ACTA ARITHMETICA
XXX (1976)

Гиперэллиптическое диофантово уравнение и числа классов идеалов

В. Г. Спринджук (Минск)

1. Введение. В недавней работе [2] доказано, что свободное от квадратов ядро $A(x)$ целочисленного многочлена $f(x)$ степени n, имеющего по крайней мере три простых корня, удовлетворяет неравенству

$$|A(x)| > c_1(\log|x|)^{(2n)^{-9/3}}, \tag{1}$$

где $c_1 > 0$ — величина, эффективно определяемая через n и коэффициенты многочлена $f(x)$, $x \neq 0$ — произвольное целое, $f(x) \neq 0$. Там же показана связь задачи об усилении неравенства (1) с проблемами величины чисел классов идеалов алгебраических числовых полей. На основе подобных соображений было найдено, что некоторые арифметические конструкции дают „почти исключительно" поля алгебраических чисел с неограниченно возрастающим числом классов идеалов (такова, например, конструкция полей Анкени–Брауэра–Чоула [4]; см. [3]). Тенденция полей алгебраических чисел иметь „в основном" большое число классов обнаруживается и непосредственно, без привлечения теории диофантовых уравнений ([14], [15]).

В этой статье мы реализуем первоначальный замысел и путем существенного усиления неравенства (1) докажем, что числа классов идеалов вещественных квадратичных полей вида $Q(\sqrt{m^{2k}-1})$ неограниченно возрастают вместе с m, пробегающим все натуральные значения (см. Теорему 2).

Наш исходный результат касается границы для решений в целых рациональных числах x, y диофантова уравнения

$$f(x) = Ay^2, \tag{2}$$

где $f(x)$ — целочисленный многочлен степени n, имеющий три простых корня. Для решений этого уравнения (при $A = 1$) Бэйкер [6] получил следующую границу:

$$\max(|x|, |y|) < \exp\exp\exp\{(n^{10n}H)^{n^2}\} \tag{3}$$

где H — высота многочлена $f(x)$, т.е. наибольший по модулю его коэффициент. В работе [2] отмечалось, что предложенный там метод дает границу типа двойной экспоненты от некоторой степени H, но в самом деле аккуратное проведение указанных там рассуждений дает границу типа одной экспоненты от степени H. Интересно отметить, что это согласуется с результатами Бэйкера [5] об уравнении (2), в котором $f(x)$ — кубический многочлен, и тем самым стирается грань между методом Морделла [8] и методом Зигеля [11].

Теорема 1. *Пусть $f(x)$ — целочисленный многочлен степени n с старшим коэффициентом 1, имеющий три простых корня α, α_1 и α_2; f_α, f_{α_1} и f_{α_2} — минимальные многочлены, D_α, D_{α_1} и D_{α_2} — дискриминанты чисел α, α_1 и α_2 соответственно; $\boldsymbol{F}$ — поле алгебраических чисел $\boldsymbol{Q}(\alpha, \alpha_1, \alpha_2)$;*

$$d = [\boldsymbol{F} : \boldsymbol{Q}(\alpha)], \quad d_1 = [\boldsymbol{F} : \boldsymbol{Q}(\alpha_1)], \quad d_2 = [\boldsymbol{F} : \boldsymbol{Q}(\alpha_2)], \quad s = [\boldsymbol{F} : \boldsymbol{Q}].$$

Тогда все целочисленные решения уравнения (2) удовлетворяют неравенству

$$\max(|x|, |y|) < \exp\{c_2 |A|^{9(d+d_1+d_2)+s} B^{4+s} (\log H)^{1+s}\}, \tag{4}$$

где $\varepsilon > 0$ — произвольно, c_2 эффективно выражается через ε и n,

$$B = |R(f', f_\alpha)|^{2d} |R(f', f_{\alpha_1})|^{2d_1} |R(f', f_{\alpha_2})|^{2d_2} |D_\alpha|^{48+6d} |D_{\alpha_1}|^{48+6d_1} |D_{\alpha_2}|^{48+6d_2},$$

$R(f', f_\alpha)$, $R(f', f_{\alpha_1})$, $R(f', f_{\alpha_2})$ — результанты соответствующих многочленов.

Доказательство этой теоремы проводится по методу, описанному в работе [2], но конструкция алгебраических единиц, предложенная Зигелем [12] (лемма 3), используется более эффективно ввиду теоремы Старка [16] (лемма 6). Целесообразность такого использования конструкции Зигеля была показана Старком [17] в применении к уравнению Туэ.

Из Теоремы 1 следует, что если $f(x)$ — нормальный полином, то вместо (1) имеем

$$|A(x)| > c_3 (\log |x|)^{1/24 - \varepsilon},$$

где $\varepsilon > 0$ — произвольно, $c_3 > 0$ — величина, эффективно выражаемая через n и ε. Это неравенство позволяет получать существенно более интересные факты о полях с большим числом классов, чем (1).

