° относительно точки O.

В свете этих уточнений предлагаем читателю самостоятельно решить задачу для случая четырех стержней (она гораздо проще предыдущей). Даны 4 стержня

OA, OB, OC, OD заданных длин a, b, c, d ($a \leq b \leq c \leq d$). Рассмотрим суммарную площадь S четырех треугольников, образованных соседними стержнями. Как следует установить стержни, чтобы S была максимальной? Чему равна $S_{\max}$?

Виктор Оксман
Колледж Западной Галилеи
Израиль

E-mail: REDC210@UVM.HAIFA.AC.IL

Определение погрешностей вычислений и решение задач с параметрами методами интервальной математики

А. Ф. Ляхов

А. Ф. Ляхов — доцент кафедры теоретической механики Нижегородского Государственного Университета, автор нашего журнала (№3-4, 1998 г.).
В статье описан математический аппарат, позволяющий учитывать распространение погрешностей при многократно повторяющихся вычислениях. Рассмотрены его приложения к задачам с параметрами. Это тематика актуальна в связи с оценкой точности компьютерных вычислительных алгоритмов.

Развитие вычислительной техники привело не только к количественному, но и качественному изменению подходов к численным методам решения математических задач. Современные компьютеры позволяют производить сложные многократно повторяющиеся вычисления. Если ранее сложность вопроса построения вычислительных алгоритмов была связана с ограниченностью скорости вычислений и количеством учитываемых знаков, то в настоящее время эти границы раздвинуты. Например, скорость численного решения задачи о колебании струны увеличилась приблизительно в двадцать раз по сравнению со скоростью решения этой задачи на ЭВМ первых поколений.

При численном решении сложных математических задачи компьютер выполняет десятки тысяч и даже миллионы арифметических операций. Например, при решении системы линейных алгебраической уравнений методом Гаусса число операций пропорционально N^3 , где N — порядок системы. На практике встречаются системы алгебраических уравнений, порядок которых имеет величину 10^3–10^4. Все это выдвинуло на первый план проблемы возникновения, распространения вычислительных погрешностей и их оценки.

В работе [1] приводятся основные правила определения погрешностей при выполнении элементарных арифметических вычислений. Однако, следует заметить, что их трудно формализовать и использовать при многократно повторяющихся вычислениях. Поэтому возникла необходимость создания правил и алгоритмов, по которым можно было бы проводить округления и вычисления погрешностей на компьютере, т.е. создание некоторой новой «компьютерной арифметики», так называемой интервальной математики [2, 3, 4].

В качестве основного объекта этой математической теории выступает вещественный интервал. Введенные правила арифметических действий на множестве интервалов качественно отличаются от традиционной арифметики вещественных чисел. Интервальная математика представляет большой научный и методический интерес для современной общеобразовательной школы. С одной стороны, она позволяет по-новому взглянуть на многие традиционные решенные задачи и проблемы, с другой стороны является образцом красивой, стройной математической теории. Её изложение вызывает большой интерес у школьников.

Заметим, что интервальная математика может служить источником тем научно-исследовательских работ по математике для школьников.

Предлагаемая статья состоит из трех частей. В первой части статьи приводится изложение некоторых основ интервальной арифметики, сопровождаемое примерами. Во второй части показано, как методы интервальной математики могут использоваться при определении погрешностей вычисления. Третья часть работы посвящена применению методов интервальной математики к решению задач с параметрами.

1. Вещественная интервальная арифметика

В качестве основных объектов исследования будем рассматривать замкнутые вещественные интервалы[1], или в дальнейшем просто интервалы, следующего вида

$$A = [a_1; a_2] = \{t \,|\, a_1 \leqslant t \leqslant a_2,\ a_1, a_2 \in R\}.$$

Множество замкнутых вещественных интервалов обозначим через $I(R)$, а элементы этого множества будем обозначать прописными буквами. Заметим, что любое вещественное число $x \in R$ может быть представлено в виде точечного интервала $X = [x; x] \in I(R)$.

Примером таких интервалов могут служить значения, получаемые при измерениях физических величин. Длина крышки стола $l = 2 \pm 0,005$ м может быть представлена в виде интервала $L = [1,995; 2,005]$. Любое вещественное число в компьютере представляется в виде $a = \bar{a} \pm \varepsilon$, т.е. его можно записать в виде интервала $A = [\bar{a} - \varepsilon; \bar{a} + \varepsilon]$, ε определяется величиной разрядной сетки используемого типа переменной для записи числа. Например, в языке Паскаль переменная вещественного типа, описанная как Real, содержит 11–12 знаков.

Введем некоторые определения и основные правила действий с интервалами.

Определение 1. Два интервала $A = [a_1; a_2]$ и $B = [b_1; b_2]$ называются равными, если они равны в теоретико-множественном смысле ($A = B \ \Leftrightarrow \ a_1 = b_1,\ a_2 = b_2$).

Отношение равенства симметрично ($A = B \ \Rightarrow \ B = A$), транзитивно ($A = B$ и $B = C \ \Rightarrow \ A = C$) и, следовательно, рефлексивно ($A = A$).

[1] В отечественной математической литературе под интервалом понимают открытое множество вещественных чисел, а замкнутое множество называется сегментом [5]. Для сохранения общепринятого изложения интервальной математики в дальнейшем будем использовать введенный термин.

Определение 2. Пусть $* \in \{+, -, \cdot, :\}$ — бинарная операция на множестве вещественных чисел. Если $A, B \in I(R)$, то $A * B = \{z = a * b | a \in A, b \in B\}$ определяет бинарную операцию на $I(R)$.

Заметим, что здесь и в дальнейшем предполагаем, что при делении $0 \notin B$.

Запишем формулы, определяющие бинарные операции.

1. $A + B = [a_1 + b_1; a_2 + b_2]$
2. $A - B = [a_1 - b_2; a_2 - b_1] = A + (-1; -1)B$
3. $A \cdot B = \left[\min\{a_1b_1, a_1b_2, a_2b_1, a_2b_2\};\ \max\{a_1b_1, a_1b_2, a_2b_1, a_2b_2\}\right]$
4. $A : B = [a_1; a_2] \cdot [\frac{1}{b_2}; \frac{1}{b_1}]$.

Результат операции $z = x * y$, где $* \in \{+, -, \cdot, :\}$ — непрерывная функция на компактном множестве, т.е. z принимает все значения от минимального до максимального значения. Следовательно, множество значений этой функции образуют замкнутый вещественный интервал.

Приведем конкретные примеры выполнения арифметических операций над интервалами.

1) $[-1; 1] + [2; 3] = [1; 4]$; $\qquad [-1; 1] + [-1; 1] = [-2; 2]$;

2) $[2; 3] - [1; 2] = [0; 2]$; $\qquad [-1; 1] - [2; 3] = [-4; -1]$;

3) $[-1; 1] \cdot [2; 3] = \left[\min(-2,\ 2,\ -3,\ 3); \max(-2,\ 2,\ -3,\ 3)\right] = [-3; 3]$;

$[2; 3] \cdot [4; 5] = [8; 15]$;

4) $[-1; 1]/[2; 3] = [-1; 1] \cdot \left[\frac{1}{3}; \frac{1}{2}\right] = \left[-\frac{1}{2}; \frac{1}{2}\right]$; $\qquad [2; 3]/[1; 2] = [2; 3] \cdot \left[\frac{1}{2}; 1\right] = [1; 3]$.

Введем унарные операции над интервалами.

Определение 3. Если $r(x)$ — непрерывная унарная операция на R, то $r(X) = [\min\limits_{x \in X} r(x); \max\limits_{x \in X} r(x)]$ определяет унарную операцию на $I(R)$.

Примером такой унарной операции могут служить функции e^x, $\ln x$, $\sin x$, $\cos x$.

Примеры.

$X = [-1; 1] \Rightarrow Y = \exp(X) \approx [0,36788; 2,7183]$,

$X = [0; 1] \Rightarrow Y = \sin(X) \approx [0; 0,84147]$

Приведем наиболее важные свойства операций над интервалами.

Пусть $A, B, C, X, Y \in I(R)$

1. $A + B = B + A$, $\quad AB = BA$ (коммутативность)
2. $(A + B) + C = A + (B + C)$, $\quad (AB)C = A(BC)$ (ассоциативность).
3. $X = [0; 0]$, $\ Y = [1; 1]$ — единственные нейтральные элементы сложения и умножения:

$A = X + A = A + X$, $\quad A = Y \cdot A = A \cdot Y$.

4. Произвольный элемент множества $I(R)$ не имеет обратного элемента ни по сложению, ни по умножению. Тем не менее $0 \in A - A$ и $1 \in A : A$, $0 \notin A$.

Покажем это на примерах:

$$[-1; 1] - [-1; 1] = [-2; 2], \quad 0 \in [-2; 2];$$

$$[2;3]/[2;3] = [2;3] \cdot \left[\frac{1}{3};\frac{1}{2}\right] = \left[\frac{2}{3};\frac{3}{2}\right], \quad 1 \in \left[\frac{2}{3};\frac{3}{2}\right].$$

5. $A(B+C) \subset AB + AC$ (субдистрибутивность),
$a(B+C) = aB + aC, \quad a \in R,$
$A(B+C) = AB + AC$ (дистрибутивность), где $bc \geqslant 0$ для всех $b \in B$ и $c \in C$.

Доказательство этих утверждений может быть проведено непосредственно вычислением правых и левых частей выражений. В качестве примера приведем доказательство коммутативности сложения

$$A + B = \{z = a + b | \, a \in A, \; b \in B\} = \{z = b + a | \, b \in B, a \in A\} = B + A.$$

Не останавливаясь на доказательстве всех тождеств, покажем на примере необходимость условия ($bc \geqslant 0$, $b \in B$, $c \in C$) в законе дистрибутивности.

Пусть $A[0;1]$, $B[1;1]$, $C[-1;-1]$ — заданные интервалы $A \cdot B = [0;1] \cdot [1;1] = [0;1]$, $A \cdot C = [0;1] \cdot [-1;-1] = \quad = [-1;0]$, $A \cdot B + A \cdot C = [-1;1]$, но $A(B+C) = [0,0] \subset [-1;1] = AB + AC$.

Введенные арифметические правила позволяют по-новому поставить вопрос о разрешимости простейших интервальных уравнений. Например, уравнение

$$A + X = B \tag{1}$$

не эквивалентно уравнению

$$X = B - A. \tag{2}$$

Запишем уравнение (1) в развернутой форме и приведем его решение

$$[a_1;a_2] + [x_1;x_2] = [b_1;b_2] \;\Rightarrow\; [a_1 + x_1; a_2 + x_2] = [b_1;b_2] \;\Rightarrow\; X_1 = [b_1 - a_1; b_2 - a_2].$$

Аналогично запишем уравнение (2)

$$[x_1;x_2] = [b_1;b_2] - [a_1;a_2] \;\Rightarrow\; X_2 = [b_1 - a_2; b_2 - a_1].$$

Можно видеть, что $X_1 \subseteq X_2$.

