СООБЩЕНИЯ

МАТЕМАТИЧЕСКАЯ ДЕДУКЦИЯ В КОМПЬЮТЕРНЫЙ ВЕК

Г. А. ТОНОЯН

Что такое математическая теорема? Этот вопрос, ответ на который вовсе не однозначен и не прост, в какой-то мере равносилен вопросу, вынесенному в заголовок известной книги Куранта-Роббинса[1]. В самом деле, по схеме, в отчетливом виде выстроенной Аристотелем, а реально известной даже до него, математика состоит из неопределяемых понятий и определений, из аксиом и теорем, причем основную роль в ней играют именно (момент «математического доказательства» или «дедуктивного вывода» является здесь самым главным) доказываемые нами теоремы. Все же остальное есть не более чем материал, из которого (и с помощью которого) математические теоремы конструируются. Таким образом, исчерпывающее определение или хотя бы достаточно полное описание самого существа понятия «математическая теорема» в значительной степени равносильно описанию сущности (а в достаточно широком смысле—даже и содержания) математики, из чего и исходит сложность этого вопроса, о которой можно судить и по названной выше книге, не содержащей ответа на поставленный в ее заголовке вопрос. Ведь не случайно же самая первая фраза в определенном смысле «основного» учебника математики нашей эпохи знаменитого «многоголового» француза Никола Бурбаки гласит: «Со времен греков говорить «математика»—значит говорить «доказательство»[2].

Разумеется, мы в данной статье не преследуем цель «описать математику» или «определить теорему». Рассмотрим лишь некоторые аспекты поставленного вопроса и, в первую очередь, остановимся на несколько неожиданных моментах, связанных с современным положением дел, а точнее, с наступившей «компьютерной эрой».

Собственно, строение «дедуктивной теории» (или «выводной науки») было достаточно подробно охарактеризовано Аристотелем, не только наметившим «основной костяк» подобной теории (неопределяемые понятия—определения; аксиомы—теоремы), но и остановившимся как на процедуре конструирования определений, так и на (достаточно сложном) процессе доказывания теорем. Разумеется, силлогистика Аристотеля[3] вовсе не исчерпала все возможные процедуры «построения доказательства», но она, по крайней мере, начала освоение этих процедур. «Аристотелева логика» тоже не охватила не только всего массива понятий и методов современной логики, далеко вышедшей за очерченные Аристотелем пределы, но и составила весьма небольшую часть даже того аппарата, который сегодня часто именуют «классической логикой» (или даже «логикой Аристотеля»). По существу, Аристотель разработал только некоторые простейшие правила

---

[1] Р. Курант, Г. Роббинс, Что такое математика? М., 1967.

[2] Н. Бурбаки, Теория множеств (Начала математики, книга первая первой части), М., 1965, с. 23.

[3] Я. Лукасевич, Аристотелевская силлогистика с точки зрения современной формальной логики, М., 1959.

оперирования с отношением «следования» (отношением $\subset$) для высказываний («силлогистика») и заложил основы учения о кванторах. Что же касается общих правил алгебры высказываний, то они (под сильным влиянием Аристотеля, разумеется) были выведены в современной Аристотелю *мегарской* школе и в продолжающей традиции мегарской школы философской школе *стоиков*. Впрочем, следует иметь в виду, что первый свод сочинений Аристотеля был составлен (Андроником Родосским) лишь почти через 300 лет после его смерти и, возможно, является весьма неполным, а посему следует говорить не о влиянии Аристотеля на мегариков, а о прямых заимствованиях из Аристотеля в работах Евклида Мегарского и его учеников и последователей. Но во всех случаях знакомый нам еще по средней школе канон «математической строгости» был создан в Древней Греции. Как указывает главный ревнитель «математической строгости» в наши дни, уже упоминавшийся выше Бурбаки, «Начиная с первых подобных текстов, ставших нам известными (датирующихся серединой V века до н. э.), идеальный «канон» математического текста уже вполне установлен», и «понятие доказательства у этих авторов (у классиков греческой математики—*Г. Т.)* ничем не отличается от нашего»[4]. Впрочем, к середине XIX в. в трудах О. Коши и его последователей уровень строгости конструкций математического анализа почти сравнялся с той «доказательностью», которую обеспечивала нам евклидова геометрия. Последние же недопустимые пробелы как в построении анализа (создание строгой теории вещественного числа), так и в области евклидовой геометрии (совершенная аксиоматика геометрии) были выполнены во второй половине XIX в. (Р. Дедекинд, Г. Кантор, К. Вейерштрасс) и на рубеже нашего и предшествующего веков (М. Пиери, Д. Гильберт, В. Ф. Каган и др.).