Теорема 2. *Пусть $k \geqslant 2$ — натуральное число, D_m и h_m дискриминант и число классов идеалов поля $\boldsymbol{K}_m = \boldsymbol{Q}(\sqrt{m^{2k}-1})$, где $m = 1, 2, \ldots$ Тогда*

$$D_m > c_4 (\log m)^{\tau(2k)/24 - \delta(k) - \varepsilon}, \tag{5}$$

$$h_m > c_5 D_m^{\frac{1}{2} - \frac{24}{\tau(2k) - \delta_1(k)} - \varepsilon}, \tag{6}$$

где $\tau(2k)$ — число делителей $2k$, величина $c_4 > 0$ эффективно выражается через k и произвольное $\varepsilon > 0$, $c_5 > 0$ выражается через k и ε (неэффективно), $\delta_1(k) = 24\delta(k)$,

$$\delta(k) = \begin{cases} 1/12 & \text{при} \quad 2 \nmid k, \ 3 \nmid k, \\ 3/32 & \text{при} \quad 2 \mid k, \ 3 \nmid k, \\ 7/48 & \text{при} \quad 2 \mid k, \ 3 \mid k, \\ 5/48 & \text{при} \quad 2 \nmid k, \ 3 \mid k. \end{cases}$$

Неравенства (5), (6) показывают, что при k с условием $\tau(2k) \geqslant 51$, если k не делится на 6, и $\tau(2k) \geqslant 52$ при k делящемся на 6, числа классов h_m неограниченно возрастают вместе с m, причем как некоторая положительная степень D_m. То же самое верно для числа классов в роде, так как по теореме Гаусса число родов оценивается величиной $O(2^{\nu(D_m)})$, где $\nu(D_m)$ — число различных простых делителей D_m, и, следовательно, есть величина порядка $O(D_m^\varepsilon)$. Мы видим, что в последовательности полей $\boldsymbol{K}_m$ содержится лишь конечное число таких, у которых в каждом роде имеется лишь один класс.

2. Леммы. Все нижеследующие леммы, кроме леммы 7, используются лишь в доказательстве Теоремы 1.

Лемма 1. *Пусть α, β — алгебраические числа степеней n и m, высот $h(\alpha)$ и $h(\beta)$ соответственно. Тогда*

$$h(\alpha\beta) \leqslant (2mn)^m h^{(n+1)m}(\alpha) h^{(m+1)n}(\beta).$$

Доказательство см. [1], стр. 715.

Лемма 2. *Пусть $\boldsymbol{L}$ — поле алгебраических чисел конечной степени над $\boldsymbol{Q}$, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — целые идеалы в $\boldsymbol{L}$, $[\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$ — их наименьшее общее кратное, $(\mathfrak{a}_i, \mathfrak{a}_j)$ — наибольший общий делитель идеалов $\mathfrak{a}_i$, $\mathfrak{a}_j$ $(i, j = 1, 2, \ldots, n)$. Тогда*

$$\prod_{i=1}^{n} \mathfrak{a}_i \text{ делит } [\mathfrak{a}_1, \ldots, \mathfrak{a}_n] \prod_{1 \leqslant i < j \leqslant n} (\mathfrak{a}_i, \mathfrak{a}_j).$$

Доказательство. Пусть $\mathfrak{p}$ — простой идеал в $\boldsymbol{L}$, $\mathfrak{p}^{\alpha_i} \| \mathfrak{a}_i$ $(i = 1, 2, \ldots, n)$. Тогда

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}_i, \mathfrak{a}_j) = \min(\alpha_i, \alpha_j), \quad \operatorname{ord}_{\mathfrak{p}}[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] = \max_{1 \leqslant i \leqslant n} \alpha_i.$$

Для доказательства леммы достаточно получить неравенство

$$\sum_{1 \leqslant i \leqslant n} \alpha_i \leqslant \max_{1 \leqslant i \leqslant n} \alpha_i + \sum_{1 \leqslant i < j \leqslant n} \min(\alpha_i, \alpha_j). \tag{7}$$

Так как выполнение этого неравенства не зависит от нумерации чисел α_i, можно допустить, что $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_n$. Тогда

$$\sum_{1\leqslant i<j\leqslant n} \min(\alpha_i, \alpha_j) = \sum_{1\leqslant i<j\leqslant n} \alpha_i = \sum_{1\leqslant i<n} (n-i)\alpha_i,$$

и (7) очевидно.

Лемма 3. *Пусть $\boldsymbol{L}$ — как в лемме 2, r — ранг группы независимых единиц поля $\boldsymbol{L}$. В $\boldsymbol{L}$ существуют независимые единицы $\eta_1, \ldots, \eta_r$ с условием*

$$\prod_{i=1}^{r} \log|\overline{\eta_i}| < c_6 R, \tag{8}$$

где $R = R_{\boldsymbol{L}}$ — регулятор поля $\boldsymbol{L}$, c_6 выражается в явном виде через степень поля $\boldsymbol{L}$, $|\overline{\eta}|$ — максимум модулей величин, сопряженных с η.

Доказательство см. [12].

