

Уравнение Туэ-Малера в относительных полях

С. В. Котов (Минск)

Памяти Ю. В. Линника посвящается

1. Введение. Пусть $F(x, y)$ — целочисленная неприводимая бинарная форма степени $n \geq 3$, p_1, \dots, p_s — фиксированные простые числа. К. Малер [25], [26], [27] доказал, что диофантово уравнение

$$(1) \quad F(x, y) = p_1^{z_1} \cdots p_s^{z_s}, \quad (x, y) = 1,$$

где $x, y, z_1 \geq 0, \dots, z_s \geq 0$ — неизвестные целые рациональные числа, имеет лишь конечное число решений. Этот результат был получен неэффективным методом и не позволял даже в принципе построить границу для решений уравнения (1).

А. Виноградов и В. Спринджук [1] указали способ эффективного анализа целочисленных решений диофантова уравнения

$$(2) \quad F(x, y) = A p_1^{z_1} \cdots p_s^{z_s}, \quad (x, y) = 1,$$

где $A \neq 0$ — целое рациональное, которое содержит в себе уравнение (1) и носит название *уравнение Туэ-Малера*. Эффективный анализ уравнения (2), предложенный в работе [1], основан на оценках линейных форм от логарифмов алгебраических чисел, полученных А. Бэйкером [17], [18], [19], [20], и p -адических аналогах таких оценок [6], [7]. Дж. Коутес [23], развивая рассуждения А. Бэйкера [21], [22] в применении к уравнению (2), получил оценку вида:

$$\max(|x|, |y|, p_1^{z_1}, \dots, p_s^{z_s}) < \exp\{c_1(\ln|A|)^{\kappa}\},$$

где $\kappa > n(s+1)+1$, $c_1 > 0$ — эффективно определяемая величина, не зависящая от A . В. Спринджук под иным углом зрения провел эффективный анализ целочисленных решений (2). Используя тонкую связь между оценками линейных форм от логарифмов алгебраических чисел в различных метриках (архimedовой и неархimedовых), он установил [9], [10] для бинарных форм $F(x, y)$ степени $n \geq 4$ ⁽¹⁾ оценку сле-

⁽¹⁾ При $n = 4$ бинарная форма $F(x, y)$ не должна быть „исключительной” в смысле [10].

дующего вида:

$$\max(|x|, |y|, p_1^{z_1}, \dots, p_s^{z_s}) < \exp\{c_2 \ln|A|(\ln \ln|A|)^{4(s+n+1)}\},$$

где $c_2 > 0$ — величина, не зависящая от A и эффективно определяемая. Он отметил также [11], [12], что в этой оценке $\ln \ln|A|$ можно заменить постоянной величиной.

Для приложений важно знать, какое влияние оказывает „высота” H_F — максимум модулей коэффициентов формы $F(x, y)$ — на величину решений уравнения (2). В этом направлении Дж. Коутес [24] доказал, что все решения x, y уравнения (2) с условием $(x, y, p_1, \dots, p_s) = 1$ удовлетворяют неравенству

$$\max(|x|, |y|) < \exp\{(\ln|A|)^z + 2^z P^{26m^2} H_F^{2v n^3}\},$$

где $z > n(s+1)+1$, $v = 64n(s+1)n^2/(z-n(s+1)-1)$, $P = \max(p_1, \dots, p_s)$. Недавно В. Спиринджук [15] получил оценку с учетом влияния всех основных параметров уравнения (2):

$$(3) \quad \begin{aligned} \max(|x|, |y|, p_1^{z_1}, \dots, p_s^{z_s}) &< \\ &< \exp\{(R + s \ln P) \left((c_3 P^{2g+1} (\ln|A| + \ln H_F + sh \ln P))^{\frac{1+\xi}{1-2\xi}} + \right. \\ &\quad \left. + (c_4 \xi^{-1} (s+1)^3 P^{2(g+1)} (R + \ln P))^{\frac{4(n+s+1)(1+\xi)}{\xi}} \right)\}, \end{aligned}$$

где R и h — соответственно регулятор и число классов идеалов поля алгебраических чисел, получаемого присоединением к полю рациональных чисел Q корня формы $F(x, y)$, $P = \max(p_1, \dots, p_s)$, g — степень поля разложения формы, ξ — любое число из интервала $0 < \xi \leq 0,48$, величины $c_3 > 0$ и $c_4 > 0$ зависят только от n и эффективно определяются.

Уравнение (2) допускает обобщение на случай формы $F(x, y)$ с целыми алгебраическими коэффициентами из некоторого поля K алгебраических чисел конечной степени над полем Q и относительно неизвестных, лежащих в кольце Z_K целых чисел поля K . Исследование уравнения такого вида интересно само по себе и важно для приложений. Пусть $F(x, y)$ — бинарная форма степени $n \geq 3$ неприводимая над полем K и с коэффициентами из Z_K ; $a, \beta_1, \dots, \beta_s \in Z_K$; идеалы (β_l) — степени различных простых идеалов p_l , $(\beta_l) = \mathfrak{P}_l^{u_l}$, $u_l > 0$ ($1 \leq l \leq s$). Уравнение

$$(4) \quad F(x, y) = a \beta_1^{z_1} \dots \beta_s^{z_s}, \quad (x, y) = 1,$$

где $x, y \in Z_K$, $z_1 \geq 0, \dots, z_s \geq 0$ — целые рациональные числа, назовем обобщенным уравнением Туэ–Малера.

Обобщая результаты К. Малера [25], [26], [27] на относительные поля, К. Дж. Парри [28], [29] доказал, что если $F(x, y)$ — бинарная форма степени $n \geq 3$ с коэффициентами из Z_K и с отличным от нуля дискриминантом, S — любое фиксированное множество простых идеалов в K , $a \neq 0$ из Z_K , то существует лишь конечное множество неассоциированных пар целых x, y в K , для которых $F(x, y)$ делится только на простые идеалы из S , $(x, y) \mid (a)$. Иными словами, если $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ — простые идеалы из S , то уравнение

$$(5) \quad (F(x, y)) = \mathfrak{P}_1^{z_1} \dots \mathfrak{P}_s^{z_s}, \quad (x, y) \mid (a)$$

в целых $x, y \in K$ и целых рациональных $z_1 \geq 0, \dots, z_s \geq 0$ имеет лишь конечное число решений, если не различать пары $\{x, y\}$ и $\{zx, zy\}$, где z — единица из K .

Уравнение (4) по форме аналогично уравнению Туэ–Малера (2), но на самом деле существенно отличаются от него, и известные способы эффективного анализа обычного уравнения Туэ–Малера [1], [9], [23] нуждаются в развитии, чтобы их можно было использовать для анализа (4). Основная особенность уравнения (4) заключается в том, что если K не совпадает с Q или с минимым квадратичным полем, то в области его решений $\{x, y\}$ есть единицы бесконечного порядка. Как мы видели, эта особенность ярко проявляется на примере уравнения (5). В. Спиринджук и автор [4] предложили способ для эффективного анализа обобщенного уравнения Туэ–Малера. Основное содержание этого способа состоит в сведении (4) к эффективному анализу уравнения

$$(6) \quad F(x, y) = \tau a \beta_1^{z_1} \dots \beta_s^{z_s}, \quad (x, y) = 1,$$

где τ — новая неизвестная, значения которой принадлежат группе единиц поля K .

В этой статье дается детальный анализ целочисленных решений уравнения (6), когда $(x, y) \mid (a)$, a — фиксированное число из Z_K , и выводится для $\max(|\eta x|, |\eta y|, p_1^{f_1 u_1 z_1}, \dots, p_s^{f_s u_s z_s})$ оценка вида (3), где η — некоторая единица поля K , $|\eta x|$ — максимум модулей величин, сопряженных с x относительно поля K (аналогично $|\eta y|$), $p_l^h = N(\mathfrak{P}_l)$ ($1 \leq l \leq s$). Используемые рассуждения являются детальной реализацией схемы, указанной в работе [4].

2. Обозначения и формулировки теорем. В дальнейшем мы используем, в основном, стандартные обозначения.

Q — поле рациональных чисел; K — конечное расширение Q степени $[K : Q] = m$; G — поле разложения формы $F(x, y)$, $[G : Q] = g$ и $[G : K] = d$; Z_G — кольцо целых чисел поля G (аналогично Z_K); $D = D_G$ — дискриминант, $h = h_G$ — число классов идеалов, $R = R_G$ —

регулятор поля G (аналогично $D' = D_K$, $h' = h_K$, $R' = R_K$ для поля K); $|\bar{a}| = \max(|a^{(i)}|)$ — наибольшая из абсолютных величин всех сопряженных $a^{(1)}, a^{(2)}, \dots$ — „размер” a ; $h(a)$ — высота алгебраического числа a ; H_F — максимальный из „размеров” коэффициентов бинарной формы $F(x, y)$ — „размер” формы $F(x, y)$.

