Проблемы логики и методологии науки

ПОНЯТИЕ АЛГОРИТМА И ЕГО МЕСТО В МАТЕМАТИКЕ*

Ю.Л. Ершов

Несмотря на то, что понятие алгоритма является едва ли не самым распространенным в современной математике, природа этого понятия становится более ясной только с появлением математической логики. С исторической точки зрения понятие алгоритма связано скорее с алгеброй, потому что именно там оно появляется впервые. Любопытно то обстоятельство, что слова *алгебра* и *алгоритм* обязаны своим возникновением имени одного человека – арабского математика Аль Хорезми (787 – ок. 850 гг.), после которого осталось несколько трактатов, и среди них один был посвящен арифметике, а другой – алгебре. В обеих книгах широко используются разнообразные алгоритмы, а сам термин *алгоритм* есть искаженное произнесение имени Аль Хорезми (*dixit algorizmi* – "так сказал Аль Хорезми"). Название же книги по алгебре – *Китат аль-мухтассар ибн хасаб* ***аль-габр*** *в'алуккабала* – привело к введению слова *алгебра* для обозначения соответствующего раздела математики.

Важность понятия алгоритма в настоящее время безусловно осознается в связи с появлением возможности быстрых вычислений, производимых компьютерами. Действие физических машин – компьютеров – основано на исполнении ими программ, которые представляют собой алгоритмы. Простые алгоритмы типа деления столбиком известны каждому школьнику из курса математики, и, казалось бы, нет более знакомой вещи в математике, чем алгоритмы. Математика имеет дело с мате-

* Исследования, нашедшие отражение в этой работе, поддержаны Российским гуманитарным научным фондом (проект № 01–03–00131). В основу статьи положен доклад перед участниками Международной студенческой конференции в Новосибирском государственном университете в апреле 2002 г.

матическими объектами, среди которых можно назвать числа, функции, множества, фигуры и т.д. Суть математики состоит в доказательстве истинных утверждений об этих объектах, и если есть такое доказательство, объект, фигурирующий в утверждении, считается существующим. Вопрос о том, где он существует: в мире идеальных сущностей, или же в уме у математика, или же во внешнем мире, – занимает в основном философов математики и не интересует нас здесь. Удивительным и весьма важным фактом является то, что алгоритм в обычном его понимании не является традиционным математическим объектом.

Для понимания этого важного факта следует обратиться к тому, что представляют собой математические утверждения. Обычно они являются дескриптивными, т.е. описывающими свойства математических объектов. В более широком смысле можно полагать, что математические утверждения описывают математическую реальность, что бы под этим ни понималось. Важно лишь то, что математические утверждения суть описание чего-то такого, чье существование по некоторым критериям допускается или постулируется.

Что касается алгоритмов, то они носят императивный характер, который виден из того, что они представляют собой предписания: сделай так-то и так-то. В этом смысле они не являются математическими объектами в традиционном их понимании, потому что императивы не есть часть математики. Это представляется странным, но следует учесть, что алгоритмы появляются в доказательствах классической математики в виде текста, который никак не подходит под определение математического объекта как чего-то такого, что описывается математическими утверждениями.

Таким образом, для понимания природы понятия алгоритма и его легитимизации в качестве математического объекта мы должны фиксировать различие между дескриптивными и императивными утверждениями. Это первая оппозиция, нужная нам при обсуждении данного вопроса. Другой полезной оппозицией будет противопоставление классической и современной математики, или, более точно, классического аксиоматического метода и современного аксиоматического метода. Наконец, крайне важным будет также разделение синтаксических и семантических аспектов математических построений. Имея в виду все три оппозиции, понятие алгоритма можно связать с понятием математического объекта.

Впервые объекты, которые можно сопоставить с алгоритмами, появились в классической алгебре. В некотором смысле именно там алгоритмы стали претендовать на то, чтобы их можно было уподобить

математическим объектам. Рождение современной математики также связано именно с алгеброй, которая ввела в обиход совершенно новые математические объекты. Известно, что собственно понятие алгоритма стало формализуемым и, стало быть, более понятным в рамках математической логики. Ситуация становится постижимой, если принять во внимание, что до возникновения математической логики алгебра в известной степени играла роль логики внутри математики [1]. Обычная логика, связанная с именем Аристотеля, относилась к законам мышления и не играла какой-либо значимой роли в математике. Кодификация же структур современной математики была осуществлена математической логикой, которую многие исследователи совсем не соотносят с законами мышления.

Важнейшим понятием математической логики является понятие терма. Терм – синтаксическое понятие, ставшее возможным после того, как в алгебре задолго до этого было введено понятие переменной. Фактически алгебра ввела формальный язык, который представлял собой исчисление переменных. Если имеется определенное число констант и переменных, можно ввести понятие терма обычным индуктивным образом: константа есть терм, переменная есть терм – и далее определяется индуктивный способ порождения слов с использованием функциональных символов языка. На термы как математические объекты можно смотреть двояким образом в зависимости от того, какие соображения представляют в некоторой задаче интерес – синтаксические или семантические.

Семантический аспект представляет собой поиск значений, которые приписываются синтаксическим объектам. Если мы изучаем натуральные числа, тогда каждому терму можно сопоставить значение – натуральное число. Вычисление значений осуществляется по заданным значениям переменных и функций. Первостепенную важность имеет равенство термов. Имеется два принципиально разных понимания такого равенства. Поскольку в терм входят переменные, постольку равенство термов можно считать тождеством, т.е. можно считать, что значения двух термов совпадают при всех значениях входящих в них переменных. Такого рода тождества являются универсальными логическими законами. Другое понимание равенства термов заключается в том, что установление равенства требует от нас нахождения таких значений переменных, при которых это равенство было бы справедливо. Именно такое понимание свойственно при решении уравнений, например диофантовых. В математической практике мы часто

имеем смешанный вариант: некоторые переменные считаются параметрами, а для остальных ищутся соответствующие значения.

Эти два понимания равенства термов обусловливают два типа операций над ними. Первая из операций – это преобразование терма с использованием тождеств термов. Вторая операция – подстановка термов вместо переменных.

Проиллюстрируем "силу" операции подстановки. Рассмотрим однобуквенный алфавит $\{u\}$и определим понятие терма так:

1) переменная u является термом;

2) если X и Y – термы, то и (слово) XY – терм.

Заметим, что термами будут в точности все непустые слова алфавита $\{u\}$. Если считать, что терм X "кодирует" положительное натуральное число $l(X)$ – длину слова X, то операция образования термов $X, Y \to XY$ соответствует операции ($l(XY) = l(X) + l(Y)$), а операция подстановки терма вместо переменной $X, Y \to (X)_Y^u$ соответствует операции *умножения* ($l((X)_Y^u = l(X) * l(Y)$).

Такого рода вещи делаются в алгебре при решении уравнений. Важность термов определяется тем, что это не только синтаксические объекты, но и фактически записи алгоритмов. Сама форма терма говорит о том, что́ именно нужно выполнить для вычисления значения терма. При этом, конечно, надо знать значения соответствующих функций.

Термы были первыми примерами нетривиального представления алгоритмов. Когда дан некоторый запас функций, термы дают некоторый запас алгоритмов. Вопрос о наличии алгоритма ни в коем случае не тривиален, что видно из, быть может, одного из наиболее важных результатов алгебры, а именно, из теоремы Галуа – Абеля о невозможности представления решений уравнений пятой степени в радикалах. Здесь речь идет об алгоритмической неразрешимости проблемы, т.е. об отсутствии алгоритма. Доказательство неразрешимости привело к появлению неклассических объектов математики – конечных групп, конечных полей и др. Именно на этом пути возникли семантические рассмотрения. Классическая математика занималась рассмотрением относительно малого числа объектов – чисел, фигур на плоскости и т.д. Но оказалось, что для решения проблем классической математики, имеющих дело с традиционными объектами, требуется ввести новые объекты. Введенные Галуа группы подстановок привели к созданию новой современной алгебры. При этом сама постановка проблем в алгебре радикально изменилась, – теперь возникает вопрос

и о том, можно ли описать все объекты, которые удовлетворяют описанным структурам. Действительно, например, классификация конечных групп представляет собой весьма впечатляющую проблему: хотя классификация завершена, многие ее результаты занимают десятки тысяч страниц, и некоторые из них помещены в малодоступных периодических изданиях. В определенном смысле эти результаты практически недоступны пользователю.

Как математические объекты термы обладают простотой, являясь в то же время мощным орудием решения проблем. Действительно, упомянутые выше две операции над термами позволяют решить многие вопросы. Например, приведение формул к нормальной форме, стандартная процедура в математической логике, есть преобразование термов.

Рассмотрим следующую систему тождеств алгебры (исчисления) высказываний:

$$
\begin{aligned}
&X \to Y \quad \equiv \neg X \vee Y\\
&\neg (X \wedge Y) \equiv \neg X \vee \neg Y\\
&\neg (X \vee Y) \equiv \neg X \wedge \neg Y\\
&\neg\neg\ X \equiv X\\
&X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)\\
&(Y \vee Z) \wedge X \equiv (Y \wedge X) \vee (Z \wedge X)
\end{aligned}
$$

Эту систему тождеств можно использовать для определения (недетерминированного) алгоритма преобразования формул языка исчисления высказываний следующим образом. Один такт работы алгоритма над формулой U: найти подформулу V формулы U, имеющую вид формулы, стоящей в левой части одного из тождеств, и перейти к формуле U', полученной из U заменой V на формулу V', соответствующей правой части этого тождества. Если такой подформулы V нет, то алгоритм останавливается; в противном случае делаем следующий такт работы над формулой U.

Нетрудно установить, что:

1) для любой формулы U после конечного числа тактов работы этого алгоритма получится формула U^* (эквивалентная формуле U), на которой алгоритм останавливается;

2) если U – формула, на которой алгоритм останавливается, то U находится в дизъюнктивной нормальной форме.

Итак, указанный алгоритм является алгоритмом приведения формул к дизъюнктивной нормальной форме.

Методы таких преобразований доказали свою эффективность во многих разделах математики и стали предметом целой теории систем переписывания термов. Алгоритмы появились в реальном виде в классической алгебре, и с точки зрения современной алгебры преобразование тождеств представляет собой полную логическую систему (с точки зрения теории алгоритмов это эквивалентные преобразования алгоритмов). Но до возникновения математической логики эти представления были неявными. Только с появлением работ Дж. Пеано по аксиоматизации теории натуральных чисел и работы Д.Гильберта по аксиоматике геометрии наряду с математическими аксиомами первостепенную важность приобрели законы логики. Классический аксиоматический метод предполагал выведение следствий из аксиом, но только с появлением математической логики способы выведения этих следствий были кодифицированы и наряду с аксиомами стали частью формализмов математики.

Это обстоятельство привело к абсолютно новой ситуации во всей математике. Классическая математика была, если можно так выразиться, наивно конструктивной. Это означает, что если доказывалась теорема существования математического объекта, то при этом давался способ его построения. Но после появления законов логики стало возможным доказательство от противного, когда доказательство теоремы существования вовсе не предполагало способа построения объекта. Поначалу новые возможности в математике вызвали яростные споры среди математиков о допустимости подобных методов. Ситуация наилучшим образом характеризуется знаменитой аксиомой выбора, имевшей самые парадоксальные следствия. Несмотря на эту парадоксальность, аксиома выбора оказалась чрезвычайно полезной при доказательстве самых различных результатов. Новые методы, связанные с понятиями и методами математической логики, стали весьма эффективными не только в современной математике, но и в математике классической.

Прежде всего, математическая логика позволила определить понятие алгоритма. С каждым алгоритмом можно связать функцию, которая вычисляет его значение. Таких функций существует значительное количество, и из них удалось выделить класс вычислимых функций. Установление смысла вычислимости представляет содержание знаменитого тезиса А. Черча. Одно из определений вычислимости принадлежит К. Геделю, и важно отметить, что знаменитая теорема Геделя о неполноте, о которой так много говорят и спорят философы, связана с понятием алгоритма. Без принятия соглашения об эффектив-

ности системы аксиом эта теорема не имеет значительного смысла [2]. Современная алгебра построила теорию квазитождеств, условных тождеств и полную систему понятий из правил. Используя условные тождества, можно формализовать все алгоритмы. Язык программирования “Пролог” показывает, что любые алгоритмы могут быть описаны квазитождествами.

Новые методы, связанные с кодификацией логических законов математического мышления, частью которых являются представления об алгоритмах и вычислимости, приводили и приводят к поистине удивительным результатам в самой математике. В качестве примера можно указать два знаменитых результата А.И.Мальцева, который в 1937 г. доказал теорему компактности, а в 1941 г. использовал эту теорему для доказательства теорем уже в самой алгебре [3]. Теорема компактности описывает математическое свойство языка первого порядка через его семантику. С точки зрения логики свойство компактности определяет тот тип следования, который мы считаем желательным при формализации математического доказательства. Оказалось, что эти на первый взгляд абстрактные рассмотрения проблем логического следования являются чрезвычайно полезными в самой математике. Таким образом, логика оказалась полезным орудием в собственно математической теории – современной алгебре.

Дальнейшие исследования показали эффективность использования математической логики (теории моделей) и в других разделах современной математики (нестандартном анализе и др.). Теория моделей стала также средством нахождения новых важных понятий в современной математике (понятие модельного компаньона А.Робинсона и т.п.). В этом аспекте теория моделей играет такую же роль, как и теория категорий. Недавние результаты Е.Хрущовского показали, что методы теории моделей можно успешно применять и для решения проблем классической математики (доказательство гипотезы Морделла – Ленга и Мамфорда). Последние работы автора настоящей статьи по теории полей классов можно рассматривать как использование теоретико-модельной идеологии для нахождения новых важных понятий в классической математике (хорошие и удивительные расширения полей алгебраических чисел вместо кольца аделей), которые позволяют построить алгоритмы для вычисления классических символов Артина.

Примечания

1. Ср., например, раздел “Математика становится машиной по производству открытий” в статье Р.Коллинза “Наука быстрых открытий как результат скрещения интеллектуальных сетей” (Философия науки. – 2002. – № 2 (13). – С. 3–26).

2. Определение вычислимых функций, данное Геделем, носило синтаксический характер, и лишь установление совпадения этого класса с классом общерекурсивных функций (вместе с формулировкой и “принятием” тезиса Черча) показало действительную значимость теоремы о неполноте.

3. Как пример приведем такую замечательную теорему: если всякая конечнопорожденная подгруппа группы G имеет точное матричное представление фиксированной степени n, то и сама группа G имеет точное матричное представление степени n.

Институт математики СО РАН,
г.Новосибирск

Ershov Ju. **The notion of algorithm and his place in mathematics.**

The article is devoted to description of the role algorithm in mathematics. The special attention deserves the idea that algorithm is considered in algebra and mathematical logic as a mathematical object in spite of normative (in contrast to descriptive) role in mathematical contexts. It is shown that proper presentation of algorithm is given in mathematical logic, and the very notion of computability so important in computer applications plays also increasing role in getting new interesting results in both classical and modern mathematics.