УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2024, Т. 166, кн. 2
С. 147–161

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 511.61

doi: 10.26907/2541-7746.2024.2.147-161

ДИОФАНТОВО УРАВНЕНИЕ, ПОРОЖДЕННОЕ ПОДПОЛЕМ КРУГОВОГО ПОЛЯ

И.Г. Галяутдинов, Е.Е. Лаврентьева[1]

[1]*Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия*

Аннотация

Построены две формы $f(x,y,z)$ и $g(x,y,z)$ третьей степени, значения которых являются нормами чисел подполей степени три круговых полей K_{13} и K_{19} соответственно. С использованием закона разложения в круговом поле решены диофантовы уравнения $f(x,y,z)=a$ и $g(x,y,z)=b,\ a,b\in\mathbb{Z},\ a\neq 0,\ b\neq 0$. Доказаны утверждения, позволяющие по каноническому разложению на простые множители чисел a и b определить, имеют ли решения собственно уравнения $f(x,y,z)=a,\ g(x,y,z)=b$.

Ключевые слова: целое алгебраическое число, группа Галуа, норма алгебраического числа, главный идеал, фундаментальный базис, закон разложения в круговом поле, диофантово уравнение

Введение

Нахождение решений диофантовых уравнений является одной из востребованных задач математики, в частности, теории чисел [1]. С помощью диофантовых уравнений могут быть описаны различные научные процессы. Диофантовы уравнения встречаются не только в математике, но и в молекулярной физике, органической химии, компьютерных алгоритмах, экономике, теории вероятностей и др. Исходя из этого, вопрос нахождения решений диофантовых уравнений актуален с древних времен и остается таковым на сегодняшний день. Часто рассматриваются диофантовы уравнения первой степени, или линейные. При этом особый интерес вызывают различные способы, в том числе частные, нахождения решений таких уравнений. Так, один их них над евклидовым кольцом рассмотрен в [2]. Поиску решения некоторого класса диофантовых уравнений, основанному на глобальном обобщении цепной дроби, посвящена работа [3].

В настоящей статье мы рассмотрим поиск решений диофантовых уравнений, использовав закон разложения в круговых полях.

Ранее мы рассмотрели решение диофантовых уравнений, использовав однозначность разложения на множители в круговых полях K_7 и K_9. В настоящей работе мы продолжили начатое исследование [4], работая с круговыми полями K_{13} и K_{19}. Отметим, что этой статьей завершается применение метода решения диофантовых уравнений с использованием круговых полей 3-й степени.

В [5, гл. 2] З.И. Боревич и И.Р. Шафаревич изучили диофантовы уравнения, представимые в виде

$$f(x) = N(\gamma) = a, \tag{1}$$

где f – форма от переменных $x = (x_1, \ldots, x_k)$, $\gamma = \alpha_1 x_1 + \ldots + \alpha_k x_k$ – число из алгебраического поля P степени k. В случае, когда $f(x)$ – полная форма [5, с. 99], ими доказано, что за конечное число действий можно описать множество решений уравнения (1).

В [4] уравнение (1) изучено в случае, когда в качестве P использовано подполе степени 3 круговых полей K_7 или K_9. В данной работе в качестве P взято подполе степени 3 круговых полей K_{13} или K_{19}.

Отметим, что в случае круговых полей с однозначным разложением на простые множители уравнение третьей степени порождается подполем только четырех круговых полей K_7, K_9, K_{13}, K_{19}.

Действительно, имеются всего 29 круговых полей с однозначным разложением на простые множители [5, с. 485]. Из них кроме указанных четырех полей по одному подполю степени 3 имеют следующие поля: $K_{21}, K_{27}, K_{28}, K_{35}, K_{36}, K_{45}, K_{84}$. Во всех этих полях в качестве подполя содержится поле K_7 или K_9. Поэтому эти поля порождают то же самое (с точностью до эквивалентности) уравнение третьей степени, что и поле K_7 или K_9.

Пусть n – положительное целое число и $\nu_n = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$. Многочлен $\Phi_n = \prod\limits_{(s,n)=1} (x - \nu_n^s)$ называют n-круговым многочленом, а расширение $K_n = \mathbb{Q}(\nu_n)$ – n-круговым полем. K_n – нормальное расширение поля $\mathbb{Q}$, его степень $[K_n : \mathbb{Q}] = \varphi(n)$ и его группа Галуа $G(K_n/\mathbb{Q})$ изоморфна мультипликативной группе $U\mathbb{Z}_n$ классов вычетов, взаимно простых с n [6, с. 213].

Используем определение нормы элемента [7, с. 174]:

$$N_{E/P}(x) = \sigma_1(x)\sigma_2(x)\ldots\sigma_k(x),$$

а также равенство, которое следует из приведенного определения:

$$N_{E/P}(xy) = N_{E/P}(x)\, N_{E/P}(y). \tag{2}$$

Элемент $N_{E/P}(x)$ неподвижен относительно $G(E/P)$, следовательно, содержится в P.

Пусть E – расширение Галуа конечной степени n поля K, F – расширение Галуа поля E конечной степени m. Для каждого элемента $x \in E$ справедливо равенство [7, с. 176]:

$$N_{F/K}(x) = (N_{E/K}(x))^m.$$

Комплексное число θ называется целым алгебраическим числом, если оно является корнем некоторого многочлена $x^n + a_1 x^{n-1} + \ldots + a_n$, где $a_1, a_2 \ldots, a_n \in \mathbb{Z}$.

Если E – расширение Галуа конечной степени k поля $\mathbb{Q}$, то все целые алгебраические числа θ, принадлежащие полю E, образуют кольцо.

Воспользуемся определением фундаментального базиса $\theta_1, \ldots, \theta_k$ поля E над $\mathbb{Q}$ [5, с. 287].

Пусть E – расширение Галуа степени $[E : \mathbb{Q}] = k$, $G(E/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_k\}$ и $\theta_1, \ldots, \theta_k$ – фундаментальный базис E. Для произвольного целого числа $\gamma \in E$

$$\gamma = x_1\theta_1 + x_2\theta_2 + \ldots + x_n\theta_n$$

вычислим его норму $N_E(\gamma)$. Имеем

$$N(\gamma) = \sigma_1(\gamma)\sigma_2(\gamma)\dots\sigma_k(\gamma) = \prod_{i=1}^{k}(\sigma_i(x_1\theta_1 + \dots + x_k\theta_k)).$$

Это равенство определяет некоторую форму $f(x_1, \dots, x_k)$, коэффициенты которой – симметрические многочлены относительно θ_i. Значит, коэффициенты этой формы будут целыми рациональными числами. Если $N_E(\gamma) = a \in \mathbb{Z}$, то получится уравнение

$$N_E(\gamma) = f(x_1, x_2, \dots, x_k) = a. \tag{3}$$

Равенство (3) означает, что решение уравнения $f(x_1, \dots, x_k) = a$ равносильно нахождению множества целых чисел поля E, норма которых в поле E равна a. Равенство (2) означает, что функция нормы обладает свойством мультипликативности. Поэтому, если $\gamma \in E$ – решение уравнения (3) и $\varepsilon \in E$ – целое число со свойством $N_E(\varepsilon) = 1$, то число $\delta = \varepsilon\gamma$ также решение уравнения (3).

Целые числа $\varepsilon \in E$ со свойством $N_E(\varepsilon) = 1$ содержатся во множестве целых чисел, для которых ε^{-1} также целое число. Такие числа ε называют единицами поля E.

Целое число $\varepsilon \in E$ является единицей поля E тогда и только тогда, когда $N_E(\varepsilon) = \pm 1$ [5, с. 106].

Единицы поля E образуют группу по умножению. Структуру этой группы описывает теорема Дирихле о единицах [5, с. 131]. Согласно этой теореме в поле E имеется конечное число единиц (их называют основными единицами поля E), через которые единственным образом выражается каждая единица поля E.

Два целых числа μ_1 и μ_2 поля E называются ассоциированными, если их отношение $\mu_1/\mu_2 = \varepsilon$ – единица поля E.