Лемма 4. *Пусть $\boldsymbol{L}$ — как в лемме 2, $l = [\boldsymbol{L} : \boldsymbol{Q}]$, $U = U_{\boldsymbol{L}}$ — группа единиц поля $\boldsymbol{L}$, порожденная единицами $\eta_1, \ldots, \eta_r$, определенными в лемме 3, $\alpha \neq 0$ — число поля $\boldsymbol{L}$. Тогда существует такая единица $\eta \in U$, что*

$$|\overline{\alpha\eta}| < N^{1/l} e^{c_7 R},$$

где $N = |\mathrm{Nm}(\alpha)|$, c_7 явно выражается через l.

Доказательство в общих чертах сходно с доказательством леммы 4.5 работы [1] и использует лемму 3.

Лемма 5. *Пусть $\boldsymbol{L}$ — как в лемме 2, $l = [\boldsymbol{L} : \boldsymbol{Q}]$, $R = R_{\boldsymbol{L}}$ — регулятор, $D = D_{\boldsymbol{L}}$ — дискриминант поля $\boldsymbol{L}$. Тогда*

$$R < c_8 |D|^{1/2} (\log |D|)^{l-1},$$

где c_8 выражается в явном виде через l.

Доказательство см. [12].

Лемма 6. *Пусть $\alpha_1, \ldots, \alpha_n$ — отличные от нуля алгебраические числа степеней не более d и высот не более $A_1, \ldots, A_n$ соответственно, где $A_i \geqslant e$ $(i = 1, 2, \ldots, n)$, $\delta > 0$ — произвольно. Если при каких-либо целых рациональных $b_1, \ldots, b_n$*

$$0 \neq |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| < e^{-\delta B}, \qquad B = \max_{1\leqslant i\leqslant n} |b_i|,$$

то при любом $\varepsilon > 0$ имеем

$$B < c_9 \Big(\prod_{i=1}^{n} \log A_i\Big)^{1+\varepsilon},$$

где c_9 эффективно выражается через n, d, δ, ε.

Доказательство см. [16], где доказано существенно более сильное утверждение.

Лемма 7. *Пусть $f_1(x), \ldots, f_s(x)$ — целочисленные многочлены, никакие два из которых не имеют общих корней, $f(x) = f_1(x) \ldots f_s(x)$. Тогда свободные от квадратов ядра $A(x), A_1(x), \ldots, A_s(x)$ чисел $f(x), f_1(x), \ldots, f_s(x)$ при любом целом x удовлетворяют неравенству*

$$|A(x)| \geqslant P^{-s} |A_1(x)| \ldots |A_s(x)|, \tag{9}$$

где

$$P = \prod_{1\leqslant i<j\leqslant s} R(f_i, f_j),$$

$R(f_i, f_j)$ — результант многочленов f_i, f_j $(i, j = 1, 2, \ldots, s)$.

Доказательство. Для любых $f_i(x)$, $f_j(x)$ существует такая пара целочисленных многочленов $A_{ij}(x)$, $B_{ij}(x)$, что

$$f_i(x) A_{ij}(x) + f_j(x) B_{ij}(x) = R(f_i, f_j).$$

Следовательно, если при каком-либо целом x простое p входит в $f_i(x)$ и $f_j(x)$, оно войдет в $R(f_i, f_j)$ и в P. Все простые p, не входящие в P, могут делить лишь одно из чисел $f_i(x)$. Если $A^*(x), A_1^*(x), \ldots, A_s^*(x)$ — части $A(x), A_1(x), \ldots, A_s(x)$ соответственно, составленные из простых p, не входящих в P, то

$$A^*(x) = A_1^*(x) \ldots A_s^*(x).$$

Но

$$|A(x)| \geqslant |A^*(x)|, \qquad |A_i^*(x)| \geqslant P^{-1} |A_i(x)|,$$

откуда следует (9).

3. Доказательство теоремы 1. В дальнейшем через $c_{10}, c_{11}, \ldots$ мы обозначаем положительные величины, не зависящие от A и коэффициентов многочлена $f(x)$ и выражаемые эффективно через n или через n и ε, что мы будем указывать записью вида $c_i = c(n)$ или $c_i = c(n, \varepsilon)$

Пусть $\boldsymbol{K} = \boldsymbol{Q}(\alpha)$. Из уравнения (2) мы видим, что справедливо разложение на идеалы в $\boldsymbol{K}$: $(x-\alpha) = \mathfrak{a}\mathfrak{b}^2$, где $\mathfrak{a} | Af'(\alpha)$. Для сопряженных идеалов $\mathfrak{a}^{(i)} | Af'(\alpha^{(i)})$. Далее,

$$(\mathfrak{a}^{(i)}, \mathfrak{a}^{(j)}) \text{ делит } (x-\alpha^{(i)}, x-\alpha^{(j)}) \text{ делит } \alpha^{(i)} - \alpha^{(j)},$$

$$\prod_{1\leqslant i<j\leqslant n} (\mathfrak{a}^{(i)}, \mathfrak{a}^{(j)}) | D_a. \tag{10}$$

