Math-Net.Ru

Общероссийский математический портал

И. Г. Галяутдинов, Е. Е. Лаврентьева, Диофантово уравнение, порожденное максимальным подполем кругового поля, *Изв. вузов. Матем.*, 2020, номер 7, 45–55

DOI: <https://doi.org/10.26907/0021-3446-2020-7-45-55>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.137.237

26 апреля 2023 г., 11:50:45

И.Г. ГАЛЯУТДИНОВ, Е.Е. ЛАВРЕНТЬЕВА

ДИОФАНТОВО УРАВНЕНИЕ, ПОРОЖДЕННОЕ МАКСИМАЛЬНЫМ ПОДПОЛЕМ КРУГОВОГО ПОЛЯ

Аннотация. С помощью фундаментального базиса поля $L_9 = \mathbb{Q}(2 \cos(\pi/9))$ находится форма $N_{L_9}(\gamma) = f(x, y, z)$ и решается диофантово уравнение $f(x, y, z) = a$. По аналогичной схеме строится форма $N_{L_7}(\gamma) = g(x, y, z)$. Решается диофантово уравнение $g(x, y, z) = a$.

Ключевые слова: целое алгебраическое число, фундаментальный базис поля алгебраических чисел, норма алгебраического числа, основные единицы алгебраического поля, диофантово уравнение.

УДК: 511.61

DOI: 10.26907/0021-3446-2020-7-45-55

1. ВВЕДЕНИЕ

В работе ([1], гл. 2) З.И. Борович и И.Р. Шафаревич изучают диофантовы уравнения, представимые в виде

$$f(x) = N(\gamma) = a, \quad (1)$$

где f — форма от переменных $x = (x_1, \dots, x_k)$, $\gamma = \alpha_1 x_1 + \dots + \alpha_k x_k$ — число из алгебраического поля P степени k . В случае, когда $f(x)$ — полная форма ([1], с. 99) доказывается, что за конечное число действий можно описать множество решений уравнения (1). Однако авторы отмечают следующее ([1], с. 138): «...изучаемый общий метод эффективного построения основных единиц и чисел модуля с данной нормой мало пригоден для практического использования ввиду чрезвычайно большого объема необходимых вычислений. Нашей целью является лишь доказательство принципиальной возможности провести построение в конечное число шагов. В ряде конкретных примеров, используя дополнительные соображения и учитывая специфику данного частного случая, обычно удается найти более простой путь. Так в параграфе 7 в качестве примера мы изложим довольно простой способ решения наших задач для случая квадратичных полей».

Наиболее древним представителем класса диофантовых уравнений, представимых в виде (1), является уравнение Пелля $x^2 - dy^2 = c$ (d — натуральное свободное от квадратов, c — целое рациональное числа). Впоследствии изучали кубичный аналог уравнения Пелля. Более поздними из них являются работы ([2], гл. 7; [3], гл. 5).

В данной работе уравнение (1) изучается в том случае, когда в качестве поля P берется максимальное подполе кругового поля K_9 или K_7 .

Поле $K_h = \mathbb{Q}(u_h)$, получающееся присоединением к полю $\mathbb{Q}$ рациональных чисел первообразного корня u_h из единицы степени h , где h — некоторое натуральное число, называют круговым полем.

Пусть $n > 2$ — произвольное натуральное число и $h = 2n$. Тогда элемент $u_h + u_h^{-1}$ порождает вещественное поле $L_n = \mathbb{Q}(u_h + u_h^{-1}) = \mathbb{Q}(2 \cos(\pi/n))$. Как известно ([4], с. 210), L_n является подполем кругового поля K_h и $[K_h : L_n] = 2$.

Так как из $\mathbb{Q} \subset L_n \subset K_h$ следует, что степень $[L_n : \mathbb{Q}]$ поля L_n является делителем степени $[K_h : \mathbb{Q}]$ поля K_h , то равенство $[K_h : L_n] = 2$ означает, что $L_n = \mathbb{Q}(2 \cos(\pi/n))$ является максимальным и вещественным подполем кругового поля $K_h = K_{2n}$.

Как известно, группа Галуа $G(K_{2n}/\mathbb{Q})$ поля K_h над $\mathbb{Q}$ изоморфна мультипликативной группе $U\mathbb{Z}_{2n}$ классов вычетов, взаимно простых с модулем $2n$ ([5], с. 213). А подполе $L_n = \mathbb{Q}(2 \cos(\pi/n))$, $2 \cos(\pi/n) = u + u^{-1}$, инвариантно относительно подгруппы $H = \{\bar{1}, \overline{-1}\} \in U\mathbb{Z}_{2n}$. Поэтому $G(L_n/\mathbb{Q}) \approx U\mathbb{Z}_{2n}/H$, т.е. группа Галуа поля L_n над $\mathbb{Q}$ изоморфна фактор-группе $U\mathbb{Z}_{2n}/H$ ([5], с. 213).

Определение 1.1 ([6], с. 174). Пусть E — расширение Галуа поля P конечной степени k и $\sigma_i (1 \leq i \leq k)$ — все различные автоморфизмы его группы Галуа $G(E/P)$. Для каждого элемента $x \in E$ называют нормой элемента $x \in E$ относительно полей E , P и обозначают через $N_{E/P}(x)$ (или просто $N_E(x)$ или даже $N(x)$, если не будет возникать недоразумений) элемент

$$N_{E/P}(x) = \sigma_1(x)\sigma_2(x) \dots \sigma_k(x).$$

Из этого определения следует $N_{E/P}(xy) = N_{E/P}(x) \cdot N_{E/P}(y)$. Элемент $N_{E/P}(x)$ неподвижен относительно $G(E/P)$, следовательно, содержится в P .

Предложение 1.1 ([6], с. 176). Пусть E — расширение Галуа поля конечной степени k поля P , а F — расширение Галуа поля конечной степени t поля E . Для каждого элемента $x \in E$ справедливо равенство $N_{F/P}(x) = (N_{E/P}(x))^m$.