Покажем вышеприведенные свойства на численном примере:

$$[1;2] + [x_1;x_2] = [2;4] \;\Rightarrow\; X_1 = [1;2].$$

$$X_2 = [2;4] - [1;2] = [0;3].$$

Рассмотрим решение другого уравнения

$$A \cdot X = B, \tag{3}$$

где $A \neq [0;0]$, $X \in I(R)$.

Введем вспомогательную функцию χ:

$$\chi = \begin{cases} a_1/a_2, & |a_1| \leqslant |a_2|, \\ a_2/a_1, & |a_1| > |a_2|. \end{cases}$$

Справедлива следующая теорема: уравнение $A \cdot X = B$ разрешимо относительно X из $I(R)$ тогда и только тогда, когда $\chi(A) \geqslant \chi(B)$.

Решение не единственно лишь в случае $\chi(A) = \chi(B) \leqslant 0$.

Проиллюстрируем теорему и утверждение на примерах.

Пример 1. Решить уравнение $[1;2] \cdot X = [1;3]$.

Можно видеть, что условия теоремы выполняются: $\chi(A) = \frac{1}{2} \geqslant \chi(B) = \frac{1}{3}$. Интервал B шире интервала A.

Согласно правилу умножения для уравнения (3), можно записать

$$\min(a_1x_1, a_1x_2, a_2x_1, a_2x_2) = b_1 \quad \max(a_1x_1, a_1x_2, a_2x_1, a_2x_2) = b_2,$$

или

$$\min(x_1, x_2, 2x_1, 2x_2) = 1, \quad \max(x_1, x_2, 2x_1, 2x_2) = 3.$$

Полагая $x_1 < x_2$, получим $X = \left[1; \frac{3}{2}\right]$.

Заметим, что уравнение

$$X = \frac{B}{A} \tag{4}$$

не эквивалентно уравнению (3). Решение уравнения (4)

$$X_1 = \frac{[1;3]}{[1;2]} = \left[\frac{1}{2}; 3\right]$$

содержит в себе интервальное решение уравнения (3).

Пример 2. Решить уравнение $[1;3] \cdot X = [2;6]$.

Условие теоремы выполнено: $\chi(A) = \chi(B) = \frac{1}{3}$. Запишем условие для определения интервала X

$$\min(x_1, x_2, 3x_1, 3x_2) = 2, \qquad \max(x_1, x_2, 3x_1, 3x_2) = 6.$$

Отсюда следует: $x_1 = 2, \quad x_2 = 2$, т.е. решение уравнения — точечный интервал $X = [2;2]$.

Пример 3. Решить уравнение $[1;3] \cdot X = [1;2]$.

Условия теоремы нарушены: $\chi(A) = \frac{1}{3} \leqslant \chi(B) = \frac{1}{2}$. По аналогии с предыдущим примером запишем

$$\min(x_1, x_2, 3x_1, 3x_2) = 1, \qquad \max(x_1, x_2, 3x_1, 3x_2) = 2.$$

Вновь полагая $x_1 < x_2$, из приведенных уравнений получим противоречие этому условию: $x_1 = 1, \ x_2 = \frac{2}{3}$, т.е. не существует интервала X, удовлетворяющего исходному уравнению.

Заметим, что уравнение, записанное в виде (4), решение имеет: $X_1 = \frac{[1;2]}{[1;3]} = \left[\frac{1}{3}; 6\right]$. С другой стороны, уравнение (3) может иметь решение, даже если B/A не определено, т.е. $0 \in A$.

Примером может служить уравнение $\left[-\frac{1}{3}; 1\right] \cdot X = [-1;2]$. Решение этого уравнения имеет вид $X = [-1;2]$.

Пример 4. Решить уравнение $[-1;3]\cdot X=[-2;6]$.

Условие теоремы не выполнено: $\chi(A)=\chi(B)=-\frac{1}{3}\leqslant 0$. Для границ интервалов запишем

$$\min(-x_1,\ -x_2,\ 3x_1,\ 3x_2)=-2,\quad \max(x_1,\ x_2,\ 3x_1,\ 3x_2)=6.$$

Отсюда следует $-x_2=-2,\quad 3x_2=6\Rightarrow x_2=2$, а $x_1=\alpha$, α — любое вещественное число меньше двух $\alpha<2$. Решение уравнения неоднозначно.

Рассмотрим связь уравнений (3), (4) и их решений с уравнением в вещественных числах

$$ax=b,$$

где $a\in A,\ b\in B$.

Все решения этого уравнения принадлежат интервалу

$$\bar{X}=\{x=b/a|\ a\in[a_1;a_2],\ b\in[b_1;b_2]\}=[a_1;a_2]/[b_1;b_2],$$

который совпадает с решением уравнения (4) и включает в себя интервал X, являющийся решением уравнения (3), т.е. $X\subseteq\bar{X}=B/A$.

Покажем это на уравнении, приведенном в первом примере.

$$[1;2]\cdot X=[1;3].$$

Пусть $a\in[1;2],\ b\in[1;3]$, тогда $\bar{X}=\{x=b/a|\ a\in[1;2],\ b\in[1;3]\}=[1;3]/[1;2]=$ $=\left[\frac{1}{2};3\right]$. Очевидно, что интервал $X=\left[1;\frac{3}{2}\right]\subset\bar{X}=\left[\frac{1}{2};3\right]$, а интервал $X_1=\bar{X}$.

Одно из основных свойств интервальных вычислений — монотонность включения интервалов.

Теорема 1. Пусть $A^{(k)},\ B^{(k)}\in I(R),\ k=1,2$, и предполагается, что

$$A^{(k)}\subseteq B^{(k)},\quad k=1,2.$$

Тогда для любой бинарной операции $*$ из $\{+,\ -,\ \cdot,\ :\}$ имеем

$$A^{(1)}*A^{(2)}\subseteq B^{(1)}*B^{(2)}.$$

Доказательство.

$$A^{(1)}*A^{(2)}=\{z=x*y|\ x\in A^{(1)},\ y\in A^{(2)}\}\subseteq\{w=u*v|\ u\in B^{(1)},\ v\in B^{(2)}\}=B^{(1)}*B^{(2)}.$$

Следствие. Пусть $A,\ B\in I(R)$ и $a\in A,\ b\in B$. Тогда $a*b\in A*B$, где $*\in\{+,\ -,\ \cdot,\ :\}$.

Заметим, что унарные операции $r(X)$ обладают сходными свойствами:

$$X\subseteq Y\ \Rightarrow\ r(X)\subseteq r(Y),\qquad x\in X\ \Rightarrow\ r(x)\in r(X).$$

На множестве вещественных интервалов может быть введено понятие расстояния между двумя интервалами, т.е. введена метрика.

Определение 4. Расстояние $q(A,B)$ между двумя интервалами A и B ($A = \quad = [a_1;a_2]$, $B=[b_1;b_2] \in I(R)$) определим равенством

$$q(A,B)=\max\{|a_1-b_1|,\ |a_2-b_2|\}.$$

Это отображение задает на $I(R)$ метрику. Действительно,

1. $q(A,B)\geqslant 0$,
2. $q(A,B)=0 \Leftrightarrow A=B$,
3. $q(A,B)=q(A,B)$,
4. $q(A,B)\leqslant q(A,C)+q(B,C)$.

Если применить введенное таким способом расстояние к точечным интервалам, то оно сведется к обычному расстоянию между вещественными числами, т.е.

$$q([a;a],[b;b])=|a-b|.$$

Введение на множестве $I(R)$ метрики превращает его в топологическое пространство. При этом понятия сходимости и непрерывности могут использоваться обычным образом, как и в случае любого метрического пространства.

Для сходящейся последовательности интервалов $A^{(k)}$ можно записать

$$\lim_{k\to\infty} A^{(k)}=A \Leftrightarrow (\lim_{k\to\infty} a_1^{(k)}=a_1, \lim_{k\to\infty} a_2^{(k)}=a_2).$$

Теорема 2. Метрическое пространство $(I(R),q)$ с метрикой из определения 4 является полным замкнутым метрическим пространством.

Теорема 3. Введенные операции сложения, вычитания, умножения и деления интервалов непрерывны.

Доказательства. Приведем доказательство для операции сложения.

Пусть $\left\{A^{(k)}\right\}_{k=0}^{\infty}$ и $\left\{B^{(k)}\right\}_{k=0}^{\infty}$ — две последовательности интервалов, причем $\lim\limits_{k\to\infty} A^{(k)}=A$ и $\lim\limits_{k\to\infty} B^{(k)}=B$.

$$\lim_{k\to\infty}(A^{(k)}+B^{(k)})=\lim_{k\to\infty}[a_1^{(k)}+b_1^{(k)};a_2^{(k)}+b_2^{(k)}]=$$

$$=[\lim_{k\to\infty}(a_1^{(k)}+b_1^{(k)});\lim_{k\to\infty}(a_2^{(k)}+b_2^{(k)})]=[a_1+b_1;a_2+b_2]=A+B.$$

Для унарных операций можно записать следующую теорему.

Теорема 5. Пусть $r(X)$ — непрерывная функция и $r(X)=[\min\limits_{x\in X} r(X);\max\limits_{x\in X} r(X)]$. Тогда $r(X)$ — непрерывное интервальное выражение.

Введем понятие абсолютной величины интервала.

Определение 5. Абсолютной величиной интервала будем называть величину

$$|A|=q(A,[0;0])=\max\{|a_1|,|a_2|\}.$$

Абсолютную величину интервала можно записать и в другом виде $|A|=\max\limits_{a\in A}|a|$.

Приведем некоторые свойства, связанные с метрикой.

Пусть $A=[a_1;a_2]$, $B=[b_1;b_2]$, $C=[c_1;c_2]$, $D=[d_1;d_2]\in I(R)$.

1. $q(A+B,\ A+C) = q(B,C)$,
2. $q(A+B,\ C+D) \leqslant q(A,C) + q(B,D)$,
3. $q(A,B) \leqslant q(C,D) + q(A+C,\ B+D)$,
4. $q(aB, aC) = |a| q(B,C),\ a \in R$,
5. $q(AB, AC) \leqslant |A| q(B,C)$.

Докажем первое утверждение

$$q(A+B,\ A+C) = \max\{|a_1 + b_1 - (a_1 + c_1)|,\ |a_2 + b_2 - (a_2 + c_2)|\} =$$

$$= \max\{|b_1 - c_1|,\ |b_2 - c_2|\} = q(BC).$$

Чтобы можно было сравнивать интервалы, введем еще одно понятие, связанное с их измерением.

Определение 5. Длинной интервала $A = [a_1, a_2]$ будем называть

$$d(A) = a_2 - a_1 \geqslant 0.$$

Множество точечных интервалов можно описать как

$$\{A \in I(R) |\, d(A) = 0\}.$$

Из определения получим очевидные свойства

$$d(A) = \max_{a,b \in A} |a - b|\,,$$

$$A \subseteq B \ \Rightarrow\ d(A) \leqslant d(B), \qquad d(A \pm B) = d(A) \pm d(B).$$

Имеет место следующая теорема.

