Н. Н. Осипов, Символьные вычисления в математических доказательствах (computer assisted proofs), *Матем. обр.*, 2020, выпуск 2, 42–47

Символьные вычисления в математических доказательствах (computer assisted proofs)

Н. Н. Осипов

В статье приводятся примеры применения систем компьютерной алгебры к доказательству теорем в элементарной геометрии, алгебре и теории чисел.

Как научная дисциплина компьютерная алгебра ориентируется на создание алгоритмов, предназначенных для точного решения математических и прикладных задач с помощью компьютера. В частности, имеющиеся в настоящее время системы компьютерной алгебры (их довольно много, несколько десятков) можно использовать как средство для доказательства различных математических теорем. Такой подход особенно актуален там, где (логически) простому методу доказательства препятствуют слишком громоздкие преобразования. В данной статье приводятся примеры таких ситуаций и показывается, как символьные вычисления позволяют преодолеть трудности технического характера.

Хорошо известно, как с помощью методов компьютерной алгебры можно доказывать (и даже получать новые) теоремы элементарной геометрии (см., например, [10]). Это стало возможным благодаря появлению и совершенствованию алгоритмов решения полиномиальных систем уравнений (алгоритм Бухбергера). Существует довольно широкий класс теорем планиметрии [7], для доказательства которых можно обойтись более элементарными средствами и тем самым избежать применения «тяжелой артиллерии коммутативной алгебры». Следующая теорема является типичным примером.

Теорема 1. *Пусть ABC — произвольный треугольник, AA_1, BB_1, CC_1 — его биссектрисы, I — инцентр треугольника ABC P_1, P_2, P_3, P_4 P_5, P_6 — инцентры треугольников AB_1I, A_1BI, BC_1I, B_1CI, CA_1I, C_1AI соответственно. Тогда шесть точек P_j лежат на одной кривой 2-го порядка.*

Первоначально эта «теорема об инцентрах» возникла в виде гипотезы и впервые была доказана именно средствами компьютерной алгебры (подробности см. в статьях [7, 8]). Попутно выяснилось, что справедлив еще целый ряд подобных теорем, в которых вместо некоторых инцентров указанных треугольников фигурируют их эксцентры. Такая роскошь стала возможной благодаря вычислительному методу доказательства, основанному на символьных преобразованиях. Позднее было найдено геометрическое доказательство [6], которое, впрочем, тоже не обходится без громоздких вычислений. Другие примеры обоснования (и опровержения) подобных элементарно-геометрических гипотез с помощью различных систем компьютерной алгебры можно найти в статьях [4, 5].

Следующий пример связан с диофантовыми уравнениями. Как известно (10-я проблема Гильберта), задача решения произвольных диофантовых уравнений алгоритмически неразрешима, поэтому создание алгоритмов решения для каких-либо классов диофантовых уравнений является содержательной проблемой как теории чисел, так и компьютерной алгебры.

Рассмотрим, например, семейство диофантовых уравнений вида

$$xy^2 + (ax^2 + bx + c)y + Ax^4 + Bx^3 + Cx^2 + Dx + E = 0. \tag{1}$$

В статье [12] предлагается алгоритм решения в целых числах уравнений этого семейства, основанный на следующей теореме.

Теорема 2. *Пусть* $(x, y) \in \mathbb{Z}^2$ *— решение уравнения* (1)*,* $x \neq 0$*. Тогда число*

$$k = \frac{c^3 y + \left(c^2 D + E^2 - bcE\right) x + c^2 E}{x^2} \tag{2}$$

является целым.

Самый простой способ доказать теорему 2 состоит в следующем. Выразим из уравнения (1) коэффициент E:

$$E = -xy^2 - (ax^2 + bx + c)y - Ax^4 - Bx^3 - Cx^2 - Dx.$$

Далее подставим это выражение в правую часть (2). После сокращения на x^2 мы получим явное, но довольно громоздкое выражение для k в виде многочлена из $\mathbb{Z}[x, y]$ (по этой причине оно здесь не приводится). Теперь очевидно, что при целых значениях x, y значения k также должно быть целыми. Теоремы типа теоремы 2 (еще один пример см. в статье [11]) служат основой для элементарной версии метода Рунге для решения диофантовых уравнений малой степени.