Кроме того, $\mathfrak{a}^{(i)} | AR(f', f_a)$. Следовательно,

$$[\mathfrak{a}^{(1)}, \ldots, \mathfrak{a}^{(n)}] | AR(f', f_a). \tag{11}$$

В силу (10), (11) по лемме 2 находим

$$\mathfrak{a}^{(1)} \dots \mathfrak{a}^{(n)} | AR(f', f_a) D_a.$$

Поэтому

$$\mathrm{Nm}(\mathfrak{a}) \leqslant |AR(f', f_a) D_a|. \tag{12}$$

Если $\mathfrak{b}'$ — целый идеал поля $\boldsymbol{K}$, лежащий в классе, обратном классу идеала $\mathfrak{b}$ и с нормой, не превосходящей $|D_{\boldsymbol{K}}|^{1/2}$, то $\mathfrak{b}\mathfrak{b}'$ — целый главный идеал (ξ'), $x - \alpha = \gamma' \xi'^2$, где $(\gamma') = \mathfrak{a}(\mathfrak{b}')^{-2}$, $g\gamma'$ — целое, $g = \mathrm{Nm}(\mathfrak{b}')^2 \leqslant |D_{\boldsymbol{K}}|$. В силу (12)

$$|\mathrm{Nm}(\gamma')| \leqslant |AR(f', f_a) D_a|. \tag{13}$$

По лемме 4, примененной к полю $\boldsymbol{L} = \boldsymbol{K}$ и числу $\alpha = \gamma'$, в $\boldsymbol{K}$ существует единица θ, для которой

$$\overline{|\gamma' \theta|} < |\mathrm{Nm}(\gamma')|^{1/m} e^{c_{10} R_{\boldsymbol{K}}}, \tag{14}$$

где $m = [\boldsymbol{K} : \boldsymbol{Q}]$, $R_{\boldsymbol{K}}$ — регулятор поля $\boldsymbol{K}$, $c_{10} = c(n)$. Можно представить θ в виде $\theta = \theta_1 \theta_2^2$, где θ_1, $\theta_2 \in U_{\boldsymbol{K}}$, θ_1 составлена из нулевых и первых степеней базисных единиц группы $U_{\boldsymbol{K}}$. Полагая $\gamma = \gamma' \theta \theta_1^{-1}$, $\xi = \xi' \theta_2^{-1}$, находим: $x - \alpha = \gamma \xi^2$, $g\gamma$ — целое, и в силу (14) и (8)

$$\overline{|\gamma|} \leqslant \overline{|\gamma' \theta|}\, \overline{|\theta_1^{-1}|} < |\mathrm{Nm}(\gamma')|^{1/m} e^{c_{11} R_{\boldsymbol{K}}},$$

где $c_{11} = c(n)$. Так как $|R(f', f_a)| < c_{12} H^{m+n-1}$, $|D_a| < c_{13} H^{2m-2}$, и по лемме 5

$$R_{\boldsymbol{K}} < c_{14} |D_{\boldsymbol{K}}|^{1/2} (\log |D_{\boldsymbol{K}}|)^{m-1},$$

то имеем

$$\overline{|\gamma|} < c_{15} |A H^{3m+n-3}|^{1/m} \exp\{c_{16} |D_{\boldsymbol{K}}|^{1/2} (\log |D_{\boldsymbol{K}}|)^{n-1}\} \tag{15}$$

(величины $c_{12}, \dots, c_{16}$ есть $c(n)$).

Аналогично, полагая $\boldsymbol{K}_1 = \boldsymbol{Q}(\alpha_1)$, $\boldsymbol{K}_2 = \boldsymbol{Q}(\alpha_2)$, мы получим: $x - \alpha_1 = \gamma_1 \xi_1^2$, $x - \alpha_2 = \gamma_2 \xi_2^2$, где γ_1, ξ_1, γ_2, ξ_2 лежат соответственно в полях $\boldsymbol{K}_1$, $\boldsymbol{K}_2$; ξ_1 и ξ_2 — целые; $g_1\gamma_1$, $g_2\gamma_2$ — целые, $g_1 \leqslant |D_{\boldsymbol{K}_1}|$, $g_2 \leqslant |D_{\boldsymbol{K}_2}|$; для γ_1 и γ_2 выполняются неравенства, аналогичные (15).

Из полученных соотношений находим

$$\alpha_1 - \alpha = \gamma \xi^2 - \gamma_1 \xi_1^2, \quad \alpha_2 - \alpha = \gamma \xi^2 - \gamma_2 \xi_2^2, \quad \alpha_1 - \alpha_2 = \gamma_2 \xi_2^2 - \gamma_1 \xi_1^2. \tag{16}$$