Теорема 6. Пусть A и B — вещественные интервалы из $I(R)$. Тогда

1. $d(AB) \leqslant d(A)|B| + |A| d(B)$,
2. $d(AB) \geqslant \max\{d(A)|B|,\ |A| d(B)\}$,
3. $d(aB) = |a| d(B),\ a \in R$,
4. $d(A^n) \leqslant n|A|^{n-1} d(A),\ n = 1, 2, \ldots,\ (A^n := A \cdot A \cdot \ldots \cdot A,\ n \text{ раз})$,
5. $d((X - x)^n) \leqslant 2(d(X))^n$, где $x \in X,\ n = 1, 2 \ldots$,
6. Если $C \in I(R),\ 0 \in C$, то $|C| \leqslant d(C) \leqslant 2|C|$.

Приведем доказательство первого утверждения.

$$d(AB) = \max_{\substack{a,a' \in A \\ b,b' \in B}} |ab - a'b'| = \max_{\substack{a,a' \in A \\ b,b' \in B}} |ab - ab' + ab' - a'b'| \leqslant$$

$$\leqslant \max_{\substack{a,a' \in A \\ b,b' \in B}} \{|a|\,|b - b'| + |b'|\,|a - a'|\} = \max_{a \in A} |a| \max_{b,b' \in B} |b - b'| + \max_{a,a' \in A} |a - a'| \max_{b' \in B} |b'| =$$

$$= d(A)|B| + |A| d(B).$$

Докажем утверждение 4 методом математической индукции. При $n = 1$ утверждение 4 обращается в равенство. Если неравенство выполняется для некоторого $n \geqslant 1$, то, используя первое свойство, для $n + 1$ получим

$$d(A^{n+1}) = d(A^n A) \leqslant d(A^n)|A| + |A^n| d(A) \leqslant n|A|^{n-1} d(A)|A| + |A|^n d(A) = (n+1)|A|^n d(A),$$

что и требовалось доказать.

Теорема 7. Пусть $A, B \in I(R)$, причем A — симметричный интервал, т.е. $A = -A$. Тогда имеют место следующие свойства:

$$AB = |B|A, \qquad d(AB) = |B|d(A).$$

Одна из основных задач интервальнои математики ставится следующим образом: оценить множество значений вещественной функции при изменении ее аргументов на некоторых интервалах.

Введем основные понятия, необходимые для этого.

Пусть дано аналитическое выражение функции $f(x; a^{(0)}, a^{(1)}, \ldots, a^{(m)})$. Будем предполагать, что все выражения составлены из операций и операндов, число которых конечно, и что эти выражения вычисляются в интервальной арифметике.

Запись

$$W(f, X; A^{(0)}, ..., A^{(m)}) = \{f(x; a^{(0)}, ..., a^{(m)}) \,|\, x \in X, a^{(k)} \in A^{(k)}, 0 \leqslant k \leqslant m\} =$$

$$= \left[\min_{\substack{x \in X \\ a^{(k)} \in A^{(k)} \\ 0 \leqslant k \leqslant m}} f(x; a^{(0)}, ..., a^{(m)}), \quad \max_{\substack{x \in X \\ a^{(k)} \in A^{(k)} \\ 0 \leqslant k \leqslant m}} f(x; a^{(0)}, ..., a^{(m)}) \right]$$

будет в дальнейшем обозначать диапазон изменения функции f, причем предполагается, что $x \in X$ и $a^{(k)} \in A^{(k)}$ не зависят друг от друга. Согласно этому определению, интервал $W(f, X; A^{(0)}, ..., A^{(m)})$ будет одним и тем же при любом аналитическом выражении для f.

Пример 3. Найти диапазон изменения функции $f(x, a) = \frac{ax}{1-x}$, $A = [0; 1]$, $X = [2; 3]$.

График функции $f(x, a)$ при $x > 1$ показан на рисунке 1.

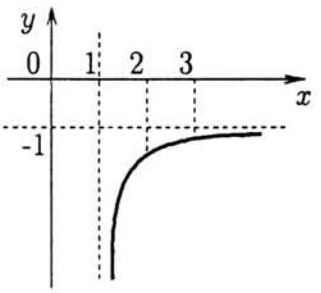


Рис. 1

Можно видеть, что минимальное значение функции будет при $x = 2$ $(f(x, a) = -2a)$, максимальное значение — при $x = 3$ $(f(x, a) = -\frac{3}{2}a)$. Следовательно, диапазон изменения функции может быть записан в виде:

$$W(f, [2; 3]; [0; 1]) = \{\frac{ax}{1-x} \mid 2 \leqslant x \leqslant 3,\ 0 \leqslant a \leqslant 1\} = [-2; 0].$$

Введем понятие интервального оценивания вещественной функции f. Пусть для f имеется аналитическое выражение. Заменив в этом выражении все вещественные операнды и операции над ними на интервальные операнды и операции, получим выражение $f(X; A^{(0)}, :, A^{(m)})$. Это выражение называется интервальной оценивающей функцией, или, для краткости, оценкой f. Очевидно, что результат оценивания функции f зависит от выбора для нее аналитического выражения.

Пример 4. Провести интервальное оценивание функции $f(x;a) = \frac{ax}{1-x}$, $A = [0;1]$, $X = [2;3]$.

$$f^{(1)}([2;3];[0;1]) = \frac{[0;1][2;3]}{1-[2;3]} = \frac{[0;3]}{[-1;-2]} = [0;3][-\frac{1}{1};-\frac{1}{2}] = [-3;0].$$

$$f^{(2)}(x;a) = \frac{a}{\frac{1}{x}-1}, \quad A = [0;1],\ X = [2;3].$$

$$f^{(2)}([2;3];[0;1]) = \frac{[0;1]}{\frac{1}{[2;3]}-1} = \frac{[0;1]}{\left[\frac{1}{3};\frac{1}{2}\right]-1} = \frac{[0;1]}{\left[-\frac{2}{3};-\frac{1}{2}\right]} = [0;1]\cdot\left[-\frac{3}{2};-\frac{2}{1}\right] = [-2;0].$$

Теорема 8. Пусть f — непрерывная вещественная функция. Предположим также, что для интервалов $Y^{(1)},\ldots,Y^{(n)}$, $B^{(0)},\ldots,B^{(m)}$ имеется оценка

$$f(Y^{(1)},\ldots,Y^{(n)},B^{(0)},\ldots,B^{(m)}).$$

Тогда для всех $X^{(k)} \subseteq Y^{(k)}$, $A^{(j)} \subseteq B(j)$, $1 \leqslant k \leqslant n$, $0 \leqslant j \leqslant m$ справедливо свойство включения

$$W(f,X^{(1)},\ldots,X^{(n)};A^{(0)},\ldots,A^{(m)}) \subseteq f(Y^{(1)},\ldots,Y^{(n)},B^{(0)},\ldots,B^{(m)}).$$

Заметим, что имеет место монотонность включения.

Пример 5. Показать свойство монотонности включения оценочных интервалов функции

$$f(x,a) = a - x/(1+x),\ x \neq -1,$$

$$X = \left[-\frac{1}{2};1\right] \subset Z = \left[-\frac{1}{2};2\right],\ A = [2;3].$$

Рассмотрев, как в примере 3 график функции $f(x,a)$, получим

$$W(f,X) = W\left(f,\left[-\frac{1}{2};1\right];[2;3]\right) = \left[\frac{3}{2};4\right] \subset f\left(\left[-\frac{1}{2};1\right];[2;3]\right) = [0;4].$$

$$W(f,Z) = W\left(f,\left[-\frac{1}{2};2\right];[2;3]\right) = \left[\frac{5}{2};4\right] \subset f\left(\left[-\frac{1}{2};2\right];[2;3]\right) = [-2;4].$$

$$W(f,X) \subset W(f,Z).$$

Покажем, как форма записи выражения, т.е. последовательность выполнения операций, влияет на интервальное оценивание функции.

Пример 6. Провести интервальное оценивание функции и сравнить с диапазоном ее изменения: $f(x) = x - x^2$, $X = [0;1]$.

Диапазон изменения функции

$$W(f,[0,1]) = \{x - x^2 | \, 0 \leqslant x \leqslant 1\} = [0, 1/4].$$

Различные варианты интервального оценивания функции.

$$f^{(0)}(x) = x - x^2 \Rightarrow f^{(0)}([0;1]) = [0;1] - [0;1] = [-1;1],$$

$$f^{(1)}(x) = x(1-x) \Rightarrow f^{(0)}([0;1]) = [0;1](1 - [0;1]) = [0;1],$$

$$f^{(2)}(x) = \frac{1}{4} - \left(x - \frac{1}{2}\right)\left(x - \frac{1}{2}\right) \Rightarrow$$

$$f^{(2)}([0;1]) = \frac{1}{4} - \left([0;1] - \frac{1}{2}\right)\left([0;1] - \frac{1}{2}\right) = \left[0; \frac{1}{2}\right],$$

$$f^{(3)}(x) = \frac{1}{4} - \left(x - \frac{1}{2}\right)^2 \Rightarrow$$

$$f^{(3)}([0;1]) = \frac{1}{4} - \left([0;1] - \frac{1}{2}\right)^2 = \left[0; \frac{1}{4}\right] = W\,(f,[0;1])\,.$$

В заключение приведем без доказательства две теоремы, связывающие величину интервала изменения функции и интервал изменения аргумента.

Теорема 9. Пусть f — вещественная функция от вещественного аргумента $x \in Y = [y_1; y_2]$, $f(x)$ — аналитическое выражение для f такое, что определено интервальное выражение $f(X)$. Будем считать, что для f выполняются условия Липшица. Тогда для $X \subseteq Y$ имеет место неравенство

$$d\,(f\,(X)) \leqslant c d\,(X)\,,\ c \geqslant 0,$$

Теорема 10. Пусть f — вещественная функция от вещественного аргумента x, дифференцируемая на интервале $X = [x_1, x_2]$ и пусть $f'(x)$ — аналитическое выражение для производной f' такое, что определено интервальное выражение $f'(X)$. Будем считать, что для f' выполняются условия Липшица, тогда

1. $W(f,X) \subseteq f(y) + f'(X) \cdot (X - y)$,
2. $q\,(W(f,X), f(y)) + f'(X)(X-y)) \leqslant c\,(d\,(X))^2$,

где $y \in X$ и константа $c \geqslant 0$.

Для более детального и глубокого ознакомления с интервальной математикой рекомендуем обратиться к работам [3,4].

2. Оценивание погрешности вычислений методами интервальной математики

В работе [1] описаны методы определения погрешностей при выполнении элементарных вычислений. Покажем, как методы интервальной математики позволяют получать эти же оценки погрешностей вычислений, но процедура получения более строго алгоритмизована.

Пусть $\bar{a}$ точное значение числа, a — приближенное значение. Абсолютная погрешность числа $\bar{a}$ обычно определяется в следующей форме $\Delta_a \geqslant |\bar{a} - a|$. Будем полагать, что $\Delta_a \ll a$.Число $\bar{a}$ можно записать в виде $\bar{a} = a \pm \Delta_a$. Следовательно, каждому числу $\bar{a}$ мы можем поставить в соответствие некоторый интервал $A = a + D_a$, здесь $D_a = [-\Delta_a; +\Delta_a]$ — интервал абсолютной погрешности.