Мы будем использовать без пояснений известные свойства функций $|\bar{a}|$ и $h(a)$ и взаимосвязь между ними [14].

Формулируемая ниже теорема содержит основной результат статьи и является „ключевой” для обоснования последующих утверждений.

Теорема 1. Пусть $F(x, y)$ — бинарная форма степени $n \geq 5$ с коэффициентами из Z_K и неприводимая над полем K , a — фиксированное число из Z_K и $(x, y) \nmid (a)$. Существует такая единица $\eta \in K$, что для всех целочисленных решений $x, y \in K$, z_1, \dots, z_s уравнения (6) справедлива оценка

$$(7) \quad \ln \{\max(|\bar{\eta}x|, |\bar{\eta}y|, p_1^{f_1 z_1}, \dots, p_s^{f_s z_s})\} < c_5 R' (R + sh \ln P) \left\{ c_6 P^{2g} (\ln |Nm(a)| + \right. \\ \left. + (\ln H_F + \ln |Nm(a)|)(R + h \ln P) + sh \ln P \right)^{(1+\xi)/(1-2\xi)} + \\ + (c_7 \xi^{-1} (s+1)^3 P^{2(g+1)} (R + h \ln P)^2)^{c_8/\xi} \right\},$$

где ξ — любое вещественное число интервала $0 < \xi < \frac{1}{2}$, положительные величины c_5, c_6, c_7 зависят только от степени поля K , степени n формы $F(x, y)$ и эффективно определяются, $c_8 = 4(sd + g + 1)(1 + \xi)$.

Пусть θ — целое алгебраическое над полем K число степени $n \geq 5$, $L = K(\theta)$, $A \neq 0$ — целое рациональное, p_1, \dots, p_s — фиксированный набор рациональных простых чисел, a — фиксированное число из Z_K . Рассмотрим уравнение

$$(8) \quad N_{L/Q}(x + \theta y) = Ap_1^{z_1} \dots p_s^{z_s}, \quad (x, y) \nmid (a),$$

где $x, y \in Z_K$, $z_1 \geq 0, \dots, z_s \geq 0$ — целые рациональные числа.

Имеет место

Теорема 2. Существует такая единица $\eta \in K$, что для всех целочисленных решений x, y, z_1, \dots, z_s уравнения (8) справедлива оценка

$$(9) \quad \ln \{(|\bar{\eta}x|, |\bar{\eta}y|, p_1^{z_1}, \dots, p_s^{z_s})\} < c_9 R' (R + sh \ln P) \left\{ c_{10} P^{2g} (\ln |A| + \right. \\ \left. + (\ln |\bar{\theta}| + \ln |Nm(a)|)(R + h \ln P) + (h + h')s \ln P \right)^{(1+\xi)/(1-2\xi)} + \\ + (c_7 \xi^{-1} (s+1)^3 P^{2(g+1)} (R + h \ln P)^2)^{c_8/\xi} \right\},$$

где величины c_7, c_8, c_9, c_{10} имеют тот же смысл, что и в (7).

Из результатов К. Малера [25], [26], [27] вытекает, что наибольший простой делитель $P(X)$ неприводимой бинарной формы $F(x, y)$ степени $n \geq 3$ с целыми рациональными коэффициентами возрастает с ростом $X = \max(|x|, |y|)$, где x, y — целые рациональные взаимно простые числа. Однако скорость этого возрастания долгое время устанавливать не удавалось, поскольку проводимые рассуждения являлись неэффективными. Впервые на реальную возможность соответствующей эффективизации указал [8] В. Спринджук. Дж. Коутес [24] установил, что

$$P(X) > c_{11} (\ln \ln X)^{1/4}, \quad X \geq X_1,$$

где $c_{11} > 0$, X_1 — величины, зависящие только от формы $F(x, y)$ и эффективно определяемые. В. Спринджук [15] получил более точную оценку для $P(X)$. Он показал, что для бинарных форм $F(x, y)$ степени $n \geq 3$ (2) справедливо неравенство

$$P(X) > c_{12} \ln \ln X, \quad X \geq X_2,$$

где $c_{12} > 0$, X_2 — вычислимые величины, зависящие только от формы $F(x, y)$. Если анализировать произвольные целочисленные бинарные формы степени $n \geq 3$, имеющие по крайней мере три различных корня, то будет иметь место оценка

$$P(X) > c_{13} (\ln \ln X \cdot \ln \ln \ln X)^{1/3}, \quad X \geq X_3,$$

где $c_{13} > 0$ и X_3 эффективно определяются по $F(x, y)$ [15].

Рассмотрим теперь бинарную форму $F(x, y)$ степени $n \geq 5$ с коэффициентами из Z_K и неприводимую над полем K .

Теорема 3. Пусть $F(x, y)$ — бинарная форма указанного вида. Тогда для наибольшей нормы $N(\mathfrak{P}) = P^f$ простых идеалов \mathfrak{P} , входящих в $F(x, y)$, справедлива оценка

$$(10) \quad N(\mathfrak{P}) > c_{14} (\ln \ln N)^f, \quad N \geq N_0,$$

где $N = \max(|Nm(x)|, |Nm(y)|)$, $(x, y) = 1$, $c_{14} > 0$ и N_0 — величины, зависящие только от поля K , формы $F(x, y)$ и эффективно определяемые.

3. Вспомогательные утверждения и леммы. Для вывода оценки (7) мы применяем предложение 1 о связи между оценками линейных форм от логарифмов алгебраических чисел в различных метриках и его p -адический аналог — предложение 2.

(2) При $n = 3$ бинарная форма $F(x, y)$ не должна быть „исключительной” в смысле [15]. См. также работу В. Спринджука О наибольшем простом делителе бинарной формы, Докл. АН БССР. 15 (5) (1971), стр. 389–391.

Предложение 1. Пусть $a_1, \dots, a_n - n \geq 2$ — отличных от нуля чисел поля G , $a_i \neq 1$ ($1 \leq i \leq n-1$); $h(a_n) \leq A$, $h(a_i) \leq B$ ($1 \leq i \leq n-1$), $A \geq 80g$ и $B \geq 80g$; h_1, \dots, h_{n-1} — целые рациональные числа, $\max(|h_i|) \leq H$ ($1 \leq i \leq n-1$), где $H \geq \exp\{2^{g+1}\}$; $\delta, \xi > 0$ — вещественные числа, $0 < \delta \leq 1$, ξ^{-1} — целое. Пусть, далее, q — простое число, удовлетворяющее неравенству

$$2q^{2g} \leq H^{\frac{4}{5}(n+1)(1+\xi)} \ln H,$$

$\dots|_q$ — q -адическое нормирование G , индуцированное простым идеалом q с нормой q^e , $S = q^{2ex} - q^{(2e-1)x}$, $e = \text{ord}_q q$; $|a_1|_q = \dots = |a_{n-1}|_q = 1$.

Тогда из неравенства

$$(11) \quad |a_n - a_1^{h_1} \dots a_{n-1}^{h_{n-1}}|_q < e^{-\delta H}$$

при условии, что $|a_n|_q \neq 1$ и $0 < \xi < \frac{1}{2}$ следует

$$(12) \quad H \leq (\ln A)^{\frac{1+\xi}{1-2\xi}} + (c_{15}(\delta^{-1} + \xi^{-1})g^2 n^2 \ln B)^{\frac{4(n+1)(1+\xi)}{\xi}},$$

где c_{15} — вычислимая абсолютная постоянная. Если же $|a_n|_q = 1$, то из (11) следует

$$(13) \quad H \leq (\ln A)^{\frac{1+\xi}{1-\xi}} + (c_{16}(\delta^{-1} + \xi^{-1})g^2 n^2 \ln B)^{\frac{4(n+1)(1+\xi)}{\xi}},$$

где c_{16} — вычислимая абсолютная постоянная, для любого ξ из интервала $0 < \xi < 1$ при условии, что

$$(14) \quad |\log(a_n^S) - h_1 \log(a_1^S) - \dots - h_{n-1} \log(a_{n-1}^S)|_q > q^{-H^{\frac{1-\xi}{1+\xi}}},$$

где $\log(\dots)$ означает q -адический логарифм, определенный в метрике $\dots|_q$.

Впервые предложение 1 приведено в [13] (теорема 2), а его подробное доказательство изложено в [14] (теорема 1).

Предложение 2. Пусть выполняются предпосылки предыдущего предложения; q — простое число, удовлетворяющее неравенству

$$(15) \quad 2q^{2g} \leq H^{\frac{4}{5}(n+1)(1+\xi)},$$

p — простое число ($p \neq q$) такое, что

$$(16) \quad p \leq \ln H$$

и в поле G определено p -адическое нормирование $\dots|_p$, причем

$$(17) \quad |a_i^T - 1|_p < p^{-\frac{1}{p-1}} \quad (1 \leq i \leq n),$$

где T — некоторое натуральное число.