Отношение ассоциированности, примененное лишь решением уравнения (3), обладает свойством эквивалентности. Это означает, что все решения уравнения (3) разбиваются на классы ассоциированных решений. Отсюда следует, что все решения из одного класса получаются из одного решения умножением на единицы с нормой 1. Число таких классов решений конечно [5, с. 107].

Таким образом, задача о нахождении всех решений уравнения (3) разбивается на две следующие задачи:

1) найти основные единицы поля E;

2) в поле E найти числа $\mu_1, \dots, \mu_s$ с нормой a так, чтобы они были попарно не ассоциированы и в то же время чтобы всякое $\mu \in E$ с нормой a было ассоциировано с одним их них, т. е. имело вид $\mu = \mu_i\varepsilon$, где $0 \le i \le s$ и ε – единица поля E.

1. Круговое поле K_{13} и его подполя

Приняты обозначения

$$u_k = \cos\frac{2k\pi}{13} + i\sin\frac{2k\pi}{13}, \quad u = u_1, \quad K_{13} = \mathbb{Q}(u), \quad \alpha_k = u_k + u_{13-k} \quad (k = 1, 3, 5, 7, 9, 11),$$

$$t_1 = \alpha_1 + \alpha_5, \quad t_3 = \alpha_3 + \alpha_{11}, \quad t_7 = \alpha_7 + \alpha_9.$$

Группа Галуа $G(K_{13}/\mathbb{Q})$ изоморфна мультипликативной группе $U\mathbb{Z}_{13}$ классов вычетов, взаимно простых с модулем 13. Автоморфизм, соответствующий классу $\overline{s}$,

обозначим через τ_s. Он действует по формуле $\tau_s(u_k) = u_{sk}$, $u_{13} = 1$. Группа $G(K_{13}/\mathbb{Q})$ циклическая и $G(K_{13}/\mathbb{Q}) = (\tau_2)$.

Подгруппу порядка s обозначим через H_s, а поле, инвариантное относительно этой подгруппы, – через F_l, где s и l связаны равенством $sl = \varphi(13) = 12$. В частности,

$$H_2 = \{\tau_1, \tau_{12}\}, \quad F_6 = \mathbb{Q}(u_1 + u_{12}) = \mathbb{Q}\left(2\cos\frac{2\pi}{13}\right), \quad H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}\},$$

$$F_3 = \mathbb{Q}(u_1 + u_5 + u_8 + u_{12}) = \mathbb{Q}(\alpha_1 + \alpha_5) = \mathbb{Q}(t_1).$$

Из включений $H_2 \subset H_4 \subset G(K_{13}/\mathbb{Q})$ следует включение полей $\mathbb{Q} \subset F_3 \subset F_6$.

Найдем группу Галуа $G(F_3/\mathbb{Q})$. Она изоморфна фактор-группе $G(K_{13}/\mathbb{Q})/H_4$ [6, с. 210]. Автоморфизм, соответствующий смежному классу $\tau_i H_4$, обозначим через σ_i и выясним, как действует этот автоморфизм. Смежные классы группы $G(K_{13}/\mathbb{Q})$ по подгруппе H_4 имеют вид

$$\tau_1 H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}\}, \quad \tau_3 H_4 = \{\tau_3, \tau_2, \tau_{11}, \tau_{10}\}, \quad \tau_7 H_4 = \{\tau_7, \tau_9, \tau_4, \tau_6\}.$$

Из того, что F_3 инвариантно относительно H_4, следует, что для любого $\lambda \in F_3$ имеют место равенства: $\lambda = \tau_1(\lambda) = \tau_5(\lambda) = \tau_8(\lambda) = \tau_{12}(\lambda)$. Действуя на эти равенства автоморфизмами τ_3 и τ_7 соответственно, найдем $\tau_3(\lambda) = \tau_2(\lambda) = \tau_{11}(\lambda) = \tau_{10}(\lambda)$ и $\tau_7(\lambda) = \tau_9(\lambda) = \tau_4(\lambda) = \tau_6(\lambda)$. Эти равенства показывают, что все автоморфизмы из одного и того же смежного класса переводят всякий элемент $\lambda \in F_3$ в один и тот же элемент. Поэтому можно считать, что

$$\sigma_1(\lambda) = \tau_1(\lambda) = \tau_5(\lambda) = \tau_8(\lambda) = \tau_{12}(\lambda), \quad \sigma_3(\lambda) = \tau_3(\lambda) = \tau_2(\lambda) = \tau_{11}(\lambda) = \tau_{10}(\lambda),$$

$$\sigma_7(\lambda) = \tau_7(\lambda) = \tau_9(\lambda) = \tau_4(\lambda) = \tau_6(\lambda) \quad \forall \lambda \in F_3.$$

Таким образом, $G(F_3/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_7\}$.

Аналогичным образом можно построить группу автоморфизмов $G(F_k/\mathbb{Q})$ для любого подполя $F_k \subset K_{13}$. В частности, $G(F_6/\mathbb{Q}) = \{\tau_1, \tau_3, \tau_5, \tau_7, \tau_9, \tau_{11}\}$.

Нужно иметь в виду, что выполняются равенства $\tau_1(\lambda) = \tau_{12}(\lambda)$, $\tau_3(\lambda) = \tau_{10}(\lambda)$, $\tau_5(\lambda) = \tau_8(\lambda)$, $\tau_7(\lambda) = \tau_6(\lambda)$, $\tau_9(\lambda) = \tau_4(\lambda)$, $\tau_{11}(\lambda) = \tau_2(\lambda)$ $\forall \lambda \in F_6$.

Необходимо построить форму $f(x, y, z)$, каждое значение которой является нормой некоторого целого алгебраического числа из поля $F_3 = \mathbb{Q}(u_1 + u_5 + u_8 + u_{12})$. Для этого следует найти какой-нибудь фундаментальный базис поля F_3.

Теорема 1. *Числа* $t_1 = \alpha_1 + \alpha_5$, $t_3 = \alpha_3 + \alpha_{11}$, $t_7 = \alpha_7 + \alpha_9$ *составляют фундаментальный базис поля* $F_3 = \mathbb{Q}(t_1)$.

Доказательство. Построим многочлен $\varphi(x) = (x - t_1)(x - t_3)(x - t_7)$. Так как $t_1 + t_3 + t_7 = -1$, $t_1t_3 + t_1t_7 + t_3t_7 = -4$, $t_1t_3t_7 = -1$, то имеем $\varphi(x) = x^3 + x^2 - 4x + 1$.

Так как $\varphi(x)$ неприводим над полем $\mathbb{Q}$, то он – минимальный многочлен числа t_1. Найдем дискриминант этого многочлена и поля $F_3 = \mathbb{Q}(t_1)$. Имеем $D(\varphi) = D(F_3) = 169 = 13^2$. Равенство дискриминантов минимального многочлена числа $t_1 \in F_3$ и поля $F_3 = \mathbb{Q}(t_1)$, в силу теоремы 7.1.7 работы [8, с. 146], означает, что числа $(1, t_1, t_1^2)$ составляют фундаментальный базис поля $F_3 = \mathbb{Q}(t_1)$.

Из равенств $t_1 + t_3 + t_7 = -1$ и $t_1^2 = -4t_1 - 3t_3 - 2t_7$ получим

$$(1, t_1, t_1^2) = (t_1, t_3, t_7)T, \quad T = \begin{Vmatrix} -1 & 1 & -4 \\ -1 & 0 & -3 \\ -1 & 0 & -2 \end{Vmatrix}.$$

Так как $\det T = -1$ и $(1, t_1, t_1^2)$ – фундаментальный базис, то (t_1, t_3, t_7) также фундаментальный базис поля $F_3 = \mathbb{Q}(t_1)$. Теорема 1 доказана.