При оценке качества измерений и вычислений используется понятие относительной погрешности $\delta_a = \frac{\Delta_a}{a} \ll 1$. В этом случае число может быть представлено в виде $\bar{a} = a(1 \pm \delta_a)$, или, переходя к интервальной форме представления погрешности, запишем $A = a(1 + E_a)$, $E_a = [-\delta_a; +\delta_a]$ — интервал относительной погрешности. Очевидно, что $D_a = a \cdot E_a$.

Запишем правила определения интервалов абсолютной погрешности при выполнении арифметических операций. Пусть вещественным числам $\bar{a}$ и $\bar{b}$ поставлены в соответствие интервалы $A = a + D_a$ и $B = b + D_b$. Будем полагать, что интервалы погрешностей малы, т.е. в дальнейшем будем пренебрегать их вторыми порядками.

Интервал абсолютной погрешности суммы запишется в виде

$$D_{a+b} = D_a + D_b.$$

Покажем, что это выражение соответствует известному представлению абсолютной погрешности суммы двух чисел

$$A + B = a + D_a + b + D_b = a + b + [-\Delta_a - \Delta_b; \Delta_a + \Delta_b] \Rightarrow$$

$$\bar{a} + \bar{b} = a + b \pm (\Delta_a + \Delta_b).$$

Интервал абсолютной погрешности разности двух чисел

$$D_{a-b} = D_a - D_b.$$

Покажем справедливость этого выражения

$$A - B = a + D_a - (b + D_b) = a - b + [-\Delta_a - \Delta_b; \Delta_a + \Delta_b] \Rightarrow$$

$$\bar{a} - \bar{b} = a - b \pm (\Delta_a + \Delta_b).$$

Интервал абсолютной погрешности произведения двух чисел может быть представлен в виде

$$D_{a \cdot b} = b \cdot D_a + a \cdot D_b.$$

При этом в силу относительной малости интервалов абсолютной погрешности пренебрегаем произведением $D_a \cdot D_b$.

$$A \cdot B = (a + D_a) \cdot (b + D_b) = a \cdot b + [-|b|\,\Delta_a - |a|\,\Delta_b; |b|\,\Delta_a + |a|\,\Delta_b] \Rightarrow$$

$$\bar{a} \cdot \bar{b} = ab \pm (|b|\,\Delta_a + |a|\,\Delta_b).$$

Интервал абсолютной погрешности частного

$$D_{a/b} = \frac{D_a}{|b|} + \frac{|a| \cdot D_b}{b^2}.$$

Это выражение, записано в предположении малости интервалов абсолютной погрешности. Покажем его справедливость

$$A/B = \frac{a + D_a}{b + D_b} = \frac{1}{b} \cdot (a + D_a) \cdot \left[\frac{1}{1 + \frac{\Delta_b}{b}}; \frac{1}{1 - \frac{\Delta_b}{b}}\right] = \frac{1}{b} \cdot (a + D_a) \cdot \left[1 - \frac{\Delta_b}{b}; 1 + \frac{\Delta_b}{b}\right] =$$

$$= \frac{1}{b} \cdot (a + D_a) \cdot \left(1 + \frac{D_b}{b}\right) = \frac{a}{b} + \frac{D_a}{|b|} + \frac{|a| \cdot D_b}{b^2} \Rightarrow$$

$$\frac{\bar{a}}{\bar{b}} = \frac{a}{b} \pm \left(\frac{\Delta_a}{|b|} + \frac{\Delta_b}{b^2}\right).$$

Запишем правила вычисления интервалов относительной погрешности.

$$E_{a+b} = \frac{|a|}{|a+b|} \cdot E_a + \frac{|b|}{|a+b|} \cdot E_b,$$

$$E_{a-b} = \frac{|a|}{|a-b|} \cdot E_a - \frac{|b|}{|a-b|} \cdot E_b,$$

$$E_{a \cdot b} = E_a + E_b,$$

$$E_{a/b} = E_a + E_b.$$

Заметим, что в выражениях абсолютной и относительной погрешности для разности двух чисел в интервальной записи знак сохраняется.

Как правило, при выполнении операций с вещественными числами результат округляется, т.е. возникает погрешность округления. Поскольку в настоящее время большинство вычислений проводится на компьютерах, то имеет смысл рассмотреть именно машинное округление.

Представление вещественных чисел в компьютере обладает рядом особенностей, связанных с его техническими возможностями. Одна из главных особенностей состоит в том, что множество вещественных чисел R_M, которые могут быть представлены в компьютере, конечно. Будем предполагать, что это множество симметрично относительно нуля, т.е. $R_M = -R_M$. Для аппроксимации вещественных чисел, лежащих в интервале $\left[\min\limits_{y \in R_M} y; \max\limits_{y \in R_M} y\right]$ используются машинные числа $\{\tilde{x}\,|\tilde{x} \in R_M\}$. Эта аппроксимация достигается с помощью отображения

$$fl : x \in R \to \tilde{x} = fl(x) \in R_M,$$

которое называется округлением, если выполнено свойство монотонности: $x \leqslant y \Rightarrow fl(x) \leqslant fl(y)$.

Особый интерес представляют так называемые направленные округления. Если для округления $\downarrow$ справедлива импликация $x \in R \Rightarrow \downarrow x \leqslant x$, то говорят, что имеет место округление вниз. Аналогично для округления вверх $-x \in R \Rightarrow \uparrow x \geqslant x$.

В соответствии с приведенным определением, вещественному интервалу ставится в соответствие некоторый машинный интервал, при этом нижняя граница вещественного интервала округляется вниз, а верхняя граница — вверх т.е. выполняется интервальное округление

$$X \in I(R) \rightarrow \updownarrow X = \updownarrow [x_1; x_2] = [\downarrow x_1; \uparrow x_2] \in I(R_M).$$

Здесь $I(R_M)$ — множество машинных интервалов.

Интервальное округление обладает следующими свойствами

$$X \in I(R),\ \updownarrow X \in I(R_M) \Rightarrow X \subseteq \updownarrow X,$$

$$X, Y \in I(R),\ \updownarrow X, \updownarrow Y \in I(R_M),\ X \subseteq Y \Rightarrow \updownarrow X \subseteq \updownarrow Y.$$

Если над двумя машинными числами x и y из R_M производится машинная операция, то ее результатом оказывается новое число, которое с учетом округления можно представить в виде $z = fl(x * y) \in R_M$. При этом мы не рассматриваем возможности переполнения. Определим машинные операции над интервалами.

Определение 6. Пусть $A, B \in I(R_M), * \in \{+, -, \cdot, /\}$, $\updownarrow$ — интервальное округление. Тогда результат операции $*$, выполненной над A и B с применением интервального округления есть

$$C = \updownarrow (A * B) \in I(R_M).$$

Для введенной машинной интервальной математики сохраняются все выше приведенные определения и теоремы.

Теорема 10. Для машинных интервальных операций справедливо следующее утверждение о монотонности включений

$$A^{(k)}, B^{(k)} \in I(R_M),\ A^{(k)} \subseteq B^{(k)},\ k = 1, 2, \Rightarrow$$

$$C^{(1)} = \updownarrow (A^{(1)} * A^{(2)}) \subseteq C^{(2)} = \updownarrow (B^{(1)} * B^{(2)}).$$

Отсюда следует

$$A, B \in I(R_M) \Rightarrow A * B \subseteq C = \updownarrow (A * B) \in I(R_M),$$

$$a \in A,\ b \in B \Rightarrow a * b \in C = \updownarrow (A * B) \in I(R_M).$$

Приведем теорему об оценке погрешностей округления.

Теорема 11. Если имеется округление fl, применение которого приводит к выполнению неравенства $\downarrow a \leqslant fl(a) \leqslant \uparrow a$, $a \in R$, то для $x, y, z \in R_M$ справедливо

$$z = fl(x * y) \in Z = \updownarrow ([x, x] * [y, y]) \in I(R_M).$$

Рассмотрим подробно, как осуществляется операция округления на компьютере. Любое действительное число представляется в компьютере в нормализованной форме в двоичной системе исчисления. Для удобства описания процедуры округления представим эти числа в десятичной системе исчисления в форме $y = f \cdot 10^n$. Пусть компьютер округляет числа до t значащих цифр. Число y перед округлением можно записать в следующем виде: $y = f_y \cdot 10^n + g_y \cdot 10^{n-t}$, где $0,1 \leqslant f_y < 1,0$ — мантисса оставляемого числа, она содержит t цифр, $0 \leqslant g_y < 1,0$ — округляемая часть числа. Абсолютная и относительная погрешности округления могут быть записаны в виде $\Delta_y = g_y \cdot 10^{n-t}$, $\delta_y = \frac{|g_y \cdot 10^{n-t}|}{|f_y \cdot 10^n|} = \frac{|g_y|}{|f_y|} \cdot 10^{-t}$. В современных компьютерах, как правило, осуществляется симметричная схема округления, т.е. $\Delta_y \leqslant 0,5 \cdot 10^{n-t}$, а

$$\delta_y \leqslant \frac{0,5 \cdot 10^{n-t}}{0,1 \cdot 10^n} = 5 \cdot 10^{-t} = 0,5 \cdot 10^{1-t}.$$

При $x = -2 \pm 0,1 \Rightarrow\updownarrow f(\updownarrow X) = -6 + [-0,51; 049] + 6 \cdot [-\delta; \delta]$.

Заметим, что относительная погрешность округления не зависит от числа y и является постоянной для каждого типа переменных, используемых при вычислении. (Для переменных, описанных в языке Паскаль как SINGLE $-\delta_y \leqslant 0,5 \cdot 10^{-6}$, EXTENDED $-\delta_y \leqslant 0,5 \cdot 10^{-18}$).

Как показано выше, при машинном округлении используется относительная погрешность, следовательно, машинный интервал, соответствующий вещественному числу a, запишется в виде

$$A = a + [-\Delta_a; \Delta_a] \Rightarrow\updownarrow A = a + [-\Delta_a - \delta_0 \cdot a; \Delta_a + \delta_0 \cdot a] \Rightarrow$$

$$\updownarrow A = a + D_a + a \cdot E_0.$$

Заметим, что, как правило, погрешность измерения больше погрешности вычислений $\Delta_a \gg \delta_0 \cdot a$.

Продемонстрируем вычисления погрешностей при выполнении последовательности операций на вышеприведенных примерах.

Пример 7. Вычислить значение функции $f(x) = x - x^2$, при $x = a \pm \varepsilon$.