2. МИНИМАЛЬНЫЕ МНОГОЧЛЕНЫ ЧИСЕЛ $2 \cos(\pi/n)$

Пусть $T_n(x)$, $n = 0, 1, 2, \dots$, — многочлены Чебышева ([7], с. 116). Как известно, они обладают свойством $T_n(\cos \varphi) = \cos(n\varphi)$ и вычисляются по рекуррентной формуле

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), \quad T_0(x) = 1, \quad T_1(x) = x, \quad n = 0, 1, 2, \dots$$

Для дальнейшего нам нужно от многочленов $T_n(x)$ Чебышева перейти к многочленам $S_n(x)$ по формуле

$$S_n(x) = 2T_n(x/2), \quad n = 0, 1, 2, \dots \quad (2)$$

Многочлены $S_n(x)$ удовлетворяют рекуррентному соотношению

$$S_{n+1}(x) = xS_n(x) - S_{n-1}(x). \quad (3)$$

Из (2), (3) следует, что многочлены $S_n(x)$ обладают следующими свойствами ([7], с. 119):

- a) $\deg S_n(x) = n$;
- b) старший коэффициент равен 1;
- c) все коэффициенты $S_n(x)$ — целые рациональные числа;
- d) $S_n(2 \cos \alpha) = 2 \cos(n\alpha)$.

Пользуясь формулой (2) и тем, что $T_0(x) = 1$, $T_1(x) = x$, построим несколько многочленов $S_n(x)$:

$$\begin{aligned} S_0(x) &= 2, \quad S_1(x) = x, \quad S_2(x) = x^2 - 2, \quad S_3(x) = x^3 - 3x, \quad S_4(x) = x^4 - 4x^2 + 2, \\ S_5(x) &= x^5 - 5x^3 + 5x, \quad S_6(x) = x^6 - 6x^4 + 9x^2 - 2, \dots \end{aligned} \quad (4)$$

Теорема 2.1. Пусть $n = 2k + 1$ — натуральное число и φ — функция Эйлера. Тогда имеются многочлены $q_n(x) \in \mathbb{Q}[x]$ степени $(1/2)\varphi(n)$ с корнями $2\cos(s\pi/n)$, где нечетное $s < n$ принимает все значения взаимно простые с n . Эти многочлены находятся рекуррентно из формул

$$q_1(S_n(x)) = q_1(x)(q_n(x))^2, \quad n = 2k + 1 \text{ простое}, \quad q_1(x) = x + 2, \quad (5)$$

$$q_m(S_q(x)) = q_n(x), \quad n = mq, \quad m, q, \quad q \text{ простое}, \quad (6)$$

$$q_m(S_q(x)) = q_m(x)q_n(x), \quad n = mq, \quad \text{НОД}(m, q) = 1, \quad q \text{ простое}. \quad (7)$$

Числа $2\cos(t\pi/n)$, где четные $t < n$ принимают все значения, взаимно простые с n , являются корнями многочлена $(-1)^d q_n(-x)$, где $d = \deg q_n(x)$.

Теорема 2.2. Пусть $n = 2k$ — натуральное число и φ — функция Эйлера. Тогда имеются многочлены $q_n(x) \in \mathbb{Q}[x]$ степени $\varphi(n)$ с корнями $2\cos(s\pi/n)$, где $s < n$ и пробегает все значения, взаимно простые с n . Эти многочлены строятся по формулам

$$q_n(x) = q_k(S_2(x)), \quad q_2(x) = x. \quad (8)$$

Теорема 2.3. Многочлены $q_n(x)$, построенные по формулам (5)–(8), неприводимы над полем $\mathbb{Q}$.

Доказательства теорем 2.1, 2.2, 2.3 содержатся в работе [8].

Теорема 2.4. Если n — натуральное число, то $2\cos(\pi/n)$ — целое алгебраическое число, а $q_n(x)$ — его минимальный многочлен.

Доказательство. Как ранее отмечено, многочлен $S_n(x)$ из (4) имеет целые рациональные коэффициенты и его старший коэффициент равен единице. Поэтому из рекуррентных формул (5)–(8) вытекает, что многочлен $q_n(x)$ также имеет целые рациональные коэффициенты и его старший коэффициент равен единице. Это означает, что его корень $2\cos(\pi/n)$ — целое алгебраическое число. Из теоремы 2.3 вытекает, что $q_n(x)$ — минимальный многочлен числа $2\cos(\pi/n)$. $\square$

Приведем примеры многочленов $q_n(x)$:

$$q_1(x) = x + 2, \quad q_2(x) = x, \quad q_3(x) = x - 1, \quad q_4(x) = x^2 - 2, \quad q_5(x) = x^2 - x - 1, \quad q_6(x) = x^2 - 3, \\ q_7(x) = x^3 - x^2 - 2x + 1, \quad q_8(x) = x^4 - 4x^2 + 2, \quad q_9(x) = x^3 - 3x - 1, \quad q_{10}(x) = x^4 - 5x^2 + 5.$$

3. ЕДИНИЦЫ И ФУНДАМЕНТАЛЬНЫЙ БАЗИС ПОЛЯ $L_9 = \mathbb{Q}(2\cos(\pi/9))$

Пусть P — расширение Галуа степени k поля $\mathbb{Q}$ и $\sigma_1, \sigma_2, \dots, \sigma_k$ — его автоморфизмы.

Целое алгебраическое число ([1], с. 109) $u \in P$ называется единицей поля P , если u^{-1} является также целым алгебраическим числом.

Предложение 3.1 ([1], с. 106). Целое алгебраическое число $u \in P$ является единицей поля P тогда и только тогда, когда его норма в P равна ± 1 , т. е.

$$N(u) = \sigma_1(u) \cdot \sigma_2(u) \cdot \dots \cdot \sigma_k(u) = \pm 1.$$

Единицы поля P образуют группу относительно умножения. Структуру этой группы описывает теорема Дирихле о единицах. В случае вещественного поля P теорема Дирихле принимает следующий вид ([1], с. 131).

Пусть $P = \mathbb{Q}(\alpha)$ — вещественное поле и $[P: \mathbb{Q}] = k$. Тогда имеются такие единицы $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{k-1}$ поля P , что любая единица u поля P однозначно представима в виде

$$u = \pm \varepsilon_1^{m_1} \cdot \varepsilon_2^{m_2} \cdot \dots \cdot \varepsilon_{k-1}^{m_{k-1}}$$

при некоторых целых рациональных числах $m_1, m_2, \dots, m_{k-1}$.

Числа $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{k-1}$ называются основными единицами поля P .

Нам нужны основные единицы поля $L_9 = \mathbb{Q}(2 \cos(\pi/9))$. Минимальный многочлен числа $\alpha = 2 \cos(\pi/9)$ имеет вид $q_9(x) = x^3 - 3x - 1$. Его корнями являются числа $\alpha_k = 2 \cos(k\pi/9)$, $k = 1, 5, 7$. Дискриминант поля L_9 : $d(L_9) = 81$.

Группа автоморфизмов $G(L_9/\mathbb{Q})$ поля L_9 изоморфна фактор-группе $U\mathbb{Z}_9/H$, где $H = \{\bar{1}, \bar{-1}\}$ — подгруппа $U\mathbb{Z}_9 = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$.