2. Диофантово уравнение, порожденное подполем $F_3 \subset K_{13}$

Пусть $\gamma \in F_3$ – целое число и $\gamma = xt_1 + yt_3 + zt_7$. Так как (t_1, t_3, t_7) также фундаментальный базис поля F_3, то x, y, z – целые рациональные числа. Найдем норму $N_{F_3}(\gamma)$. Имеем

$$N_{F_3}(\gamma) = \tau_1(\gamma)\tau_3(\gamma)\tau_7(\gamma) = (xt_1 + yt_3 + zt_7)(xt_3 + yt_7 + zt_1)(xt_7 + yt_1 + zt_3).$$

Это равенство определяет норму $f(x, y, z)$, коэффициенты которой – симметрические многочлены относительно t_1, t_3, t_7, и их можно вычислить. Найдем

$$f(x, y, z) = -(x^3 + y^3 + z^3) - 3(x^2y + y^2z + z^2x) + 10(x^2z + y^2x + z^2y) - 19xyz. \quad (4)$$

Таким образом, в случае $E = F_3 = \mathbb{Q}(t_1)$ уравнение (3) примет вид

$$N_{F_3}(\gamma) = f(x, y, z) = a, \quad (5)$$

где $f(x, y, z)$ – форма из равенства (4).

Решение уравнения (5) нужно начинать с описания множества единиц с нормой 1 поля F_3. Базисные элементы t_1, t_3, t_7 являются корнями многочлена $\varphi(x) = x^3 + x^2 - 4x + 1$ и имеют норму $N_{F_3}(t_i) = -1$ $(i = 1, 3, 7)$.

По теореме Дирихле о единицах в поле F_3 должны быть две основные единицы. В работе [8, с. 377] приведена таблица основных единиц тридцати вполне вещественных полей степени 3. Среди них имеется и поле F_3 с дискриминантом $D(F_3) = 169$. Согласно этой таблице основными единицами поля F_3 являются числа $\delta_1 = 2 + 2\theta - \theta^2$ и $\delta_2 = -\theta$, где θ – корень многочлена $\varphi_1(x) = -\varphi(-x) = x^3 - x^2 - 4x - 1$. Если перейти к нашим обозначениям, то $\delta_2 = -\theta = t_1 = \alpha_1 + \alpha_5$ и $\delta_1 = t_3 = \alpha_3 + \alpha_{11}$. Норма этих единиц равна (-1). При решении диофантовых уравнений нужны единицы с нормой $+1$. Поэтому будем считать, что основными единицами поля F_3 являются числа $\varepsilon_1 = -t_1$, $\varepsilon_2 = -t_3$.

Далее, нужно найти полный набор неассоциированных решений уравнения (5) в зависимости от правой части a.

Сначала предположим, что $a = p$ – простое число. В этом случае наличие решения уравнения (5) зависит от порядка числа p по модулю 13. Порядок s числа p по модулю 13 является делителем $\varphi(13) = 12$. Значит, порядок s числа p по модулю 13 равен одному из чисел 1, 2, 3, 4, 6, 12. Рассмотрим все эти случаи.

Случай 1. Порядок простого числа p по модулю 13 равен 1, т. е. $p \equiv 1 \pmod{13}$ и p имеет вид $p = 13k + 1$.

K_{13} – круговое поле с однозначным разложением на множители, и все идеалы его кольца целых чисел главные. Поэтому согласно закону разложения в круговом поле [5, с. 358] или [1, с. 241] имеем $(p) = (\gamma_1)(\gamma_2)\dots(\gamma_{12})$, где γ_i – попарно неассоциированные элементы поля K_{13} и норма $N_{K_{13}}((\gamma_i)) = p$ $(1 \le i \le 12)$. Но норма главного идеала с точностью до знака равна норме порождающего элемента [1, с. 250]. Поэтому для любого $\gamma_i = \gamma$ имеем

$$N_{K_{13}}((\gamma)) = |N_{K_{13}}(\gamma)| = |\tau_1(\gamma)\tau_2(\gamma)\dots\tau_{12}(\gamma)| = p. \quad (6)$$

Положим $\lambda_1 = \tau_1(\gamma)\tau_5(\gamma)\tau_8(\gamma)\tau_{12}(\gamma)$, $\lambda_3 = \tau_3(\gamma)\tau_2(\gamma)\tau_{11}(\gamma)\tau_{10}(\gamma)$, $\lambda_7 = \tau_7(\gamma)\tau_9(\gamma)\tau_4(\gamma)\tau_6(\gamma)$. Можно убедиться, что автоморфизмы подгруппы $H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}\}$ оставляют числа $\lambda_1, \lambda_3, \lambda_7$ на месте. Значит, $\lambda_i \in F_3 = \mathbb{Q}(t_1)$, $i = 1, 3, 7$.

Так как $G(F_3/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_7\}$ и $\sigma_1(\lambda_1) = \tau_1(\gamma)\tau_5(\gamma)\tau_8(\gamma)\tau_{12}(\gamma) = \lambda_1$, $\sigma_3(\lambda_1) = \tau_3(\gamma)\tau_2(\gamma)\tau_{11}(\gamma)\tau_{10}(\gamma) = \lambda_3$, $\sigma_7(\lambda_1) = \tau_7(\gamma)\tau_9(\gamma)\tau_4(\gamma)\tau_6(\gamma) = \lambda_7$, то равенство (6) примет вид

$$N_{K_{13}}((\gamma)) = |N_{K_{13}}(\gamma)| = |\lambda_1\lambda_3\lambda_7| = |\sigma_1(\lambda_1)\sigma_3(\lambda_1)\sigma_7(\lambda_1)| = |N_{F_3}(\lambda_1)| = p.$$

Аналогично получим равенства $|N_{F_3}(\lambda_3)| = p$ и $|N_{F_3}(\lambda_7)| = p$. При этом из того, что γ_i $(1 \le i \le 12)$ попарно не ассоциированы, следует, что $\lambda_1, \lambda_3, \lambda_7$ также попарно не ассоциированы. Таким образом, доказана

Теорема 2. *Пусть $f(x, y, z)$ – форма из равенства* (4) *и $p = 13k+1$ – простое число. Тогда уравнение $N_{F_3}(\gamma) = f(x, y, z) = p$ имеет решение $\lambda \in F_3$. Полный набор его неассоциированных решений состоит из чисел $\sigma_1(\lambda), \sigma_3(\lambda), \sigma_7(\lambda)$.*

Случай 2. Порядок простого числа p по модулю 13 равен 2, т. е. $p^2 \equiv 1 \pmod{13}$. Это означает, что p имеет вид $p = 13k + 12$. По закону разложения в круговом поле имеем $(p) = A_1A_2A_3A_4A_5A_6$ и $N_{K_{13}}(A_i) = p^2$, $1 \le i \le 6$.

Попарно различные простые идеалы $A_i \in K_{13}$, согласно следствию 2 работы [9, с. 72], являются идеалами кольца целых чисел подполя степени $\frac{1}{2}(\varphi(13)) = 6$, т. е. поля F_6. Из того, что K_{13} – поле с однозначным разложением на множители, следует, что эти идеалы A_i являются главными. Значит, имеются такие попарно неассоциированные целые числа $\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6$ поля F_6, что $(p) = (\gamma_1)(\gamma_2)(\gamma_3)(\gamma_4)(\gamma_5)(\gamma_6)$ и $N_{K_{13}}((\gamma_i)) = p^2$, $1 \le i \le 6$.