Выполнение каждой операции сопровождается округлением с относительной погрешностью δ, $(E = [-\delta; \delta])$. Интервал изменения переменной x с учетом погрешности округления при его машинном представлении запишется в виде $\updownarrow X = a + [-\varepsilon - a \cdot \delta; \varepsilon + a \cdot \delta]$. Пренебрегая квадратичными членами, т.е. полагая, что $\varepsilon \gg \varepsilon^2$, $\varepsilon \cdot \delta, \delta^2$, для интервальной оценивающей функции получим

$$\updownarrow f(\updownarrow X) = \updownarrow X - (\updownarrow X^2 + a^2 \cdot E) + |a - a^2| \cdot E$$

или

$$\updownarrow f(\updownarrow X) = [a - \varepsilon, a + \varepsilon] - [a - \varepsilon, a + \varepsilon]^2 + a^2 \cdot [-\delta, \delta] + |a(1 - a)| \cdot [-\delta, \delta].$$

Преобразуя выражение согласно с введенными правилами при $a > 0$, получим

$$\updownarrow f(\updownarrow X) = \left[a - a^2 - \varepsilon \cdot (1 + 2a); a - a^2 + \varepsilon \cdot (1 + 2a)\right] + \left(a^2 + |a\,(1 - a)|\right) \cdot [-\delta; \delta].$$

Если $a < 0$, то

$$\updownarrow f(\updownarrow X) = \left[a - a^2 - \varepsilon \cdot (1 - 2a)\,; a - a^2 + \varepsilon \cdot (1 - 2a)\right] + \left(a^2 + |a\,(1 - a)|\right) \cdot [-\delta; \delta]\,.$$

Приведем значения интервалов при конкретных численных значениях x. При $x = 2 \pm 0,1 \Rightarrow \updownarrow f(\updownarrow X) = -2 + [-0,51; 049] + 6 \cdot [-\delta; \delta]$. Легко видеть, что исходная погрешность в результате вычислений существенно возрастает. Причем, поскольку исходное выражение не симметрично относительно нуля, то и погрешность изменяется не симметрично.

Предлагаемая вычислительная схема некорректна при a, близком к нулю или к единице, поскольку в этих случаях абсолютная погрешность вычислений будет сравнима с самой вычисляемой величиной.

Заметим также, что сравнение полученных интервалов с интервалами из примера 6 также не правомочно. Действительно, если $X = [0; 1]$, то в наших представлениях это соответствует $a = \frac{1}{2}$, $\varepsilon = \frac{1}{2}$ и ε нельзя считать малым числом.

Оценим диапазон изменения функции

$$W(f) = \left[\min_{x \in X} f(x); \max_{x \in X} f(x)\right], \quad X = [a - \varepsilon, a + \varepsilon]\,.$$

График функции $f(x)$ имеет следующий вид:

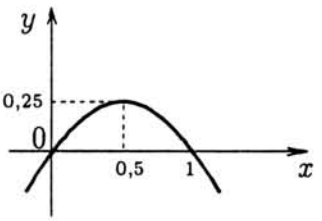


Рис. 2

Можно видеть, что если $a - \varepsilon < 0,5$, то минимум функции будет при $a + \varepsilon$, а максимум при $a - \varepsilon$.

$$W(f) = \left[a - a^2 + \varepsilon - 2a\varepsilon - \varepsilon^2; a - a^2 - \varepsilon + 2a\varepsilon - \varepsilon^2\right].$$

Если $0,5 \geqslant a - \varepsilon \geqslant 0$, то максимум функции будет при $a + \varepsilon$, а минимум при $a - \varepsilon$

$$W(f) = \left[a - a^2 - \varepsilon + 2a\varepsilon - \varepsilon^2; a - a^2 + \varepsilon - 2a\varepsilon - \varepsilon^2\right].$$

Если $0,5 \in X$, то наибольшее значение функции равно $f(0,5) = 0,25$, а минимум функции будет определяться расположением a относительно вершины параболы

$$W(f) = [\min(|f(a - \varepsilon)|\,, |f(a + \varepsilon)|); 0,25]\,.$$

Заметим, что $W(f) \subseteq \updownarrow f(\updownarrow X)$.

3. Применение методов интервальной математики для решения задач с параметрами

Один из наиболее трудных для понимания разделов школьной математики связан с решением задач с параметрами. Эти задачи часто встречаются на вступительных экзаменах. Интерес к ним со стороны предметных комиссий по математике обусловлен тем, что задачи с параметрами, как правило, допускают решение несколькими способами и позволяют выявить логические способности абитуриентов, уровень их математической культуры, умение находить решение в сложных нестандартных ситуациях.

Среди всего множества задач с параметрами можно выделить целый класс задач, которые формулируются в терминах интервальной математики и допускают решение ее методами[2]. Действительно, пусть имеется некоторое уравнение с параметром $F(x,a)=0$. Поставим следующую задачу: найти область изменения параметра a, при котором все решения уравнения принадлежат некоторому интервалу $x\in[x_1;x_2]$. Может быть сформулирована и обратная задача.

Рассмотрим ряд конкретных задач.

Задача 1. Найти интервал изменения положительного корня уравнения

$$x^2-2bx+c=0,$$

если $b\in[b_1;b_2]$, $c\in[c_1;c_2]$; здесь $b_1>0$.

Решение. Положительный корень уравнения определяется выражением

$$x=b+\sqrt{b^2-c}.$$

Подставляя в это выражение интервальные значения параметров, получим диапазон изменения x $(X=[x_1;x_2])$

$$X=[b_1;b_2]+\sqrt{[b_1;b_2]^2-[c_1;c_2]},$$

полагая, $b_1^2\geqslant c_2$, запишем

$$X=\left[b_1+\sqrt{b_1^2-c_2};b_2+\sqrt{b_2^2-c_1}\right].$$

Поставим обратную задачу. Например, найти область изменения параметра c при $b=1$ и $x\in X=[x_1;x_2]$. Из предыдущего выражения запишем

$$x_1=1+\sqrt{1-c_2},\ x_2=1+\sqrt{1-c_1}\Rightarrow$$

$$c_1=1-(x_2-1)^2,\ c_2=1-(x_1-1)^2.$$

Например, если $x\in[2;3]\Rightarrow c\in[-3;0]$.

Сформулируем типовую для многих приложений постановку задачи.

[2]Существует большое количество пособий по решению уравнений с параметрами методами элементарной математики, например, [6].

Задача 2. С какой точностью ε_2 должен быть измерен коэффициент c для того, чтобы положительный корень x был определен с точностью ε_0, если коэффициент b определен с точностью ε_1?

Решение. Для интервалов погрешностей можно записать

$$[x-\varepsilon_0; x+\varepsilon_0] = [b-\varepsilon_1; b+\varepsilon_1] + \sqrt{[b-\varepsilon_1; b+\varepsilon_1]^2 - [c-\varepsilon_2; c+\varepsilon_2]} \qquad (5)$$

или в соответствии с правилами интервальной математики, получим

$$[x-\varepsilon_0; x+\varepsilon_0] = [b-\varepsilon_1; b+\varepsilon_1] + \sqrt{b^2-c}\cdot\left[1-\frac{1}{2}\frac{2\varepsilon_1 b+\varepsilon_2}{b^2-c}; 1+\frac{1}{2}\frac{2\varepsilon_1 b+\varepsilon_2}{b^2-c}\right]. \qquad (6)$$

Отсюда следует: $\varepsilon_2 = 2(\varepsilon_0-\varepsilon_1)\sqrt{b^2-c} - 2\varepsilon_1 b$.

Запишем второе решение уравнения (6), перенося интервал $[b-\varepsilon_1; b+\varepsilon_1]$ в левую часть уравнения, получим

$$[x-\varepsilon_0; x+\varepsilon_0] - [b-\varepsilon_1; b+\varepsilon_1] = \sqrt{b^2-c}\cdot\left[1-\frac{1}{2}\frac{2\varepsilon_1 b+\varepsilon_2}{b^2-c}; 1+\frac{1}{2}\frac{2\varepsilon_1 b+\varepsilon_2}{b^2-c}\right] \Rightarrow$$

$$\Rightarrow\ \varepsilon_2 = 2(\varepsilon_0+\varepsilon_1)\sqrt{b^2-c} - 2\varepsilon_1 b.$$

Заметим, что, например, в физических исследованиях при экспериментальном определении коэффициентов уравнения налагают требование одинаковой точности определения всех его членов. При этом возникают завышенные требования к точности измерений коэффициентов по сравнению с точностью этих коэффициентов, определенных по конечной формуле решения. Действительно, если за основу определения погрешности коэффициента взять исходное квадратное уравнение, то можно поставить следующую задачу:

$$[c-\varepsilon_2; c+\varepsilon_2] = 2[b-\varepsilon_1; b+\varepsilon_1]\cdot[x-\varepsilon_0; x+\varepsilon_0] - [x-\varepsilon_0; x+\varepsilon_0]^2.$$

Для погрешности получим

$$\varepsilon_2 = 2\cdot(\varepsilon_0+\varepsilon_1)\cdot\left(b+\sqrt{b^2-c}\right) + 2\cdot\varepsilon_0 b.$$

Сравнивая полученные выражения ε_2, можно видеть, что последнее значение наибольшее.

Задача 3. (задача № 7.11 из [6].) При каких значениях параметра a неравенство

$$2 > |x+a| + x^2$$

имеет положительное решение?

Предложенной задаче сопоставим задачу в терминах интервальной математики. Рассмотрим функцию $f(x,a) = |x+a| + x^2$. Найти интервал изменения параметра a $A = [a_1; a_2]$, если $f \in [0;2], x \in [0;+\infty]$.

Из неравенства запишем $|[x_1+a_1; x_2+a_2]| + [x_1^2; x_2^2] = [f_1; f_2]$. Остановимся на особенностях записи функции модуля.

Если $x_1 + a_1 \geqslant 0$, то получим

$$x_1 + a_1 + x_1^2 = f_1,$$

$$x_2 + a_2 + x_2^2 = f_2.$$

Поскольку наименьшее значение $x = 0$, то максимальное значение параметра a равно $a_2 = f_2 = 2$. Минимальное значение параметра $a = 0$.

Если $x_2 + a_2 < 0$, то получим

$$-x_1 - a_1 + x_1^2 = f_2,$$

$$-x_2 - a_2 + x_2^2 = f_1.$$

Отсюда следует

$$-x_1 - f_2 + x_1^2 = a_1,$$

$$-x_2 - f_1 + x_2^2 = a_2.$$

Минимальное значение параметра будет при $x_1 = \frac{1}{2}$, $a_1 = -\frac{9}{4}$, максимальное значение параметра $a_2 = -\frac{1}{4}$.

Если $x_1 + a_1 < 0$, а $x_2 + a_2 \geqslant 0$, то значения параметра будут лежать в интервале $\left[-\frac{1}{4}; 0\right]$.

Объединяя полученные интервалы, получим $a \in \left[-\frac{9}{4}; 2\right]$. Соответсвенно, решение исходной задачи: $a \in \left(-\frac{9}{4}; 2\right)$.

Задача 4. (задача № 12.12 из [6].) При каких значениях параметра a неравенство

$$a\left(4 - \sin x\right)^4 - 3 + \cos^2 x + a > 0$$

справедливо при любых значениях x?

Решение. Запишем функцию, соответствующую данному неравенству

$$f(x, a) = a\left(4 - \sin x\right)^4 - 3 + \cos^2 x + a.$$

Заметим, что условие ее положительности означает, что интервал изменения представляется в виде

$$W\left(f, X; A\right) = \left[0; +\infty\right].$$

Учитывая

$$\cos^2 x \in \left[0; 1\right], \ \left(4 - \sin x\right)^4 \in \left[81; 625\right],$$

получим

$$f(X; A) = \left[a_1; a_2\right] \cdot \left[81; 625\right] - \left[3; 3\right] + \left[0; 1\right] + \left[a_1; a_2\right].$$

или

$$f(X; A) = \left[82 \cdot a_1 - 3; \ 626 \cdot a_2 - 2\right].$$

Сравнивая полученный интервал, с интервалом изменения функции и учитывая $W \subseteq f(X; A)$, запишем для нижней границы интервалов

$$82 \cdot a_1 - 3 = 0 \Rightarrow a_1 = \frac{3}{82}.$$

Следовательно, исходное неравенство будет выполняться для любых x при $a_1 > \frac{3}{82}$.

В заключение автор выражает благодарность доценту кафедры дифференциальных уравнений и математического анализа Чистякову Вячеславу за проявленный к работе интерес и ценные замечания.

Литература.

[1]. Ляхов А.Ф. Элементарная теория погрешностей. — Математическое образование, № 3-4, 1998, с.82-104.

[2]. А.Г. Яковлев. Интервальные вычисления — предмет исследования и полезный инструмент. — Сб. Интервальные вычисления. № 1, 1991, с.10-26.

[3]. Г. Алефельд, Ю. Херцбергер. Введение в интервальные вычисления. — М.:Мир, 1987, с.360.

[4]. Калмыков С.А., Шокина Ю.И., Юлдашев З.Х. Методы интервального анализа. — Новосибирск, Наука, 1986, с.224.

[5]. Математический энциклопедический словарь. — М.: «Сов. энциклопедия», 1988, с.847.

[6]. Амелькин В.В., Рабцевич В.Л. Задачи с параметрами. Справочное пособие по математике. — «Асар», 1996, с.464.

Ляхов Александр Федорович,
кандидат физико-математических наук
доцент кафедры теоретической механики ННГУ

603600 г. Н.Новгород,
проспект Ю.А. Гагарина, д. 23-а, ННГУ,
механико-математический факультет,
кафедра теоретической механики.

E-mail: Lyakhov@mm.unn.ac.ru

Вопросы высшей математики в русской школе до 1917 года

Р. З. Гушель

В подборке материалов по истории математического образования в России освещается вопрос внедрения элементов высшей математики в программу средних учебных заведений, как он рассматривался в конце XIX – начале XX века.

Вопрос о необходимости включения элементов высшей математики в курс отечественной средней школы имеет уже двухсотлетнюю историю. В программы мужских гимназий, открытых в соответствии с первым университетским Уставом 1804 года, входили и элементы аналитической геометрии, и элементы анализа бесконечно малых. Анализ был исключен из гимназической программы в 1819 году, аналитическая геометрия — в 1845.

Несмотря на исключение этих разделов с середины XIX столетия, вопрос о необходимости их возвращения в школу постоянно поднимался педагогами как средней, так и высшей школы. Активными борцами за введение элементов высшей математики в среднюю школу были, в частности, академики М. В. Остроградский (1801-1862), В. Я. Буняковский (1804-1889) и П. Л. Чебышев (1821-1894). Последний предложил в 1858 г. свой проект программы по математике, содержавший и некоторые вопросы анализа бесконечно малых, но этот проект был отклонен Министерством народного просвещения [1].

К концу XIX столетия движение за обновление содержания математического образования и введения в среднюю школу элементов анализа, аналитической геометрии и некоторых других разделов математики приняло в педагогической среде достаточно массовый характер, что отразилось, в том числе, и на тематике публикаций педагогических журналов.

В материалах Московского совещания 1899 года по вопросам о средней школе [2] и Трудах Высочайше учрежденной комиссии по вопросу об улучшениях в средней общеобразовательной школе (1900) [1], созванной по инициативе министра народного просвещения Н. П. Боголепова, эти вопросы также активно обсуждались. И в программу по математике, составленную подкомиссией во главе с Н. И. Билибиным, были включены некоторые вопросы высшей математики. Но убийство Н. П. Боголепова в 1901 году остановило работу по введению этой программы в школу.

Среди вопросов, которые обсуждались и на Московском совещании, и в комиссии Н. П. Боголепова, было право реалистов на продолжение образования в университете, право, которого они в то время были лишены. Было принято решение о введении в реальных училищах дополнительного восьмого класса с тем, чтобы его выпускников допустить в университет, на медицинский и физико-математический факультеты. Этот вопрос после 1901 года снят не был. Программа по математике разрабатывалась комиссией во главе с профессором С.-Петербургского университета К. А. Поссе (1847-1928). К 1905 году эта программа была составлена и в 1907/1908 учебном году введена [4]. (См. Приложение I.)

В течение десяти лет по этой программе работали все реальные училища, а с 1914 года — и коммерческие училища. В 1911 году близкая к этой программа была введена и в кадетских корпусах. Вопрос о соответствующих изменениях и в классических гимназиях много обсуждался, были составлены даже программы для гимназий, предусматривавшие фуркацию в старших классах и изучение в естественнонаучном отделении элементов высшей математики, но события 1917 года приостановили эту работу.

Анализируя программу дополнительного класса реальных училищ, видим, какие большие разделы по анализу и аналитической геометрии изучались в то время в средней школе. Многие из указанных здесь вопросов после 1917 года никогда в массовой школе не изучались. И по этой программе было написано много учебников, в том числе такими авторами, как А. П. Киселев, К. Н. Рашевский, Н. И. Билибин и другими. Вопросы методики обучения этим разделам стали предметом обсуждения и среди педагогов, и в печати. Современным педагогам было бы, на наш взгляд, полезно познакомиться с учебной и методической литературой того времени, чтобы использовать опыт прошлого в своей работе.

Ниже предлагаются (в сокращении) доклад преподавателя частной гимназии из С.-Петербурга Ф. В. Филипповича "Постановка преподавания начал анализа в средней школе", сделанный им на пленарном заседании Первого Всероссийского съезда преподавателей математики в декабре 1911 года, и статья профессора Харьковского университета Д. М. Синцова (1867-1946) "О преподавании аналитической геометрии в средней школе", опубликованная в журнале "Математическое образование" за 1914 год.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Метельский Н. В. Очерки истории методики математики. Минск, 1968.

2. Совещания, проходившие в 1899 году в Московском учебном округе по вопросам о средней школе. М., 1899. Вып. 1-6.

3. Труды Высочайше учрежденной комиссии по вопросу об улучшениях в средней общеобразовательной школе. СПб., 1900. Вып. 1-8.

4. Программа математики для дополнительного класса реальных училищ... от 30 июня 1906г. // Журнал Министерства народного просвещения. 1907. №1.

5. Труды I Всероссийского съезда преподавателей математики. СПб., 1913. Тт. 1-3.

6. Билибин Н. И. Основания анализа бесконечно малых. Для реальных училищ. СПб., 1907.

7. Горячев Д. Н. Основания аналитической геометрии на плоскости. М., 1908.

8. Горячев Д. Н. Основания анализа бесконечно малых. М.-Пг., 1923. Изд. 8 (Изд. 2 - 1908.).

9. Киселев А. П. Начала дифференциального и интегрального исчислений. М.-Пг., 1917. Изд.7.

10. Пенионжкевич К. Б. Основания анализа бесконечно малых. Для реальных училищ. Сумы, 1909.

11. Пенионжкевич К. Б. Основания аналитической геометрии. СПб., 1911.

12. Рашевский К. Н. Основания аналитической геометрии. М., 1911. Изд. 3.

13. Рашевский К. Н. Основания анализа бесконечно малых. Для реальных училищ. М., 1913.

14. Попруженко М. Г. Материалы по методике анализа бесконечно малых в средней школе. СПБ., 1912. 91с.

Приложение I. Программа математики для дополнительного класса реальных училищ, утвержденная министерством народного просвещения и подлежащая введению в действие, на основании циркулярного предложения министерства народного просвещения от 30 июня 1906 г. №12414, с 1907-1908 учебного года

Журнал Министерства народного просвещения. 1907. №1.

I. АРИФМЕТИКА

Основные теоремы о делимости чисел. Общий наибольший делитель двух целых чисел. Решение неопределенных уравнений 1-ой степени с двумя неизвестными в числах целых и положительных.

II. АЛГЕБРА

Комплексные числа. Действия над ними: сложение, вычитание, умножение, деление, возвышение в степень (бином Ньютона) и извлечение квадратного корня.

Основные свойства целой функции и ее корней. Частные случаи: функция $x^n - a^n$ и функция $ax^{2p} + bx^p + c$.

Посторонние решения. Исследование уравнений I степени с одною неизвестною и системы двух уравнений I степени с двумя неизвестными. Случаи неопределенности и несовместимости.

III. ТРИГОНОМЕТРИЯ

Тригонометрические (круговые) функции дуги. Изменения значений тригонометрических функций при изменении дуги (аргумента) от $-\infty$ до $+\infty$.

Формулы приведения тригонометрических функций какой ни есть дуги к тригонометрическим функциям дуги, заключенной между 0 и $\pi/4$. Соотношения между тригонометрическими функциями одной и той же дуги.

Теорема сложения (тригонометрические функции суммы и разности дуг). Тригонометрические функции кратной дуги и половины дуги.

Представление суммы и разности синусов и косинусов в виде произведений. Понятие об обратных круговых функциях. Тригонометрические уравнения.

Неравенства $\sin x < x < \operatorname{tg} x$ и $x - sinx < x^3/4$ для дуг, заключенных между 0 и $\pi/2$, и вытекающая из этих неравенств возможность приближенного вычисления тригонометрических функций.

IV. ОСНОВАНИЯ АНАЛИТИЧЕСКОЙ ГЕОМЕТРИИ

Определение положения точки на плоскости прямоугольными координатами. Расстояние двух точек, выраженное в прямоугольных координатах их. Выражение прямоугольных координат средины прямоугольного отрезка через координаты его концов.

Прямая. Различные виды уравнения прямой: 1) уравнение, решенное относительно одной из координат; 2) уравнение, содержащее отрезки осей координат; 3) нормальное уравнение прямой и 4) общее уравнение I степени. Уравнение прямой, проходящей через данную точку. Уравнение прямой, проходящей через две данные точки. Координаты точки пересечения двух данных прямых. Угол между двумя прямыми; условия их параллельности и перпендикулярности. Расстояние точки от прямой. Выражение площади треугольника.

Пересечение начала координат.

Круг. Его уравнение в прямоугольных координатах.

Полярные координаты. Архимедова спираль. Общая идея координат и геометрических мест.

Сечение поверхности прямого кругового конуса плоскостями, не проходящими через вершину. Три типа сечений: эллипс, парабола, гипербола. Характеристическое свойство их, выражающееся в постоянстве отношения расстояний каждой точки их от фокуса и директрисы. Уравнения в полярных координатах. Уравнения в прямоугольных координатах, отнесенные к вершине. Уравнения эллипса и гиперболы, отнесенные к центру и осям. Эллипс как проекция круга. Уравнения эллипса и гиперболы в биполярных координатах. Уравнение касательной в данной точке кривой. Диаметры эллипса, гиперболы и параболы.

V. ОСНОВАНИЯ АНАЛИЗА БЕСКОНЕЧНО МАЛЫХ.

Основания учения о пределах. Приложение учения о пределах к измерению длины окружности, площади круга, поверхностей и объемов цилиндра, конуса и шара. Предел отношения $\frac{\sin x}{x}$ при стремлении x к нулю. Предел бинома $(1+1/n)^n$ при неограниченном возрастании n. Натуральная система логарифмов. Модуль.