Автоморфизм, соответствующий смежному классу $\bar{\lambda}H$ (λ нечетное) обозначим через σ_λ . Таким образом, $G(L_9/\mathbb{Q}) = \{\sigma_1, \sigma_5, \sigma_7\}$ и σ_λ действует на α по формуле $\sigma_\lambda(\alpha_k) = \alpha_{\lambda k} = 2 \cos(k\lambda\pi/9)$, $\lambda = 1, 5, 7$. Вычислим норму примитивного элемента $\alpha \in L_9$. Имеем $N_{L_9}(\alpha) = \sigma_1(\alpha)\sigma_5(\alpha)\sigma_7(\alpha) = \alpha_1 \cdot \alpha_5 \cdot \alpha_7 = 1$. На основании предложения 3.1 убеждаемся, что все корни многочлена $q_9(x) = x^3 - 3x - 1$ являются единицами поля $L_9 = \mathbb{Q}(\alpha)$.

В работе ([9], с. 377) приводится таблица, где указаны основные единицы тридцати вполне вещественных полей третьей степени. В этой таблице охвачены поля K , дискриминанты которых удовлетворяют условию $0 < d(K) \leq 1101$.

Согласно указанной таблице основными единицами поля L_9 (в наших обозначениях) являются числа $-\alpha_1 = -2 \cos(\pi/9) = -\alpha$, $-\alpha_5 = 2 + \alpha - \alpha^2$. Нормы этих единиц равны -1. При решении диофантовых уравнений необходимо использовать единицы с нормой 1. Поэтому в качестве основных единиц поля L_9 мы берем числа $\varepsilon_1 = \alpha_1 = \alpha$, $\varepsilon_2 = \alpha_5 = -2 - \alpha + \alpha^2$.

Для дальнейшего нам нужен фундаментальный базис ([1], с. 287) поля L_9 . Этот базис можно получить из нескольких источников. В частности, из теоремы 7.1.7 работы ([9], с. 146) вытекает, что числа $1, \alpha, \alpha^2$ ($\alpha = 2 \cos(\pi/9)$) составляют фундаментальный базис поля $L_9 = \mathbb{Q}(\alpha)$.

4. ДИОФАНТОВО УРАВНЕНИЕ, ПОРОЖДЕННОЕ ПОЛЕМ $L_9 = \mathbb{Q}(2 \cos(\pi/9))$

Теперь мы можем выписать явный вид уравнения (1) в случае поля $P = L_9 = \mathbb{Q}(2 \cos(\pi/9))$.

Пусть γ — произвольное целое число поля $L_9 = \mathbb{Q}(\alpha)$, $\alpha = 2 \cos(\pi/9)$, $\gamma = x + y\alpha + z\alpha^2$. Так как $a = (1, \alpha, \alpha^2)$ — фундаментальный базис, то x, y, z — целые рациональные числа. Вычислим $N(\gamma) = N_{L_9}(\gamma)$. Имеем $N(\gamma) = \sigma_1(\gamma)\sigma_5(\gamma)\sigma_7(\gamma) = (x + y\alpha_1 + z\alpha_1^2)(x + y\alpha_5 + z\alpha_5^2)(x + y\alpha_7 + z\alpha_7^2)$. Учитывая, что $\alpha_1, \alpha_5, \alpha_7$ — корни многочлена $q_9(x) = x^3 - 3x - 1$, находим

$$N_{L_9}(\gamma) = f(x, y, z) = x^3 + y^3 + z^3 + 6x^2z - 3y^2x + 9z^2x - 3z^2y - 3xyz. \quad (9)$$

Таким образом, в случае $P = L_9$ уравнение (1) принимает вид

$$N_{L_9}(\gamma) = f(x, y, z) = a, \quad (10)$$

где $f(x, y, z)$ — форма из равенства (9).

Изучим сначала уравнение (10) в том случае, когда $a = p$ — простое число. Если уравнение $N(\gamma) = f(x, y, z) = p$ имеет решение $\gamma = \delta$, то $N(\delta) = \sigma_1(\delta)\sigma_5(\delta)\sigma_7(\delta) = p$. А это означает, что простое число p в поле L_9 разлагается на множители. Это обстоятельство подсказывает, что можно воспользоваться законом разложения в круговом поле и применить его к случаю K_9 . Отметим, что $K_9 = K_{18}$ — круговое поле с однозначным разложением на простые множители ([1], с. 485).

Разложение простого числа p в круговом поле K_n зависит от его порядка s по модулю n . Этот порядок s является делителем $\varphi(n)$. В случае поля K_9 имеем $n = 9$ и $\varphi(9) = 6$. Так как делителями числа 6 являются числа 1, 2, 3 и 6, то порядок простого числа, взаимно простого с 9, равен одному из чисел 1, 2, 3, 6.

Рассмотрим все возможные случаи.

Случай 1. Простое число p имеет порядок 1, т. е. $p \equiv 1 \pmod{9}$.

Из закона разложения следует, что число p разлагается в произведение шести простых множителей. Эти множители попарно различны и норма в K_9 каждого множителя равна p . Если μ — одно из этих чисел, то $N(\mu) = p$. Группа Галуа $G(K_9/\mathbb{Q})$ изоморфна группе $U\mathbb{Z}_9 = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$. Автоморфизм, соответствующий классу $\bar{\lambda}$, обозначим через τ_λ . Тогда норма μ в поле K_9 вычисляется по формуле

$$p = N_{K_9}(\mu) = \tau_1(\mu)\tau_2(\mu)\tau_4(\mu)\tau_5(\mu)\tau_7(\mu)\tau_8(\mu). \quad (11)$$

Подполе $L_9 \subset K_9$ инвариантно относительно автоморфизмов подгруппы $H = \{\tau_1, \tau_8\}$. Автоморфизм поля L_9 , соответствующий классу $\tau_\lambda H$ (λ нечетно), обозначим через σ_λ .

Рассмотрим произведения $\tau_1(\mu)\tau_8(\mu)$, $\tau_2(\mu)\tau_7(\mu)$, $\tau_4(\mu)\tau_5(\mu)$. Все эти три числа инвариантны относительно автоморфизмов τ_1 и τ_8 из подгруппы H . Значит, все эти три числа входят в L_9 .

