УДК 51(091)

О ВВЕДЕНИИ ГРУППОВОЙ СТРУКТУРЫ НА МНОЖЕСТВЕ ТОЧЕК КУБИКИ И РЕШЕНИИ ДИОФАНТОВЫХ УРАВНЕНИЙ

Лавриненко Т.А.[1], **Михно Г.А.**[2]
[1]Российский экономический университет им. Г.В. Плеханова, г. Москва
[2]Кафедра вычислительной математики

Поступила в редакцию 20.11.2014, после переработки 18.12.2014.

В статье рассматриваются малоизученные аспекты введения групповой операции на множестве точек кубики в связи с исследованием диофантовых уравнений. Особое внимание уделяется теории индексов У. Стори.

Ключевые слова: диофантовы уравнения, арифметика эллиптических кривых, методы касательной и секущей, сложение точек кубики.

Вестник ТвГУ. Серия: Прикладная математика. 2014. № 4. С. 95–104.

Введение

В любом профессиональном научном сообществе на определенном этапе развития науки неизбежно возникает интерес к истории этой науки, к вопросам генезиса основных ее понятий и методов. Данная статья посвящена неизвестным или малоизученным аспектам введения групповой структуры на множестве точек кубики в связи с задачей решения диофантовых уравнений 3-ей степени. Точнее, мы будем рассматривать проблему решения в рациональных числах диофантова уравнения 3-ей степени вида

$$f(x,y)=0, \tag{1}$$

где $f(x,y)$ – неприводимый над $\mathbb{C}$ многочлен 3-ей степени от переменных x,y с рациональными коэффициентами. Можно сформулировать эту проблему и геометрически как задачу отыскания рациональных точек (то есть точек с рациональными координатами) на плоской алгебраической кривой 3-го порядка, или кубики, задаваемой в декартовых координатах уравнением (1). Если от координат x, y по формулам $x=\frac{u}{w}$, $y=\frac{v}{w}$ перейти к однородным координатам u, v, w, то уравнение (1) преобразуется в уравнение вида

$$F(u,v,w)=0, \tag{2}$$

где $F(u,v,w)$ – однородный многочлен 3-ей степени от переменных u,v,w с рациональными коэффициентами. Переход к уравнению (2) соответствует более общему рассмотрению плоской кривой на проективной плоскости P^2. Заметим, что без

ограничения общности коэффициенты в (2) можно считать целыми и что задача решения уравнения (2) в рациональных числах в силу однородности $F(u, v, w)$ эквивалентна задаче решения (2) в целых числах.

Как известно, плоская алгебраическая кривая 3-го порядка может иметь род 0 или 1. В случае рода 0 по одной известной рациональной точке кубики можно найти выражения для координат всех ее рациональных точек в виде рациональных функций одного параметра. Для кривых рода 1, или эллиптических, дело обстоит гораздо сложнее: в этом случае множество рациональных точек кубики нельзя униформизировать с помощью рациональных функций одного параметра, и для нахождения рациональных точек применяют методы касательной и секущей, позволяющие находить по одной или двум известным рациональным точкам только одну новую рациональную точку кривой. **Метод касательной** состоит в нахождении новой рациональной точки кривой по известной рациональной точке P как точки пересечения кривой с касательной к ней в P , а **метод секущей** – в нахождении новой рациональной точки кривой по двум известным рациональным точкам A и B как точки пересечения кривой с прямой, проходящей через A и B. Эти методы можно итерировать, используя в них новые найденные точки и таким образом получая на каждом шаге применения одного из этих методов, вообще говоря, еще одно рациональное решение (1). Методы касательной и секущей лежат также в основе определения операции сложения рациональных точек кривой (1) и позволяют описать структуру множества $X(\mathbb{Q})$ всех рациональных точек кубики рода 1, о чем мы скажем ниже.

Заметим, что сложение точек плоской эллиптической кривой 3-го порядка можно определить для любых двух точек этой кривой, не обязательно рациональных. Сделать это можно геометрически или аналитически. В обоих случаях принято вначале приводить уравнение (1) к нормальной вейерштрассовой форме

$$y^2 = x^3 + ax + b. \tag{3}$$

Если кривая (1) рассматривается над полем $\mathbb{Q}$, то это всегда можно сделать с помощью бирациональных преобразований (с коэффициентами из $\mathbb{Q}$) при условии, что (1) обладает хотя бы одной рациональной точкой. Аналогичное утверждение справедливо и в случае поля $\mathbb{R}$ (с $a, b \in \mathbb{R}$). В случае поля $\mathbb{Q}$ можно считать, что $a, b \in \mathbb{Z}$. Если же (1) рассматривается над полем $\mathbb{C}$, то такое приведение с помощью бирациональных преобразований возможно всегда. Бесконечно удаленную точку $(0 : 1 : 0)$ кривой (3) обозначим P_0.

При геометрическом подходе сумму точек A и B определяют с помощью методов касательной и секущей:

$$A + B = P_0 \circ (A \circ B),$$

где $(A \circ B)$ – точка, получаемая по A и B с помощью метода секущей, если $A \neq B$, или касательной, если $A = B$. Для любой точки $C(x, y)$ точка $C' = P_0 \circ C$ симметрична C относительно оси OX и имеет координаты $(x, -y)$. Другими словами, $A + B$ – это отражение точки $(A \circ B)$ относительно оси OX. Точка P_0 является нулем относительно введенной операции сложения.

При аналитическом подходе используется параметризация точек кубики (3), рассматриваемой над полем $\mathbb{C}$, с помощью эллиптических функций Вейерштрас-

са $\wp(z)$ и $\wp'(z)$ с решеткой периодов $L[\omega_1, \omega_2]$. Эта параметризация задает биекцию между значениями комплексного параметра $z(modL)$ и комплекснозначными точками $P(z) = (\wp(z), \frac{1}{2}\wp'(z))$ кривой (3), при этом бесконечно удаленной точке $(0:1:0)$ сопоставляется параметр $z = 0$. Тогда суммой двух точек A и B с эллиптическими параметрами z_1 и z_2 (или эллиптическими аргументами, согласно [1]) называется точка с эллиптическим параметром $z_1 + z_2$.

Можно установить, что оба эти определения эквивалентны (см., например, [2]). Из аналитического определения сложения точек легко следует, что множество $X(\mathbb{C})$ всех точек эллиптической кривой (3) (над полем $\mathbb{C}$) образует относительно этой операции абелеву группу. Исходя из геометрического определения сложения точек нетрудно получить, что если в уравнении (3) $a, b \in \mathbb{Q}$, то множество $X(\mathbb{Q})$ всех рациональных точек кубики (3) образует подгруппу абелевой группы $X(\mathbb{C})$. Важнейший факт арифметики эллиптических кривых был доказан Л. Дж. Морделлом в 1922 г. Он состоит в том, что группа $X(\mathbb{Q})$ является конечно порожденной.

1. Понятие индекса рациональной точки кубики и оперирование с индексами (Сильвестр)

Исследования И.Г. Башмаковой показали, что методы касательной и секущей восходят еще к Диофанту (3 век н.э.), который применял их алгебраический эквивалент при решении некоторых типов неопределенных уравнений, вообще не используя геометрического языка (см., например, [3]; об истории этих методов после Диофанта см. [3–10]). Первые же попытки ввести с помощью методов касательной и секущей операцию на множестве рациональных точек кубики принадлежат, как было установлено в [8] (см. также [9]), Дж. Дж. Сильвестру, опубликовавшему в 1879/80 годах мемуар [11]. В [11] рассматривается множество Ω всех рациональных точек кривой (2), порожденное одной ее рациональной точкой P_1 с помощью всевозможных применений методов касательной и секущей[1], и множество Ω_1, порожденное точками из $(\Omega \cup I)$, где I – произвольная известная точка перегиба кубики. Сильвестр предлагает остроумный алгоритм нумерации точек из Ω_1, сопоставляя каждой такой точке, отличной от I, некоторое натуральное число или натуральное число со штрихом, называемое ее индексом. Развивая теорию индексов, или «теорию рациональной деривации», как ее называет Сильвестр, он получает ряд результатов о структуре множества Ω_1. В своем исследовании он использует факты из теории алгебраических кривых, но нигде не применяет аналитический аппарат теории эллиптических кривых.

В целях дальнейшего рассмотрения кратко изложим конструкцию Сильвестра. Он вводит запись $(m, n) = p$ или $m, n = p$, означающую, что точка p находится по точкам m и n методом секущей, если $m \neq n$, и методом касательной, если $m = n$. Причем в этой записи в качестве m, n и p могут фигурировать и сами точки, и их индексы. Исходной точке P_1 кубики он приписывает индекс 1, точке (1,1) - индекс 2, точке (2,2) - индекс 4, и далее по правилу

$$(1, 3k+1) = 3k+2, \quad (2, 3k+2) = 3k+4, \quad k \in \mathbb{N}.$$

[1]Во второй части работы Сильвестр отказывается от требования рациональности P_1 и рассматривает множество всех точек кубики, порожденное произвольной ее точкой.

Таким образом получается последовательность точек, содержащихся в Ω, с индексами

$$1,\ 2,\ 4,\ 5,\ 7,\ 8,\ 10,\ 11,\ 13,\ ...,3k+1,\ 3k+2,\ 3k+4,\ 3k+5,\ ..., \tag{4}$$

представляющими собой все натуральные числа, не делящиеся на 3. В [11] доказывается, что множество (4) замкнуто относительно всевозможных применений методов касательной и секущей и, следовательно, совпадает со всем множеством Ω.

Построив «шкалу рациональных производных» (4) точки P_1 кубики, Сильвестр дополняет ее, используя для этого произвольную известную точку перегиба I кубики. Точке кубики, коллинеарной точке с индексом m из (4) и точке I, приписывается тот же индекс, но со штрихом: $(m, I) = m'$. Далее вводятся точки с индексами, делящимися на 3, по правилу:

$$(1', 3k-1) = 3k,$$

и таким образом получается «пополненная шкала рациональных производных» точки P_1:

$$\{1,\ 2,\ 3,\ ...,n,\ ...\} \cup \{1',\ 2',\ 3',\ ...,n',\ ...\}. \tag{5}$$

Если к (5) присоединить еще точку I с индексом 0, то получится множество точек, замкнутое относительно всевозможных применений методов касательной и секущей, то есть это множество совпадает со всем Ω_1. Сильвестр устанавливает это, получая правила для нахождения индекса точки $C = (A, B)$, где A и B – точки с индексами из (5). Эти правила распадаются на целый ряд случаев, различающихся по тому, какие остатки от деления на 3 имеют индексы и есть ли у них штрихи или нет. Например, если $r = 3i+1$, $s = 3j+1$, то $(r, s) = r + s$, $(r', s') = (r + s)'$. Если при этом $s \geqslant r$, то $(r, s') = s - r$ и $(r', s) = (s - r)'$; если $r = 3i+1$, $s = 3j+2$, то $(r, s') = (r + s)'$, если при этом $s \geqslant r$, то $(r, s) = s - r$, и так далее. Сильвестр отмечает, что во всех этих случаях результат применения метода секущей к двум индексам есть или их сумма, или их разность (если не обращать внимания на штрихи) [11, с.70]. Он также отмечает, что координаты точек множества Ω_1 являются рациональными функциями относительно координат исходной точки P_1 и точки перегиба I.

Нетрудно показать, что если эллиптическая кривая 3-го порядка задана в нормальной вейерштрассовой форме (3), в качестве точки перегиба I взята бесконечно удаленная точка $(0 : 1 : 0)$ и α – эллиптический параметр исходной точки P_1, то последовательности (5) индексов точек множества Ω_1 будет соответствовать следующая последовательность эллиптических параметров этих точек:

$$\{\alpha,\ -2\alpha,\ 3\alpha,\ 4\alpha,\ -5\alpha,\ 6\alpha,\ ...,\ -(3k-1)\alpha,\ 3k\alpha,\ (3k+1)\alpha,\ ...\} \cup$$

$$\{-\alpha,\ 2\alpha,\ -3\alpha,\ -4\alpha,\ 5\alpha,\ -6\alpha,\ ...,(3k-1)\alpha,\ -3k\alpha,\ -(3k+1)\alpha,\ ...\} \tag{6}$$

(подробнее об этом см. [8], [9]). Таким образом, индексы точек (если не обращать внимания на штрихи) есть просто модули коэффициентов при α у эллиптических параметров этих точек. Если исходная точка P_1 рациональна, то множество Ω_1, рассмотренное Сильвестром, с современной точки зрения есть не что иное, как подгруппа группы рациональных точек кубики, порожденная одной рациональной точкой (с эллиптическим параметром α). В [11] были сделаны первые шаги по изучению ее строения. Однако, к осознанию того, что на множестве Ω_1 можно

задать групповую структуру, сам Сильвестр не пришел. Введенная им бинарная операция $(\cdot,\cdot)$ не была групповой, а правила оперирования с индексами – достаточно громоздкими. В результате групповая структура множества Ω_1 оказалась завуалированной, а все рассмотрения – усложненными.

2. Теория индексов У. Стори

Существуют различные мнения по поводу того, когда при изучении множества рациональных точек кубической кривой рода 1 стала рассматриваться групповая операция сложения точек. Например, в [3] говорится, что структуру абелевой группы на множестве рациональных точек кубики ввел А.Пуанкаре в 1901 году [1], при этом он использовал эллиптическую параметризацию точек кубики. Н. Шаппахер утверждает, что «понятие абелевой группы было окончательно введено в теорию рациональных точек на кубиках (эллиптических кривых) только к середине 1920-х годов. Вейль был, по-видимому, первым автором, который стал его систематически использовать» [12, с.179]. Но в любом случае историки математики сходятся в том, что после Сильвестра дальнейший прогресс в изучении множества рациональных точек кубики рода 1 был связан с мемуаром Пуанкаре [1]. Мы покажем, что на самом деле уже в 1880 году американский математик У.Стори в [13] кардинально упростил теорию индексов Сильвестра таким образом, что введение операции сложения точек на кубике в современном ее понимании становилось вполне естественным.

В [13] прежде всего отмечается, что «теория рациональной деривации» Сильвестра на кубической кривой была развита «для целей решения арифметической задачи [то есть для задачи о рациональных точках кубики – Т.Л.], но имеет интерес сама по себе с геометрической точки зрения» [13, с.356]. Далее ставится цель «развить эту новую теорию индексов в более общей и симметричной форме» и соединить ее с теорией параметров. Мы указывали выше на связь между индексом точки и ее эллиптическим параметром. На эту связь и обратил внимание Стори. Он ставит задачу так изменить определение индексов, чтобы индекс точки из Ω_1 стал просто равным коэффициенту n у эллиптического параметра $n\alpha$ этой точки [13, с.357]. Он отмечает, что при определенной параметризации неособой кубики с помощью эллиптических функций условие колинеарности трех ее точек с параметрами μ, μ' и μ'' имеет вид:

$$\mu + \mu' + \mu'' \equiv 0 \ (mod(\omega,\, \omega')),$$

где ω, ω' – примитивные периоды эллиптических функций, используемых для параметризации. И далее Стори пишет, что это условие коллинеарности «должно быть нашим руководством при приписывании индексов, чтобы могло существовать упомянутое соотношение между индексом и параметром, то есть для индексов a, b, c трех коллинеарных точек сохраняется фундаментальная формула $a + b + c = 0$» [13, с.357-358]. Стори записывает это равенство в виде

$$[a, b] = -(a + b), \tag{7}$$

где $[a, b]$ означает индекс точки кубики, полученной из точек с индексами a и b с помощью метода секущей, если $a \neq b$, и методом касательной, если $a = b$ (у Сильвестра используется обозначение (a, b)).

Руководствуясь равенством (7), Стори модифицирует процедуру Сильвестра построения множеств Ω и Ω_1 следующим образом. Фиксированной произвольной точке перегиба кубики I он приписывает индекс 0, начальной точке P_1 – индекс 1, а точке $[1,1]$ в соответствии с правилом (7) – индекс (-2) (а не 2, как у Сильвестра). И далее, в соответствии с (7), вводятся индексы точек множества Ω:

$$1 - \text{индекс начальной точки}; \qquad [1,1] = -2;$$

$$[-2,-2] = 4; \qquad [4,1] = -5;$$

$$[-5,-2] = 7; \qquad [7,1] = -8;$$

$$[-8,-2] = 10; \qquad [10,1] = -11;$$

и так далее. Таким образом, точки множества Ω вводятся в той же последовательности, что и у Сильвестра, но при этом изменяется правило, по которому индексы приписываются вводимым точкам. В результате вначале определяются все индексы вида $3m+1$, $m \in \mathbb{Z}$. Стори доказывает, что для любых двух индексов такого вида справедливо рвенство (7). Доказательство аналогично доказательствам Сильвестра для правил оперирования с индексами и опирается на факт из теории алгебраических кривых, который в обозначениях Стори может быть записан следующим образом:

$$[[a,b],[c,d]] = [[a,c],[b,d]]. \tag{8}$$

Далее в [13] вводятся точки с индексами вида $3n-1$, $n \in \mathbb{Z}$. Стори называет точку, коллинеарную с данной точкой A и точкой перегиба I, противоположной к A. Точке, противоположной точке с индексом a, в соответствии с (7), приписывается индекс $-(a)$, то есть $[a,0] = -a$. Рассмотрев все точки, противоположные точкам с индексами вида $3m+1$, $m \in \mathbb{Z}$, Стори получает точки с индексами вида $3n-1$, $n \in \mathbb{Z}$. Для любых двух точек такого вида также доказывается равенство (7). Для этого используется следующий факт из теории алгебраических кривых: точки, противоположные трем коллинеарным точкам кубики относительно одной и той же точки перегиба, также коллинеарны. Поэтому если для двух точек с индексами a и b справедливо (7), то это равенство справедливо и для противоположных точек: $[-a,-b] = -[a,b] = -(-(a+b)) = a+b = -((-a)+(-b))$. Наконец, с помощью равенства $[3m-1,1] = -3m$ вводятся точки с индексами, кратными 3. В результате получается множество точек кубики, совокупность индексов которых совпадает с $\mathbb{Z}$. Далее доказывается, что для любых двух индексов $a, b \in \mathbb{Z}$ выполняется (7). В основе этого доказательства лежат уже упоминавшиеся факты из теории алгебраических кривых.

Таким образом, благодаря новому определению индексов «рациональных производных» начальной точки P_1 вся теория индексов приобрела в [13] более простой и ясный вид. Целый набор данных Сильвестром правил оперирования с индексами был заменен одним единственным равенством (7). Был существенно упрощен и сам вывод этого правила.

Оставалось заметить, что операция сложения чисел-индексов в $\mathbb{Z}$ индуцирует операцию сложения точек кубики из множества Ω_1, порожденного одной рациональной точкой кубики с помощью всевозможных применений методов касательной и секущей и с участием фиксированной точки перегиба I. Другими словами, в качестве суммы точек A и B с индексами a и b, соответственно, нужно взять точку

C с индексом $a+b$. Очевидно, так определенное сложение точек будет групповой операцией на множестве Ω_1 в силу того, что таковым является сложение на множестве $\mathbb{Z}$. Нулевым элементом в Ω_1 является точка перегиба I с индексом, равным 0, а противоположные элементы относительно этой операции – это такие точки A и B, для индексов которых выполнено равенство $a+b=0$, то есть $b=-a$. Именно такие точки называли противоположными и Сильвестр, и Стори. Геометрически они характеризуются тем, что лежат на одной прямой с I.

Из равенства (7) следует, как можно определить групповую операцию сложения точек геометрически. Так как $a+b=-[a,b]$, то точка C с индексом $a+b$ получается из точек A и B с индексами a и b следующим образом: с помощью метода секущей (или касательной, если $A=B$) по точкам A и B кубики находится точка C' и затем в качестве C берется точка кубики, противоположная C' относительно точки перегиба I. Если кубическая кривая рода 1 задана в нормальной вейерштрассовой форме (3) и в качестве I взята бесконечно удаленная точка этой кривой $P_0(0:1:0)$, то приходим к определению сложения точек кубики, приведенному в начале статьи: $A+B=P_0\circ(A\circ B)$.

Во второй части своей работы Стори снова возвращается к вопросу о связи между индексами и параметрами точек на кубической кривой и более подробно говорит о параметризации кубики. Он отмечает, что координаты произвольной точки неособой кубики (то есть эллиптической кривой) могут быть представлены как эллиптические функции одной переменной и что это представление, по-видимому, ввел Клебш в 1864 году. В качестве простейшего такого представления, в котором используются эллиптические функции Якоби, Стори приводит следующее: $x:y:z=sn\mu:(cn\mu\cdot dn\mu):sn^3\mu$. Он вводит обозначение (μ) для точки кубики, которой соответствует значение параметра μ из параллелограмма периодов. Сейчас принято использовать параметризацию, как упоминалось выше, с помощью эллиптических функций Вейерштрасса $\wp(z)$ и $\wp'(z)$. Стори снова отмечает, что если в качестве исходной точки при построении множества Ω_1 взята точка с эллиптическим параметром μ, то точка, индекс которой равен a, будет иметь эллиптический параметр $a\mu$. В его обозначениях это выглядит так: $a\ of\ (\mu)=(a\mu)$. Следовательно,

$$\Omega_1=\{(a\mu)|a\in\mathbb{Z},\ \mu-\ \text{эллиптический параметр исходной точки}\}. \tag{9}$$

Теория индексов, развитая в [13], в сочетании с использованием параметризации неособой кубики с помощью эллиптических функций применяется в [13] для решения некоторых задач теории эллиптических кривых. Мы не будем на них останавливаться, так как это увело бы нас слишком далеко от темы настоящей статьи. Отметим лишь следующее. Теория индексов Сильвестра первоначально была создана для исследования структуры множества рациональных точек кубики. И хотя эта теория, существенно улучшенная, применялась Стори уже для других задач, она, разумеется, могла быть применена и для той задачи, в связи с которой возникла.

Заключение

Введение в историко-математический оборот работы У. Стори [13] заполняет еще одну лакуну в истории групповой операции на множестве точек кубики, а точнее, ее предыстории. Действительно, сам Стори не рассматривал явно операцию

сложения точек, задающую на кубике структуру абелевой группы. Используемая им запись $[a, b]$ служит для обозначения индекса точки, которая получается по методу касательной или секущей, и, следовательно, операция $[\cdot, \cdot]$ не была групповой. Но построив теорию индексов, в отличие от Сильвестровой простую и ясную, и сопоставив каждой точке кубики из Ω_1 некоторое целое число – ее индекс, Стори, так же как и Сильвестр, заменил непосредственное оперирование с точками кубики оперированием с их индексами-числами. Сложение же индексов является групповой операцией. Причем соответствие между сложением индексов, относительно которого множество $\mathbb{Z}$ образует абелеву группу, и геометрической процедурой нахождения новой точки на кубике по двум известным точкам задавалось в достаточно простой форме равенством $a + b = -[a, b]$.

Заметим, что и в мемуаре Пуанкаре 1901 г. [1], базовом для дальнейшего развития арифметики алгебраических кривых, мы также не найдем явно введенной операции сложения точек кубики ранга 1. Интересно, что Пуанкаре, рассматривая в [1] вопрос о всех рациональных точках, порожденных одной ее рациональной точкой с помощью методов касательной и секущей, вводит точки множества Ω точно в той же последовательности, что и Сильвестр, и Стори[2]. Пуанкаре получает описание множества Ω с помощью эллиптических параметров этих точек, имеющих вид $(3n + 1)\alpha$, $n \in \mathbb{Z}$. В некотором смысле Сильвестр и Стори пошли даже дальше Пуанкаре в этом вопросе, не останавливаясь на построении множества Ω, а дополнив его точкой перегиба кубики и построив таким образом множество Ω_1. С современной точки зрения Ω_1 – это циклическая подгруппа группы рациональных точек кубики и групповая структура множества Ω_1 уже просматривается в исследовании Стори.

Наконец, в работе Стори [13] мы впервые сталкиваемся с использованием аналитического аппарата теории эллиптических кривых для исследования структуры множества Ω_1. Именно благодаря такому использованию Стори удается построить стройную теорию индексов с простым правилом оперирования с ними. Он дал также и простое описание множества Ω_1 в виде (9), используя параметризацию неособой кубики с помощью эллиптических функций. В этом отношении он был предшественником Пуанкаре.

Список литературы

[1] Poincaré H. Sur les propriétés arithmétiques des courbes algébriques // Journal de Mathematiques Pures et Appliquees. 1901. Vol. 7. (Русский перевод: Пуанкаре А. Об арифметических свойствах алгебраических кривых. Избранные труды. Т. 2. М.: Наука, 1972.)

[2] Ленг С. Эллиптические функции. М.: Наука, 1984. 312 с.

[3] Башмакова И.Г. Диофант и диофантовы уравнения. М.: Наука, 1972. 68 с.

[4] Bashmakova I.G. Arithmetic of algebraic curves from Diophantus to Poincaré // Historia Mathematica. 1981. Vol. 8, № 4. Pp. 393–416.

[2] Неясно, был ли знаком Пуанкаре с исследованиями Сильвестра и Стори [11], [13]. В [1] вообще нет ссылок на работы других авторов, хотя результаты других математиков там приводятся. Например, результаты, изложенные Пуанкаре для кривых рода 0, были опубликованы Гильбертом и Гурвицем на 11 лет раньше выхода в свет [1].

[5] Башмакова И.Г., Славутин Е.И. История диофантова анализа от Диофанта до Ферма. М.: Наука, 1984. 256 с.

[6] Weil A. Number Theory. An Approach through History: from Hammurapi to Legendre. Boston, etc.: Birkhäuser, 1983. 376 p.

[7] Лавриненко Т.А. Диофантовы уравнения в работах Л. Эйлера. Развитие идей Леонарда Эйлера и современная наука. Сборник статей. М.: Наука, 1988.

[8] Лавриненко Т.А. Решение неопределенных уравнений 3-й и 4-й степени в рациональных числах в 19 в. ВИНИТИ АН СССР, №3669-83. 1982.

[9] Лавриненко Т.А. Из истории арифметики алгебраических кривых в XIX в. // Историко-математические исследования. 1999. № 38(3).

[10] Лавриненко Т.А. О работах Джеймса Сильвестра по диофантову анализу // Функциональные пространства. Дифференциальные операторы. Проблемы математического образования. Тезисы докладов Второй международной конференции. М.: Физматлит, 2003.

[11] Sylvester J.J. On certain ternary cubic-form equations // American Journal of Mathematics. 1879. Vol. 2, № 3. Pp. 280–285.

[12] Schappacher N. Dévelopment de la loi de groupe sur une cubique. Séminaire de Théorie des Nombres de Paris 1988/89 (Progress in Mathematics 91). Boston: Birkhäuser, 1991.

[13] Story W.E. On the theory of rational derivation on a cubic curve // American Journal of Mathematics. 1880. Vol. 3.

Библиографическая ссылка

Лавриненко Т.А., Михно Г.А. О введении групповой структуры на множестве точек кубики и решении диофантовых уравнений // Вестник ТвГУ. Серия: Прикладная математика. 2014. № 4. С. 95–104.

Сведения об авторах

1. **Лавриненко Татьяна Алексеевна**
доцент кафедры высшей математики Российского экономического университета им. Г.В. Плеханова.

Россия, 117997, г. Москва, Стремянный переулок, д. 36, РЭУ им. Г.В. Плеханова. E-mail: tatiana_lavrinenko@mail.ru

2. **Михно Галина Алексеевна**
доцент кафедры вычислительной математики Тверского государственного университета.

Россия, 170100, г. Тверь, ул. Желябова, д. 33, ТвГУ. E-mail: gamikhno@gmail.com

ON THE INTRODUCTION OF A GROUP STRUCTURE ON A CUBIC AND SOLVING DIOPHANTINE EQUATIONS

Lavrinenko Tatyana Alekseyevna
Associate professor of Mathematics department,
Plekhanov Russian University of Economics
Russia, 117997, Moscow, 36 Stremyanny per.

Mikhno Galina Alekseyevna
Associate professor of Computational Mathematics department, Tver State University
Russia, 170100, Tver, 33 Zhelyabova str., TSU.

Received 20.11.2014, revised 18.12.2014.

Insufficiently explored aspects of the group operation introduction on the set of cubic's points are discussed. We consider how this problem is related with Diophantine equations. Special attention is paid to W.Story's theory of indices.

Keywords: diophantine equations, the arithmetic of elliptic curves, the tangent and secant methods, the addition of points on cubic.

Bibliographic citation

Lavrinenko T.A., Mikhno G.A. On the introduction of a group structure on a cubic and solving diophantine equations. *Vestnik TvGU. Seriya: Prikladnaya matematika* [Herald of Tver State University. Series: Applied Mathematics], 2014, no. 4, pp. 95–104. (in Russian)