Разумеется, в период «от Аристотеля (или даже Пифагора) до Гильберта» (две с половиной тысячи лет!) наблюдался определенный прогресс в области формального описания понятия «математической теории». Однако он был достаточно несуществен, и потому производимое Бурбаки сопоставление древнегреческой математики с современной совершенно правомерно. Конечно, уже Лейбницу (а позднее, скажем, Г. Грассману или Дж. Булю) была ясна необоснованность идущего от Аристотеля требования «самоочевидности» неопределяемых понятий. Впрочем, и сам Аристотель хорошо понимал неясность этого скорее подразумеваемого им, чем явно формулируемого требования и затратил немало усилий (а последующие философы—вплоть до Канта и Гегеля—и того больше) на попытку хоть как-то охарактеризовать свои «неопределяемые понятия» (категории). С другой стороны, те же авторы (Лейбниц—в XVII столетии, Грассман и Буль—в XIX) склонны были полностью отречься от тезиса об «очевидной бесспорности» аксиом. Однако в своем подходе к математике Лейбниц, Грассман и Буль полемизировали не с глубоко ими уважаемыми корифеями античной мысли, а скорее, с современными им учеными, во многом склонными к отреченью от заветов эллинизма. Впрочем, еще до Буля или Грассмана возникла неевклидова геометрия Лобачевского, послужившая доказательством отсутствия в геометрии (а если и так, то, вероятно, и во всех других разделах математики) какой-то a priori заданной системы аксиом, наметившая определенную п р о и з в о л ь н о с т ь выбора аксиоматики, зависимость

[4] Н. Б у р б а к и, указ. соч., с. 299.

ее от «произвола» исследователя (аксиоматический аспект неевклидовой геометрии глубже всего продумал Янош Бойаи).

Определенным крахом аристотелевской программы явилось выяснение того факта, что сама логика математического вывода не единственна, что априорно заданной логики не существует (причем, разные логические системы с одинаковым основанием могут претендовать на копирование системы работы нашего мозга!), как и не существует априорно заданной геометрии—именно это обстоятельство ни Аристотелем, ни Лейбницем, ни Булем не было предусмотрено. Более того, крайний рационалист Лейбниц считал, что участие бога в функционировании Вселенной ограничивается первоначальным актом творения и созданием универсальной системы логических исследований, аксиоматики логики, вложенной им в наш разум и позволяющей нам далее уж чистым «умственным усилием» раскрыть все законы природы (до него в несколько менее отчетливой форме то же самое утверждал и Декарт). Это убеждение Лейбница было полностью родственно глубокой вере Канта в «божественный» характер евклидовой геометрии. Неединственность логики послужила толчком к появлению равноправных «математик» (подобно тому, как, начиная с эпохи Лобачевского—Бойаи—Гаусса, мы вынуждены признавать существование нескольких равноправных геометрий). Ведь доказательство (математической) теоремы, проводимое в рамках одной логической системы (гильбертов формализм[5], расселовский логицизм[6], интуиционизм Брауэра—Вейля[7], столь излюбленный ленинградской школой— А. А. Марков, Н. А. Шанин и др.—конструктивизм[8]), может оказаться несостоятельным в рамках другой системы. Не в меньшей мере разрушают классическую «логику математики» парадоксы теории множеств или сам факт неединственности аксиоматического описания столь основного «строительного камня» всей математики, как понятие множества[9]. Новые трудности возникают здесь в связи с известной теоремой Гёделя[10]. От всех этих трудностей на практике математики предпочитают попросту отмахнуться, но специалисты по основаниям математики и философии математики не имеют права забывать о них.

Впрочем, здесь мы хотим, в основном, коснуться не этих неоднократно обсуждавшихся в литературе вопросов, а совсем других, по-

---

[5] См.: Д. Гильберт, П. Бернайс, Основания математики, т. I, II, М., 1982.

[6] A. N. Whitehead, B. Russell, Principia mathematica, vol. 1—3, N. Y. 1925—1927.

[7] А. Гейтинг, Интуиционизм, М., 1965; С. Клини, Р. Весли, Основания интуиционистской математики, М., 1978; А. Г. Драгалин, Математический интуиционизм: введение в теорию доказательств, М., 1979.