Тогда для p -адических чисел $a^{Th_i} = \exp(h_i \log(a_i^T))$ из неравенства

$$(18) \quad |a_n^T - a_1^{Th_1} \dots a_{n-1}^{Th_{n-1}}|_p < p^{-\delta H},$$

при условии, что $|a_n|_q \neq 1$ и $\frac{8(n+1)\ln \ln H}{\ln H} \leq \xi < \frac{1}{2}$, следует

$$(19) \quad H \leq (T \ln(gA))^{\frac{1+\xi}{1-2\xi}} + (c_{17} \delta^{-1} g^2 p n \ln(gB))^{\frac{4(n+1)(1+\xi)}{\xi}},$$

где c_{17} — вычислимая абсолютная постоянная. Если же $|a_n|_q = 1$, то из (18) следует

$$(20) \quad H \leq (T \ln(gA))^{\frac{1+\xi}{1-\xi}} + (c_{18} \delta^{-1} g^2 p n \ln(gB))^{\frac{4(n+1)(1+\xi)}{\xi}},$$

где c_{18} — вычислимая абсолютная постоянная, для любого ξ из интервала $\frac{8(n+1)\ln \ln H}{\ln H} \leq \xi < 1$ при условии, что выполняется (14).

Доказательство предложения 2 подобно доказательству теоремы 2 из работы [9], при этом необходимо сделать те изменения в выборе основных параметров, о которых сказано в [14].

Укажем иную, более компактную, запись условия (14). Из того, что

$$|a_i^{Sh_i} - 1|_q \leq q^{-\epsilon_q} < q^{-\frac{1}{q-1}}$$

следует

$$|a_i^{Sh_i} - 1|_q = |\exp(h_i a_i^S) - 1|_q = |h_i \log(a_i^S)|_q$$

($1 \leq i \leq n$, $h_n = 1$) и (14) равносильно неравенству

$$(21) \quad |(a_1^{h_1} \dots a_{n-1}^{h_{n-1}} a_n^{-1})^S - 1|_q > q^{-H^{\frac{1-\xi}{1+\xi}}}.$$

В дальнейшем через c_{19}, c_{20}, \dots мы будем обозначать положительные величины, зависящие только от m — степени поля K и n — степени бинарной формы $F(x, y)$ (в противном случае будет оговорено) и эффективно определяемые.

Нам окажутся полезными следующие леммы.

Лемма 1. Существуют такие независимые алгебраические единицы $\varepsilon_1, \dots, \varepsilon_k$ ($k \leq g-1$) поля G , что все элементы матрицы

$$(\ln |\varepsilon_j^{(\sigma)}|)_{j,\sigma=1,\dots,k}$$

по абсолютной величине не превосходят $c_{19} R$, а элементы обратной матрицы не превосходят c_{20} , при этом

$$(22) \quad R < c_{21} |D|^{1/2} (\log |D|)^{g-1}.$$

Справедливость леммы вытекает из результатов работы [30].

Очевидно, что единицы $\varepsilon_1, \dots, \varepsilon_k$ порождают группу E , которая является подгруппой E_G — группы единиц поля G .

Лемма 2. Пусть $a \in G$, $Nm(a) = A \neq 0$. Тогда существует такая единица $\varepsilon \in E$, что

$$a^{(\sigma)} \varepsilon^{(\sigma)} = |A|^{1/g} e^{\delta(\sigma)}, \quad |\delta(\sigma)| \leq M \quad (1 \leq \sigma \leq g),$$

где $M = c_{22}R$ и для R верна оценка (22).

Доказательство следует из леммы 1 и рассуждений описанных в доказательстве леммы 4.5 из [14].

Заметим, что относительно поля K леммы 1 и 2 имеют свои аналоги.

Лемма 3. Если $a \in G$, S — натуральное число, $|...|_q$ — q -адическое нормирование поля $G(\zeta_0)$, ζ_0 — первообразный корень степени S из 1, то

$$|a - \zeta|_q = |a^S - 1|_q |S|_q^{-1},$$

где ζ — некоторый корень степени S из 1.

Доказательство см. в [14], лемма 1.6.

Лемма 4. Пусть a — целое алгебраическое число, отличное от нуля. Тогда

$$|a|_q |Nm(a)| \geq 1,$$

где $|...|_q$ — q -адическая норма.

Доказательство следует из „формулы произведения” (см. [5], стр. 91).

Лемма 5. Пусть θ — алгебраическое над полем K число степени $n \geq 4$, $\theta_1, \dots, \theta_n$ — сопряженные числа с $\theta = \theta_1$ относительно K ; S — натуральное число; $|...|_q$ — q -адическое нормирование поля $K(\theta_1, \dots, \theta_n, \zeta_0)$, где ζ_0 — первообразный корень степени S из 1, ζ_i — произвольные различные корни степени S из 1 ($3 \leq i \leq n$), отличные от 1. Если выражение

$$\zeta_{ij} = (1 - \zeta_i) \frac{\theta_2 - \theta_j}{\theta_1 - \theta_i} - (1 - \zeta_j) \frac{\theta_2 - \theta_i}{\theta_1 - \theta_j}$$

отлично от нуля, то

$$|\zeta_{ij}|_q \geq c_{23}(\hbar(\theta))^{-c_{24}S}.$$

Доказательство см. в [14], лемма 2.6.

Лемма 6. Пусть p — простой идеал в G , T — натуральное число, $a, \beta \in G$, причем

$$(a, p) = 1 \quad \text{и} \quad \text{ord}_p(a - \beta) > \text{ord}_p T.$$

Тогда

$$\text{ord}_p(a^T - \beta^T) = \text{ord}_p(a - \beta) + \text{ord}_p T.$$

Доказательство см. в [9], лемма 3.5.

Дадим следующие определения.

Алгебраическое над полем K число θ степени $n \geq 4$ называется исключительным, если существует такая нумерация его сопряженных $\theta_1, \dots, \theta_n$ относительно поля K , что выполняются равенства

$$(23) \quad \frac{\theta_1 - \theta_i}{\theta_2 - \theta_i} \cdot \frac{\theta_2 - \theta_j}{\theta_1 - \theta_j} = \frac{1 - \zeta_i}{1 - \zeta_j}$$

для любых индексов i, j ($i \neq j$; $3 \leq i, j \leq n$), где $\zeta_i, \zeta_j \neq 1$ — некоторые различные корни из 1.

Бинарная форма $F(x, y)$ степени $n \geq 4$ с коэффициентами из Z_K называется исключительной, если ее корни являются исключительными числами.

Имеет место

Лемма 7. Если $F(x, y)$ — неприводимая над полем K бинарная форма степени $n \geq 5$, то она не является „исключительной”.

Доказательство проводится по аналогии с рассуждениями, приведенными в [12], лемма 1.4.

4. Анализ уравнения (6). Пусть

$$(24) \quad F(x, y) = a_0(x - \theta'_1 y) \dots (x - \theta'_n y)$$

— разложение формы $F(x, y)$ в поле $G = K(\theta'_1, \dots, \theta'_n)$, $[G : K] = g$. Учитывая равенство (6), производим в Z_G разложение на идеалы правой части (24):

$$(25) \quad (a_0(x - \theta'_1 y) \dots (x - \theta'_n y)) = (a_0)^{U_1} \dots p_t^{U_t},$$

простые идеалы p_1, \dots, p_t входят в простые в Z_K идеалы $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ и $t \leq sd$, где $[G : K] = d$. Умножаем обе части (25) на идеал $(a_0)^{n-1}$ и положим $\theta_i = a_0 \theta'_i$ ($1 \leq i \leq n$), $x' = a_0 x$, $y' = y$. Можем записать

$$(26) \quad (x' - \theta_i y') = a_t p_1^{U_1} \dots p_t^{U_t} \quad (1 \leq i \leq n),$$

где идеал $a_t | (a_0^{n-1} a)$, $U_t \leq U_1$ ($1 \leq t \leq l$).

Полагая $U_{tl} = h u_{tl} + r_{tl}$, $0 \leq r_{tl} < h$ ($1 \leq i \leq n$, $1 \leq l \leq t$), из (26) получаем

$$(27) \quad (x' - \theta_i y') = (\pi_i \varrho_1^{u_{1i}} \dots \varrho_t^{u_{ti}}),$$

$(\varrho_l) = p_l^h$ и $(\pi_i) = a_t p_1^{r_{1i}} \dots p_t^{r_{ti}}$ — главные идеалы, причем $\varrho_l, \pi_i \in Z_G$. Так как

$$N_G(\pi_i) = N_G(a_t) \prod_{l=1}^t N_G(p_l^{r_{li}}),$$

то можно считать в силу леммы 2 (в результате умножения на подходящую единицу поля G), что

$$(28) \quad \begin{aligned} |\pi_i| &\leq \left(|Nm_K(a)|^d \max_{(l)} N_G(p_l)^{sd(h-1)} \right)^{1/g} e^M < \\ &< |Nm_K(a)| P^{shg} e^M \quad (1 \leq i \leq n), \end{aligned}$$

где $N_G(p_l) = p_l^{f'_l}$ ⁽³⁾ ($1 \leq f'_l \leq g$), $P = \max_{(l)} (p_l)$ ($1 \leq l \leq t$). Также устанавливаем, что

$$(29) \quad |\varrho_i| \leq \left(\max_{(l)} N_G(p_l) \right)^{(h-1)/g} e^M < P^h e^M.$$

Переходя после подобной „нормировки”⁽⁴⁾ от равенства идеалов в (27) к равенству чисел, имеем

$$(30) \quad x' - \theta_i y' = \pi_i \varrho_1^{u_{1i}} \dots \varrho_t^{u_{ti}} \varepsilon_i' \quad (1 \leq i \leq n),$$

где $\varepsilon_i' \in E$.