Пусть $\boldsymbol{L} = \boldsymbol{Q}(\alpha, \alpha_1, \alpha_2, \sqrt{\gamma}, \sqrt{\gamma_1}, \sqrt{\gamma_2})$. Из (16) мы видим, что целые числа $\xi\sqrt{\gamma} - \xi_1\sqrt{\gamma_1}$, $\xi\sqrt{\gamma} - \xi_2\sqrt{\gamma_2}$, $\xi_2\sqrt{\gamma_2} - \xi_1\sqrt{\gamma_1}$, лежащие в $\boldsymbol{L}$, имеют абсолютные нормы, по модулю не превосходящие $c_{17} H^{3n^3}$, $c_{17} = c(n)$. Следовательно, по лемме 4, в группе единиц $U_{\boldsymbol{L}}$ найдутся такие единицы $\varepsilon_1, \varepsilon_2, \varepsilon_3$, что

$$\xi\sqrt{\gamma} - \xi_1\sqrt{\gamma_1} = \varepsilon_1 \lambda_1, \quad \xi\sqrt{\gamma} - \xi_2\sqrt{\gamma_2} = \varepsilon_2 \lambda_2, \quad \xi_2\sqrt{\gamma_2} - \xi_1\sqrt{\gamma_1} = \varepsilon_3 \lambda_3, \tag{17}$$

где λ_i — целые числа из $\boldsymbol{L}$,

$$\max(\overline{|\lambda_1|}, \overline{|\lambda_2|}, \overline{|\lambda_3|}) < (c_{17} H^{3n^3})^{1/l} e^{c_7 R}. \tag{18}$$

Из (17) получаем

$$\delta_1 \lambda_1 - \delta_2 \lambda_2 = \lambda_3, \quad \delta_1 = \varepsilon_1 \varepsilon_3^{-1}, \quad \delta_2 = \varepsilon_2 \varepsilon_3^{-1}. \tag{19}$$

Положим

$$\delta_1 = \eta_1^{x_1} \dots \eta_r^{x_r}, \quad \delta_2 = \eta_1^{y_1} \dots \eta_r^{y_r},$$

$$X = \max |x_i|, \quad Y = \max |y_i|, \quad Z = \max |x_i - y_i| \quad (i = 1, 2, \dots, r).$$

Из (19), переходя к сопряженным полям $\boldsymbol{L}^{(j)}$ $(j = 1, 2, \dots, l)$, получаем

$$\left| \frac{\lambda_1^{(j)}}{\lambda_3^{(j)}} \right| |(\eta_1^{(j)})^{x_1} \dots (\eta_r^{(j)})^{x_r}| = \left| \left(-\frac{\lambda_2^{(j)}}{\lambda_3^{(j)}} \right) (\eta_1^{(j)})^{y_1} \dots (\eta_r^{(j)})^{y_r} - 1 \right| \quad (j = 1, 2, \dots, l).$$

К правой части этого равенства мы применим лемму 6. Из неравенства (18) по лемме 1 получаем

$$\log h \left(-\frac{\lambda_2^{(j)}}{\lambda_3^{(j)}} \right) < c_{18} (R + \log H),$$

и по лемме 3

$$\log h \left(-\frac{\lambda_2^{(j)}}{\lambda_3^{(j)}} \right) \prod_{i=1}^{r} \log h(\eta_i^{(j)}) < c_{19} R (R + \log H),$$

где c_{18} и c_{19} есть $c(n)$. Следовательно, по лемме 6

$$\left| \frac{\lambda_1^{(j)}}{\lambda_3^{(j)}} \right| |(\eta_1^{(j)})^{x_1} \dots (\eta_r^{(j)})^{x_r}| \geqslant e^{-\delta Y} \quad (j = 1, 2, \dots, l) \tag{20}$$

при любом $\delta > 0$, если только

$$Y \geqslant c_{20} [R(R + \log H)]^{1+\varepsilon}, \tag{21}$$

где $\varepsilon > 0$ — произвольно, $c_{20} = c(n, \delta, \varepsilon)$. Из (18) и (20) следует

$$\sum_{i=1}^{r} x_i \log |\eta_i^{(j)}| \geqslant -\delta Y - c_{21} (R + \log H), \tag{22}$$

где $c_{21} = c(n)$.

Аналогично, из (19) находим

$$\left|\frac{\lambda_3^{(j)}}{\lambda_1^{(j)}}\right| |(\eta_1^{(j)})^{-x_1}\dots(\eta_r^{(j)})^{-x_r}| = \left|\frac{\lambda_2^{(j)}}{\lambda_1^{(j)}}(\eta_1^{(j)})^{y_1-x_1}\dots(\eta_r^{(j)})^{y_r-x_r}-1\right| \quad (j=1,2,\dots,l),$$

что при

$$Z \geqslant c_{22}[R(R+\log H)]^{1+\varepsilon} \tag{23}$$

дает

$$\sum_{i=1}^{r} x_i \log|\eta_i^{(j)}| \leqslant \delta Z + c_{23}(R+\log H), \tag{24}$$

где $c_{22}=c(n,\delta,\varepsilon)$, $c_{23}=c(n)$. Из системы неравенств (22), (24) выделяется подсистема из r „основных" неравенств, скажем, с матрицей $(\log|\eta_i^{(j)}|)_{i,j=1,2,\dots,r}$, причем в силу (8) элементы обратной матрицы по модулю не превосходят $c_{24}=c(n)$. Поэтому из (22), (24) следует

$$X \leqslant c_{25}\delta\max(Y,Z)+c_{26}(R+\log H), \tag{25}$$

где c_{25} и c_{26} есть $c(n)$, если только выполняются неравенства (21), (23).