Пусть $\tau_1(\mu)\tau_8(\mu) = \delta$. Тогда

$$\tau_1(\delta) = \tau_8(\delta) = \tau_1(\mu)\tau_8(\mu) = \sigma_1(\delta), \quad \tau_2(\delta) = \tau_7(\delta) = \tau_2(\mu)\tau_7(\mu) = \sigma_7(\delta),$$

$$\tau_4(\delta) = \tau_5(\delta) = \tau_4(\mu)\tau_5(\mu) = \sigma_5(\delta)$$

и равенство (11) принимает вид

$$p = \sigma_1(\delta)\sigma_5(\delta)\sigma_7(\delta) = N_{L_9}(\delta). \quad (12)$$

Это равенство означает, что имеется число $\delta \in L_9$, норма которого равна p . Другими словами, если $a = p$ — простое число и $p \equiv 1 \pmod{9}$, то уравнение (10) имеет решение в L_9 .

Тогда выясним, сколько различных решений имеет уравнение (10).

Говорят, что числа $\delta_1, \delta_2, \dots, \delta_r$ составляют полный набор неассоциированных решений, если

- а) эти числа попарно неассоциированы и норма каждого из них равна p ;
- б) любое число λ с нормой p ассоциировано с одним из чисел δ_i .

Из закона разложения вытекает, что все числа $\tau_i(\mu)$ из равенства (11) попарно неассоциированы. Отсюда следует, что произведения

$$\tau_1(\mu)\tau_8(\mu) = \sigma_1(\delta), \quad \tau_2(\mu)\tau_7(\mu) = \sigma_7(\delta), \quad \tau_4(\mu)\tau_5(\mu) = \sigma_5(\delta)$$

также попарно неассоциированы. Это означает, что полный набор неассоциированных решений уравнения (10) при $a = p$, $p \equiv 1 \pmod{9}$ состоит минимум из трех чисел.

С другой стороны, если для некоторого числа λ имеем $N_{L_9}(\lambda) = \sigma_1(\lambda)\sigma_3(\lambda)\sigma_7(\lambda) = p$, то в силу однозначности разложения в поле K_9 получаем, что число $\lambda = \sigma_1(\lambda)$ ассоциировано с одним из чисел $\sigma_i(\delta)$ из разложения (12). Это означает, что полный набор неассоциированных решений уравнения (10) при $a = p$ и $p \equiv 1 \pmod{9}$ состоит из трех чисел.

Таким образом, доказана

Теорема 4.1. Пусть $L_9 = \mathbb{Q}(\alpha)$, $\alpha = 2 \cos(\pi/9)$, p — простое число, $p \equiv 1 \pmod{9}$ и $f(x, y, z)$ — форма из равенства (9). Тогда уравнение $N_{L_9}(\gamma) = f(x, y, z) = p$ имеет решение $\gamma = \delta$. Полный набор неассоциированных решений состоит из трех чисел $\delta_1 = \sigma_1(\delta)$, $\delta_2 = \sigma_5(\delta)$, $\delta_3 = \sigma_7(\delta)$ и общее решение задается равенством $\gamma_{i,k,l} = \delta_i \varepsilon_1^k \varepsilon_2^l$, $i = 1, 2, 3$, $k, l \in \mathbb{Z}$.

Задача 4.1. Пусть $f(x, y, z)$ — форма из равенства (9) и $p = 19$. Необходимо найти полный набор неассоциированных решений уравнения

$$N(\gamma) = f(x, y, z) = 19. \quad (13)$$

Решение. Так как $19 \equiv 1 \pmod{9}$, то согласно теореме 4.1 уравнение (13) имеет решение. Чтобы найти это решение в форме $f(x, y, z)$ фиксируем значение двух переменных. Пусть $y = 1, z = 0$. Тогда находим $f(x, 1, 0) = x^3 - 3x + 1$ и $f(3, 1, 0) = 19$. Это означает, что норма числа $\delta = 3 + \alpha$, $\alpha = 2\cos(\pi/9)$, равна девятнадцати. Тогда согласно теореме 4.1 числа

$$\delta_1 = \sigma_1(\delta) = 3 + \alpha, \quad \delta_2 = \sigma_5(\delta) = 3 + \alpha_5 = 1 - \alpha + \alpha^2, \quad \delta_3 = \sigma_7(\delta) = 3 + \alpha_7 = 5 - \alpha^2 \quad (14)$$

составляют полный набор неассоциированных решений уравнения (13).

Случай 2. Порядок простого числа p равен двум, т.е. $p^2 \equiv 1 \pmod{9}$.

Значит, p имеет вид $p = 9k + 8$. Числа этого класса порождают подгруппу $M = \{\bar{1}, \bar{8}\} \subset UZ_9$. При изоморфизме $G(K_9/\mathbb{Q}) \approx UZ_9$ подгруппе M соответствует подгруппа $H = \{\tau_1, \tau_8\}$, относительно которой инвариантно подполе

$$L_9 = \mathbb{Q}(u_1 + u_8) = \mathbb{Q}(2\cos(\pi/9)) \subset K_9.$$

По закону разложения для простого числа вида $p = 9k + 8$ имеем $(p) = A_1 A_2 A_3$, где A_i — попарно различные простые идеалы кольца целых чисел поля K_9 и $N_{K_9}(A_i) = p^2$. Так как каждый идеал в кольце целых алгебраических чисел поля K_9 является главным, то $A_i = (\lambda_i)$ для некоторого простого $\lambda_i \in K_9$. Пусть (λ) — любой из идеалов $(\lambda_1), (\lambda_2), (\lambda_3)$. Тогда из предложения 14.1.2 ([10], с. 250) вытекает

$$(p)^2 = (N_{K_9}(\lambda)) = (\tau_1(\lambda)\tau_2(\lambda)\tau_4(\lambda)\tau_5(\lambda)\tau_7(\lambda)\tau_8(\lambda)) = ((\lambda_1)(\lambda_2)(\lambda_3))^2.$$

Из однозначности разложения следует, что каждый идеал (λ_i) в произведение в левой части равенства входит ровно два раза. Таким образом, подгруппа H является стабилизатором идеала (λ) относительно естественного действия группы G на множестве идеалов $\{A_1, A_2, A_3\}$ и, следовательно, $(\tau_1(\lambda)) = (\tau_8(\lambda)) = (\lambda)$. Пусть R — кольцо целых алгебраических чисел поля L_9 . Хорошо известно, что R — кольцо главных идеалов. Тогда по следствию 2 работы ([12], с. 72) следует, что в кольце R идеал (p) является произведением трех попарно различных простых идеалов. Значит, для некоторых попарно неассоциированных простых элементов $\lambda'_1, \lambda'_2, \lambda'_3$ из кольца R выполнены равенства

$$R \cap (\lambda_1) = (\lambda'_1), \quad R \cap (\lambda_2) = (\lambda'_2), \quad R \cap (\lambda_3) = (\lambda'_3) \text{ и } (p) = (\lambda'_1)(\lambda'_2)(\lambda'_3).$$