Отметим следующий факт, который будет использован в дальнейшем. Пусть $e' = \varepsilon_1' \dots \varepsilon_k' = \varepsilon_1^{v_1} \dots \varepsilon_k^{v_k}$. Полагаем $W_j = nw_j + v_j$, $0 \leq v_j < n$ ($1 \leq j \leq k$) и $e = \varepsilon_1^{-w_1} \dots \varepsilon_k^{-w_k}$. Тогда

$$(31) \quad e^n e' = \varepsilon_1^{v_1} \dots \varepsilon_k^{v_k}$$

и $e\varepsilon_i' = \varepsilon_1^{v_{1i}} \dots \varepsilon_k^{v_{ki}}$ ($1 \leq i \leq n$). В силу (31) можем записать, что

$$(32) \quad \sum_{i=1}^n v_{ji} = v_j < n \quad (1 \leq j \leq k).$$

Умножая обе части (30) на e , получаем

$$(33) \quad X - \theta_i Y = \pi_i \varrho_1^{u_{1i}} \dots \varrho_t^{u_{ti}} \varepsilon_1^{v_{1i}} \dots \varepsilon_k^{v_{ki}} = \mu_i \quad (1 \leq i \leq n),$$

где $X = ex'$, $Y = ey'$, причем выполняются неравенства (28), (29) и (32).

Из (33), исключая X и Y , получаем систему равенств

$$(34) \quad (\theta_j - \theta_i) \mu_i - (\theta_i - \theta_l) \mu_j - (\theta_j - \theta_l) \mu_l = 0$$

при любых различных индексах i, j, l ($1 \leq i, j, l \leq n$).

Цель дальнейших рассуждений состоит в том, чтобы найти оценку сверху для

$$H = \max_{(i,j,l)} (|u_{il}|, |v_{jl}|)$$

($1 \leq l \leq t$, $1 \leq i \leq n$, $1 \leq j \leq k$), позволяющую оценить $|\mu_i|$.

⁽³⁾ Заметим, что $N(\mathfrak{P}) = N_K(\mathfrak{P}) = P^f$ и $f|f'$ поскольку $N_G(p) = N_K(N_{G/K}(p)) = P^{f'}$ (см., например, [2], стр. 144–146).

⁽⁴⁾ После „нормировки” мы сохраним прежние обозначения, чтобы не усложнять записи.

Без ограничения общности можем считать, что $u_{12} = \max_{(l,i)} (|u_{li}|)$.

Из (34) выделяем подсистему

$$(35) \quad (\theta_2 - \theta_1) \mu_i - (\theta_i - \theta_1) \mu_2 - (\theta_2 - \theta_i) \mu_1 = 0 \quad (3 \leq i \leq n).$$

Допустим, что

$$(36) \quad \varrho_1^u \| ((\theta_2 - \theta_i) \pi_1 \varrho_1^{u_{1i}}, \varrho_1^{u_{12}}),$$

тогда

$$\varrho_1^{u-hu_{11}-r_{11}} \| (\theta_2 - \theta_i) \alpha_1,$$

следовательно, $\varrho_1^{u-hu_{11}-r_{11}}$ входит в $Nm_G(\theta_2 - \theta_i) N_G(\alpha_1)$. Так как $|Nm_G(\theta_2 - \theta_i)| \leq (2nH_F)^g$, а $N_G(\alpha_1) \leq |Nm_G(a_0^{n-1} a)| \leq H_F^{(n-1)g} |Nm_K(a)|^d$, то

$$(37) \quad u \leq 1/\ln 2(g \ln 2n + g \ln H_F + d \ln |Nm_K(a)|) + hu_{11} + r_{11}.$$

По предложению $u_{12} \geq u_{1i}$, поскольку $\varrho_1^{hu_{11}}$ входит в идеалы $(X - \theta_2 Y)$ и $(X - \theta_i Y)$ ($i \neq 2$; $1 \leq i \leq n$), следовательно, в $((\theta_2 - \theta_i) Y)$. Пусть $\varrho_1^u \| (Y)$ и $u'_i = \min(u', hu_{11})$. Рассмотрим случай, когда $u'_i = hu_{1i}$ (или $hu_{1i} \leq u'$). Поскольку $\text{ord}_{\varrho_1}(X - \theta_i Y) \geq \min(\text{ord}_{\varrho_1}(X), \text{ord}_{\varrho_1}(\theta_i Y))$, то $\varrho_1^{hu_{1i}} \|(X)$ и $\varrho_1^{hu_{1i}} \|(X, Y)$. Так как $(X, Y) = (a_0 x, y)$ и $(a_0 x, y) | a_0 a$, то

$$hu_{11} \leq 1/\ln 2(g \ln H_F + d \ln |Nm_K(a)|).$$

Рассматривая второй случай: $u'_i = u'$ (или $u' < hu_{11}$) и аналогично рассуждая, находим $u' \leq 1/\ln 2(g \ln H_F + d \ln |Nm_K(a)|)$. Далее, $\varrho_1^{hu_{11}-u'_i} \| (\theta_2 - \theta_i)$, тогда $\varrho_1^{hu_{11}-u'_i}$ входит в $Nm_G(\theta_2 - \theta_i)$ и $hu_{11} - u'_i \leq g/\ln 2(\ln 2n + \ln H_F)$. Таким образом,

$$hu_{11} \leq 1/\ln 2(g \ln 2n + 2 \ln H_F + d \ln |Nm_K(a)|) \quad (i \neq 2; 1 \leq i \leq n).$$

Учитывая, что $r_{11} < h$, из (37) заключаем,

$$u < c_{25}(\ln H_F + \ln |Nm_K(a)| + \ln |Nm_K(a)| + h) = U.$$

Если $hu_{12} \leq U$, то мы имеем удовлетворительную оценку для u_{12} .

Если же $hu_{12} > U$, то из (36) следует, что

$$\varrho_1^u \| ((\theta_2 - \theta_i) \pi_1 \varrho_1^{u_{1i}}).$$

Отсюда, в силу (35), имеем

$$\varrho_1^u \| ((\theta_2 - \theta_1) \pi_1 \varrho_1^{u_{11}})$$

и ϱ_1 не входит в отношение

$$\frac{(\theta_2 - \theta_1) \pi_1}{(\theta_2 - \theta_i) \pi_1} \varrho_1^{u_{1i}-u_{11}}$$

для любого индекса $i = 3, \dots, n$.

Из (35) заключаем, что

$$(38) \quad 1 - \frac{(\theta_2 - \theta_1)\mu_i}{(\theta_2 - \theta_i)\mu_1} \equiv 0 \pmod{p_1^{hu_{12}-U}},$$

где

$$\frac{(\theta_2 - \theta_1)\mu_i}{(\theta_2 - \theta_i)\mu_1} = \left[\frac{(\theta_2 - \theta_1)\pi_i}{(\theta_2 - \theta_i)\pi_1} \varrho_1^{u_{11}-u_{1i}} \right] \prod_{l=2}^t [\varepsilon_l]^{u_{li}-u_{1i}} \prod_{j=1}^k [\varepsilon_j]^{v_{ji}-v_{j1}},$$

$$\max_{(i,j)} (|u_{ii} - u_{1i}|, |v_{ji} - v_{j1}|) \leq 2H \quad (3 \leq i \leq n)$$

и каждое число в прямых скобках есть p_1 -адическая единица. Нам необходимо получить в неархимедовой (p_1 -адической) метрике оценку снизу для выражения, стоящего в левой части (38). Для этого используем предложение 2, предварительно проверив выполнение его условий.

Из (28) и (29) следует, что

$$h(\pi_i) \leq (2|Nm_K(a)|P^{sh}e^M)^g < (|Nm_K(a)|P^{sh}e^M)^{c_{26}} \quad (1 \leq i \leq n)$$

и

$$h(\varrho_l) \leq (2P^h e^M)^g < (P^h e^M)^{c_{27}} \quad (1 \leq l \leq t).$$

Высоты чисел $\theta_2 - \theta_1$ и $\theta_2 - \theta_i$ не превосходят $(4nH_F)^g$. Так как

$$|u_{11} - u_{ii}| \leq c_{28} (\ln H_F + \ln |Nm_K(a)|) = U',$$

то

$$h(\varrho_1^{u_{11}-u_{1i}}) < (P^h e^M)^{c_{29}U'} \quad (i \neq 2; 1 \leq i \leq n).$$

Следовательно,

$$h\left(\frac{(\theta_2 - \theta_i)\pi_1}{(\theta_2 - \theta_i)\pi_i} \varrho_1^{u_{11}-u_{1i}}\right) < (|Nm_K(a)|P^{h(s+U')}e^{MU'}H_F)^{c_{30}} \quad (3 \leq i \leq n).$$

В силу оценок леммы 1 имеем

$$h(\varepsilon_j) \leq (2e^{c_{19}R})^g < e^{c_{31}R} \quad (1 \leq j \leq k).$$

Полагаем

$$(39) \quad A = (|Nm_K(a)|P^{h(s+U')}e^{MU'}H_F)^{c_{30}}$$

и

$$(40) \quad B = \max((P^h e^M)^{c_{27}}, e^{c_{31}R}).$$

Пусть $\dots|_{p_1}$ — p_1 -адическое нормирование поля G , индуцированное простым идеалом p_1 с нормой $N_G(p_1) = p_1^f$. Считаем, что p_1 удовлетворяет неравенству (16) ибо в противном случае сразу получаем оценку сверху для H . Пусть, далее, $T = p_1^{2e_1 f_1} - p_1^{(2e_1-1)f_1}$, где $e_1 =$

$= \text{ord}_{p_1} p_1$. Очевидно, что

$$\left| \left(\frac{(\theta_2 - \theta_i)\pi_1}{(\theta_2 - \theta_i)\pi_i} \varrho_1^{u_{11}-u_{1i}} \right)^T - 1 \right|_{p_1} < p_1^{-\frac{1}{p_1-1}} \quad (3 \leq i \leq n),$$

$$|\varrho_l^T - 1|_{p_1} < p_1^{-\frac{1}{p_1-1}} \quad (2 \leq l \leq t)$$

и

$$|\varepsilon_j^T - 1|_{p_1} < p_1^{-\frac{1}{p_1-1}} \quad (1 \leq j \leq k).$$

Пусть q — простое число, удовлетворяющее неравенству $P < q < 2P$ (такое q существует, см. [16], стр. 849), $\dots|_q$ — q -адическое нормирование поля G , индуцированное некоторым простым делителем q в Z_G . Можно считать, что выполняется условие (15), налагаемое на q , так как в противном случае мы имеем сразу оценку сверху для H .

Предположим, что H не удовлетворяет ни одному из неравенств (19) или (20) с A и B , определенными (39) и (40) соответственно. Согласно формулировке предложения 2, рассматриваем возможности: или

$$(41) \quad \left| \frac{(\theta_2 - \theta_i)\pi_1}{(\theta_2 - \theta_i)\pi_i} \varrho_1^{u_{11}-u_{1i}} \right|_q \neq 1$$

для некоторого индекса i ($3 \leq i \leq n$), или же эта норма равна 1.

Допустим, что выполняется (41). Тогда имеет место неравенство

$$(42) \quad \left| 1 - \left(\frac{(\theta_2 - \theta_i)\mu_i}{(\theta_2 - \theta_i)\mu_1} \right)^T \right|_{p_1} \geq p_1^{-2sH}$$

для хотя бы одного индекса i ($3 \leq i \leq n$) при

$$(43) \quad H > \frac{1}{2} \left(T \ln(gA) \right)^{\frac{1+\xi}{1-2\xi}} + \frac{1}{2} (c_{17} \delta^{-1} g^2 p_1 (sd + g - 1) T \ln(gB))^{\frac{4(sd+g)(1+\xi)}{\xi}},$$

$$\text{если } \frac{8(sd+g-1)\ln\ln H}{\ln H} \leq \xi < \frac{1}{2}.$$

Теперь предположим, что ни при каком индексе $i = 3, \dots, n$ не выполняется (41). Для дальнейшего применения предложения 2 необходимо установить неравенство

$$(44) \quad \left| \log \left(\left(\frac{(\theta_2 - \theta_i)\pi_1}{(\theta_2 - \theta_i)\pi_i} \varrho_1^{u_{11}-u_{1i}} \right)^S \right) - \sum_{l=2}^t (u_{li} - u_{1i}) \log(\varrho_l^S) - \sum_{j=1}^k (v_{ji} - v_{j1}) \log(\varepsilon_j^S) \right|_q > q^{-(2H)^{\frac{1-\xi}{1+\xi}}}$$

для какого-либо индекса i ($3 \leq i \leq n$), где $\log(\dots)$ — q -адический логарифм в метрике $|\dots|_q$, S определено в формулировке предложения 2.

Допустим, что справедливо неравенство, противоположное (43). Учитывая это, в силу (21) можем записать

$$(45) \quad \left| \left(\frac{(\theta_2 - \theta_1) \mu_i}{(\theta_2 - \theta_i) \mu_1} \right)^S - 1 \right|_q \leq q^{-(2H)^{\frac{1-\xi}{1+\xi}}} \quad (3 \leq i \leq n).$$

Рассмотрим поле $G(\zeta_0)$, где ζ_0 — первообразный корень степени S из 1 и $|\dots|_q$ — продолжение q -адического нормирования $|\dots|_q$ из G на $G(\zeta_0)$. Применим к (45) лемму 3. Получаем

$$\left| \frac{(\theta_2 - \theta_1) \mu_i}{(\theta_2 - \theta_i) \mu_1} - \zeta_i \right|_q \leq |S|_q^{-1} q^{-(2H)^{\frac{1-\xi}{1+\xi}}} = q^{-v}$$

для некоторого корня ζ_i ($3 \leq i \leq n$) степени S из 1. Принимая во внимание (34), находим

$$(46) \quad \left| (1 - \zeta_i) \frac{\theta_2 - \theta_i}{\theta_1 - \theta_i} - \frac{\mu_2}{\mu_1} \right|_q \leq q^{-(v+v_i)},$$

где

$$q^{-v_i} = \left| \frac{\theta_2 - \theta_i}{\theta_1 - \theta_i} \right|_q \quad (3 \leq i \leq n).$$

Заметим, что $\zeta_i \neq 1$ при любом индексе $i = 3, \dots, n$. Действительно, если $\zeta_i = 1$, то из (46) следует:

$$|\mu_2|_q \leq |\mu_1|_q q^{-(v+v_i)} \leq q^{-(v+v_i)}.$$

Так как

$$|\mu_2|_q \geq |Nm_G(a_0 a)|^{-1} \geq H_F^{-g} |Nm_K(a)|^{-d},$$

то

$$(47) \quad v + v_i \leq 1/\ln q (g \ln H_F + d \ln |Nm_K(a)|).$$

Поскольку $(\theta_2 - \theta_i)$ — целое, то $|\theta_2 - \theta_i|_q \leq 1$. Далее, по лемме 4

$$|\theta_1 - \theta_i|_q \geq |Nm_G(\theta_1 - \theta_i)|^{-1} \geq (2nH_F)^{-g}.$$

Таким образом,

$$v_i \geq g/\ln q (\ln 2n + \ln H_F) \quad (3 \leq i \leq n)$$

и из (47) следует

$$v \leq 1/\ln q (d \ln |Nm_K(a)| - g \ln 2n)$$

или

$$(48) \quad H < \frac{1}{2} (1/\ln q (d \ln |Nm_K(a)| - g \ln 2n) + 2g)^{\frac{1+\xi}{1-\xi}},$$

поскольку $|S|_q^{-1} \leq S < q^2$. Мы считаем, что выполняется неравенство, противоположное (48), иначе имеем сразу удовлетворительную оценку сверху для H . Следовательно, $\zeta_i \neq 1$ ($3 \leq i \leq n$) и из (46) мы выводим

$$(49) \quad \left| (1 - \zeta_i) \frac{\theta_2 - \theta_i}{\theta_1 - \theta_i} - (1 - \zeta_j) \frac{\theta_2 - \theta_j}{\theta_1 - \theta_j} \right|_q \leq q^{-(v+v_i)},$$

где $v' = \min_{(i,j)} (v_i, v_j)$, для любой пары индексов i, j ($i \neq j$; $3 \leq i, j \leq n$).

Можем считать, что

$$(50) \quad (1 - \zeta_i) \frac{\theta_2 - \theta_i}{\theta_1 - \theta_i} - (1 - \zeta_j) \frac{\theta_2 - \theta_j}{\theta_1 - \theta_j} = 0.$$

Если же допустить, противное, то, применяя лемму 5, получаем

$$H \leq \frac{1}{2} (c_{32} q^{2g} / \ln q \ln H_F + 2g)^{\frac{1+\xi}{1-\xi}}.$$

Мы приходим к удовлетворительной оценке сверху для H . Поэтому предполагаем справедливость (50), откуда

$$(51) \quad \frac{\theta_1 - \theta_i}{\theta_2 - \theta_i} \cdot \frac{\theta_2 - \theta_j}{\theta_1 - \theta_j} = \frac{1 - \zeta_i}{1 - \zeta_j},$$

где $\zeta_i, \zeta_j \neq 1$ — различные корни степени S из 1 ($i \neq j$; $3 \leq i, j \leq n$). Но по условию теоремы 1 бинарная форма $F(x, y)$ неприводима над K и имеет степень $n \geq 5$, следовательно, в силу леммы 7 равенства (51) не имеют места. Таким образом, наше допущение противоречиво и справедливо неравенство (44).

Тогда, на основании предложения 2, выполняется (42) при

$$(52) \quad H > \frac{1}{2} (T \ln(gA))^{\frac{1+\xi}{1-\xi}} + \frac{1}{2} (c_{18} \delta^{-1} g^2 p_1 (sd+g-1) \ln(gB))^{\frac{4(sd+g)(1+\xi)}{1-\xi}},$$

$$\text{если } \frac{8(sd+g-1) \ln \ln H}{\ln H} \leq \xi < 1.$$

Из сравнения (38) по лемме 6 находим, что

$$(53) \quad \text{ord}_{p_1} \left(1 - \left(\frac{(\theta_2 - \theta_1) \mu_i}{(\theta_2 - \theta_i) \mu_1} \right)^T \right) = hu_{12} - U + \text{ord}_{p_1} T,$$

поскольку $\text{ord}_{p_1} T = \text{ord}_{p_1} p_1^{(2e_1-1)f_1} = e_1(2e_1-1)f_1' < 2g^3 < hu_{12} - U$. Из (42) и (53) заключаем, что $hu_{12} - U + \text{ord}_{p_1} T \leq 2\delta H$. Таким образом, мы устанавливаем, что $u_{12} < 2\delta H + U$, или

$$(54) \quad u_l < 3\delta H \quad (1 \leq l \leq t, 1 \leq i \leq n).$$

Следующая наша задача состоит в том, чтобы получить оценку сверху для $|v_{ji}|$ ($1 \leq j \leq k$, $1 \leq i \leq n$).

Обратимся вновь к системе равенств (34), не фиксируя, вначале, индексы i, j, l . Допустим, что $|v_{12}| = \max_{(i,j)} (|v_{ji}|)$ ($1 \leq j \leq k$, $1 \leq i \leq n$).

Полагаем $V_{ji} = v_{j2} - v_{ji}$, $V_i^j = \max_{(j)} (|V_{ji}|)$ ($1 \leq j \leq k$) и

$$(55) \quad V_1 = \max_{(i)} (V_i) \quad (i \neq 2; 1 \leq i \leq n).$$

С учетом этого, выделяем из (34) подсистему ⁽⁵⁾

$$(56) \quad (\theta_2 - \theta_1)\mu_i - (\theta_i - \theta_1)\mu_2 - (\theta_2 - \theta_i)\mu_1 = 0 \quad (3 \leq i \leq n).$$

Переходя к сопряженным с полем $G = G^{(1)}$ полям $G^{(2)}, \dots, G^{(g)}$, получаем из (56) систему равенств

$$(57) \quad 1 - \frac{(\theta_2^{(\sigma)} - \theta_i^{(\sigma)})\mu_i^{(\sigma)}}{(\theta_2^{(\sigma)} - \theta_1^{(\sigma)})\mu_1^{(\sigma)}} = \frac{(\theta_i^{(\sigma)} - \theta_1^{(\sigma)})\mu_2^{(\sigma)}}{(\theta_i^{(\sigma)} - \theta_2^{(\sigma)})\mu_1^{(\sigma)}}$$

для каждого σ ($1 \leq \sigma \leq g$).

Сейчас нам необходимо указать оценку снизу для абсолютной величины выражения, стоящего в левой части (57). Воспользуемся предложением 1.

Как и ранее устанавливаем, что

$$h\left(\frac{(\theta_2^{(\sigma)} - \theta_i^{(\sigma)})\pi_1^{(\sigma)}}{(\theta_2^{(\sigma)} - \theta_1^{(\sigma)})\pi_i^{(\sigma)}}\right) \leqslant (|Nm_K(a)|P^{sh}e^M H_F)^{c_{33}} \quad (3 \leq i \leq n),$$

$$h(\varrho_l^{(\sigma)}) \leqslant (P^h e^M)^{c_{34}} \quad (1 \leq l \leq t).$$

Полагаем

$$(58) \quad A = (|Nm_K(a)|P^{sh}e^M H_F)^{c_{33}}$$

и

$$(59) \quad B = \max((P^h e^M)^{c_{34}}, e^{c_{31}R}).$$

Пусть q — простое число, как и прежде, $|\dots|_q$ — q -адическое нормирование поля $G^{(\tau)}$, индуцированное некоторым простым делителем q в $Z_{G^{(\tau)}}$.

Предположим, что H не удовлетворяет ни одному из неравенств (12) или (13) с A и B , определенными (58) и (59) соответственно. Учитывая условия предложения 1, рассматриваем два случая: либо

$$(60) \quad \left| \frac{(\theta_2^{(\sigma)} - \theta_i^{(\sigma)})\pi_1^{(\sigma)}}{(\theta_2^{(\sigma)} - \theta_1^{(\sigma)})\pi_i^{(\sigma)}} \right|_q \neq 1$$

для хотя бы одного индекса $i = 3, \dots, n$, либо эта норма равна 1.

⁽⁵⁾ Подсистема (56) может отличаться, вообще говоря, от подсистемы (35).

Допустим, что справедливо (60). Тогда имеет место неравенство

$$(61) \quad \left| 1 - \frac{(\theta_2^{(\sigma)} - \theta_1^{(\sigma)})\mu_i^{(\sigma)}}{(\theta_2^{(\sigma)} - \theta_i^{(\sigma)})\mu_1^{(\sigma)}} \right| \geq e^{-2\delta_1 H}$$

для некоторого индекса i ($3 \leq i \leq n$) при

$$(62) \quad H > \frac{1}{2}(\ln A)^{\frac{1+\xi}{1-2\xi}} + \frac{1}{2}(c_{15}(\delta_1^{-1} + \xi^{-1})g^2(sd+g)^2 \ln B)^{\frac{4(sd+g+1)(1+\xi)}{\xi}},$$

где $0 < \xi < \frac{1}{2}$.

Теперь рассмотрим второй случай: ни при каком индексе $i = 3, \dots, n$ не выполняется (60). Для применения предложения 1 нужно иметь неравенство

$$(63) \quad \left| \log \left(\left(\frac{(\theta_2^{(\sigma)} - \theta_i^{(\sigma)})\pi_1^{(\sigma)}}{(\theta_2^{(\sigma)} - \theta_1^{(\sigma)})\pi_i^{(\sigma)}} \right)^S \right) - \sum_{l=1}^t (u_{li} - u_{1l}) \log ((\varrho_l^{(\sigma)})^S) - \sum_{j=1}^k (v_{ji} - v_{j1}) \log ((\varepsilon_j^{(\sigma)})^S) \right|_q > q^{-(2H)^{1+\frac{1-\xi}{2}}}$$

хотя бы для одного индекса i ($3 \leq i \leq n$), где $\log(\dots)$ — q -адический логарифм в метрике $|\dots|_q$, S определено в формулировке предложения 1. Но справедливость (63) можно доказать, рассуждая, как и ранее. Тогда, применяя предложение 1, мы заключаем, что выполняется (61) в предположении

$$(64) \quad H > \frac{1}{2}(\ln A)^{\frac{1+\xi}{1-2\xi}} + \frac{1}{2}(c_{16}(\delta_1^{-1} + \xi^{-1})g^2(sd+g)^2 \ln B)^{\frac{4(sd+g+1)(1+\xi)}{\xi}},$$

где $0 < \xi < 1$.

Из (57) и (61) имеем

$$(65) \quad \left| \frac{(\theta_2^{(\sigma)} - \theta_i^{(\sigma)})\mu_2^{(\sigma)}}{(\theta_2^{(\sigma)} - \theta_1^{(\sigma)})\mu_1^{(\sigma)}} \right| \geq e^{-2\delta_1 H}$$

для каждого σ ($1 \leq \sigma \leq g$).

Поскольку норма правой части (57) равна

$$\frac{Nm_G(\theta_i - \theta_1)}{Nm_G(\theta_i - \theta_2)},$$

то при любом σ правая часть (60) оценивается сверху величиной $\exp\{g(2\delta_1 H + \ln 2n + \ln H_F)\}$. Принимая это во внимание и неравенство

(65), находим

$$(66) \quad \left| \ln \frac{(\theta_i^{(\sigma)} - \theta_1^{(\sigma)}) \mu_2^{(\sigma)}}{(\theta_i^{(\sigma)} - \theta_2^{(\sigma)}) \mu_1^{(\sigma)}} \right| < g(2\delta_1 H + \ln 2n + \ln H_F),$$

где σ пробегает все изоморфизмы поля G . Учитывая явный вид $\mu_1^{(\sigma)}$ и $\mu_2^{(\sigma)}$, из (66) получаем

$$\left| \ln \frac{(\theta_i^{(\sigma)} - \theta_1^{(\sigma)}) \pi_2^{(\sigma)}}{(\theta_i^{(\sigma)} - \theta_2^{(\sigma)}) \pi_1^{(\sigma)}} \right| + \sum_{l=1}^t (u_{l2} - u_{l1}) \ln |\varrho_l^{(\sigma)}| + \sum_{j=1}^k (v_{j2} - v_{j1}) \ln |e_j^{(\sigma)}| < c_{35} \delta H,$$

откуда

$$(67) \quad \left| \sum_{j=1}^k (v_{j2} - v_{j1}) \ln |e_j^{(\sigma)}| \right| < \omega \quad (1 \leqslant \sigma \leqslant g),$$

где $\omega = c_{36} \delta_1 H + c_{37} s(M + h \ln P) \delta H$. Из системы неравенств (67) можно выделить подсистему с матрицей $(\ln |e_j^{(\sigma)}|)$, указанной в лемме 1, что, возможно, потребует иной нумерации сопряженных величин поля G . Во избежание усложнения обозначений, мы считаем, что для элементов матрицы

$$(68) \quad (\ln |e_j^{(\sigma)}|)_{j,\sigma=1,\dots,k}$$

справедливы оценки из леммы 1. Так как единицы e_1, \dots, e_k независимы, то определитель d матрицы (68) отличен от нуля. Тогда

$$(69) \quad v_{j2} - v_{j1} = d_j d^{-1} \quad (1 \leqslant j \leqslant k),$$

$$d_j = \begin{vmatrix} \ln |e_1^{(1)}| & \dots & \omega_1 \omega & \dots & \ln |e_k^{(1)}| \\ \dots & \dots & \dots & \dots & \dots \\ \ln |e_1^{(k)}| & \dots & \omega_k \omega & \dots & \ln |e_k^{(k)}| \end{vmatrix},$$

где ω_σ — некоторые числа с условием $|\omega_\sigma| < 1$ ($1 \leqslant \sigma \leqslant k$). Раскрывая определитель d_j по j -ому столбцу, получаем в силу (69)

$$|v_{j2} - v_{j1}| < \frac{\omega}{|d|} \sum_{\sigma=1}^k |d_{j\sigma}|,$$

где $d_{j\sigma}$ — алгебраическое дополнение элемента $\omega \omega_\sigma$ в определителе d_j (или элемента $\ln |e_j^{(\sigma)}|$ в определителе d). По лемме 1

$$\left| \frac{d_{j\sigma}}{d} \right| \leqslant c_{20},$$

следовательно,

$$(70) \quad |v_{j2} - v_{j1}| < c_{38} \omega \quad (1 \leqslant j \leqslant k).$$

Неравенства (55) и (70) позволяют заключить, что

$$(71) \quad |(n-1)v_{12} + (v_{11} + v_{13} + \dots + v_{1n})| < c_{39} \omega.$$

Поскольку имеет место (32), то из (71) следует $|v_{12}| < c_{40} \omega$ и

$$(72) \quad |v_{ji}| < c_{40} \omega \quad (1 \leqslant j \leqslant k, 1 \leqslant i \leqslant n).$$

Положим $\delta_2 = \max(\delta_1, \delta')$, где $\delta' = s(M + h \ln P) \delta$. Тогда (72) можно переписать в виде

$$(73) \quad |v_{ji}| < c_{41} \delta_2 H$$

для любых значений индексов $j = 1, \dots, k$ и $i = 1, \dots, n$.

Из неравенств (54) и (73) получаем

$$H < (c_{41} + 3) \delta_2 H$$

или

$$(74) \quad 1 < (c_{41} + 3) \delta_2.$$

При $\delta_2 = \frac{1}{2}(c_{41} + 3)^{-1}$ неравенство (74) противоречиво, следовательно, какое-либо из исходных предположений о величине H — неравенство (43), (52), (62) или (64) — неверно. Тогда, учитывая, что $T < P^{2g}$ и $\delta_2 = \max(\delta_1, s(M + h \ln P) \delta) = \frac{1}{2}(c_{41} + 3)^{-1}$, можем записать

$$H \leqslant \frac{1}{2} \left\{ \left(c_{42} P^{2g} (\ln |Nm_K(a)| + \right. \right. \\ \left. \left. + (\ln H_F + \ln |Nm_K(a)|)(R + h \ln P + sh \ln P) \right)^{\frac{1+\xi}{1-2\xi}} + \right. \\ \left. + (c_{43} \xi^{-1} s^3 P^{2(g+1)} (R + h \ln P)^2)^{\frac{c_{44}s}{\xi}} \right\},$$

где $0 < \xi < \frac{1}{2}$. Зная явный вид μ_i ($1 \leqslant i \leqslant n$), имеем

$$(75) \quad |\mu_i| \leqslant |\varrho_i| |\varrho_1|^{u_{1i}} \dots |\varrho_t|^{u_{ti}} |\varepsilon_1|^{v_{1i}(g-1)} \dots |\varepsilon_k|^{v_{ki}(g-1)} < \\ < (|Nm_K(a)| P^{sh} e^M H_F)^{c_{45}} (P^{sh} e^M)^{c_{46} H} = \mathcal{L}.$$

Так как $|Nm_G(\mu_i)| = |Nm_G(\mu'_i)| = \mathcal{L}^g$, где $\mu'_i = x' - \theta_i y'$, то в силу леммы 2 заключаем, что найдется такая единица $\eta \in K$, для которой

$$(76) \quad |\eta \mu'_i| \leqslant \mathcal{L} e^{c_{47} R'}$$

Из (75) и (76) следует

$$(77) \quad \max(|\eta x|, |\eta y|) < \exp \left\{ c_{48} R' (R + sh \ln P) \left((c_{42} P^{2g} (\ln |Nm_K(a)| + \right. \right. \\ \left. \left. + (\ln H_F + \ln |Nm_K(a)|)(R + h \ln P + sh \ln P) \right)^{\frac{1+\xi}{1-2\xi}} + \right. \\ \left. + (c_{43} \xi^{-1} s^3 P^{2(g+1)} (R + h \ln P)^2)^{\frac{c_{44}s}{\xi}} \right) \right\}.$$

Далее замечаем, что

$$(78) \quad \left| Nm_K \left(\prod_{i=1}^n \mu_i' \right) \right| = |Nm_K(a_0^{n-1}) \cdot Nm_K(F(x, y))| \leqslant \\ \leqslant H_F^{(n-1)m} |Nm_K(a)| p_1^{f_1 u_{12}} \cdots p_s^{f_s u_{s2}}.$$

Из (75), (76), (77) и (78) получаем оценку (7).

5. Доказательства теорем 2 и 3.

Доказательство теоремы 2. Так как $L = K(\theta)$, то

$$(79) \quad Nm_{L/Q}(x + \theta y) = N_{K/Q}(Nm_{L/K}(x + \theta y)).$$

На основании (8) и (79) можем записать, что

$$(80) \quad (Nm_{L/K}(x + \theta y)) = a \mathfrak{P}_1^{z_1} \cdots \mathfrak{P}_t^{z_t},$$

где идеал $a|A$, простые идеалы $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ входят в простые числа p_1, \dots, p_s и $t \leq s$.

Полагая $z'_l = h' z_l'' + r_l$, $0 \leq r_l < h'$ ($1 \leq l \leq t$), из (80) получаем

$$(81) \quad (Nm_{L/K}(x + \theta y)) = a' (\beta_1)^{z_1''} \cdots (\beta_t)^{z_t''},$$

где $a' = a \mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_t^{r_t}$ и $(\beta_l) = \mathfrak{P}_l^{h'}$ ($1 \leq l \leq t$). Очевидно, что идеал a' является главным, как отношение главных идеалов, т.е. $a' = (a)$. Переходя в (81) от идеалов к числам и замечая, что $Nm_{L/K}(x + \theta y) = F(x, y)$ — бинарная форма степени $n \geq 5$ с коэффициентами из Z_K и неприводимая над полем K , можем записать

$$(82) \quad F(x, y) = \tau a \beta_1^{z_1''} \cdots \beta_t^{z_t''}, \quad (x, y) \mid (a),$$

где τ — некоторая единица из поля K .

Уравнение (82) имеет тот же вид, что и (6). Следовательно, его целочисленные решения можно охарактеризовать оценкой (7). Учитывая, что $|Nm(a)| < |A| P^{c_4 s h'}$, $H_F < n! |\theta|^n$ и $\max(z_l) < c_{50} h' \max(z_l'')$ ($1 \leq l \leq s$, $1 \leq l_1 \leq t$), выводим оценку (9).