Подобным же образом мы найдем

$$Y \leqslant c_{27}\delta\max(X,Z)+c_{28}(R+\log H), \tag{26}$$

где c_{27} и c_{28} есть $c(n)$, в предположении, что

$$X \geqslant c_{29}[R(R+\log H)]^{1+\varepsilon}, \quad c_{29}=c(n,\delta,\varepsilon). \tag{27}$$

Допустив, что неравенства (21), (23), (27) выполняются одновременно, мы находим, что (25), (26) также выполняются одновременно. Так как $Z \leqslant X+Y$, взяв $\delta=(3c_{25})^{-1}$, из (25) получаем

$$X \leqslant \tfrac{1}{2}Y+\tfrac{3}{2}c_{26}(R+\log H).$$

Аналогично, из (26) следует

$$Y \leqslant \tfrac{1}{2}X+\tfrac{3}{2}c_{28}(R+\log H),$$

что в сравнении с предыдущим дает

$$X < (c_{28}+2c_{26})(R+\log H).$$

Мы получаем противоречие с неравенством (27), следовательно, наше допущение о совместном выполнении неравенств (21), (23), (27) неверно, и мы находим

$$\min(X,Y,Z) \leqslant c_{30}[R(R+\log H)]^{1+\varepsilon}, \tag{28}$$

где $c_{30}=c(n,\varepsilon)$ с учетом того, что мы взяли $\delta=(3c_{25})^{-1}$.

Обратившись снова к (19), мы замечаем в силу (8), (18), что грубые оценки дают

$$X < c_{31}YR+c_{32}(R+\log H),$$

где c_{31} и c_{32} есть $c(n)$. Аналогичные неравенства связывают любую другую пару величин X, Y, Z. Следовательно, из (28) получаем

$$\max(X,Y) < c_{33}R[R(R+\log H)]^{1+\varepsilon},$$

где $c_{33}=c(n,\varepsilon)$. Это неравенство дает

$$\max(|\overline{\delta_1}|,|\overline{\delta_2}|) < \exp\{c_{34}R^{3+\varepsilon}(R+\log H)^{1+\varepsilon}\}, \tag{29}$$

где $c_{34}=c(n,\varepsilon)$.

Полагая $\mu_1=\delta_1\lambda_1$, $\mu_2=\delta_2\lambda_2$, из (17) находим

$$\xi\sqrt{\gamma}-\xi_1\sqrt{\gamma_1}=\mu_1\varepsilon_3, \quad \xi\sqrt{\gamma}-\xi_2\sqrt{\gamma_2}=\mu_2\varepsilon_3, \tag{30}$$

причем из (18), (29) следует

$$\max(|\overline{\mu_1}|,|\overline{\mu_2}|) < \exp\{c_{35}R^{3+\varepsilon}(R+\log H)^{1+\varepsilon}\}, \tag{31}$$

где $c_{35}=c(n,\varepsilon)$. Исключая ε_3 из соотношений (30), получаем

$$\xi_2=\sigma\xi+\tau\xi_1, \quad \sigma=\frac{(\mu_1-\mu_2)\sqrt{\gamma}}{\mu_1\sqrt{\gamma_2}}, \quad \tau=\frac{\mu_2\sqrt{\gamma_1}}{\mu_1\sqrt{\gamma_2}}. \tag{32}$$

В силу оценки (15), аналогичных оценок для $|\overline{\gamma_1}|$, $|\overline{\gamma_2}|$, и оценки (31), по лемме 1 находим, что высоты $h(\sigma)$, $h(\tau)$ чисел σ и τ удовлетворяют неравенствам

$$\max(h(\sigma),h(\tau)) < c_{36}|A|^{c_{37}}\exp\{c_{38}R^{3+\varepsilon}(R+\log H)^{1+\varepsilon}+c_{39}D_0^{1/2}(\log D_0)^{n-1}\}, \tag{33}$$

где $D_0=\max(|D_K|,|D_{K_1}|,|D_{K_2}|)$, c_{36}, c_{37}, c_{39} есть $c(n)$, $c_{38}=c(n,\varepsilon)$.

Теперь первые два из уравнений (16) имеют вид

$$\alpha_1-\alpha=\gamma\xi^2-\gamma_1\xi_1^2,$$
$$\alpha_2-\alpha=\gamma\xi^2-\gamma_1(\overline{\sigma}\xi+\overline{\tau}\xi_1)^2,$$
$$\overline{\sigma}=\sigma\sqrt{\gamma_2/\gamma_1}, \quad \overline{\tau}=\tau\sqrt{\gamma_2/\gamma_1}.$$