[8] А. А. Марков, О логике конструктивной математики, М., 1974; A. Calder, Constructive mathematics (Scientific American, vol. 141, October, № 4, 1979, pp. 146—171). В. Н. Тростников, Конструктивные процессы в математике, М., 1975. На Западе лидерами конструктивизма являются американец Е. Бишоп и немец Г. П. Лоренуен. Однако развиваемые этими учеными логические системы не во всех деталях совпадают с той, которой придерживается школа Маркова-Шанина.

[9] П. Коэн, Р. Хирш, Неканторовская теория множеств (Природа, 1969, № 4, с. 43—51).

[10] Ср. обсуждение этого вопроса: Ю. Манин, Теорема Гёделя (Природа, 1975, № 12, с. 80—87).

рожденных научной атмосферой сегодняшнего дня. Колоссальная экспансия математики, огромное расширение области ее применения породило сосуществование на первый взгляд двух одновременно функционирующих и, в каком-то смысле, одинаково уважаемых (и даже одинаково необходимых человеку в его неуклонном стремлении вперед, о чем «прикладные математики» иногда и забывают) «математик»—«чистой» и «прикладной». Притом эти две «математики» руководствуются совсем разными принципами «доказательности», разными критериями истинности, можно даже сказать—разной логикой, так что «теоремы» прикладной математики зачастую имеют настолько отличную от теорем чистой математики природу, что специалист по абстрактной алгебре или топологии теоремами их никогда не назовет[11]. При этом никакой четкой грани между чистой и прикладной наукой нет. Невозможно указать, какие разделы математики могут в дальнейшем понадобиться ученым-нематематикам той или иной специальности. Для иллюстрации нашей мысли можно еще раз сослаться на достаточно тривиальный пример астрофизика Джинса, отрицавшего возможность какого-либо использования в физике теории групп незадолго до создания Германом Вейлем и Юджином (или Эйгеном) Вигнером теоретико-групповых методов квантово-механических исследований и грядущего расцвета этих методов как чуть ли не основного аппарата физиков-теоретиков (а значит и экспериментаторов, реализующих намеченные теоретиками научные и технические системы). Менее избитые примеры могут дать нам, скажем, теория множеств и переживающая ныне невиданный расцвет топология, еще лет 10—15 тому назад рассматривавшаяся как дисциплина, не имеющая никакого прикладного значения, а ныне применяющаяся на практике[12], или еще недавно казавшаяся полностью далекой от практики теория чисел, ныне неожиданно оказавшаяся весьма важной для (компьютерной) криптографии[13]. Границы между чистой и «прикладной» математикой никак нельзя считать установленными и не поддающимися пересмотру. Эти неизбежно расплывчатые границы имеют достаточно субъективный характер и изменяются не только с течением времени, но и в зависимости от выбранного нами «эксперта», устанавливающего их. Заметим еще, что «прикладных математик» одновременно существует много: со своими методами, подходами и уровнями строгости. Книги, о которых мы упоминали выше, целиком ориентированы на «классическую прикладную математику», используемую в механике, физике, астрономии, технике. Совсем другой инструментарий и другой подход к математике наблюдается у экономистов, причем в области теоретических схем (а не численных расчетов) строгость методов «экономической математики» и полнота используемых в ней моделей, пожалуй, близки сегодня к чистой математике, но не к техническим наукам. Видимо, другие методики нужны биологам, имеющим дело с системами небывалой сложности, и, если, скажем, в генетике методы математического моделирования

---

[11] Ср.: И. И. Блехман, А. Д. Мышкис, Я. Г. Пановкс, Прикладная математика: предмет, логика, особенности подходов, Киев, 1983; Механика и прикладная математика, логика и особенности приложений математики, М., 1983.

[12] Я. А. Смородинский, П. А. Дирак (Успехи физических наук, т. 148, 1986. с. 533).

[13] K. Rosen, Elementary Number Theory and Applications, Reading (mass.), 1984; M. R. Schreoder, Number Theory in Science and Communication, N. Y., 1984.

вполне себя оправдывают, то в целом «биологическая математика», вероятно, еще не создана.