Так как действие группы $G(L_9/\mathbb{Q})$ на множестве идеалов $\{(\lambda'_1), (\lambda'_2), (\lambda'_3)\}$ транзитивно, то $N_{L_9}((\lambda'_1)) = N_{L_9}((\lambda'_2)) = N_{L_9}((\lambda'_3))$ и, следовательно,

$$p^3 = N_{L_9}(p) = N_{L_9}((\lambda'_1))N_{L_9}((\lambda'_2))N_{L_9}((\lambda'_3)).$$

Таким образом, $N_{L_9}((\lambda'_1)) = p$ и, следовательно, $|N_{L_9}(\lambda'_1)| = p$. Доказана

Теорема 4.2. Пусть $f(x, y, z)$ — форма из равенства (9) и порядок простого числа p равен двум. Тогда уравнение $N_{L_9}(\gamma) = f(x, y, z) = p$ имеет решение $\lambda \in L_9$. Полный набор неассоциированных решений состоит из трех чисел $\lambda_1 = \sigma_1(\lambda)$, $\lambda_2 = \sigma_5(\lambda)$, $\lambda_3 = \sigma_7(\lambda)$.

Задача 4.2. Найти полный набор неассоциированных решений уравнения $f(x, y, z) = 17$.

Решение. По теореме 4.2 это уравнение имеет решение. Действительно, $f(3, -1, 0) = 17$. Значит, число $\lambda = 3 - \alpha$ имеет норму $N_{L_9}(\lambda) = 17$ и числа $\lambda_1 = \sigma_1(\lambda) = 3 - \alpha$, $\lambda_2 = \sigma_5(\lambda) = 3 - \alpha_5 = 5 + \alpha - \alpha^2$, $\lambda_3 = \sigma_7(\lambda) = 1 + \alpha^2$ составляют полный набор его неассоциированных решений.

Случай 3. Порядок простого числа p равен трем, т.е. $p^3 \equiv 1 \pmod{9}$.

Такие простые числа имеют вид $9k + 4$ или $9k + 7$. Они порождают подгруппу $H_4 = \{\tau_1, \tau_4, \tau_7\}$, относительно которой инвариантно поле $K_3 = \mathbb{Q}(\sqrt{-3})$. Из закона разложения вытекает, что эти простые числа p представляются в виде $p = \lambda_1 \cdot \lambda_2$, где λ_1, λ_2 — различные

простые числа поля K_3 и $N_{K_9}(\lambda_i) = p^3$. Так как $K_3 \cap L_9 = \mathbb{Q}$, то $\lambda_1, \lambda_2 \notin L_9$ и уравнение $N_{L_9}(\gamma) = f(x, y, z) = p$ не имеет решения.

Случай 4. Порядок простого числа p равен шести, т.е. $p^6 \equiv 1 \pmod{9}$, $p = 9k + 2$ и $p = 9k + 5$.

Простые числа вида $p = 9k + 2$ и $p = 9k + 5$ порождают всю группу Галуа $G(K_9/\mathbb{Q})$. Относительно всей группы инвариантно только поле рациональных чисел. Значит, простое число p разлагается на множители в поле $\mathbb{Q}$. Причем число простых множителей должно быть равно одному. Это означает, что разложение имеет вид $p = p$. Поэтому уравнение $N_{L_9}(\gamma) = f(x, y, z) = p$ не имеет решения в поле L_9 .

Из случаев 3, 4 вытекает

Теорема 4.3. Пусть $L_9 = \mathbb{Q}(2 \cos(\pi/9))$, $f(x, y, z)$ — форма из равенства (9) и p — простое число вида $p = 9t + k$, $k = 2, 4, 5, 7$. Тогда уравнение $N_{L_9}(\gamma) = f(x, y, z) = p$ не имеет решения.

Случай 5. Каждое простое число, взаимно простое с 9, находится в одном из следующих классов: $\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}$ и они уже рассмотрены. Осталось изучить случай $p = 3$.

В этом случае, из закона разложения вытекает, что число $p = 3$ делится на куб простого числа $\mu \in L_9$. Это означает, что имеет место

Теорема 4.4. Пусть $L_9 = \mathbb{Q}(2 \cos(\pi/9))$, $f(x, y, z)$ — форма из равенства (9). Тогда уравнение $N_{L_9}(\gamma) = f(x, y, z) = 3$ имеет решение и полный набор его неассоциированных решений состоит из одного числа.

Задача 4.3. Найти формулу общего решения уравнения $N_{L_9}(\gamma) = f(x, y, z) = 3$.

Решение. Находим $f(x, 1, 0) = x^3 - 3x + 1$. Отсюда $f(-1, 1, 0) = 3$. Значит, число $\mu = -1 + \alpha$ имеет норму 3: $N_{L_9}(\mu) = (-1 + \alpha_1)(-1 + \alpha_5)(-1 + \alpha_7) = 3$, $\alpha_1 = \alpha$. Числа $\mu_1 = -1 + \alpha_1$, $\mu_2 = -1 + \alpha_5$, $\mu_3 = -1 + \alpha_7$ делятся друг на друга. Поэтому общее решение имеет вид

$$\gamma_{k,l} = \mu_1 \varepsilon_1^k \varepsilon_1^l, \quad \mu_1 = -1 + \alpha, \quad \varepsilon_1 = 2 \cos(\pi/9), \quad \varepsilon_2 = 2 \cos(5\pi/9), \quad k, l \in \mathbb{Z}.$$

Переходим к изучению общего случая, когда в правой части уравнения (10) произвольное целое рациональное число $a \neq 0$.

Определение 4.1. Если уравнение $N(\gamma) = f(x, y, z) = a$ имеет решение в L_9 , то будем говорить, что a является нормой.

Лемма 4.1. Если a_1 и a_2 являются нормой, то их произведение $a_1 \cdot a_2$ — также норма.

Доказательство. Из условий леммы вытекает, что имеются целые числа $\delta_1 \in L_9, \delta_2 \in L_9$ такие, что $N_{L_9}(\delta_1) = a_1, N_{L_9}(\delta_2) = a_2$. Тогда $N_{L_9}(\delta_1 \delta_2) = N_{L_9}(\delta_1) N_{L_9}(\delta_2) = a_1 \cdot a_2$. Это означает, что уравнение $f(x, y, z) = a_1 \cdot a_2$ имеет решение, при этом решение $\gamma = \delta_1 \cdot \delta_2$ находится как произведение решений соответственно уравнений $f(x, y, z) = a_1$ и $f(x, y, z) = a_2$. $\square$

Определение 4.2. Норму a назовем первичной, если она не является произведением норм, отличных от единицы.