Исключая из этой системы ξ_1, мы получим для ξ уравнение

$$\zeta_1\xi^4+\zeta_2\xi^2+\zeta_3^2=0, \tag{34}$$

где

$$\zeta_1=4\overline{\sigma}^2\overline{\tau}^2\gamma_1\gamma-(\gamma-\overline{\tau}^2\gamma-\overline{\sigma}^2\gamma_1)^2,$$
$$\zeta_2=4\overline{\sigma}^2\overline{\tau}^2\gamma_1(\alpha-\alpha_1)+2(\gamma-\overline{\tau}^2\gamma-\overline{\sigma}^2\gamma_1)\big(\overline{\tau}^2(\alpha-\alpha_1)-\alpha+\alpha_2\big),$$
$$\zeta_3=\overline{\tau}^2(\alpha-\alpha_1)-\alpha+\alpha_2.$$

Хотя бы одно из чисел ζ_3, ζ_2 отлично от нуля, так как в противном случае $\sigma = 0$, что, в силу определения этого числа (32), влечет $\alpha_1 = \alpha_2$. Следовательно, уравнение (34) нетривиально. На основе (15), аналогичных оценок для $|\overline{\gamma_1}|, |\overline{\gamma_2}|$ и (33) получаем оценку для $|\xi|^2$, которая имеет вид, аналогичный правой части (33) с иными величинами c_{36}, c_{37}, c_{38}, c_{39}. В силу равенства $x - a = \gamma\xi^2$ и оценки (15) получаем аналогичное неравенство для $|x|$:

$$|x| < c_{40}|A|^{c_{41}} \exp\{c_{42}R^{3+\varepsilon}(R+\log H)^{1+\varepsilon} + c_{43}D_0^{1/2}(\log D_0)^{n-1}\}, \tag{35}$$

где c_{40}, c_{41}, c_{43} есть $c(n)$, $c_{42} = c(n, \varepsilon)$.

Для доказательства теоремы остается оценить сверху регулятор R поля $\boldsymbol{L}$. В силу леммы 5 достаточно оценить дискриминант $D_{\boldsymbol{L}}$. Рассматривая $\boldsymbol{L}$ как поле, получаемое из $\boldsymbol{Q}$ последовательным присоединением целых чисел $a, a_1, a_2, g\sqrt{\gamma}, g_1\sqrt{\gamma_1}, g_2\sqrt{\gamma_2}$, в силу мультипликативного свойства дифферент относительных полей мы видим, что дифферента поля $\boldsymbol{L}$ войдет делителем в произведение дифферент последовательно присоединяемых чисел. Поэтому дискриминант $D_{\boldsymbol{L}}$, как норма дифференты, войдет делителем в абсолютную норму числа

$$\Delta = f_a'(a)f_{a_1}'(a_1)f_{a_2}'(a_2)2g\sqrt{\gamma}2g_1\sqrt{\gamma_1}2g_2\sqrt{\gamma_2}.$$

Мы имеем

$$\mathrm{Nm}(\Delta) = D_a^{l/m}D_{a_1}^{l/m_1}D_{a_2}^{l/m_2}(8gg_1g_2)^l\big(\mathrm{Nm}(\gamma)\big)^{l/ma}\big(\mathrm{Nm}(\gamma_1)\big)^{l/ma_1}\big(\mathrm{Nm}(\gamma_2)\big)^{l/ma_2},$$

где $m = [\boldsymbol{K}:\boldsymbol{Q}]$, $e = [\boldsymbol{K}(\sqrt{\gamma}):\boldsymbol{K}]$, и аналогично определены m_1, m_2, e_1, e_2. В силу того, что $g \leqslant |D_{\boldsymbol{K}}|$, а $|\mathrm{Nm}(\gamma)|$ оценивается правой частью (13) и верны аналогичные неравенства для $g_1, g_2, |\mathrm{Nm}(\gamma_1)|, |\mathrm{Nm}(\gamma_2)|$, находим

$$|\mathrm{Nm}(\Delta)| \leqslant 8^l|A|^{4(d+d_1+d_2)}|D_a|^{l+12d}S^{4d}|D_{a_1}|^{l+12d_1}S_1^{4d_1}|D_{a_2}|^{l+12d_2}S_2^{4d_2},$$

где $S = |R(f', f_a)|$, аналогично определены S_1, S_2, и мы учитываем, что $|D_{\boldsymbol{K}}| \leqslant |D_a|$, аналогично для $|D_{\boldsymbol{K}_1}|, |D_{\boldsymbol{K}_2}|$. Следовательно, из неравенства $|D_{\boldsymbol{L}}| \leqslant |\mathrm{Nm}(\Delta)|$ по лемме 5 находим

$$R < c_{44}|A|^{2(d+d_1+d_2)}B(\log|A| + \log B)^{l-1},$$

где

$$B = S^{2d}S_1^{2d_1}S_2^{2d_2}|D_a|^{\frac{l}{2}+6d}|D_{a_1}|^{\frac{l}{2}+6d_1}|D_{a_2}|^{\frac{l}{2}+6d_2}.$$

Обращаясь к (35), мы видим, что

$$|x| < c_{40}\exp\{c_{45}|A|^{8(d+d_1+d_2)+\varepsilon}B^{4+\varepsilon}(\log H)^{1+\varepsilon}\},$$

чем и завершается доказательство Теоремы 1.