Доказательство теоремы 3. Допустим, что

$$(83) \quad (F(x, y)) = \mathfrak{P}_1^{z_1} \cdots \mathfrak{P}_s^{z_s}$$

— разложение формы $F(x, y)$ на простые идеалы в поле K . Из равенства (83) находим, что

$$(84) \quad F(x, y) = \tau a \beta_1^{z_1} \cdots \beta_s^{z_s}, \quad (x, y) = 1,$$

где $(a) = \mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_s^{r_s}$, $0 \leq r_l < h'$, и $(\beta_l) = \mathfrak{P}_l^{h'}$ ($1 \leq l \leq s$), а τ — некоторая единица из поля K .

Уравнение (84) имеет вид (6). Учитывая, что $s \leq \pi(P) < cP/\ln P$, где c — постоянная Чебышева (см. [16], стр. 850), по теореме 1 находим

для какого-либо конкретного ξ (например, $\xi = \frac{1}{4}$), что

$$N < \exp\{c_{51} P^{c_{52} P/\ln P}\},$$

откуда следует неравенство

$$\ln \ln N < c_{53} P \quad \text{при} \quad N \geq N_0$$

и оценка (10).

6. Заключение. Из оценки (7) следует, что для показателей z_1, \dots, z_s в (4) существует лишь конечное число возможностей и они могут быть явно указаны. Следовательно, анализ уравнения (4) сводится к анализу конечного числа обобщенных уравнений Туэ⁽⁶⁾, откуда выводится граница для $\max(|x|, |y|)$. Для анализа целочисленных решений обобщенного уравнения Туэ можно использовать, например, метод В. Спиринджука, изложенный в работе [14] и который применен в этой статье.

Из предыдущих рассуждений ясно, почему в теореме 1 мы оцениваем сверху $\max(|x|, |y|)$, а не $\max(|x|, |y|)$. Как уже отмечалось, это — проявление специфики уравнения (6). В связи с этим интересно отметить следующий факт: если $F(x, y)$ — бинарная форма степени не менее 5 с коэффициентами из Z_K без кратных корней, x и y принимают целые значения в Z_K , причем $|\bar{y}| \leq |\bar{x}|^{1-\varepsilon}$ (ε — фиксировано в интервале $(0, 1)$) при $|\bar{x}| \geq x_0(\varepsilon)$, то для целочисленных решений уравнения (6) с этим условием будет справедлива оценка

$$(85) \quad \ln \{\max(|x|, p_1^{u_1 f_1}, \dots, p_s^{u_s f_s})\} < \\ < c_{54} (R + sh \ln P) \left\{ (c_{55} (\ln |Nm(a)| + \ln H_F + R + sh \ln P))^{\frac{1+\xi}{1-\xi}} + \right. \\ \left. + (c_{56} \xi^{-1} \varepsilon^{-1} (s+1)^2 (R + h \ln P))^{\frac{4(sd+g+1)(1+\xi)}{\xi}} \right\},$$

где $0 < \xi < \frac{1}{2}$, выписанные параметры и величины c_{54} , c_{55} , c_{56} , имеют тот же смысл, что и в оценке (7). Оценка (85) выводится без труда из работы автора [3]. Для этого следует при получении необходимых промежуточных оценок учитывать влияние основных параметров уравнения (6) в том стиле, как это сделано в настоящей работе.

Из неравенства (22) следует, что в оценках (7) и (9) можно выразить величины R , R' , h и h' через m , d , D' и H_F , а если поле K — минимальное поле, содержащее коэффициенты $F(x, y)$, то можно и D' заменить через m , d , H_F . Таким образом получаются оценки через легко доступные параметры уравнения.

⁽⁶⁾ Обобщенным уравнением Туэ мы называем уравнение вида $F(x, y) = a$, где $F(x, y)$ — неприводимая над полем K бинарная форма с коэффициентами из Z_K , $a \in Z_K$.

Очевидно, что результаты теоремы 1, 2, 3 справедливы для бинарных форм $F(x, y)$ и алгебраических чисел θ степени $n = 4$, если они не являются „исключительными“.

Предположение о том, что (β_i) — степени различных простых идеалов, не является существенным ограничением: можно считать, что это различные идеалы, отличные от единичного, поскольку возможен переход от произвольных $(\beta_i) \neq 1$ к (β_i) , являющимся степенями различных простых идеалов.

Наконец, определение скорости возрастания $N(\mathfrak{P})$ при $N \rightarrow \infty$ для неприводимых бинарных форм $F(x, y)$ степеней $n = 3, 4$ и произвольных бинарных форм степени $n \geq 3$ с целыми алгебраическими коэффициентами, имеющих по крайней мере три различных корня, требует дополнительного исследования. В частности, срабатывает в данной ситуации схема рассуждений работы [15] и возможно получение аналогичных оценок.

Автор выражает признательность профессору В. Г. Спринджуку за полезное обсуждение содержания статьи.

Литература

- [1] А. И. Виноградов и В. Г. Спринджук, *О представлении чисел бинарными формами*, Матем. заметки 3 (4) (1968), стр. 369–376.
- [2] Э. Гекке, *Лекции по теории алгебраических чисел*, Москва–Ленинград 1940.
- [3] С. В. Котов, *О норме идеальных делителей бинарной формы с алгебраическими коэффициентами*, Изв. АН БССР. Сер. физ.-матем. наук 3 (1972), стр. 14–22.
- [4] С. В. Котов и В. Г. Спринджук, *Эффективный анализ уравнения Туэ–Малера в относительных полях*, Докл. АН БССР 17 (5) (1973), стр. 393–395.
- [5] С. Ленг, *Алгебраические числа*, Москва 1966.
- [6] В. Г. Спринджук, *К теореме Байкера о линейных формах с логарифмами*, Докл. АН БССР 11 (9) (1967), стр. 767–769.
- [7] — *Оценки линейных форм с p -адическими логарифмами алгебраических чисел*, Изв. АН БССР. Сер. физ.-матем. наук 4 (1968), стр. 5–14.
- [8] — *Эффективизация в некоторых задачах теории диофантовых приближений*, Докл. АН БССР 12 (4) (1968), стр. 293–297.
- [9] — *Новое применение p -адического анализа к представлениям чисел бинарными формами*, Изв. АН СССР. Сер. матем., 34 (1970), стр. 1038–1063.
- [10] — *Эффективная оценка рациональных приближений к алгебраическим числам*, Докл. АН БССР 14 (8) (1970), стр. 681–684.
- [11] — *Улучшение оценки рациональных приближений к алгебраическим числам*, Докл. АН БССР 15 (2) (1971), стр. 101–104.
- [12] — *О рациональных приближениях к алгебраическим числам*, Изв. АН СССР. Сер. матем., 35 (1971), стр. 991–1007.
- [13] — *Об оценке единиц алгебраических числовых полей*, Докл. АН БССР 15 (12) (1971), стр. 1065–1068.
- [14] — *Об оценке решений уравнения Туэ*, Изв. АН СССР. Сер. матем., 36 (1972), стр. 712–741.

- [15] В. Г. Спринджук, *О структуре чисел, представленных бинарными формами*, Докл. АН БССР 17 (8) (1973), стр. 685–688.
- [16] П. Л. Чебышев, *Избранные труды*, Москва 1955.
- [17] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika, 13 (1966), стр. 204–216.
— *Linear forms in the logarithms of algebraic numbers, II*, Mathematika 14 (1967), стр. 102–107.
— *Linear forms in the logarithms of algebraic numbers, III*, Mathematika 14 (1967), стр. 220–228.
— *Linear forms in the logarithms of algebraic numbers, IV*, Mathematika 15 (1968), стр. 204–216.
- [18] — *Contributions to the theory of Diophantine equations. I, On the representation of integers by binary forms*, Philos. Trans. Royal Soc., London, A 263 (1968), стр. 173–191.
- [19] — *Contributions to the theory of Diophantine equations. II, The Diophantine equation $y^2 = x^3 + k$* , Philos. Trans. Royal Soc., London, A 263 (1968), стр. 193–208.
- [20] J. Coates, *An effective p -adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), стр. 279–305.
- [21] — *An effective p -adic analogue of a theorem of Thue. II, The greatest prime factor of a binary form*, Acta Arith. 16 (1970), стр. 399–412.
- [22] K. Mahler, *Zur Approximation algebraischer Zahlen. I, Über den grössten Primteiler binärer Formen*, Math. Ann. 107 (1933), стр. 691–730.
- [23] — *Zur Approximation algebraischer Zahlen. II, Über die Anzahl der Darstellungen ganzen Zahlen durch Binärformen*, Math. Ann. 108 (1933), стр. 37–55.
- [24] — *Zur Approximation algebraischer Zahlen. III, Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen*, Acta Math. 62 (1934), стр. 91–166.
- [25] C. J. Parry, *The p -adic generalization of the Thue–Siegel theorem*, J. London Math. Soc. 15 (1940), стр. 293–305.
- [26] — *The p -adic generalization of the Thue–Siegel theorem*, Acta Math. 83 (1950), стр. 1–100.
- [27] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen, 9 (1969), стр. 71–86.

ИНСТИТУТ МАТЕМАТИКИ АН БССР

Поступило 29. 9. 1973

(466)