Следующие два примера относятся к алгебре (точнее, к теории конечных полей). Мы будем использовать некоторые базовые факты о конечных полях $\mathbb{F}_q$ где q есть степень простого числа p (см., например, [3], а также общий учебник алгебры [1]).

Рассмотрим сравнение

$$x^3 + x^2 - 2x - 1 \equiv (\mathrm{mod}\, p),$$

где p — простое число. Экспериментируя с разными p, можно обнаружить такую закономерность: сравнение разрешимо для $p = 7$, а также для $p \equiv \pm 1 \pmod 7$; для остальных p оно неразрешимо. Оказывается, это связано с тем, что многочлен в левой части сравнения имеет специальные «тригонометрические» корни:

$$x^3 + x^2 - 2x - 1 = \prod_{j=1}^{3} \Big(x - 2\cos(2\pi j/7)\Big) \tag{3}$$

Более того, (почти) такая же закономерность наблюдается и для других кубических многочленов, имеющих корни в поле $\mathbb{Q}(2\cos\left(2\pi/7\right))$.

Предложение 1. *Пусть* $f(x) \in \mathbb{Z}[x]$ *— кубический многочлен со старшим коэффициентом* 1*. Предположим, что* $f(x)$ *неприводим над полем рациональных чисел* $\mathbb{Q}$*, но имеет корень в поле* $\mathbb{Q}\big(2\cos(2\pi/7)\big)$*. Тогда сравнение*

$$f(x) \equiv (\mathrm{mod}\, p)$$

разрешимо для тех и только тех простых p *для которых* $D_f \equiv 0 \pmod p$ *или же* $p \equiv \pm 1 \pmod 7$*. Здесь* D_f *— дискриминант многочлена* $f(x)$*.*

Доказательство. Удобно рассуждать в терминах уравнения

$$f(x) = 0 \tag{4}$$

над конечным полем $\mathbb{F}_p$ из p элементов. Пусть $\xi_j = 2\cos(2\pi j/7)$ — корни многочлена (3) и $\xi = \xi_1$ Ясно, что

$$\mathbb{Q}(\xi_1, \xi_2, \xi_3) = \mathbb{Q}(\xi) \qquad [\mathbb{Q}(\xi) : \mathbb{Q}] = 3.$$

Пусть $\alpha = a_0 + a_1\xi + a_2\xi^2$ — корень $f(x)$ в поле $\mathbb{Q}(\xi)$. Тогда другие корни $f(x)$ суть

$$\alpha_j = a_0 + a_1\xi_j + a_2\xi^2, \qquad j = 2,\, 3,$$

поскольку расширение $\mathbb{Q}(\xi)/\mathbb{Q}$ является нормальным, а многочлен $f(x)$ неприводим над $\mathbb{Q}$. Прямым вычислением (например, в СКА Maple) находим

$$f(x) = (x-\alpha)(x-\alpha_2)(x-\alpha_3) = \\ = x^3 + (-3a_0 + a_1 - 5a_2)x^2 + (3a_0^2 - 2a_1^2 + 6a_2^2 - 2a_0a_1 + 10a_0a_2 - a_1a_2)x - \\ - a_0^3 - a_1^3 - a_2^3 + a_0^2a_1 - 5a_0^2a_2 + 2a_0a_1^2 - 6a_0a_2^2 + a_0a_1a_2 + 2a_1a_2^2 + a_1^2a_2.$$

Дискриминант такого многочлена $f(x)$ равен

$$D_f = 7^2(a^3 - a_1a^2 - 2a^2a_2 + a^3)^2$$

Более того, все коэффициенты a_k должны быть целыми числами. Действительно, так как $f(x) \in \in \mathbb{Z}[x]$ нормирован, число α должно быть целым алгебраическим. Хорошо известно, что кольцо целых алгебраических чисел поля $\mathbb{Q}(\eta)$ есть $\mathbb{Z}[\eta]$, где

$$\eta = cos(2\pi/7) + i\sin(2\pi/7)$$

есть примитивный корень 7-й степени из единицы (см., например, [2, гл. IV]). Поскольку $\xi = \eta + \eta^{-1}$, отсюда легко получить, что кольцо целых алгебраических чисел поля $\mathbb{Q}(\xi)$ совпадает с $\mathbb{Z}[\xi]$.

I. Предположим, что $f(a) = 0$ для некоторого $a \in \mathbb{F}_p$, где p не делит D_f (т. е. $p \neq 7$ и p не делит $a_2^3 - a_1a_2^2 - 2a_1^2a_2 + a_1^3$). Пусть

$$b = \frac{b_0 + b_1a + b_2a^2}{a_2^3 - a_1a_2^2 - 2a_1^2a_2 + a_1^3},$$

где

$$b_0 = -a_0a_1^2 - a_0^2a_2 - a_2^3 + 2a_1a_2^2 + 2a_0a_1a_2 - 3a_0a_2^2,$$
$$b_1 = a_1^2 - 2a_1a_2 + 3a_2^2 + 2a_0a_2,$$
$$b_2 = -a_2.$$

С помощью Maple легко проверить, что $b \in \mathbb{F}_p$ удовлетворяет равенству

$$b^3 + b^2 \ - 2b - 1 = 0. \tag{5}$$

Пусть $\omega \in \mathbb{F}_{p^2}^*$ — корень многочлена $x^2 - bx + 1 \in \mathbb{F}_p[x]$ Имеем $b = \omega + \omega^{-1}$ Подставив это в (5) и упростив, мы получим

$$\omega^6 + \omega^5 + \cdots + 1 = 0.$$

Отсюда $\omega^7 = 1$, при этом $\omega \neq 1$ (так как $p \neq 7$). Значит, $\mathrm{ord}(\omega) = 7$ и по теореме Лагранжа $p^2 - 1 = |\mathbb{F}_{p^2}^*|$ делится на 7. Таким образом, $p \equiv \pm 1 \pmod 7$.

II. Если p делит D_f, то уравнение (4) разрешимо. Действительно, в противном случае многочлен $f(x)$ будет неприводимым над $\mathbb{F}_p$ и, следовательно, не сможет иметь кратных корней, что противоречит равенству $D_f = 0$ в $\mathbb{F}_p$.

III. Предположим, что $p \equiv \pm 1 \pmod 7$. Тогда уравнение (4) также разрешимо. Чтобы показать это, рассмотрим два случая.

(a) Пусть $p \equiv 1 \pmod 7$ Поскольку мультипликативная группа $\mathbb{F}_p^*$ является циклической, существует $\omega \in \mathbb{F}_p^*$ для которого $\omega^7 = 1$ и $\omega \neq 1$. Для $b = \omega + \omega^{-1} \in \mathbb{F}_p$ имеет место равенство (5). Тогда для

$$a = a_0 + a_1b + a_2b^2$$

мы получим $f(a) = 0$ в $\mathbb{F}_p$, что и требовалось.

(b) Пусть $p \equiv -1 \pmod 7$ По аналогии с (a) существует такой $\omega \in \mathbb{F}_{p^2}^*$, для которого $\omega^7 = 1$ и $\omega \neq 1$. Как следствие, $\omega^{p+1} = 1$, т. е. $\omega^p = \omega^{-1}$. Пусть $b = \omega + \omega^{-1}$. Тогда

$$\varphi(b) = (\omega + \omega^{-1})^p = \omega^p + \omega^{-p} = \omega^{-1} + \omega = b,$$

где $\varphi\colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ — автоморфизм Фробениуса. Значит, $b \in \mathbb{F}_p$. Далее можно рассуждать так же, как и в (a). Предложение доказано.

Замечание. В случае $p \equiv \pm 1 \pmod 7$ уравнение (4) имеет три корня.

Предложение 2. *Пусть $p \neq 7$ и $p \not\equiv \pm 1 \ ((\mathrm{mod}\, 7))$. Тогда*

$$\sum_{a \in \mathbb{F}_p} \frac{1}{a^3 + a^2 - 2a - 1} = \begin{cases} \frac{2}{7} & \text{при } p \equiv \pm 2 \ ((\mathrm{mod}\, 7)) \\ -\frac{1}{7} & \text{при } p \equiv \pm 3 \ ((\mathrm{mod}\, 7)) \end{cases}$$

Доказательство. Для вычисления указанной суммы можно воспользоваться следующим общим утверждением.

Лемма. *Пусть $f(x), g(x) \in \mathbb{F}_p[x]$ — два многочлена, при этом $g(x)$ неприводим над $\mathbb{F}_p$, $n = \deg g(x) > 1$ и $\deg f(x) < n$. Тогда*

$$\sum_{\alpha \in \mathbb{F}_p} \frac{f(\alpha)}{g(\alpha)} = \sum_{j=0}^{n-1} \left(\frac{f(\alpha)}{g'(\alpha)(\alpha^p - \alpha)} \right)^{p^j},$$

где $\alpha \in \mathbb{F}[x]/g(x) \cong \mathbb{F}_{p^n}$ — корень $g(x)$.

В нашем случае

$$f(x) = 1; \quad g(x) = x^3 + x^2 - 2x - 1. \tag{6}$$

Как следует из предложения 1, при $p \neq 7$ и $p \not\equiv \pm 1 \pmod 7$ многочлен $g(x)$ неприводим над $\mathbb{F}_p$. Для многочленов (6) имеем

$$\beta = \frac{f(\alpha)}{g'(\alpha)(\alpha^p - \alpha)} = \frac{1}{(3\alpha^2 + 2\alpha - 2)(\alpha^p - \alpha)}. \tag{7}$$

Пусть ω — корень многочлена $x^2 - \alpha x + 1$. Тогда

$$\alpha = \omega + \omega^{-1}, \qquad \omega^7 = 1, \quad \alpha^p = \omega^p + \omega^{-p}.$$

Далее рассмотрим два случая.

(a) $p \equiv \pm 2 \pmod 7$. Здесь $\alpha^p = \omega^2 + \omega^{-2}\alpha^2 - 2$, так что

$$\beta = \frac{1}{(3\alpha^2 + 2\alpha - 2)(\alpha^2 - \alpha - 2)} = \frac{2 - \alpha - \alpha^2}{7}.$$

Значит,

$$\beta^p = \frac{2 - \alpha^p - \alpha^{2p}}{7} = \frac{1 + \alpha}{7}, \qquad \beta^{p^2} = \frac{1 + \alpha^p}{7} = \frac{-1 + \alpha^2}{7}.$$

Следовательно, искомая сумма $\beta + \beta^p + \beta^{p^2} = 2/7$.

(b) $p \equiv \pm 3 \pmod 7$. Теперь имеем $\alpha^p = \omega^3 + \omega^{-3} = 1 - \alpha - \alpha^2$, так что

$$\beta = \frac{1}{(3\alpha^2 + 2\alpha - 2)(1 - 2\alpha - \alpha^2)} = \frac{\alpha^2 - 2}{7}.$$

В этом случае искомая сумма $\beta + \beta^p + \beta^{p^2} = -1/7$. Предложение доказано.

Можно предложить другой, в некотором смысле более элементарный способ вычисления суммы из предложения 2, не привлекающий конечные расширения поля $\mathbb{F}_p$.

Пусть $\zeta = \cos(2\pi/N) + i\sin(2\pi/N)$ — первообразный корень N-й степени из единицы в поле комплексных чисел $\mathbb{C}$.

1. Рассмотрим сумму

$$S = \sum_{k=0}^{N-1} \frac{1}{\zeta^{3k} + \zeta^{2k} - 2\zeta^k - 1}. \tag{8}$$

Формально, S принадлежит круговому полю $\mathbb{Q}(\zeta)$, но фактически S является рациональным числом при любом N (легко следует из основной теоремы о симметрических многочленах). Более того, с помощью теории вычетов (комплексный анализ) можно показать, что

$$S = N \sum_{j=1}^{3} \frac{1}{(3\xi_j^2 + 2\xi_j - 2)(\xi_j - \xi_j^{N+1})} - N, \tag{9}$$

где $\xi_j = 2\cos(2\pi j/7) = \eta^j + \eta^{-j}$ (подробности см. в статье [9]).

2. Пусть $I = (p)$ — простой идеал в кольце целых чисел $\mathbb{Z}$ и $\mathbb{Z}_I \subset \mathbb{Q}$ — соответствующее локальное кольцо (см., например, [2 гл. I]). Положим $N = p-1$ и рассмотрим подкольцо $\mathbb{Z}_I[\zeta] \subset \mathbb{Q}(\zeta)$. Покажем, что все слагаемые суммы (8) лежат в $\mathbb{Z}_I[\zeta]$ если $p \neq 7$ и $p \neq \pm 1$ $((\mathrm{mod}\, 7))$. Действительно, можно доказать, что

$$\prod_{k=0}^{N-1} (\zeta^{3k} + \zeta^{2k} - 2\zeta^k - 1) = (-1)^N \prod_{j=1}^{3} (\xi_j^N - 1)$$