4. Доказательство Теоремы 2. Если $f(x)$ — целочисленный многочлен, имеющий хотя бы три простых корня, то пусть $\sigma(f) = \min(d + d_1 + d_2)$, d, d_1, d_2 определены в Теореме 1 и минимум берется по всем тройкам простых корней $f(x)$. Если $f(x)$ не имеет трех простых корней, то полагаем $\sigma^{-1}(f) = 0$. Из Теоремы 1 следует, что свободное от квадратов ядро $A(x)$ числа $f(x) \neq 0$ при целом $x \neq 0$ удовлетворяет неравенству

$$|A(x)| > c_{46}(\log|x|)^{\sigma^{-1}(f)/8-\varepsilon}, \tag{36}$$

где $c_{46} > 0$ зависит от степени и коэффициентов $f(x)$. Если $f(x) = f_1(x)\dots f_s(x)$, где $f_i(x)$ — целочисленные попарно взаимно простые многочлены, то по лемме 7 в силу неравенства (36), примененного к каждому $f_i(x)$, находим

$$|A(x)| > c_{47}(\log|x|)^{\sigma^{-1}/8-\varepsilon}, \tag{37}$$

где

$$\sigma^{-1} = \sum_{i=1}^{r}\sigma^{-1}(f_i). \tag{38}$$

Пусть $a(x)$, $b(x)$, $g(x)$ — целочисленные многочлены, связанные с $f(x)$ соотношением

$$a^2(x)f(x) - b^2(x)g(x) = \pm 1, \tag{39}$$

т.е. $g(x)$ — свободный от квадратов делитель многочлена $a^2(x)f(x) \mp 1$ в кольце целочисленных многочленов. Считаем, что $f(x)$ имеет положительный старший коэффициент и m — натуральное число, для которого $f(m) > 0$. Тогда можно считать $a(m) > 0$, $b(m) > 0$, $g(m) > 0$. Из равенства (39) замечаем, что алгебраическое число

$$\eta = a(m)\sqrt{f(m)} + b(m)\sqrt{g(m)} > 1$$

является единицей, а его квадрат есть положительная степень основной единицы ε_m вещественного квадратичного поля $\boldsymbol{K}_m = \boldsymbol{Q}(\sqrt{f(m)g(m)})$. Следовательно, $\log\varepsilon_m \leqslant c_{48}\log m$, где c_{48} явно определяется через степень и коэффициенты многочленов $a(x)$ и $f(x)$. Так как свободное от квадратов ядро числа $f(m)g(m)$ не меньше свободного от квадратов ядра $f(m)$, то в силу (37) мы видим, что дискриминант D_m поля $\boldsymbol{K}_m$ удовлетворяет неравенству

$$D_m > c_{49}(\log m)^{\sigma^{-1}/8-\varepsilon}, \tag{40}$$

где σ определено равенством (38). Следовательно,

$$\log\varepsilon_m < c_{50}D_m^{8\sigma+\varepsilon}.$$

Так как по теореме Зигеля [13]

$$h_m \log \varepsilon_m > c_{51} D_m^{1/2-\varepsilon},$$

то при $\sigma < 1/16$ получаем содержательное неравенство

$$h_m > c_{52} D_m^{1/2-8\sigma-\varepsilon}. \tag{41}$$

Оценка (40) показывает, что D_m неограниченно возрастает вместе с m.

Полагая теперь $f(x) = x^{2k}-1$, мы видим, что (38) выполняется при $a(x) = 1$, $b(x) = x^k$, $g(x) = 1$. Построим для $f(x)$ разложение на множители $f_1(x), \ldots, f_s(x)$. Имеем

$$x^{2k}-1 = \prod_{d \mid 2k} P_d(x),$$

где $P_d(x)$ — полиномы деления круга. При $d \neq 1, 2, 3, 4, 6$ степень $P_d(x)$, равная $\varphi(d)$, не меньше 4. В остальных случаях она равна 1 или 2. Поэтому необходимо учитывать делимость k на 2 и 3.

1) $2 \nmid k$, $3 \nmid k$. В качестве „основных" множителей $f_i(x)$ принимаем $P_d(x)$ при $d \neq 1, 2$. Для них величины $\sigma(P_d)$ равны 3, их число равно $\tau(2k)-2$, и мы получаем

$$\sigma^{-1} = \big(\tau(2k)-2\big)/3.$$

2) $2 \mid k$, $3 \nmid k$. Для $P_d(x)$ при $d \neq 1, 2, 4$ величина $\sigma(P_d)$ равна 3, в то время $\sigma(P_1 P_4) = 4$. Поэтому

$$\sigma^{-1} = \tfrac{1}{4} + \big(\tau(2k)-3\big)/3.$$

3) $2 \mid k$, $3 \mid k$. Для $P_d(x)$ при $d \neq 1, 2, 3, 4, 6$ находим $\sigma(P_d) = 3$, в то время как $\sigma(P_1 P_3) = \sigma(P_2 P_4) = 4$. