ЧТО ДЕЛАТЬ ПОСЛЕ УСТАНОВЛЕНИЯ НЕРАЗРЕШИМОСТИ АЛГОРИФМИЧЕСКОЙ ПРОБЛЕМЫ?

Ю.Матиясевич

Ленинград, СССР

Наша встреча представляет довольно редкую возможность обсуждать не только математические результаты, но и говорить "вокруг" математики. Я хочу воспользоваться этим случаем и рассмотреть вопрос, который здесь уже затрагивался, а именно, как поступать с алгорифмически неразрешимыми проблемами. Я буду рассматривать только одну конкретную алгорифмическую проблему, которая может служить иллюстрацией положения с алгорифмическими проблемами вообще.

Мы знаем из чрезвычайно содержательных докладов профессора Г.Земанека, что Аль-Хорезми не был знаком с работами Диофанта. Последний рассмотрел в своих работах большое число конкретных уравнений специального типа, который теперь носит его имя.

Вообразим на мгновение, что Аль-Хорезми все же был знаком с результатами Диофанта, которые для разных уравнений были получены с помощью ad hoc методов. В духе Аль-Хорезми было бы попытаться найти единый метод, пригодный для всех диофантовых уравнений. (В действительности эта проблема была поставлена через десять столетий Давидом Гильбертом в его знаменитых "Математических проблемах"). Но теперь мы знаем, что Аль-Хорезми потерпел бы неудачу в попытке найти такой единый метод. Мы можем доказать, что не существует алгорифма, который позволял бы по произвольному диофантову уравнению узнавать, есть ли у него решения. Возникает вопрос: что мы выгадали от такого доказательства?

Один из возможных ответов на этот вопрос таков: нахождение какого-либо алгорифма экономит, по крайней мере теоретически, рабочее время квалифицированных математиков, поскольку теперь за соответствующую проблему смогут взяться менее

квалифицированные математики или вообще ЭВМ. Доказательство несуществования алгорифма для какой-либо проблемы также экономит рабочее время математиков, поскольку теперь они не станут тратить свое время и усилия на неизбежно бесплодные попытки найти алгорифм для решения рассматриваемой проблемы. В некотором смысле такое доказательство (и только оно!) дает математикам "моральное право" отложить проблему в сторону.

Но был ли бы Аль-Хорезми удовлетворен нашим доказательством невозможности разрешающей процедуры для диофантовых уравнений? Вероятно, что нет. Вспомним, что исходной проблемой была не массовая проблема, касающаяся всех диофантовых уравнений сразу, а проблема решения конкретных и довольно простых уравнений, изучавшихся Диофантом. Можно сказать, что исходная проблема была "переобобщена". С интуитивной точки зрения невозможность единой разрешающей процедуры для диофантовых уравнений вызвана тем, что среди них есть некоторые очень сложные уравнения. Я хотел бы дать вам представление о таких уравнениях, известных в настоящее время.

Рассмотрим следующую систему диофантовых уравнений, которая легко может быть преобразована в одно уравнение:

$$elg^2 + \alpha = (b - xy)q^2,\ q = b^{5^{60}},\ \lambda + q^4 =$$
$$= 1 + \lambda b^5,\ \theta + 2z = b^5,\ l = u + t\theta,$$
$$e = y + m\theta,\ n = q^{16},\ r = [g + eq^2 + lq^5 +$$
$$+ (2(e - z\lambda)(1 + xb^5 + g)^4 + \lambda b^5 + \lambda b^5 q^4)q^4][n^2 - n] +$$
$$+ [q^3 - bl + 1 + \theta\lambda q^3 + (b^5 - 2)q^5][n^2 - 1],$$
$$p = 2ws^2r^2n^2,\ p^2k^2 - k^2 + 1 = \tau^2,\ 4(c - ksn^2)^2 +$$
$$+ \eta = k^2,\ k = r + 1 + hp - h,\ a = (wn^2 + 1)rsn^2,$$
$$c = 2r + 1 + \varphi,\ d = bw + ca - 2c + 4a\gamma - 5\gamma,$$
$$d^2 = (a^2 - 1)c^2 + 1,\ f^2 = (a^2 - 1)i^2c^4 + 1,$$
$$(d + of)^2 = ((a + f^2(d^2 - a))^2 - 1)(2r + 1 + jc)^2 + 1.$$

Эту систему уравнений построил Дж.Р.Джоунс (J.P.Jones), который доказал, что не существует алгорифма, который позволял бы узнать по произвольным значениям параметров u,x,y,z, имеет ли эта система решение в натуральных числах. Рассматриваемая система является одной из простейших ныне известных алгорифмически неразрешимых параметрических систем, однако ясно, что она намного сложнее любой конкретной системы диофан-

товых уравнений, когда-либо рассматривавшихся в теории чисел.

Теперь можно ставить более скромную проблему о существовании разрешающей процедуры для какого-либо собственного подкласса всех диофантовых уравнений. И действительно, в этом направлении был достигнут известный прогресс К.Л.Зигелем (K.L.Seigel) в 1972 г. (неразрешимость общего случая известна с 1970 г.). А именно, он рассмотрел уравнения второй степени и нашел для них соответствующий алгорифм. Это воодушевляет на поиск алгорифмов для уравнений третьей, четвертой степени и т.д. Ясно, что это занятие для специалистов по теории чисел. Однако, как только они встретят непреодолимые трудности, специалисты по теории алгорифмов смогут попытаться показать принципиальный характер трудностей, доказав алгорифмическую неразрешимость соответствующей массовой проблемы. Для рассматриваемого нами примера известно, что не существует разрешающей процедуры для уравнений четвертой степени. Таким образом, единственным открытым случаем остается класс уравнений третьей степени, который является вызовом как специалистам по теории чисел, так и специалистам по теории алгорифмов.

Предположим теперь, что мы узнали ответ для случая уравнений третьей степени, что тогда? Очевидно, можно ввести более тонкую классификацию, например, ограничивая как степень, так и число неизвестных (в действительности выбор классификации может оказаться критическим, особенно для успеха в нахождении разрешающей процедуры). Введя более тонкую классификацию, мы получим снова поле деятельности как для специалистов по теории чисел, так и для специалистов по теории алгорифмов.

Резюмируя, можно сказать, что доказательство алгорифмической неразрешимости массовой проблемы никогда не является заключительной точкой наших исследований, это всегда отправная точка для изучения более тонких вопросов. Образно говоря, мы можем быть более или менее удовлетворены алгорифмами, которые мы нашли, но мы никогда не можем быть вполне удовлетворены нашими теоремами о невозможности алгорифмов. Аль-Хорезми не одобрил бы это.