Переменная независимая (аргумент) и зависимая (функция). Явная и неявная функция. Непрерывное изменение аргумента. Понятие о непрерывности функции для данного значения аргумента и для данной области аргумента. Примеры

непрерывных функций; функция a^x. Геометрическое представление функций.

Понятие о производной и дифференциале функции. Геометрическое и механическое значение производной.

Производные суммы, разности, произведения и частного.

Производные и дифференциал сложной функции. Производная обратной функции.

Производные функций: степенной, показательной, логарифмической и тригонометрических.

Геометрическое представление свойства непрерывной функции: "если функция непрерывна в некоторой области аргумента и на границах этой области имеет противоположные знаки, то она обращается в нуль внутри этой области".

Геометрическое представление теоремы Ролля; теорема Лагранжа.

Признаки возрастания и убывания функций. Наибольшие и наименьшие значения функций для данной области аргумента; их разыскание.

Уравнение касательной и нормали к данной кривой в данной точке; касательная к эллипсу, гиперболе и параболе.

Понятие об определенном интеграле. Приложение к определению площадей. Понятие о неопределенном интеграле.

Приложение II. Ф. В. Филиппович. Постановка преподавания начал анализа в средней школе

Труды I-го Всероссийского Съезда Преподавателей математики. СПб., 1913. Т.I. (Перепечатано со значительными сокращениями)

Наглядно-лабораторное обучение, графика, функциональное мышление и начала дифференциального и интегрального исчисления призваны реформировать традиционное преподавание математики, как в отношении содержания, так и в отношении методов.

Так как возражения противников реформы обучения математике, между прочим, сводятся к сомнениям и даже к отрицаниям того, чтобы высшую математику можно было отнести к предметам общего образования, то я позволю себе, по мере возможности, рассмотреть этот вопрос в своем докладе.

Необходимость введения анализа бесконечно малых в среднюю школу вытекает:

А) из тенденции сближения науки со школой.

В самом деле, из истории преподавания нам известно, что развитие науки всегда, хотя и с большими опозданиями, вносит свой корректив в школьные программы. Но для того, чтобы провести реформу, необходима подготовительная работа обмена мнений, необходима суровая критика традиционного обучения математике.

За последние десятилетия со стороны науки идут нападки на современное обучение математике. Представители научного мира (Ф. Клейн, Пуанкаре, Борель,

Таннери и др.) горячо нападают на отсталость школьной математики от науки. Действительно, средняя школа игнорирует почти все развитие математики, начиная с XVII столетия. Из всего богатства методов, внесенных в европейскую науку со времен эпохи Возрождения, только логарифмы получили право гражданства. Таким образом, курс алгебры в наших гимназиях заканчивается математическими открытиями начала XVII столетия. Так как, по взглядам новой педагогики, одна из задач общего образования есть "способность понимать все наше культурное развитие", то, очевидно, что такая цель не может быть достигнута без расширения математических знаний.

Итак, учащихся не следует искусственно задерживать на средневековом уровне математики, и тогда мы успеем их познакомить с великими открытиями творцов европейской математики; труды Декарта, Лейбница и Ньютона им будут известны хотя бы в самых общих чертах.

B) Начала дифференциального и интегрального исчислений должны быть призваны освежить школьную математику также и соответственно запросам жизни. Химию, физику, технику, страховое дело и прочее можно понять лишь в слабой степени, если не иметь хотя бы незначительных сведений из области высшей математики. Но если мы желаем проникнуть глубже в тайны вышеупомянутых наук, то мы непременно должны воспользоваться орудием анализа бесконечно малых. По словам проф. Дж. В. А. Юнга, "исчисление бесконечно малых есть учение об изменениях и может быть названо, в строгом смысле слова, математикой природы". Вообще, без высшей математики явления природы вполне понятны быть не могут. Стало быть, начала дифференциального и интегрального исчислений должны войти в общеобразовательный курс средней школы, ибо они дают нам великолепное орудие в руки, чтобы удовлетворять запросам жизни.

C) И соображения общепедагогического характера говорят в пользу введения анализа бесконечно малых в среднюю школу. Этот новый отдел возбуждает в высшей степени интерес у учащихся к изучению математики. А интерес есть критерий пригодности той или другой части курса математики. Ключ настоящей реформы есть интерес. И поэтому курс математики должен быть предложен ученикам в наиболее интересной для них форме.

Кроме того, в курсе исчисления бесконечно малых и формальная цель будет хорошо представлена. Здесь лучше всего подчеркивается всемогущество математического метода. Математика является как бы отвлеченной формой естествознания, и в данном случае она, действительно, дисциплинирует мышление наших учеников, дает драгоценный материал для упражнения в строго-логическом мышлении. А это как раз соответствует новым взглядам на преподавание математики, т.е. тому, чтобы в старших классах средней школы преобладали логические тенденции. Следовательно, ценность начал исчисления бесконечно малых коренится в том, что они являются воплощением действительно существующих соотношений, связывают реальный мир с математическим.

В связи с введением анализа бесконечно малых в среднюю школу возникают разногласия по поводу построения самого курса. Новые французские учебные планы, "Меранская" программа в Германии и др. настаивают на введении идеи

функциональной зависимости. Реформаторы всех направлений присоединяются к этому требованию. Действительно, объяснить какое-нибудь явление в природе — это значит выяснить его генезис и связь с другими явлениями. В виду этого лучше всего развивать идею функциональной зависимости в математике. Учение о функциях есть центральное учение всей математики, потому что функциональная зависимость есть математическое выражение великого закона изменяемости соотношения всех явлений; установление ее есть сущность и конечная цель всей науки. Поэтому мы, сторонники реформы, требуем, чтобы весь курс математики был сконцентрирован около идеи функциональной зависимости и расширен первоначальными понятиями анализа бесконечно малых. Начала дифференциального и интегрального исчислений не должны составлять самостоятельного отдела — "учения о функциях" — и являться какой-то "надстройкой" над школьным курсом так называемой элементарной математики.

Еще до начала анализа бесконечно малых должны мы подготовлять почву для ясного, отчетливого и возбуждающего новые идеи преподавания элементов дифференциального и интегрального исчислений. Еще с младших классов средней школы следует проводить красной нитью в течение всего курса школьной математики идею функциональной зависимости. В этом-то и заключается точное понимание аналитической геометрии и начал дифференциального и интегрального исчислений.

Целью преподавания высшей математики в средней школе ни в коем случае не должно быть только усвоение механизма, техники дифференцирования и интегрирования. При такой методе начала дифференциального и интегрального исчислений потеряли бы всю свою общеобразовательную и воспитательную ценность.

По моему мнению, мы должны воспользоваться задачами из физики, химии, техники и др., чтобы на них выяснить происхождение основных понятий дифференциального и интегрального исчислений. Например, какая-нибудь задача из естествознания дает нам возможность составить функцию, изобразить ее графически, затем исследовать и под конец найти ее производную. Подходя таким образом к понятию о производной, мы всегда должны выяснить, в чем сущность задачи дифференциального исчисления и давать наглядное представление (графическое изображение). После графического изображения идет идея и понятие производной, а под конец — термин и символ производной.

При такой системе преподавания ученики вникают в математичность жизни природы и видят наглядно, какое колоссальное значение математики со стороны ее метода.

Как всякий отдел математики, так и анализ бесконечно малых должен быть построен концентрически. Еще с V класса при графическом изображении эмпирических функций мы должны подготовлять почву для дифференциального исчисления. А в VI и VII классах при проведении идеи функциональной зависимости на уроках алгебры следует учащихся знакомить с понятием о производной, а на уроках геометрии — с понятием об интеграле.

Относительно методики анализа могу сказать, что я в своей практике не останавливался детально ни на теории пределов, ни на непрерывности функций. Я

добивался отчетливых понятий у учащихся, а механическая часть, относящаяся к дифференцированию и интегрированию, имела у меня второстепенное значение. Строгих аналитических доказательств я избегал и их заменял графическими иллюстрациями.

С таким небольшим содержанием курса анализа бесконечно малых можно решать массу трудных и важных задач как в научном, так и в практическом отношении. Интерес, возбуждаемый в учениках этими задачами, отражается и на их успешности по другим отделам математики.

Я надеюсь, что Съезд выскажется точно, определенно и в положительном смысле в пользу введения начал дифференциального и интегрального исчислений с элементами аналитической геометрии в общеобразовательный курс средней школы. И после такого компетентного и авторитетного голоса я глубоко уверен, что мы от единичных усилий перейдем к коллективному труду. Перед всеми нами — педагогами математики — стоит общее дело, успех которого требует совместных усилий, обмена мнений, взаимной критики и проверки наших опытов.

Приложение III. Д. М. Синцов. О преподавании аналитической геометрии в средней школе

ж. Математическое образование. 1914. №3. С. 113-120. (Перепечатано с сокращениями.)

Преподавание начал так называемой высшей математики в средней школе находится у нас в России в стадии развития. Первый крупный шаг — учебные планы реальных училищ, утвержденные Министерством Народного Просвещения.

Затем эти предметы введены в учебные планы кадетских корпусов. Остаются лишь классические гимназии, и надо надеяться, что и в них соответствующие преобразования — дело недалекого будущего.

Но на пути ускорения этих преобразований и их плодотворного развития лежит ряд препятствий.

Помимо принципиальных предубеждений, разделяемых, надеемся, лишь меньшинством преподавательского персонала, тормозом является введение специального курса сепаратною мерою без общего пересмотра всего учебного плана и согласования с новыми отделами всего предыдущего курса. Несогласованность нового предмета с остальным школьным строем проявляется и в том, что этот предмет не входит в состав конкурсных испытаний, а это отражается неизбежно на отношении к нему учеников 7-го класса, поглощенных мыслью о предстоящих испытаниях.

Немало трудностей доставила на первых порах и новизна предмета, за время преподавания основательно забытого и далекого от всего того, с чем приходилось

иметь дело преподавателю. И тем более, поэтому, затруднений доставило и доставляет отсутствие хороших учебников и задачников по специальному курсу и еще более — отсутствие подробных инструкций.

Новые планы не сопровождались объяснительною запискою и методическими указаниями. Между тем, это было особенно важно ввиду того, что предмет являлся совершенно новым и методика предмета в русской литературе совершенно не разработана. Иностранная литература преподавателю и мало доступна, да и там, в сущности, методике аналитической геометрии посвящено не слишком много сочинений. Поэтому, может быть, не лишними явятся нижеследующие соображения

Аналитическая геометрия отличается введением метода координат, дающим возможность сводить решение геометрических проблем, выполняемое в чистой геометрии посредством построений, то есть операций непосредственно над геометрическими образами, на вычисления — на операции над числами и буквенными символами. Это введение метода координат заключает в себе две идеи:

Первая — определение положения точки плоскости посредством пары чисел, ее КООРДИНАТ, замена ТОЧКИ совокупностью двух чисел — ее координат в некоторой системе. Вторая — выражение линий посредством уравнений или замена ЛИНИИ уравнением между определяющими точки ее числами по отношению к некоторой системе координат.