Математизация гуманитарных наук, скорее всего, потребует создания какого-то нового аппарата, адекватно отображающего наблюдаемые в человеческом обществе и в человеческой культуре закономерности—и характер этого аппарата, и степень «доказательности» используемых в нем конструкций предсказать сегодня невозможно. Вполне возможно, например, что в ряде случаев нам придется отказаться от столь привычной для нас абстракции натурального ряда и принципа математической индукции, как того требует, например, возникший в значительной степени в связи с наступлением «века компьютеров» ультраинтуипионизм[14]. Ведь ясно, что весь (бесконечный!) натуральный ряд чисел никаким реальным объектом не является и возможно, что легкость постижения нами этого на самом деле в каком-то смысле даже и противоестественного объекта[15] связана всего лишь со специфическим устройством нашей нервной системы—за пересчет 1—2—3—... отвечает левое полушарие головного мозга человека, в каком-то смысле специализированное на алгоритмических процедурах того типа, какой задается принципом математической индукции[16]. Ясно, однако, что сегодня еще не наступило время для серьезного обсуждения «математики будущего», приспособленной к обслуживанию новых дисциплин, некоторые из которых, скорее всего, еще только должны родиться.

Хотелось бы остановиться подробнее на том, какое влияние может оказывать на математику широкая компьютеризация производства, быта, образования, культуры. Влияние это достаточно многогранно, и связанные с ним общенаучные проблемы в значительной степени все еще не разработаны. Мы тут скорее их назовем, нежели решим.

Начнем с указания на появление в настоящее время целого комплекса новых направлений прикладной математики, связанных непосредственным образом с компьютерами. Из их числа, в силу некоторой парадоксальности самого направления, назовем здесь уже упоминавшуюся выше прикладную теорию чисел, лежащую в основе важных ветвей современных «компьютерных наук». Известно, что колоссальный объем информации, в значительной степени хранящейся («банки данных») и передаваемой с помощью компьютеров, является одним из характернейших особенностей нашей эпохи, когда «запасы информации» и владение этими запасами становятся чуть ли не самым важным показателем экономического, промышленного и социального развития страны, скажем, как некогда ее энерговооруженность[17]. При этом чрезвычайно важным становится вопрос как о методах рациональной передачи этой информации (о методах ее кодирования и декодирования), так и о методах ее шифровки, поскольку значительную часть передаваемой информации (например, почти всю деловую корреспонденцию торговых и промышленных фирм, работа-

---

[14] См.: Философская энциклопедия, т. 3—5, М., 1964, 1967, 1970, т. 3, с. 336, 402, 446; т. 4, с. 60, 208, 489, 570; т. 5, с. 216.

[15] Ср.: П. К. Рашевский, О догмате натурального ряда (Успехи математических наук, т. 28, вып. 4 (172), 1973, с. 243—246).

[16] Ср.: С. Спрингер, Г. Дейч, Левый мозг, правый мозг, М., 1983.

[17] См. Г. Р. Громов, Национальные информационные ресурсы: проблемы промышленной эксплуатации, М., 1985.

ющих в условиях жесткой конкуренции и широко распространенного промышленного шпионажа) требуется скрыть от лиц, которые могли бы использовать ее во вред отправителю. Именно решение такого рода проблем ныне тесно связано с тонкими разделами «высшей математики» (теории чисел).

Старшее поколение ныне работающих математиков хорошо помнит то время, когда «формальная» или «символическая» алгебра именовалась «абстрактной алгеброй». Здесь прилагательное «абстрактная» акцентирует чуждость «символической» или «аксиоматической» алгебры Э. Нетер—Б. Л. ван дер Вардена всяким приложениям. Если понятие «группы» еще могло быть применимо в прикладных исследованиях, думали сами математики, то такие «чудища», как, скажем, конечные поля Галуа, созданы лишь для того, чтобы отрабатывать на них методику «чисто математических» рассуждений и радовать людей своим внутренним совершенством и красотой. Но современная теория кодирования, имеющая в наш «информационный век» огромное прикладное значение, целиком построена на широком использовании глубоких алгебраических конструкций, начинающихся именно с конечных полей Галуа. Математическая тонкость и абсолютная нетривиальность используемого аппарата обратили в сторону «прикладной теории кодирования» многих видных математиков из разных стран мира (у нас к их числу относятся, например, алгебраист С. Д. Берман и известный специалист по математическим методам статистической физики Р. Л. Добрушин) и определили несколько неожиданное название известного обзора[18] теории кодирования, принадлежащего известному американскому математику Норману Левинсону: «Теория информации—контрпример к принадлежащей Г. Г. Харди концепции прикладной математики», ибо знаменитый кембриджский математик Гарольд Харди, выдающийся специалист по теории чисел, резко противопоставляет «чистую математику» как область мышления, доставляющую наиболее полное ощущение совершенства и красоты, гораздо более бедной и эстетически менее привлекательной прикладной математике[19].