Из предложения 14.1.3 [1, с. 250] следует, что норма главного идеала с точностью до знака совпадает с нормой порождающего элемента. Поэтому, если (γ) – любой идеал из разложения (p), то $N_{K_{13}}((\gamma)) = |N_{K_{13}}(\gamma)| = p^2$. Но $\gamma \in F_6$. Поэтому согласно предложению [7, с. 176] имеем $|N_{K_{13}}(\gamma)| = (N_{F_6}(\gamma))^2 = p^2$ или

$$|N_{F_6}(\gamma)| = |\tau_1(\gamma)\tau_3(\gamma)\tau_5(\gamma)\tau_7(\gamma)\tau_9(\gamma)\tau_{11}(\gamma)| = p. \tag{7}$$

Введем обозначения $\delta_1 = \tau_1(\gamma)\tau_5(\gamma)$, $\delta_3 = \tau_3(\gamma)\tau_{11}(\gamma)$, $\delta_7 = \tau_7(\gamma)\tau_9(\gamma)$ и вычислим $N_{F_3}(\delta_1)$. Так как

$$\sigma_1(\delta_1) = \tau_1(\gamma)\tau_5(\gamma) = \delta_1, \quad \sigma_3(\delta_1) = \tau_3(\gamma)\tau_{11}(\gamma) = \delta_2, \quad \sigma_7(\delta_1) = \tau_7(\gamma)\tau_9(\gamma) = \delta_7,$$

то равенство (7) примет вид $|N_{F_6}(\gamma)| = |N_{F_3}(\delta_1)| = p$. Аналогично можно получить равенства $|N_{F_3}(\delta_3)| = p$ и $|N_{F_3}(\delta_7)| = p$. Из того, что множители p из разложения (7) попарно не ассоциированы, следует, что числа $\sigma_1, \sigma_3, \sigma_7$ также попарно не ассоциированы. Таким образом, доказана

Теорема 3. *Пусть $f(x, y, z)$ – форма из равенства* (4) *и $p = 13k+12$ – простое число. Тогда уравнение $N_{F_3}(\gamma) = f(x, y, z) = p$ имеет решение $\delta \in F_3$ и числа $\sigma_1(\delta), \sigma_3(\delta), \sigma_7(\delta)$ составляют полный набор его неассоциированных решений.*

Случай 3. Порядок простого числа p по модулю 13 равен 4, т. е. $p^4 \equiv 1 \pmod{13}$.

Этому условию удовлетворяют простые числа видов $p = 13k + 5$ и $p = 13k + 8$. По закону разложения в круговом поле [5, с. 358] или [1, с. 241] имеем $(p) = A_1\,A_2\,A_3$, где A_i – попарно различные простые идеалы и $N_{K_{13}}(A_i) = p^4$, $i = 1, 2, 3$. По следствию 2 работы [9, с. 72] A_1, A_2, A_3 являются идеалами кольца целых чисел поля степени $\frac{1}{4}(\varphi(13)) = 3$, т. е. поля $F_3 = \mathbb{Q}(t_1)$. Из того, что K_{13} – поле с однозначным разложением, следует, что эти идеалы A_i являются главными. Это означает, что имеются такие попарно неассоциированные целые числа $\lambda_1, \lambda_2, \lambda_3 \in F_3$, что $(p) = (\lambda_1)(\lambda_2)(\lambda_3)$ и $N_{K_{13}}((\lambda_i)) = p^4$, $i = 1, 2, 3$.

Но норма главного идеала с точностью до знака совпадает с нормой порождаемого элемента [1, с. 250], поэтому, если (λ) – любой из идеалов $(\lambda_1), (\lambda_2), (\lambda_3)$, то $N_{K_{13}}((\lambda)) = |N_{K_{13}}(\lambda)| = p^4$. Так как $\lambda \in F_3$, то согласно предложению [7, с. 176] имеем $|N_{K_{13}}(\lambda)| = (N_{F_5}(\lambda))^4 = p^4$. Отсюда $|N_{F_3}(\lambda)| = |\sigma_1(\lambda)\sigma_3(\lambda)\sigma_7(\lambda)| = p$. Так как λ – любое из попарно неассоциированных чисел $\lambda_1, \lambda_2, \lambda_3$, то доказана

Теорема 4. *Пусть $f(x, y, z)$ – форма из равенства (4) и $p = 13k + 5$ или $p = 13k + 8$ – простое число. Тогда уравнение $N_{F_3}(\gamma) = f(x, y, z) = p$ имеет решение $\delta \in F_3$ и числа $\delta_1 = \sigma_1(\delta)$, $\delta_2 = \sigma_3(\delta)$, $\delta_3 = \sigma_7(\delta)$ составляют полный набор его неассоциированных решений.*

Случай 4. Порядок простого числа p по модулю 13 равен 3, т. е. $p^3 \equiv 1 \pmod{13}$. Такие числа имеют вид $p = 13k + 3$ или $p = 13k + 9$. Можно установить, что простые числа порядка 3 разлагаются на 4 простых множителя в подполе F_4 степени 4. Но $F_4 \cap F_3 = \mathbb{Q}$. Это означает, что простые числа видов $p = 13k + 3$ или $p = 13k + 9$ в поле $F_3 = \mathbb{Q}(t)$ остаются простыми и уравнение $F_3(\gamma) = f(x, y, z) = p$ не имеет решения.

Случай 5. Простое число p имеет порядок 6, т. е. $p^6 \equiv 1 \pmod{13}$. Это означает, что p имеет вид $p = 13k+4$ или $p = 13k+10$. Повторив рассуждения для случая 4, убедимся, что и в случае 5 в поле F_3 нет числа с нормой p.

Случай 6. Порядок простого числа p равен 12, т. е. $p^{12} \equiv 1 \pmod{13}$. Такие числа имеют вид $p = 13k + t$, $t = 2, 6, 7, 11$. По закону разложения такие числа остаются простыми в поле K_{13} и всех его подполях.

Объединив итоги случаев 4, 5, 6, убедимся, что имеет место

Теорема 5. *Пусть $f(x, y, z)$ – форма из равенства (4) и p – простое число вида $p = 13k+t$, $t = 2, 3, 4, 6, 7, 9, 10, 11$. Тогда уравнение $N_{K_{13}}(\gamma) = f(x, y, z) = p$ не имеет решения.*

Теорема 6. *Пусть $f(x, y, z)$ – форма из равенства (4), p – простое число вида $p = 13k + s$ $(1 \le s \le 12)$, $F_3 = \mathbb{Q}(t_1)$ и $H_4 \subset G(K_{13}/\mathbb{Q})$ – подгруппа автоморфизмов, относительно которой инвариантно поле F_3. Уравнение $N_{F_3}(\gamma) = f(x, y, z) = p$ имеет решение тогда и только тогда, когда автоморфизм $\tau_s \in H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}, \}$, т. е. $s \in \{1, 5, 8, 12\}$.*

Доказательство. Если $p = 13k + 1$, то утверждение следует из теоремы 2, если $p = 13k + 5$ или $p = 13k + 8$, то – из теоремы 4, если $p = 13k + 12$, то – из теоремы 3. Если же $p = 13k + t$, $t = 2, 3, 4, 6, 7, 9, 10, 11$, то в силу теоремы 5 наше уравнение не имеет решения. Теорема 6 доказана.

Рассмотрим теперь случай, когда в правой части уравнения стоит простое число $p = 13$. В этом случае согласно предложению 13.2.7 работы [1, с. 242] имеется главный идеал (λ) такой, что $(13) = (\lambda)^{12}$ и $N_{K_{13}}((\lambda)) = 13$. Отсюда по предложению 14.1.2 работы [1, с. 250] получим

$$N_{K_{13}}((\lambda)) = |N_{K_{13}}(\lambda)| = |\tau_1(\lambda)\tau_2(\lambda)\dots\tau_{12}(\lambda)| = 13.$$

Введем обозначения

$$\sigma_1(\lambda) = \tau_1(\lambda)\tau_5(\lambda)\tau_8(\lambda)\tau_{12}(\lambda), \quad \sigma_3(\lambda) = \tau_3(\lambda)\tau_{11}(\lambda)\tau_2(\lambda)\tau_{10}(\lambda),$$

$$\sigma_7(\lambda) = \tau_7(\lambda)\tau_9(\lambda)\tau_4(\lambda)\tau_6(\lambda).$$

Отсюда, повторив рассуждения, проведенные при изучении случая 1, найдем

$$|\delta_1\delta_3\delta_7| = |\sigma_1(\delta_1)\sigma_3(\delta_1)\sigma_7(\delta_1)| = |N_{F_3}(\delta_1)| = 13.$$

Числа $\sigma_1(\delta_1), \sigma_3(\delta_1), \sigma_7(\delta_1)$ порождают один и тот же идеал (δ_1). Поэтому имеем $(13) = (\delta_1)^3$. Это означает, что доказана

Теорема 7. *Пусть $f(x, y, z)$ – форма из равенства (4). Тогда уравнение*

$$N_{F_3}(\gamma) = f(x, y, z) = 13 \tag{8}$$

имеет решение $\delta \in F_3$ и полный набор неассоциированных решений состоит из одного числа δ.