Лемма 4.2. Первичными являются

- a) все простые числа вида $p = 9t + 1$;
- b) все простые числа вида $p = 9t + 8$;
- c) простое число 3;
- d) числа p^3 , где p — любое простое число, указанное в теореме 4.3.

Доказательство. То, что простые числа видов $p = 9t + 1, 9t + 8$ — первичные нормы, вытекает соответственно из теорем 4.1, 4.2, а утверждение о том, что $p = 3$ — первичная норма вытекает из теоремы 4.4.

Пусть теперь p — инертное в L_9 простое число, т. е. p — одно из чисел, перечисленных в теореме 4.3. Тогда число p нормой не является. Вычислим норму числа p :

$$N_{L_9}(p) = \sigma_1(p)\sigma_5(p)\sigma_7(p) = p^3.$$

Таким образом, p^3 — первичная норма. $\square$

Лемма 4.3. Пусть a — норма, а p — инертное в L_9 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 L_9 . Так как a — норма, то имеется целое число $\lambda \in L_9$ такое, что $N_{L_9}(\lambda) = \sigma_1(\lambda)\sigma_5(\lambda)\sigma_7(\lambda) = a$.

Так как $a \vdots p$ и p — простое в L_9 число, то, по крайней мере, один из трех множителей $\sigma_i(\lambda)$ должен делиться на p . Пусть, например, $\sigma_5(\lambda) \vdots p$ и $\sigma_5(\lambda) = p\mu$, $\mu \in L_9$ — целое число. Применяя к равенству $\sigma_5(\lambda) = p\mu$ автоморфизм $\sigma_5^{-1} = \sigma_7$, находим $\lambda = p\sigma_7(\mu)$. Здесь $\sigma_7(\mu)$ — целое число и поэтому λ делится на p . Тогда получаем $N_{L_9}(\lambda) = p^3 \cdot \sigma_1(\mu)\sigma_5(\mu)\sigma_3(\mu) = a$, т. е. $a \vdots p^3$. $\square$

Объединяя леммы 4.1, 4.2, 4.3 и учитывая, что $L_9 = \mathbb{Q}(2\cos(\pi/9)) \subset K_9$ и K_9 — круговое поле с однозначным разложением на множители, получаем следующее утверждение.

Теорема 4.5. Пусть $L_9 = \mathbb{Q}(2\cos(\pi/9))$ и $f(x, y, z)$ — форма из равенства (9) и $a \neq 0$ — целое рациональное число. Диофантово уравнение $N_{L_9}(\gamma) = f(x, y, z) = a$ имеет решение тогда и только тогда, когда степень инертного в L_9 простого числа, входящего в каноническое разложение числа a , делится на три.

Задача 4.4. Найти формулу общего решения уравнения $N_{L_9}(\gamma) = f(x, y, z) = 171$.

Решение. Число $171 = 3^2 \cdot 19$ является произведением трех первичных норм 3, 3 и 19.

В задаче 4.1 указаны три попарно неассоциированных числа с нормой 19. Это числа $\delta_1 = 3 + \alpha, \delta_2 = 1 - \alpha + \alpha^2, \delta_3 = 5 - \alpha^2$. А в задаче 4.3 указаны числа с нормой 3. Все они получаются из числа $\mu_1 = -1 + \alpha$ умножением на единицы поля L_9 . Отсюда находим, что всего три попарно неассоциированных числа имеют норму 171. Это числа $\lambda_1 = \mu_1^2\sigma_1$, $\lambda_2 = \mu_1^2\sigma_2$, $\lambda_3 = \mu_1^2\sigma_3$. Все решения уравнения задаются формулой

$$\gamma_{i,k,l} = \lambda_i \varepsilon_1^k \varepsilon_2^l, \quad i = 1, 2, 3, \quad k, l \in \mathbb{Z}.$$

Задача 4.5. Найти формулу общего решения уравнения $N_{L_9}(\gamma) = f(x, y, z) = 289$.

Решение. Число $289 = 17^2$ представляется в виде произведения двух первичных норм 17 и 17. В задаче 4.2 показано, что 17 является нормой трех попарно неассоциированных чисел $\lambda_1 = 3 - \alpha, \lambda_2 = 5 + \alpha - \alpha^2, \lambda_3 = 1 + \alpha^2$. Отсюда следует, что норму $17^2 = 289$ имеют следующие шесть попарно неассоциированных чисел: $\delta_1 = \lambda_1^2, \delta_2 = \lambda_1\lambda_2, \delta_3 = \lambda_1\lambda_3, \delta_4 = \lambda_2^2, \delta_5 = \lambda_2\lambda_3, \delta_6 = \lambda_3^2$. Это означает, что формула общего решения имеет вид

$$\gamma_{i,k,l} = \delta_i \varepsilon_1^k \varepsilon_2^l, \quad i = \overline{1, 6}, \quad k, l \in \mathbb{Z}.$$

Замечание. Из результатов, полученных выше, следует, что сравнение $x^3 - 3x - 1 \equiv 0 \pmod{p}$, где p — простое число, имеет три решения в точности тогда, когда $p \equiv 1, 8 \pmod{9}$. Последнее утверждение также следует из общих результатов работы [12], в

которой проблема существования трех решений сравнения $x^3 + ax + b \equiv 0 \pmod{p}$, где p — простое число, решена полностью для абелевых многочленов третьей степени.

5. ДИОФАНТОВО УРАВНЕНИЕ, ПОРОЖДЕННОЕ ПОЛЕМ $L_7 = \mathbb{Q}(2 \cos(\pi/7))$

Минимальный многочлен $q_7(x)$ числа $\alpha = 2 \cos(\pi/7)$ имеет вид $q_7(x) = x^3 - x^2 - 2x + 1$. Его корни $\alpha_s = 2 \cos(s\pi/7)$, $s = 1, 3, 5$. Дискриминант поля L_7 равен $d(L_7) = 49$.

Поле $L_7 = \mathbb{Q}(2 \cos(\pi/7)) \subset K_7 = \mathbb{Q}(u)$, где u — первообразный корень из 1 седьмой степени. Группа Галуа $G(K_7/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\} \approx U\mathbb{Z}_7$. Поле L_7 инвариантно относительно автоморфизмов подгруппы $H = \{\tau_1, \tau_6\}$. Группа Галуа $G(L_7/\mathbb{Q})$ изоморфна фактор-группе $G(K_7/\mathbb{Q})/H$. Автоморфизм поля L_7 , соответствующий смежному классу $\tau_s H$ (s нечетное), обозначим через σ_s . Если $\lambda \in L_7$, то $\tau_1(\lambda) = \tau_6(\lambda)$, $\tau_2(\lambda) = \tau_5(\lambda)$, $\tau_3(\lambda) = \tau_4(\lambda)$. Поэтому имеем $\tau_1(\lambda) = \sigma_1(\lambda)$, $\tau_3(\lambda) = \sigma_3(\lambda)$, $\tau_5(\lambda) = \sigma_5(\lambda)$.