Понять и усвоить эти идеи можно на приложении к прямой линии и кругу, и это должно составить, по-моему, первую и главную часть курса аналитической геометрии в средней школе.

Но помимо этого, курсу аналитической геометрии ставятся еще добавочные задачи.

Во-первых, необходимо ознакомить с основными свойствами конических сечений. Встречаясь в физике и космографии, эллипс и парабола должны быть известны учащимся.

Разумеется, можно было бы давать чисто геометрическую их теорию. Но сочинения Аполлония Пергийского не стало таким популярным, как "Начала" Евклида, и никому из древних не приходило в голову выдержки из сочинений Аполлония присоединять к "Началам". Поэтому и не привилось, вероятно, включение основных понятий о конических сечениях в круг ведения элементарной геометрии, и теория их вошла всецело в аналитическую геометрию. В университетском курсе аналитической геометрии теория конических сечений стала главной частью, поглотившею все остальное.

В элементарном курсе аналитической геометрии на плоскости, какой может быть дан в средней школе, этот отдел должен занять совершенно иное, скорее, подчиненное, придаточное положение. Его целью должно быть лишь первоначальное ознакомление с некоторыми, наиболее важными для приложений, свойствами этих кривых, и, если позволяет время, то ознакомление это может быть выполнено параллельно и аналитическим, и элементарно-геометрическим путем (в духе Аполлония), более привычном для учащихся.

Такова вторая часть курса аналитической геометрии для средней школы. Этим не исчерпывается, однако, ни содержание курса, как его намечает министерская

программа, ни задача его в связи с потребностями курса анализа бесконечно малых и с точки зрения подготовки к высшей школе.

Давая возможность применять графический метод для изображения хода изменения любой функции, аналитическая геометрия является на помощь при выработке самого понятия о функции. И понятие производной, может быть, всего проще и нагляднее связывается с геометрическим ее построением, как тангенса угла касательной.

Поэтому естественным переходом от аналитической геометрии к анализу бесконечно малых является отдел о графическом изображении функций, расширяющей понятие о кривой и знакомящей с некоторыми наиболее важными, теоретически и технически, кривыми.

Здесь же найдет себе место и применение полярных координат к уравнениям Архимедовой спирали, конических сечений и т.д.

Устанавливая такой порядок, я, разумеется, имею ввиду логическое развитие самого курса аналитической геометрии, вне связи с потребностями преподавания.

Мне было указано, что такой порядок изложения сильно сокращает время, которое может быть отведено для прохождения курса анализа бесконечно малых. В свое время я сам держался того порядка, чтобы изложение дифференциального исчисления вести параллельно с изложением аналитической геометрии. Однако я все же думаю, что понятие о функции и функциональной зависимости лучше всего выводится при помощи графических иллюстраций и методов аналитической геометрии, и самое определение производной очень удобно связывать с угловым коэффициентом касательной.

Важно, чтобы, приступая к графическому изображению функций, учащиеся уже освоились бы с прямою линией и с какою-нибудь кривою, и, конечно, проще всего это ознакомление начинать с круга. С этим запасом можно с гораздо большим удобством заняться выяснением понятия функции.

Не буду останавливаться на введении самой системы декартовых координат при помощи подбора житейских примеров (план, шахматная доска, рисование по клеткам, вышивание на канве). Самая идея координат усваивается очень легко и не нуждается в очень подробных разъяснениях Кроме того, можно сказать, что это ознакомление может быть выполнено ранее — в младших классах.

Я хочу указать еще только одно, на желательность связать с аналитической геометрией вопрос о решении неопределенных уравнений.

Ученики часто выносят из средней школы убеждение, что такие уравиения имеют только целые решения. Надо указать, что этого нет, что они имеют бесчисленное множество решений, но целых только ограниченное количество. И это удобнее всего сделать в связи с методом координат, указав, что всякое неопределенное уравнение можно графически изобразить прямою относительно некоторой системы прямоугольных координат, и целые решения суть те, которые имеют обе координаты целые и лежат в вершинах сети, если взята графленая бумага.

Несколько слов о моем учителе математики

О. В. Никишкина

В докладе на Всероссийской конференции по математическому образованию (см. предыдущий выпуск нашего журнала) заслуженный учитель России Роман Григорьевич Хазанкин перечислил качества "идеального" учителя математики и отметил, что учителя, близкие к идеалу, у нас есть и достойны того, чтобы о них знали. Пришедшее в редакцию письмо подтверждает этот тезис и показывает, какие качества учителя ценят его ученики, в том числе и через много лет после окончания учебы.

Мария Дмитриевна Лунева была нашим классным руководителем и учителем математики в 8-й школе Волгограда (теперь это гимназия №5).

Любовь к математике уже жила в нас изначально, когда мы собрались в этот класс. Но чувство это становилось все сильнее благодаря Марии Дмитриевне. Имея каждый день несколько уроков математики, мы еще с удовольствием ходили к нашей учительнице на факультатив. В математику, казалось бы — сухую науку, она могла вносить интересные образы. Однажды рассказав, она потом часто напоминала нам такую шутку. Задают задачу физику и математику: дан пустой чайник, кран и плита. Как вскипятить воду? Оба отвечают, что надо налить в чайник воду, поставить на плиту и довести до кипения. Тогда их спрашивают, как решать эту задачу, если чайник уже наполнен водой? Физик говорит, что тогда его надо сразу ставить на плиту и кипятить. А вот математик отвечает, что воду надо сначала вылить, чтобы свести эту задачу к уже решенной. Таким вот оригинальным образом Мария Дмитриевна подсказывала нам ход решения.

Благодаря Марии Дмитриевне все мои одноклассники поступили в вузы, не имея репетиторов по математике. Нам вполне хватило школьных знаний. Когда из провинциального класса больше трети училось в Москве — это тоже ее заслуга. Она готовила нас в МГУ, МФТИ и учила не бояться сложных задач. Если отчитываться результатами, то надо сказать, что в школьное время мы занимали призовые места не только на городских, но и на областных олимпиадах по математике. А сейчас один наш одноклассник является доктором физико-математических наук (кстати, он процитировал на собеседовании при поступлении в МФТИ совет Марии Дмитриевны "ступай на физтех — человеком будешь" в ответ на вопрос, зачем он сюда поступает).

Мария Дмитриевна учила нас не только математике, она учила нас жизни. Я не помню, о чем конкретно она говорила однажды весь урок, но вместо математики мы прослушали лекцию на тему любви и жизни. Мы обожали такие ее "отступления" от занятий вовсе не потому, что мечтали отлынить от урока (мы все-таки учились в математическом классе), а потому что нам были потрясающе интересны ее рассуждения и мысли, ее образы.

Она сдружила наш класс (мы учились вместе только два последних школьных года), выезжая с нами на однодневные уборки помидоров для помощи волгоградским совхозам и работая там вместе с нами, а не покрикивая на нас командным тоном, как это делали некоторые другие учителя. Она сплотила нас, выбираясь с нами в походы с ночевкой за Волгу. Она доверяла нам, когда месяц мы жили в Волгоградской области, отрабатывая летнюю практику. Кстати, мы — единственный класс! — не имели от нее никаких ограничений на время возвращения вечером и на игру в карты, что являлось предметом зависти со стороны ребят из других классов. Надеюсь, мы не очень злоупотребляли ее доверием. Результатом ее усилий стала не прекращающаяся и поныне дружба нашего класса. Во-первых, у нас в классе поженились ни много ни мало четыре пары! Во-вторых, вот уже 23 года, как мы окончили школу, а регулярно встречаемся и стараемся быть в курсе дел друг друга. Спасибо Вам за это, любимая наша учительница! Это Вы научили нас дружбе.

Мария Дмитриевна совершенно не меняется с годами. С ней по-прежнему легко и интересно общаться. И мы по-прежнему любим своего классного руководителя, классного учителя математики и желаем ей здоровья и оптимизма.

Содержание журнала "Математическое образование" за 1999 – 2000 гг.

N 1 (8), январь – март 1999 г.

N 2-3 (9-10), апрель – сентябрь 1999 г.

N 4 (11), октябрь – декабрь 1999 г.

N 1 (12), январь – март 1999 г.

N 2 (13), апрель – июнь 2000 г.

N 3 (14), июль – сентябрь 2000 г.

N 4 (15), октябрь – декабрь 2000 г.

О Фонде математического образования и просвещения

Фонд математического образования и просвещения создан в конце 1996 г. с целью обеспечения условий, способствующих сохранению богатых традиций математического образования и науки в России. Фонд сотрудничает с организациями и гражданами, желающими участвовать в благородном деле сохранения лучших традиций и высокого качества математического образования в России. Фонд поддерживает образовательные инициативы, способствующие поставленной цели. Особое внимание оказывает образовательным инициативам в провинции, как в виде издательской поддержки, так и финансовой помощи. Фонд издает научную, учебную и методическую литературу в области математики и смежных наук.

Условия подписки и приема материалов

По вопросам подписки на журнал обращайтесь по адресу: 111250, Москва, ул. Солдатская, д. 8, корп. 2, к. 69.

Контактные телефоны: (095) 362-82-56, (095) 261-53-12.

Этот же адрес и телефоны для корреспонденции Фонда.

Страница Фонда в сети Internet: www.fmop.dnttm.ru

e-mail: fmop@dnttm.ru

Стоимость подписки на каждый из номеров 1-4 за 2000 год (включая стоимость пересылки) – 35 рублей.

Для получения номеров журнала необходимо выслать в адрес редакции копию платежного документа, подтверждающего оплату подписки. Сообщите адрес, по которому вы хотели бы получать журнал. В платежном документе укажите, что перевод делается для журнала "Математическое образование", номер журнала за 2000 г., количество экземпляров.

Реквизиты для перечисления:

Получатель: ИНН 7725080165 Фонд математического образования и просвещения

Расчетный счет и банк получателя:

р/с 40703810138120100114 в Московском банке СБ РФ, Лефортовском отделении №6901/019 г. Москвы, к/с 30101810600000000342, БИК 044525342

С сентября 2000 выходит "Обозрение Z" — научно-популярное приложение к журналу "Математическое образование". Условия подписки (адрес, реквизиты, стоимость одного номера) — те же, что и для журнала.

Вы также можете заказать необходимое вам количество отдельных номеров журнала за предыдущие годы. В этом случае пересылка осуществляется наложенным платежом или на основании платежного документа (реквизиты те же). В заказе (в платежном документе) укажите, за какие номера и в каком количестве экземпляров за номер, делается перечисление.

Стоимость одного экземпляра журнала (с учетом пересылки) — 30 руб., сдвоенных номеров 3-4 (6-7) за 1998 г. и 2-3 (9-10) за 1999 г. — 40 руб.

Редакция принимает рукописи материалов с четко прорисованными формулами. По согласованию с редакцией принимаются материалы в электронном виде, обязательно прилагать распечатку.

Рукописи не возвращаются и не рецензируются. После публикации авторские права сохраняются за авторами материалов. Авторы опубликованных материалов получают бесплатно по 10 экз. соответствующего выпуска журнала.

Мнение редакции не всегда совпадает с мнением авторов.

Contents