Мы так подробно остановились на ситуации с современной («компьютерной») прикладной теорией чисел еще и потому, что здесь необходимо учесть одно новое обстоятельство, достаточно поучительное с позиций интересующего нас вопроса об отличии современных подходов к «математической дедукции» (т. е. к доказательству математических теорем), тех, которые пришли к нам из эпохи античности. Дело в том, что существенную роль в современных методах шифровки (и дешифровки) сообщений играют простые числа, а также то обстоятельство, что компьютерные методы генерации таких чисел порождают колоссальные простые числа при использовании ограниченного машинного времени. Но вот выяснение того, является ли данное число простым или составным, и разложение этого числа на простые множители требует таких усилий, которые не под силу самым мощным из ныне существующих ЭВМ в условиях наличия у них неизбежно ограниченного запаса рабочего времени. Однако в некоторых случаях даже и генерация больших простых чисел с полной проверкой простоты получаемого числа оказывается экономически не-

---

[18] N. Levinson, Coding Theory: a Counter-example te G. H. Hardy's Conception of applied mathematics (Amer. Math. Monthly, vol. 77, № 3. 1970, pp. 249—258).

[19] G. H. Hardy, A Mathematiciads Apology, Cambridge, 1981.

выгодной в силу затрат на эксплуатацию ЭВМ. И более рациональным оказывается не доводить эту проверку до конца, используя в качестве «простого» числа, о котором лишь с очень большой степенью уверенности (но не со 100%-ной уверенностью!) можно говорить, что оно простое. Вот это широко используемое в современной криптографии понятие «почти наверняка простого числа» уж во всяком случае для античной математики является совершенно чуждым. Однако древнегреческой математике чужда не только эта в конце концов достаточно частная деталь, но и другие, гораздо более важные моменты «компьютерной» математики второй половины (или, скорее, даже последней трети) XX столетия. Широко используемые ныне в разных разделах математики «компьютерные» доказательства теорем (т. е. доказательства, в той или иной мере использующие современную вычислительную технику), самым знаменитым из которых, бесспорно, является блестящее решение знаменитой проблемы четырех красок[20], породили уже серьезную дискуссию о самом смысле слова «доказательство» (а что, если компьютер ошибся?) и о том, в какой мере использующие компьютер рассуждения могут считаться доказательствами[21]. Эта проблема, привлекавшая внимание чуть ли не всех выдающихся математиков конца XIX и первой половины XX столетия, требовала доказательства, что каждую географическую карту на плоскости или на сфере (на глобусе) можно «правильно» раскрасить четырьмя красками (т. е. так, чтобы любые две «страны», имеющие общий участок границы, были закрашены в разные цвета). Отсутствие серьезного прогресса в решении этой задачи в течение более чем столетия породило даже сомнения в справедливости ее утверждения, пока в 1976 г. не стало известно, что требуемое доказательство получено с существенным использованием компьютеров. Заметим, что и в нашей стране, и за рубежом широко распространились слухи о некорректности принадлежавшего Хакену и Аппелю решения проблемы четырех красок. Сомнения такого рода высказывались и печатно. Однако ныне имеется уже и независимое от схемы Хакена-Аппеля (хоть и родственное ей) «второе машинное доказательство» теоремы о четырех красках (опубликованное пока, впрочем, лишь частично)[22]. Это доказательство требует всего лишь около 50 часов машинного времени для технической проверки определенных гипотез, а не 2000 часов, как первое доказательство. Ныне специалисты считают, что истинность теоремы о четырех красках уже не вызывает сомнений. Последнее, однако, никак не снимает вопроса о статусе этого предложения в системе математических наук (теорема? вовсе не теорема?). Заметим еще, что если публикация не охватывает целиком

---

[20] K. Appel, W. Haken, The Solution of the Four-Color-Map problem (Scientific American, september, 1977, pp. 108–121); их же, The Four-Color problem (Mathematics Today (ed. L. A. Steen). N. Y., 1979, pp. 153–180); И. М. Яглом, Четырех красок достаточно /Природа, 1977, № 6, с. 20–25/.

[21] Th. Tymoczko, The Four-Color problem and its philosophical significance (Journal of Philosophy, vol. 76, № 2, 1979, pp. 57–83); E. R. Swart, The Philosophical Implications of the Four-Color Problem (Amer. Math. Monthly, vol. 87, № 9, 1980, pp. 697–707); см. также: Th. Tymoczko, New Direction in the Philosophy of Mathematics, Boston, 1986.

[22] F. Allaire, Another Proof of the Four-Color Theorem 1, Proc. of the Seventh Manitoba Conference on Numerical Mathematics and Conputing, Univ. Manitoba, Winnipeg, Man. 1977, pp. 3–72.

«безмашинную» часть доказательства теоремы о четырех красках (вторая часть работы докладывалась на конференции по «компьютерной математике» и обсуждалась со специалистами, но пока не опубликована), то и основная публикация[23] группы Аппеля-Хакена тоже не полная в строго математическом смысле, ибо технически наиболее сложная часть рассуждения по своему объему «не влезала в журнал», и авторы вынуждены были оговорить, что они согласны прислать соответствующий (весьма объемный) текст любому желающему его проверить (таких желающих оказалось очень мало). Аналогично обстояло дело и в случае с предшествующей работой[24], также выполненной с помощью компьютера. Один довольно-таки большой отрывок из этой работы был аккуратно переписан авторами (что заняло очень много места) и сдан в библиотеку Иельского университета США, из которой любой желающий мог затребовать фотокопию соответствующих листов. Но ведь и в «докомпьютерную» эру (еще в XIX столетии), скажем, выполненное одним любителем построение циркулем и линейкой правильного 65537-угольника нигде невозможно было опубликовать из-за объема работы. Соответствующий текст автором был тщательно переписан и сложен в чемодан, который долгие годы хранился в библиотеке математического института Гёттингенского университета, но никогда не был никем до конца разобран.

Обращаясь к рассмотрению использующих компьютер математических доказательств, следует сказать, что принципиальное участие компьютера мало чем отличается от использования иных «вспомогательных» технических средств (набросков, чертежей, просто записей на бумаге и т. д.), которые ведь тоже чужды «чистой логике». По мнению Е. Р. Суарта[25], ныне все математические доказательства можно разбить на следующие 4 группы:

1) доказательства, которые могут быть проведены в уме с использованием логических ходов, так сказать, «заложенных» в наш интеллект (и формализованных Аристотелем и более поздними авторами);

2) доказательства, проведение которых требует использования тех или иных «простых» технических средств—в первую очередь, карандаша и бумаги;

3) теоремы, доказательства которых с помощью карандаша и бумаги требуют колоссальных интеллектуальных и даже просто трудовых затрат (скажем, тысяч «человеко-часов» работы) и в которых поэтому желательно использование компьютера, гарантирующего в

---

[23] K. Appel, W. Haken, Every planar map is four colorable, part I: Discharging (Illinois J. Math., vol. 21, 1977, pp. 429—490); K. Appel, W. Haken, J. Koch, Every planar map is four colorable, part II, Reducibility (Illinois J. Math. vol. 21, 1977, pp. 491—567).

[24] O. Ore, The Four Color Problem. N. Y., 1967, O. Ore, J. Stemple, Numerical Calculations on the Four-Color problem (Journal of Combinatorial Theory, vol. 8, 1970, pp. 65—78).

[25] Е. Р. Суарт (см. сн. 24) предлагает ввести в рассмотрение новый тип математических предложений, промежуточных между теоремой и гипотезой (больше, чем гипотеза, но все же меньше, чем теорема); впрочем, здесь, возможно, следовало бы различать «почти теоремы» (но все еще немного гипотезы) от «почти гипотез» (но уже немного и теорем) и приписать им название «агнограммы», поскольку в их отношении мы вынуждены в каком-то смысле оставаться агностиками—в таком случае можно было бы говорить о классификационной агнограмме для конечных простых групп.

таких случаях—и это очень важно—большую надежность решения задачи, чем «ручное» ее доказательство с привлечением громоздких записей, схем, таблиц, чертежей и т. д.;

4) теоремы, доказательства которых в настоящее время неизбежно требуют привлечения компьютера, ибо здесь объем «ручной» работы превосходит возможности любого коллектива.

При этом с позиций античных философов «теоремой», видимо, надо было бы считать лишь предложения, доказательства которых попадают в категорию 1), что, однако, нелепо. Ясно ведь, что в случае уже минимально сложных доказательств использование записей существенно уменьшает возможность ошибки, и лишь оно гарантирует возможность проверки доказательства иным лицом: методика перипатетиков[26] была хороша для обсуждения общих (скажем, морально-этических) проблем, но не для доказательства сложных теорем. С другой стороны, резкой границы между категориями 2) и 3), разумеется, не существует, ибо указание на «колоссальность» ручной работы является достаточно расплывчатым (как не существует и четкой границы между категориями 1) и 2) в приведенной выше классификации). Граница между категориями 3) и 4) тоже не совсем отчетлива и, кроме того, явно зависит от времени. Так, например, Д. Коэн утверждал, что он в состоянии перевести теорему о четырех красках из категории 4) (к которой она сегодня твердо принадлежит) в категорию 3). Ему это, скорее всего, не удалось, но, возможно, это удастся кому-либо позже. Разумеется, доказательства предложений, принадлежащих категории 4), выходят за рамки аристотелевой программы логического вывода (например, к числу «правил логического вывода» и допустимых логических процедур здесь приходится присоединять и «логику» того конкретного алгоритмического языка, на котором записаны машинные программы участвующего в доказательстве компьютера). Но ведь мы сегодня считаем эту программу вовсе не безупречной, да и реально почти никогда (кроме простейших теорем типа утверждения—$(а+в)^2=а^2+2ав+в^2$) не стремимся свести доказательство непосредственно к аксиомам. Поэтому у нас нет никаких оснований исключать «компьютерные» доказательства из допустимого инструментария математика, выделив выводимые с помощью ЭВМ теоремы в какой-то новый разряд «истин» (как на этом настаивает, например, Т. Тимошко).

Увы, «компьютеризация» доказательной математики приводит иногда и к «теоремам», которые невозможно отнести ни к одной из перечисленных выше категорий—к числу их относится, например, «теорема» о классификации конечных простых групп, обсуждение которой заслуживает специального разговора, так что здесь мы ограничимся лишь указанием на посвященную этому результату (теореме? почти теореме? гипотезе?) статью[27]. Укажем здесь также на еще одну своеобразную особенность многих «машинных доказательств» теорем (в частности, доказательства теоремы о четырех красках), строго говоря, с вопросами «логики доказательства» не связанную, но достаточно типичную для нашей эпохи в целом. Нам хорошо известно, что

---

[26] Перипатетики—от греческого «Peripatein» (расхаживающий вокруг)—общее название учеников и последователей Аристотеля, культивирующих обсуждение философских проблем в процессе прогулок по садам «Ликея»—виллы в окрестностях Афин, где помещалась школа Аристотеля—или по галереям (Peripator) этой виллы.

[27] Д. Горенстейн, Грандиозная теорема (В мире науки, 1986, № 2, с. 62—74).

«основную теорему высшей математики», как ее часто называли ранее. или формулу Ньютона-Лейбница, устанавливающую связь между дифференцированием и интегрированием: $\frac{d}{dx}\int_a f(t)dt = f(x)$, впервые доказал учитель Ньютона Исаак Барроу, а, скажем, «основную теорему алгебры» (теорему о существовании (вещественного или комплексного) корня у каждого алгебраического уравнения с, вообще говоря, комплексными коэффициентами) доказал Гаусс. Мы знаем также, что «ослабленную гипотезу Гольбаха» (утверждение, что каждое достаточно большое нечетное число представляется в виде сумм трех простых чисел) доказал И. М. Виноградов, а проблему о раскраске карт на любой отличной от плоскости или сферы поверхности без границ (скажем, на замкнутой поверхности) решили Г. Рингель и Дж. Т. Янгс, а вот кто доказал теорему о четырех красках? Мы зачастую приписываем это выдающееся открытие двум совместно работавшим математикам—Аппелю и Хакену, сделавшим первое сообщение о решении проблемы о красках, но справедливо ли это? В публикациях (в частности см. сноску 23) наряду с этими двумя фамилиями появилась еще и фамилия Джона Коча, руководителя группы программистов, работающих над этой задачей. Видимо, уместно было бы вставить в список «победителей» и учителя Хакена Генрика Хееша, впервые обсудившего возможные пути машинного решения знаменитой задачи. Но на самом деле это выдающееся достижение математической науки XX в. принадлежит большому коллективу исследователей, в который, так сказать, «на равных правах» входили математики, программисты и компьютеры. С этой точки зрения попытка увязать решение задачи о раскраске карт на плоскости всего с двумя-тремя фамилиями является не более чем пережитком предшествующей эпохи—эпохи одиноких творцов, создававших нетленные ценности духа в тиши своих кабинетов. Ныне дело обстоит иначе: характерные для нашего времени произведения искусства—кино-и телепостановки, или, скажем, ансамбли электронной музыки—создаются чуть ли не индустриальными методами—большими объединениями людей и технических устройств, и трансурановые элементы открываются авторами, которых, может быть, уместнее всего именовать не фамилиями, а как «Дубна», «ЦЕРН» (западноевропейский международный центр атомной физики в Швейцарии) или «Беркли» (Калифорнийскому университету в г. Беркли под Сан-Франциско принадлежит крупнейшая из американских атомных лабораторий). А, скажем, одно из самых замечательных физических открытий последних лет—открытие так называемых промежуточных векторных бозонов[28]—зарегистрировано в заметке[29], список авторов которой содержит 138 фамилий, представляющих многочисленные университеты и лаборатории Европы и Америки.

Так что же означает сегодня, в нашу компьютерную эру[30], «мате-

---

[28] См.: Фундаментальная структура материи, М., 1984, с. 191.

[29] Арнисон и др., Экспериментальное наблюдение электронов с большим поперечным импульсом, сопровождаемых недостающей энергией при $\sqrt{S}=540$ ГэВ (Успехи физических наук, т. 141, вып. 3, 1983, с. 501—516); см. также: Д. Б. Клайн, К. Руббиа, С. Ван дер Меер, Поиски промежуточных бозонов (там же, т. 131, вып. 1, 1983, с. 135—152).

[30] Говоря о «компьютерной эре», мы имеем в виду всю современную науку и культуру, для которых компьютеры можно считать символом, но которая вовсе не

матическое доказательство»? И доказана или нет в некотором смысле основная теорема (или «основная агнограмма»—см. сноску 27) теории (конечных) групп—«классификационная теория для простых групп»? Ответы на эти вопросы вовсе не однозначны. Но именно неоднозначность ответа на эти крайне важные для математики вопросы и делает, как нам кажется, их обсуждение особенно важным. Ведь, если мы не знаем, что такое доказательство (дедуктивный метод) или что такое теорема, то значит и смысл термина «математика» нам полностью не ясен.

ՄԱԹԵՄԱՏԻԿԱԿԱՆ ԴԵԴՈՒԿՑԻԱՆ ԿՈՄՊՅՈՒՏԵՐԱՅԻՆ ԴԱՐՈՒՄ

Գ. Ա. ՏՈՆՈՅԱՆ

Ամփոփում

Վերջին տասնամյակում մաթեմատիկայում օգտագործվող «մեքենայական» մեթոդները, մաթեմատիկական ապացուցումների խստությունը որոշ կասկածների է ենթարկվել։ Արդի պայմաններում նորովի է դրվում մաթեմատիկական գիտության կարգավիճակը (ստատուսը) գիտությունների ընդհանուր համակարգում։ Անհրաժեշտություն է զգացվում մեթոդաբանական տեսանկյունից քննել մաթեմատիկական ապացուցման հասկացության էությունն ու աստիճանական զարգացման ընթացքը։ Քննադատական վերլուծության կարիք ունի մաթեմատիկական ապացուցման հասկացության փիլիսոփայական իմաստավորումը մաթեմատիկայի փիլիսոփայության տարբեր ուղղությունների կողմից։ Ներկայումս խիստ աղճատվել է մաթեմատիկական ապացուցման հասկացության դասական ըմբռնումը։ Հանրահայտ է «չորս գույների պրոբլեմի» լուծման ընթացքի օրինակով որոշ մեթոդաբանական հետևություններ անելը մաթեմատիկական դեդուկցիայի մասին։

MATHEMATICAL DEDUCTION IN THE COMPUTER AGE

TONOYAN G. A.

Summary

During the last decade the „mechanical" methods employed in mathematics have put the exactness of mathematical demonstrations under suspicion. Under modern conditions the status of the mathematical science is set anew in the general system of sciences. Some necessity is felt to examine the essence and the course of gradual development of demonstration from a methodological point of view. The philosophical sense of the comprehension of mathematical demonstration needs a critical analysis by the various trends of mathematical philosophy. At present the classical comprehension of mathematical demonstration has greatly been distorted. It is common knowledge to make certain methodological conclusions regarding mathematical deductions according to the example of the solution of the „problem of four colours".

исчерпывается моментами, связанными с использованием ЭВМ—так, например, то почти не затронутое в настоящей статье, но весьма важное для нашей темы обстоятельство, что математика сегодня знает много равноправных логических систем, связано с открытием и эксплуатацией компьютеров лишь косвенно.