Запишем формулу общего решения уравнения (8). Из равенства $f(x, -1, 0) = -x^3 + 3x^2 + 10x + 1$ найдем $f(1, -1, 0) = 13$. Значит, $\delta = t_1 - t_3$ – решение и $N_{F_3}(\delta) = (t_1 - t_3)(t_3 - t_7)(t_7 - t_1) = 13$. Указанные три делителя числа 13 должны быть ассоциированы. Действительно, если $\delta_1 = t_1 - t_3$, $\delta_2 = t_3 - t_7$, $\delta_3 = t_7 - t_1$, $\varepsilon_1 = -t_1$, $\varepsilon_2 = -t_3$, то $\delta_1 = \delta_2\varepsilon_1$, $\delta_2 = \delta_3\varepsilon_2$. Отсюда следует, что $(\delta_1) = (\delta_2) = (\delta_3)$ и $(13) = (\delta_1)^3$. Общее решение уравнения (8) имеет вид $\gamma_{k,l} = (t_1 - t_3)\varepsilon_1^k\varepsilon_2^l$, $k, l \in \mathbb{Z}$, $\varepsilon_1 = -t_1$, $\varepsilon_2 = -t_3$.

Перейдем к изучению общего случая, когда в правой части уравнения (5) стоит произвольное целое рациональное число $a \neq 0$.

Определение 1. Целое рациональное число $a \neq 0$ будем называть нормой, если уравнение $N_{F_3}(\gamma) = f(x, y, z) = a$ имеет решение.

Лемма 1. *Если a_1 и a_2 являются нормами, то a_1a_2 – также норма.*

Доказательство. Из условий следует, что имеются такие $\delta_1 \in F_3$, $\delta_2 \in F_3$, что $N_{F_3}(\delta_1) = a_1$, $N_{F_3}(\delta_2) = a_2$. Тогда $N_{F_3}(\delta_1\delta_2) = N_{F_3}(\delta_1)N_{F_3}(\delta_2) = a_1a_2$. Это означает, что уравнение $f(x, y, z) = a_1a_2$ имеет решение $\gamma = \delta_1\delta_2$, которое находится как произведение решений уравнений $f(x, y, z) = a_1$ и $f(x, y, z) = a_2$. Лемма 1 доказана.

Определение 2. Норму a назовем первичной, если она является нормой простого элемента поля F_3.

Лемма 2. *Первичными нормами являются: – все простые числа видов $p = 13k + t$, $t = 1, 5, 8, 12$; – простое число 13; – числа p^3, где p – инертное в F_3 простое число, т. е. $p = 13k + t$, $t = 2, 3, 4, 6, 7, 9, 10, 11$.*

Доказательство. То, что простые числа вида $p = 13k + t$, $t = 1, 5, 8, 12$, – первичные нормы, вытекает из теорем 2, 4, 3 соответственно. Из теоремы 7 следует, что простое число $p = 13$ также первичная норма. Пусть теперь p – инертное в F_3 простое число, т. е. $p = 13k + t$, $t = 2, 3, 4, 6, 7, 9, 10, 11$. Тогда в силу теоремы 5 число p нормой не является. Вычислим норму самого простого в F_3 числа p. Имеем $N_{F_3}(p) = \sigma_1(p)\sigma_3(p)\sigma_7(p) = p^3$.

Таким образом, p^3 – первичная норма. Лемма 2 доказана.

Лемма 3. *Пусть a – норма, а p – инертное в F_3 простое число. Тогда, если a делится на p, то a делится на p^3.*

Доказательство. По условию леммы простое число p остается простым и в поле $F_3 = \mathbb{Q}(t_1)$. Так как a – норма, то имеется такое целое число $\lambda \in F_3$, что $N_{F_3}(\lambda) = \sigma_1(\lambda)\sigma_3(\lambda)\sigma_7(\lambda) = a$. Так как $a \vdots p$ и p – простые числа, то, по крайней

мере, один из трех множителей $\sigma_i(\lambda)$ делится на p. Пусть $\sigma_3(\lambda)\vdots p$ и $\sigma_3(\lambda) = p\mu$, $\mu \in F_3$ – целое число. Применив к равенству $\sigma_3(\lambda) = p\mu$ автоморфизм $\sigma_3^{-1} = \sigma_7$, найдем $\lambda = p\sigma_7(\mu)$. Здесь $\sigma_7(\mu)$ – целое число, поэтому λ делится на p. Тогда получим $N_{F_3}(\lambda) = p^3\sigma_1(\mu)\sigma_3(\mu)\sigma_7(\mu) = a$, т. е. a делится на p^3. Лемма 3 доказана.

Объединив леммы 1 – 3, получим следующее утверждение.

Теорема 8. *Пусть $F_3 = \mathbb{Q}(t_1)$, $f(x, y, z)$ – форма из равенства (4) и $a \neq 0$ – целое рациональное число. Диофантово уравнение $N_{F_3}(\gamma) = f(x, y, z) = a$ имеет решение тогда и только тогда, когда степень инертного в F_3 простого числа, входящего в каноническое разложение числа a, делится на 3.*

Приведем примеры уравнений вида $N_{F_3}(\gamma) = f(x, y, z) = a$, где $f(x, y, z)$ – форма из равенства (4). Требуется установить, имеет ли данное уравнение решение в поле $F_3 = \mathbb{Q}(t_1)$. Если имеет, то нужно указать полный набор его неассоциированных решений.

Примеры уравнений.

2.1. $N_{F_3}(\gamma) = f(x, y, z) = 5$.

2.2. $N_{F_3}(\gamma) = f(x, y, z) = 29$.

2.3. $N_{F_3}(\gamma) = f(x, y, z) = 53$.

2.4. $N_{F_3}(\gamma) = f(x, y, z) = 200$.

Решения.

Пример 2.1. В правой части этого уравнения простое число $p = 5 = 13 \cdot 0 + 5$. Автоморфизм $\tau_5 \in H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}\}$. Согласно теореме 6 данное уравнение имеет решение. Действительно, $f(x, 1, 0) = -x^3 - 3x^2 + 10x - 1$ и $f(1, 1, 0) = 5$. Значит, $\delta = t_1 + t_3$ – решение этого уравнения и числа $\delta_1 = \sigma_1(\delta) = t_1 + t_3$, $\delta_2 = \sigma_3(\delta) = t_3 + t_7$, $\delta_3 = \sigma_7(\delta) = t_7 + t_1$ составляют полный набор его неассоциированных решений.

Пример 2.2. В правой части уравнения простое число $p = 29 = 13 \cdot 2 + 3$. Автоморфизм τ_3 не входит в подгруппу $H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}\}$. По теореме 6 данное уравнение решения не имеет.

Пример 2.3. В правой части уравнения простое число $p = 53 = 13 \cdot 4 + 1$. Автоморфизм $\tau_1 \in H_4 = \{\tau_1, \tau_5, \tau_8, \tau_{12}\}$, и уравнение имеет решение. Действительно, $f(x, -2, 0) = -x^3 + 6x^2 + 40x + 8$ и $f(1, -2, 0) = 53$, т. е. $\lambda = t_1 - 2t_3$ – решение, а числа $\lambda_1 = \sigma_1(\lambda) = t_1 - 2t_3$, $\lambda_2 = \sigma_2(\lambda) = t_3 - 2t_7$, $\lambda_3 = \sigma_7(\lambda) = t_7 - 2t_1$ составляют полный набор его неассоциированных решений.

Пример 2.4. В правой части уравнения составное число $a = 200 = 2^3 \cdot 5^2$. В его разложение входит инертное в поле F_3 простое число $p = 2$, и его степень делится на 3. По теореме 8 данное уравнение имеет решение.

Число $a = 2^3 \cdot 5 \cdot 5$ представляется в виде произведения трех первичных норм 2^3, 5 и 5. Полный набор неассоциированных решений нашего уравнения находится как произведение полных наборов соответствующих уравнений. В примере 2.1 показано, что полный набор неассоциированных решений уравнения $f(x, y, z) = 5$ состоит из чисел $\delta_1 = t_1 + t_3$, $\delta_2 = t_3 + t_7$, $\delta_3 = t_7 + t_1$, а все решения уравнения $f(x, y, z) = 2^3$ ассоциированы с числом $p = 2$. Поэтому полный набор неассоциированных решений уравнения $f(x, y, z) = 200$ состоит из следующих шести чисел: $\lambda_1 = 2\delta_1^2 = -8t_1 - 6t_3 - 6t_7$, $\lambda_2 = 2\delta_2^2 = -6t_1 - 8t_3 - 6t_7$, $\lambda_3 = 2\delta_3^2 = -6t_1 - 6t_3 - 8t_7$, $\lambda_4 = 2\delta_1\delta_2 = 4t_1 + 2t_7$, $\lambda_5 = 2\delta_1\delta_3 = 2t_3 + 4t_7$, $\lambda_6 = 2\delta_2\delta_3 = 2t_1 + 4t_3$.

3. Круговое поле K_{19} и его подполя

Приняты обозначения

$$\nu_k = \cos\frac{2k\pi}{19} + i\sin\frac{2k\pi}{19},\quad \nu = \nu_1,\quad K_{19} = \mathbb{Q}(\nu),\quad \beta_k = \nu_k + \nu_{19-k}\quad (k - \text{нечетно}),$$

$$s_1 = \beta_1 + \beta_7 + \beta_{11},\quad s_3 = \beta_3 + \beta_5 + \beta_{17},\quad s_9 = \beta_9 + \beta_{13} + \beta_{15}.$$

Группа Галуа $G(K_{19}/\mathbb{Q})$ изоморфна мультипликативной группе $U\mathbb{Z}_{19}$ классов вычетов, взаимно простых с модулем 19. Автоморфизм, соответствующий классу $\overline{s}$, обозначим через τ_s. Он действует по формуле $\tau_s(\nu_k) = \nu_{sk}$, $\nu_{19} = 1$. Группа $U\mathbb{Z}_{19}$ циклическая, и $U\mathbb{Z}_{19} = (\overline{2})$. Отсюда следует, что $G(K_{19}/\mathbb{Q}) = (\tau_2)$.

Подгруппу порядка s обозначим через M_s, а поле, инвариантное относительно этой подгруппы, – через E_l, где s и l связаны равенством $sl = \varphi(19) = 18$.

В частности, имеем $M_2 = (\tau_{18}) = \{\tau_{18}, \tau_1\}$, $M_3 = (\tau_7) = \{\tau_7, \tau_{11}, \tau_1\}$, $M_6 = (\tau_8) = \{\tau_8, \tau_7, \tau_{18}, \tau_{11}, \tau_{12}, \tau_1\}$.

Из включений $M_2 \subset M_6$ и $M_3 \subset M_6$ по теории Галуа следуют включения $E_3 \subset E_9$ и $E_3 \subset E_6$.

Группа Галуа $G(E_3/\mathbb{Q})$ изоморфна фактор-группе $G(K_{19}/\mathbb{Q})/M_6$, смежные классы которой имеют вид

$$\tau_1 M_6 = \{\tau_1, \tau_7, \tau_8, \tau_{11}, \tau_{12}, \tau_{18}\},\quad \tau_3 M_6 = \{\tau_3, \tau_2, \tau_5, \tau_{14}, \tau_{17}, \tau_{16}\},$$

$$\tau_9 M_6 = \{\tau_9, \tau_6, \tau_{15}, \tau_4, \tau_{13}, \tau_{10}\}.$$

Повторив рассуждения, приведенные в п. 1 при изучении подполей поля K_{13}, можно убедиться, что все автоморфизмы смежного класса $\tau_i M_6$ $(i = 1, 3, 9)$ любой элемент $\gamma \in E_3$ переводят в один и тот же элемент. Имея в виду этот факт, можно считать, что $G(E_3/\mathbb{Q}) \cong \{\tau_1, \tau_3, \tau_6\}$.

Найдем теперь минимальный многочлен числа $s_1 = \beta_1 + \beta_7 + \beta_{11}$. Сопряженными к s_1 являются числа

$$\tau_1(s_1) = s_1 = \beta_1 + \beta_7 + \beta_{11},\quad \tau_3(s_1) = \beta_3 + \beta_{17} + \beta_5 = s_3,$$

$$\tau_9(s_1) = \beta_9 + \beta_{13} + \beta_{15} = s_9.$$

Многочлен минимальной степени с рациональными коэффициентами с корнем s_1 имеет вид $\psi(x) = (x - s_1)(x - s_3)(x - s_9)$. Так как $s_1 + s_3 + s_9 = -1$, $s_1 s_3 + s_1 s_9 + s_3 s_9 = -6$, $s_1 s_3 s_9 = 7$, то $\psi(x) = x^3 + x^2 - 6x - 7$.

Многочлен $\psi(x)$ неприводим над полем $\mathbb{Q}$ рациональных чисел, и он – минимальный многочлен числа $s_1 = \beta_1 + \beta_7 + \beta_{11}$. Это означает, что s_1 – алгебраическое число степени 3. Можно убедиться, что все автоморфизмы подгруппы M_6 оставляют на месте число $s_1 = \beta_1 + \beta_7 + \beta_{11} = \nu_1 + \nu_7 + \nu_8 + \nu_{11} + \nu_{12} + \nu_{18}$, поэтому $s_1 \in E_3$ и s_1 можно принять в качестве примитивного элемента поля E_3.

Таким образом, установлено, что поле, инвариантное относительно группы $M_6 = \{\tau_1, \tau_7,\ \tau_8, \tau_{11}, \tau_{12}, \tau_{18}\}$, – это $E_3 = \mathbb{Q}(s_1)$.

Теорема 9. *Корни многочлена $\psi(x)$, т. е. числа s_1, s_3, s_9, составляют фундаментальный базис поля $E_3 = \mathbb{Q}(s_1)$.*

Доказательство. Дискриминант $D(\psi)$ многочлена $\psi(x)$ равен дискриминанту $D(E_3)$ поля E_3; $D(\psi) = D(E_3) = 361 = 19^2$. Отсюда в силу теоремы 7.1.7 работы [8, с. 146] получим, что числа $(1, s_1, s_1^2)$ составляют фундаментальный базис поля

$E_3 = \mathbb{Q}(s_1)$. Имеют место равенства $1 = -s_1 - s_3 - s_9$, $s_1 = s_1$, $s_1^2 = -4s_1 - 5s_3 - 4s_9$ или в матричной форме $(1, s_1, s_1^2) = (s_1, s_3, s_9)T$, где

$$T = \begin{Vmatrix} -1 & 1 & -4 \\ -1 & 0 & -5 \\ -1 & 0 & -4 \end{Vmatrix}, \quad \det T = 1.$$

Значит, (s_1, s_3, s_9) наряду с базисом $(1, s_1, s_1^2)$ также является фундаментальным базисом поля $E_3 = \mathbb{Q}(s_1)$. Теорема 9 доказана.