Как показано в [13], числа $\alpha_1, \alpha_3, \alpha_5$ составляют фундаментальный базис поля L_7 . Это означает, что если $\gamma \in L_7$ — целое число и $\gamma = x\alpha_1 + y\alpha_3 + z\alpha_5$, то x, y, z — целые рациональные числа.

Вычислим норму $N_{L_7}(\gamma)$. Так как $G(L_7/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5\}$ и автоморфизм σ_s действует по формуле $\sigma_s(\alpha_k) = \alpha_{sk}$, то

$$N_{L_7}(\gamma) = \sigma_1(\gamma) \cdot \sigma_3(\gamma) \cdot \sigma_5(\gamma) = (x\alpha_1 + y\alpha_3 + z\alpha_5)(x\alpha_3 + y\alpha_5 + z\alpha_1)(x\alpha_5 + y\alpha_1 + z\alpha_3).$$

Учитывая, что $\alpha_1, \alpha_3, \alpha_5$ — корни многочлена $q_7(x) = x^3 - x^2 - 2x + 1$, находим

$$N_{L_7}(\gamma) = -x^3 - y^3 - z^3 + 4(x^2y + y^2z + z^2x) - 3(x^2z + y^2x + z^2y) + xyz = g(x, y, z). \quad (15)$$

Таким образом, в случае $P = L_7$ уравнение (1) принимает вид

$$N(\gamma) = g(x, y, z) = a, \quad (16)$$

где $g(x, y, z)$ — форма из равенства (15) и $a \in \mathbb{Z}$.

Решение уравнения (16) нужно начинать с построения основных единиц поля L_7 .

В работе ([9], с. 377) приводится таблица, где указаны основные единицы тридцати вполне вещественных полей третьей степени, среди которых содержится поле $L_7 = \mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$, где $\alpha = 2 \cos(\pi/7)$, $\theta = 2 \cos(2\pi/7)$.

Минимальные многочлены $q_7(x)$ и $P_7(x)$ соответственно чисел α и θ имеют вид

$$q_7(x) = x^3 - x^2 - 2x + 1, \quad P_7(x) = -q_7(-x) = x^3 + x^2 - 2x - 1.$$

Согласно указанной таблице основными единицами поля L_7 являются числа $-1 + \theta + \theta^2 = -\alpha_1$ и $2 - \theta^2 = \alpha_3$. Но нормы этих единиц равны -1 . Поэтому в качестве основных единиц поля L_7 берем числа $\varepsilon_1 = -\alpha_1$, $\varepsilon_2 = -\alpha_3$.

Это означает, что первая часть задачи описания множества решений уравнения (16) решена. Остается найти полный набор неассоциированных решений этого уравнения. Этот полный набор зависит от правой части уравнения (16). Если полный набор неассоциированных решений известен при $a = a_1$ и $a = a_2$, то в силу мультипликативности нормы можно найти полный набор неассоциированных решений и при $a = a_1 \cdot a_2$.

Поэтому сначала рассматривается случай, когда $a = p$ — простое число. Так как $\varphi(9) = \varphi(7) = 6$, то законы разложения в полях K_9 и K_7 вполне аналогичны. Следствием этого является то, что решение уравнения (16) находится по той же схеме, что и (10). Поэтому сформулируем только окончательный результат и приведем примеры.

Теорема 5.1. Пусть $L_7 = \mathbb{Q}(2 \cos(\pi/7))$, $g(x, y, z)$ — форма из равенства (15). Уравнение $N_{L_7}(\gamma) = g(x, y, z) = a$ имеет решение тогда и только тогда, когда степень простого числа вида $p = 7k + t$, $t = 2, 3, 4, 5$, входящего в разложение числа a , делится на три.

Теоремы 4.5 и 5.1 могут быть перенесены на случай максимального подполя L_n произвольного кругового поля K_{2n} . Сложности, возникающие при переходе от случаев $n = 9$ или $n = 7$ к случаю большего n , носят скорее технический характер. В частности, с ростом n возрастает степень L_n , следовательно, число слагаемых в форме $f(x)$ из уравнения (1).

Задача 5.1. Найти полный набор неассоциированных решений уравнения $N_{L_7}(\gamma) = g(x, y, z) = 29$.

Решение. Число 29 имеет порядок 1, т. е. $29 \equiv 1 \pmod{7}$. Поэтому имеется $\lambda \in L_7$ такое, что $N_{L_9}(\lambda) = 29$. Действительно, $g(x, 1, 0) = -x^3 + 4x^2 - 3x - 1$ и $g(-2, 1, 0) = 29$. Это означает, что $\delta = -2\alpha_1 + \alpha_3$ — решение, $\delta_1 = \sigma_1(\delta) = -2\alpha_1 + \alpha_3$, $\delta_2 = \sigma_3(\delta) = -2\alpha_3 + \alpha_5$, $\delta_3 = \sigma_5(\delta) = -2\alpha_5 + \alpha_1$ — полный набор неассоциированных решений.

Задача 5.2. Найти решение уравнения $N_{L_7}(\gamma) = g(x, y, z) = 13$.

Решение. Так как $13 \equiv 6 \pmod{7}$ и $13^2 \equiv 1 \pmod{7}$, то 13 имеет порядок 2 по модулю 7 и решение имеется. Действительно, $g(-1, y, 0) = -y^3 + 3y^2 + 4y + 1$ и $g(-1, 2, 0) = 13$. Значит, $\delta = -\alpha_1 + 2\alpha_3$ — решение, а числа $\delta_1 = -\alpha_1 + 2\alpha_3$, $\delta_2 = -\alpha_3 + 2\alpha_5$, $\delta_3 = -\alpha_5 + 2\alpha_1$ составляют полный набор неассоциированных решений. Общее решение задается формулой

$$\gamma_{i,k,l} = \delta_i \varepsilon_1^k \varepsilon_2^l, \quad i = 1, 2, 3, \quad k, l \in \mathbb{Z}.$$

Задача 5.3. Найти все целые числа поля L_7 с нормой 169.

Решение. Так как $169 = 13^2$, то числа с нормой 169 можно найти как произведение чисел с нормой 13. Это означает, что полный набор неассоциированных решений будет состоять из чисел $\lambda_1 = \delta_1^2, \lambda_2 = \delta_2^2, \lambda_3 = \delta_3^2, \lambda_4 = \delta_1\delta_2, \lambda_5 = \delta_1\delta_3, \lambda_6 = \delta_2\delta_3$, где $\delta_1 = -\alpha_1 + 2\alpha_3, \delta_2 = -\alpha_3 + 2\alpha_5, \delta_3 = -\alpha_5 + 2\alpha_1$. Все числа поля L_7 с нормой 169 можно получить из формулы $\gamma_{i,k,l} = \lambda_i \varepsilon_1^k \varepsilon_2^l, i = 1, 2, 3, 4, 5, 6, k, l \in \mathbb{Z}, \varepsilon_1 = -\alpha_1 = -2 \cos(\pi/7), \varepsilon_2 = -\alpha_3 = -2 \cos(3\pi/7)$.

В частности,

$$\lambda_1 = \delta_1^2 = 6\alpha_1 + 14\alpha_3 + 13\alpha_5, \quad (N(\lambda_1) = g(6, 14, 13) = 169),$$

$$\lambda_1 \varepsilon_1 = \alpha_1 + 15\alpha_3 + 8\alpha_5, \quad (N(\lambda_1 \varepsilon_1) = g(1, 15, 8) = 169),$$

$$\lambda_1 \varepsilon_2 = -\alpha_1 - 22\alpha_3 - 9\alpha_5, \quad (N(\lambda_1 \varepsilon_2) = g(-1, -22, -9) = 169),$$

$$\lambda_1 \varepsilon_1 \varepsilon_2 = -7\alpha_1 - 29\alpha_3 - 21\alpha_5, \quad (N(\lambda_1 \varepsilon_1 \varepsilon_2) = g(-7, -29, -21) = 169) \text{ и т. д.}$$

Задача 5.4. Имеется ли в поле L_7 число с нормой 52?

Решение. Разложение числа $52 = 2^2 \cdot 13$ содержит инертное в поле L_7 простое число 2, степень которого не делится на три. Поэтому из теоремы 5.1 следует, что в поле L_7 нет числа с нормой 52.

Задача 5.5. Записать общее решение уравнения $N_{L_7}(\gamma) = g(x, y, z) = 7$.

Решение. Из закона разложения следует, что число 7 в поле L_7 делится на куб простого числа. Имеем $g(x, 1, 0) = -x^3 + 4x^2 - 3x - 1$ и $g(-1, 1, 0) = 7$. Значит, $\lambda = -\alpha_1 + \alpha_3$ — решение и $(-\alpha_1 + \alpha_3)(-\alpha_3 + \alpha_5)(-\alpha_5 + \alpha_1) = 7$. Но $(-\alpha_3 + \alpha_5) = (-\alpha_1 + \alpha_3) \varepsilon_1^{-1} \varepsilon_2^{-1}, (-\alpha_5 + \alpha_1) = (-\alpha_1 + \alpha_3) \varepsilon_2^{-1}$. Таким образом, $7 = (-\alpha_1 + \alpha_3)^3 \mu$, где $\mu = \varepsilon_1^{-2} \varepsilon_2^{-1}$ — единица поля L_7 . Общее решение задается формулой

$$\gamma_{k,l} = (-\alpha_1 + \alpha_3) \varepsilon_1^k \varepsilon_2^l, \quad k, l \in \mathbb{Z}.$$

В частности, $\gamma_{1,0} = (-\alpha_1 + \alpha_3) \varepsilon_1 = 2\alpha_1 + 3\alpha_3 + 2\alpha_5$ и $g(2, 3, 2) = 7$ и т. д.

Мы благодарны семинару кафедры алгебры и математической логики КФУ под руководством профессора М.М. Арсланова за возможность выступления с содержанием данной статьи. Выражаем признательность членам семинара за их конструктивные замечания.

Выражаем глубокую благодарность А.Н. Абызову за внимание к нашей работе и за неоценимую консультацию.

ЛИТЕРАТУРА

- [1] Боревиц З.И., Шафаревич И.Р. *Теория чисел* (Наука, М., 1985).
- [2] Edward J. Barbeau *Pell's Equation*, Springer-Verlag, New York (2003).
- [3] Hambleton S.A., Williams H.C. *Cubic Fields with Geometry*, Springer International Publishing (2018).
- [4] Ван дер Варден *Алгебра* (Наука, М., 1976).
- [5] Кострикин А.И. *Введение в алгебру. Ч. III* (Физматлит, М., 2001).
- [6] Бурбаки Н. *Многочлены и поля. Упорядоченные группы* (Наука, М., 1965).
- [7] Прасолов В.В. *Многочлены* (МЦИМО, 2003).
- [8] Галяутдинов И.Г., Лаврентьева Е.Е. *Многочлены, порождающие максимальные вещественные подполя круговых полей*, Учен. зап. Казанск. ун-та., Сер. Физ.-матем. науки, **158** (4), 2016, 469–481.
- [9] Alaca S., Williams K.S. *Introductory algebraic number theory*, Cambridge Univ. Press., 2004.
- [10] Айерлэнд К., Роузен М. *Классическое введение в современную теорию чисел* (Мир, М., 1987).
- [11] Marcus D.A. *Number fields*, Springer-Verlag, New York (2018).
- [12] Huard J.G., Spearman B.K., Williams K.S. *The primes for which an abelian cubic splits*, J. Math. 17, Tokyo (1994).
- [13] Galyautdinov I.G., Lavrentyeva E.E. *Normal basis of the maximal real subfield of a circular field*, Lobachevskii J. Math., 2019, **40** (5), 630–639.

Ильдархан Галяутдинович Галяутдинов
Казань, Россия

Елена Евгеньевна Лаврентьева
Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,
e-mail: ialee-4@mail.ru

I.G. Galyautdinov and E.E. Lavrentyeva

Diophantine equation generated by the maximal subfield of a circular field

Abstract. Using the fundamental basis of the field $L_9 = \mathbb{Q}(2 \cos(\pi/9))$, the form $N_{L_9}(\gamma) = f(x, y, z)$ is found and the Diophantine equation $f(x, y, z) = a$ is solved. A similar scheme is used to construct the form $N_{L_7}(\gamma) = g(x, y, z)$. The Diophantine equation $g(x, y, z) = a$ is solved.

Keywords: algebraic integer number, fundamental basis of an algebraic number field, norm of algebraic number, basic units of an algebraic field, diophantine equation.

Ildarkhan Galyautdinovich Galyautdinov
Kazan, Russia

Elena Evgen'evna Lavrentyeva
Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,
e-mail: ialee-4@mail.ru