для любого N (см. [9]). Следовательно, нужно лишь убедиться в том, что

$$\prod_{j=1}^{3} \left(\xi^{p-1} - \xi_j\right) \not\equiv 0 \ (\mathrm{mod}\, p).$$

Для этого заметим, что

$$\xi^p = (\eta^j + \eta^{-j})^p \equiv \eta^{pj} + \eta^{-pj} = \eta^{rj} + \eta^{-rj} = \xi_{rj} \ (\mathrm{mod}\, p),$$

где $p \equiv r \ (\mathrm{mod}\, 7)$ и $r \in \{\pm 2, \pm 3\}$, Если, например, $r = \pm 2$ то получим

$$\prod_{j=1}^{3} (\xi^p - \xi_j) = (\xi_2 - \xi_1)(\xi_3 - \xi_2)(\xi_1 - \xi_3) \equiv 7 \ (\mathrm{mod}\, p)$$

(и аналогично в случае $r = \pm 3$).

3. Теперь можно воспользоваться гомоморфизмом

$$\psi\colon \mathbb{Z}_I[\zeta] \to \mathbb{F}_p,$$

который определяется условием $\psi(\zeta) = c$, где c — фиксированный генератор мультипликативной группы $\mathbb{F}_p^*$. Другими словами, имеет место равенство

$$\psi(S) = \sum_{\alpha \in \mathbb{F}_p^*} \frac{1}{\alpha^3 + \alpha^2 - 2\alpha - 1}.$$

Это позволяет найти искомую сумму, вычислив правую часть равенства (9) по модулю p. Но, фактически, этот другой путь очень близок к тому, что предложен выше (достаточно сравнить выражение (7) для β с выражением для слагаемых в правой части (9)).

Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ в рамках мероприятий по созданию и развитию региональных НОМЦ (Соглашение 075-02-2020-1534/1).

Литература

1. Винберг Э.Б. Курс алгебры: Электронное издание. - М.: МЦНМО, 2014.

2. Ленг С. Алгебраические числа. - М.: Мир, 1966.

3. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. - М.: Мир, 1988.

4. Есаян А.Р., Добровольский Н.Н. Компьютерное доказательство гипотезы о центроидах // Чебышевский сборник. - 2017. - Т. 18. - № 1. - С. 73-91.

5. Есаян А.Р., Якушин А.В. Экспериментальное обоснование гипотез в GeoGebra // Чебышевский сборник. - 2017. - Т. 18. - № 1. - С. 92-108.

6. Каюмов О.Р., Каширина К.Е. Элементарное доказательство гипотезы Штейнгартца для биссектрис // Математическое образование. - 2015. № 3. - С. 3-13.

7. Осипов Н.Н. О механическом доказательстве планиметрических теорем рационального типа // Программирование. - 2014. - № 2. - С. 41-50.

8. Осипов Н.Н. Компьютерное доказательство теоремы об инцентрах // Математическое просвещение. Сер. 3. - Вып. 18. - М.: МЦНМО, 2014. - С. 205-216.

9. Осипов Н.Н. О вычислении конечных тригонометрических сумм // Математическое просвещение. Сер. 3. - Вып. 23. - М.: МЦНМО, 2019. - С. 174-208.

10. Chou S.-C. Mechanical Geometry Theorem Proving. - Dordrecht: D. Reidel Publishing Company, 1988.

11. Osipov N.N., Kytmanov A.A. An algorithm for solving a family of diophantine equations of degree four which satisfy Runge's condition // Компьютерная алгебра: материалы Международной конференции. Москва, 17-21 июня 2019 г. / отв. ред. С.А. Абрамов, Л.А. Севастьянов. - Москва: РУДН, 2019. - С. 154-160.

12. Osipov N.N., Dalinkevich S.D. An algorithm for solving a quartic diophantine equation satisfying Runge's condition // Computer Algebra in Scientific Computing. CASC 2019. Lecture Notes in Computer Science. - Vol. 11661. - Springer, 2019. - P. 377-392.

Осипов Николай Николаевич,
профессор кафедры "Прикладная математика
и компьютерная безопасность" Института
космических и информационных технологий
Сибирского федерального университета (Красноярск),
доктор физико-математических наук.

E-mail: nnosipov@rambler.ru