4. Диофантово уравнение, порожденное подполем $E_3 \subset K_{19}$

Пусть $\gamma \in E_3$ – целое число и $\gamma = xs_1 + ys_3 + zs_9$. Так как (s_1, s_3, s_9) – фундаментальный базис поля E_3, то x, y, z – целые рациональные числа. Вычислим норму $N_{E_3}(\gamma)$. Имеем $N_{E_3}(\gamma) = \tau_1(\gamma)\tau_3(\gamma)\tau_9(\gamma) = (xs_1 + ys_3 + zs_9)(xs_3 + ys_9 + zs_1)(xs_9 + ys_1 + zs_3)$. Учитывая, что s_1, s_3, s_9 – корни многочлена $\psi(x) = x^3 + x^2 - 6x - 7$, найдем

$$g(x, y, z) = 7(x^3 + y^3 + z^3) - 17(x^2y + y^2z + z^2x) + 2(x^2z + y^2x + z^2y) + 23xyz. \quad (9)$$

Таким образом, в случае $E = E_3$ уравнение (3) примет вид

$$N_{E_3}(\gamma) = g(x, y, z) = a, \quad (10)$$

где $g(x, y, z)$ – форма из равенства (9).

Для решения уравнения (10) нужны основные единицы поля E_3 с нормой $+1$.

В работе [8, с. 377] приведена таблица основных единиц тридцати вполне вещественных полей степени 3. Среди них имеется и поле E_3 с дискриминантом 361. Примитивный элемент этого поля в таблице обозначен через θ, и он является корнем многочлена $\psi(x) = x^3 + x^2 - 6x - 7$. У нас корни этого многочлена обозначены через s_1, s_3, s_9. Поэтому имеем $\theta = t_1$. В таблице первая основная единица имеет вид $e_1 = 4 + \theta - \theta^2$. В наших обозначениях $e = t_1 + t_3$. Норма $N_{E_3}(e_1) = -1$. Поэтому нужно считать, что первая основная единица поля E_3 имеет вид $\varepsilon = -e_1 = -t_1 - t_3$.

Вторая основная единица по упомянутой таблице имеет вид $e_2 = 5 - \theta^2 = -s_1 - s_9$. Норма $N_{E_3}(e_2) = 1$. Поэтому вторая основная единица поля E_3 имеет вид $\varepsilon_2 = e_2 = -t_1 - t_9$.

Основные единицы поля E_3 выбраны: $\varepsilon_1 = -t_1 - t_3$, $\varepsilon_2 = -t_1 - t_9$. Далее нужно найти полный набор неассоциированных решений уравнения (10) в зависимости от правой части a. Это делается в точности по той же схеме, что и при решении уравнения (5) в поле $F_3 \subset K_{13}$. Поэтому ограничимся тем, что сформулируем две итоговые теоремы и приведем примеры.

Теорема 10. *Пусть $g(x, y, z)$ – форма из равенства (9), p – простое число вида $p = 19k + t$ $(1 \le t \le 18)$, $E_3 = \mathbb{Q}(s_1)$ и $M_6 \subset G(K_{19}/\mathbb{Q})$ – подгруппа автоморфизмов, относительно которой инвариантно поле E_3. Уравнение*

$$N_{E_3}(\gamma) = g(x, y, z) = p \quad (11)$$

имеет решение тогда и только тогда, когда автоморфизм $\tau_t \in M_6 = \{\tau_1, \tau_7, \tau_8, \tau_{11}, \tau_{12}, \tau_{18}\}$, т. е. $t = 1, 7, 8, 11, 12, 18$.

По этой теореме, если простое число p имеет вид

$$p = 19k + t, \quad t = 2, 3, 4, 5, 6, 9, 10, 13, 14, 15, 16, 17, \quad (12)$$

то уравнение (11) не имеет решений. Это означает, что простые числа вида (12) остаются простыми и в поле $E_3 = \mathbb{Q}(s_1)$. Поэтому их называют инертными в поле E_3.

Теорема 11. *Пусть $g(x,y,z)$ – форма из равенства (9) и $a \neq 0$ – целое рациональное число. Уравнение $N_{E_3}(\gamma) = g(x,y,z) = a$ имеет решение тогда и только тогда, когда степень инертного в E_3 простого числа, входящего в разложение числа a, делится на 3.*

Приведем примеры уравнений вида $N_{E_3}(\gamma) = g(x,y,z) = a$, где $g(x,y,z)$ – форма из равенства (9). Требуется установить, имеет ли данное уравнение решение в поле $E_3 = \mathbb{Q}(s_1)$. Если имеет, то нужно указать полный набор его неассоциированных решений.

Примеры уравнений.

4.1. $N_{E_3}(\gamma) = g(x,y,z) = 7$.
4.2. $N_{E_3}(\gamma) = g(x,y,z) = 37$.
4.3. $N_{E_3}(\gamma) = g(x,y,z) = 3$.
4.4. $N_{E_3}(\gamma) = g(x,y,z) = 999$.
4.5. $N_{E_3}(\gamma) = g(x,y,z) = 49$.
4.6. $N_{E_3}(\gamma) = g(x,y,z) = 259$.

Решения.

Пример 4.1. В правой части этого уравнения простое число $7 = 19\cdot 0 + 7$ и автоморфизм $\tau_7 \in M_6 = \{\tau_1, \tau_7, \tau_8, \tau_{11}, \tau_{12}, \tau_{18}\}$. Согласно теореме 10 данное уравнение имеет решение. Действительно, $g(x,0,0) = 7x^3$ и $g(1,0,0) = 7$. Значит, $\delta = s_1$ – решение уравнения 4.1, а числа $\delta_1 = \tau_1(\delta) = s_1$, $\delta_2 = \tau_3(\delta) = s_3$, $\delta_3 = \tau_9(\delta) = s_9$ – полный набор его неассоциированных решений. Умножив эти решения на любую степень основной единицы, можно получить другие решения, ассоциированные с ними. Например,
$\delta_1\varepsilon_1 = s_1(-s_1 - s_3) = 3s_1 + 3s_3 + s_9$, $g(3,3,1) = 7$ или
$\delta_2\varepsilon_1 = s_3(-s_1 - s_3) = 3s_1 + 2s_3 + 2s_9$, $g(3,2,2) = 7$ и т. д.

Пример 4.2. $N_{E_3}(\gamma) = g(x,y,z) = 37$. Из $37 = 19\cdot 1 + 18$ и $\tau_{18} \in M_6$ следует, что решение имеется. Действительно, $f(x,2,0) = 7x^3 - 34x^2 + 8x + 56$ и $f(1,2,0) = 37$. Решением является число $\lambda = s_1 + 2s_3$, а числа $\lambda_1 = \tau_1(\lambda) = s_1 + 2s_3$, $\lambda_2 = \tau_3(\lambda) = s_3 + 2s_9$, $\lambda_3 = \tau_9(\lambda) = s_9 + 2s_1$ составляют полный набор неассоциированных решений.

Пример 4.3. $N_{E_3}(\gamma) = g(x,y,z) = 3$.

Из теоремы 10 следует, что это уравнение не имеет решений.

Пример 4.4. $N_{E_3}(\gamma) = g(x,y,z) = 999$.

В разложение числа $a = 999 = 3^3 \cdot 37$ входит одно инертное в E_3 простое число $p = 3$, и его степень делится на 3. По теореме 11 это уравнение имеет решение, и полный набор его неассоциированных решений находится как произведение решений уравнений $g(x,y,z) = 3^3$ и $g(x,y,z) = 37$. В примере 4.2 указано, что числа $\lambda_1 = s_1 + 2s_3$, $\lambda_2 = s_3 + 2s_9$, $\lambda_3 = s_9 + 2s_1$ составляют полный набор неассоциированных решений уравнения $g(x,y,z) = 37$. Значит, числа $3\lambda_1 = 3s_1 + 6s_3$, $3\lambda_2 = 3s_3 + 6s_9$, $3\lambda_3 = 3s_9 + 6s_1$ составляют полный набор неассоциированных решений уравнения $g(x,y,z) = 999$.

Пример 4.5. $N_{E_3}(\gamma) = g(x,y,z) = 49$.

В разложении числа $a = 49 = 7^2$ нет инертного в E_3 простого числа. По теореме 11 это уравнение имеет решение, и это решение находится как произведение двух решений уравнения 4.1, т. е. чисел $\delta_1 = s_1$, $\delta_2 = s_3$, $\delta_3 = s_9$. Поэтому полный

набор неассоциированных решений уравнения $g(x,y,z)=49$ состоит из следующих шести чисел:

$$s_1^2=-4s_1-5s_3-4s_9,\quad s_3^2=-4s_1-4s_3-5s_9,\quad s_9^2=-5s_1-4s_3-4s_9,$$

$$s_1s_3=s_1+2s_3+3s_9,\quad s_1s_9=2s_1+3s_3+s_9,\quad s_3s_9=3s_1+s_3+2s_9.$$

Пример 4.6. $N_{E_3}(\gamma)=g(x,y,z)=259$.

В разложении числа $a=259=7\cdot 37$ нет инертного в поле E_3 простого числа. По теореме 11 это уравнение имеет решение, которое находится как произведение решений уравнения 4.1 и 4.2, т. е. чисел $\delta_1=s_1$, $\delta_2=s_3$, $\delta_3=s_9$ и $\lambda_1=s_1+2s_3$, $\lambda_2=s_3+2s_9$, $\lambda_3=s_9+2s_1$. Отсюда следует, что полный набор неассоциированных решений уравнения 4.6 состоит из следующих девяти чисел:

$$\delta_1\lambda_1=-2s_1-s_3+2s_9,\quad \delta_2\lambda_2=2s_1-2s_3-s_9,\quad \delta_3\lambda_3=-s_1+2s_3-2s_9,$$

$$\delta_1\lambda_2=5s_1+8s_3+5s_9,\quad \delta_2\lambda_3=5s_1+5s_3+8s_9,\quad \delta_3\lambda_1=8s_1+5s_3+5s_9,$$

$$\delta_1\lambda_3=-6s_1-7s_3-7s_9,\quad \delta_2\lambda_1=-7s_1-6s_3-7s_9,\quad \delta_3\lambda_2=-7s_1-7s_3-6s_9.$$

Заключение

Итак, мы получили полное описание случаев решения диофантовых уравнений с помощью однозначного разложения на множители в круговых полях, работая с уравнениями третьей степени.

Отметим, что в случае круговых полей с однозначным разложением на простые множители уравнение третьей степени порождается подполем только четырех круговых полей: K_7, K_9, K_{13}, K_{19}.

Таким образом, мы завершили исследование, начатое в статье [4], и подвели общий итог работы с диофантовыми уравнениями третьей степени, решая их с помощью однозначности разложения в круговых полях.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Список литературы

1. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
2. *Пачев У.М., Кодзоков А.Х., Езаова А.Г., Токбаева А.А., Гучаева З.Х.* Об одном способе решения линейных уравнений над евклидовым кольцом // Вестник КРАУНЦ. Физ.-мат. науки. 2024. Т. 46, № 1. С. 9–21. https://doi.org/10.26117/2079-6641-2024-46-1-9-21.
3. *Брюно А.Д.* От диофантовых приближений до диофантовых уравнений // Препринты ИПМ им. М.В. Келдыша. 2016. № 1. 20 с. https://doi.org/10.20948/prepr-2016-1.
4. *Галяутдинов И.Г., Лаврентьева Е.Е.* Диофантово уравнение, порожденное максимальным подполем кругового поля // Изв. вузов. Матем. 2020. № 7. С. 45–55.
5. *Боревич З.И., Шафаревич И.Р.* Теория чисел. М.: Наука, 1985. 504 с.
6. *Кострикин А.И.* Введение в алгебру. Часть III. М.: Физматлит, 2001. 272 с.
7. *Бурбаки Н.* Алгебра. Многочлены и поля. Упорядоченные группы. М.: Наука, 1965. 300 с.

8. *Alaca S., Williams K.S.* Introductory Algebraic Number Theory. New York, NY: Cambridge Univ. Press, 2004. 428 p.

9. *Marcus D.A.* Number Fields. 2nd ed. Ser.: Universitext. Cham: Springer, 2018. xviii, 203 p. https://doi.org/10.1007/978-3-319-90233-3.

Поступила в редакцию 10.05.2024
Принята к публикации 18.06.2024

Галяутдинов Ильдархан Галяутдинович, кандидат физико-математических наук
E-mail: *gmarat_68@mail.ru*
Лаврентьева Елена Евгеньевна, кандидат педагогических наук, доцент кафедры информационных систем
Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *ialee-4@mail.ru*

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)
UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)
2024, vol. 166, no. 2, pp. 147–161

ORIGINAL ARTICLE
doi: 10.26907/2541-7746.2024.2.147-161

Diophantine Equation Generated by the Subfield of a Circular Field

I.G. Galyautdinov , E.E. Lavrentyeva[a]***
[a] *Kazan Federal University, Kazan, 420008 Russia*
E-mail: **gmarat_68@mail.ru*, ***ialee-4@mail.ru*

Received May 10, 2024; Accepted June 18, 2024

Abstract

Two forms $f(x, y, z)$ and $g(x, y, z)$ of degree 3 were constructed, with their values being the norms of numbers in the subfields of degree 3 of the circular fields K_{13} and K_{19}, respectively. Using the decomposition law in a circular field, Diophantine equations $f(x, y, z) = a$ and $g(x, y, z) = b$, where $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ were solved. The assertions that, based on the canonical decomposition of the numbers a и b into prime factors, make it possible to determine whether the equations $f(x, y, z) = a$ and $g(x, y, z) = b$ have solutions were proved.

Keywords: algebraic integer, Galois group, norm of algebraic number, principal ideal, fundamental basis, decomposition law in circular field, Diophantine equation

Conflicts of Interest. The authors declare no conflicts of interest.

References

1. Ireland K., Rosen M. *Klassicheskoe vvedenie v sovremennuyu teoriyu chisel* [A Classical Introduction to Modern Number Theory]. Moscow, Mir, 1987. 416 p. (In Russian)

2. Pachev U.M., Kodzokov A.Kh., Ezaova A.G., Tokbaeva A.A., Guchaeva Z.Kh. On one way to solve linear equations over a Euclidean ring. *Vestn. KRAUNTs. Fiz.-Mat. Nauki*, 2024, vol. 46, no. 1, pp. 9–21. https://doi.org/10.26117/2079-6641-2024-46-1-9-21. (In Russian)

3. Buno A.D. From Diophantine approximations to Diophantine equations. *Prepr. IPM im. M.V. Keldysha*, 2016, no. 1. 20 p. https://doi.org/10.20948/prepr-2016-1. (In Russian)

4. Galyautdinov I.G., Lavrentyeva E.E. Diophantine equation generated by the maximal subfield of a circular field. *Russ. Math.*, 2020, vol. 64, no. 7, pp. 38–47. https://doi.org/10.3103/S1066369X20070051.

5. Borevich Z.I., Shafarevich I.R. *Teoriya chisel* [Number Theory]. Moscow, Nauka, 1985. 504 p. (In Russian)

6. Kostrikin A.I. *Vvedenie v algebru* [Introduction to Algebra]. Pt. III. Moscow, Fizmatlit, 2001. 272 p. (In Russian)

7. Bourbaki N. *Algebra. Mnogochleny i polya. Uporyadochennye gruppy* [Algebra. Polynomials and Fields. Ordered Groups]. Moscow, Nauka, 1965. 300 p. (In Russian)

8. Alaca S., Williams K.S. *Introductory Algebraic Number Theory*. New York, NY, Cambridge Univ. Press, 2004. 428 p.

9. Marcus D.A. *Number Fields*. 2nd ed. Ser.: Universitext. Cham, Springer, 2018. xviii, 203 p. https://doi.org/10.1007/978-3-319-90233-3.

⟨ ***Для цитирования:*** *Галяутдинов И.Г., Лаврентьева Е.Е.* Диофантово уравнение, порожденное подполем кругового поля // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2024. Т. 166, кн. 2. С. 147–161.
URL: https//doi.org/10.26907/2541-7746.2024.2.147-161. ⟩

⟨ ***For citation:*** Galyautdinov I.G., Lavrentyeva E.E.Diophantine equation generated by the subfield of a circular field. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2024, vol. 166, no. 2, pp. 147–161.
URL: https//doi.org/10.26907/2541-7746.2024.2.147-161. (In Russian) ⟩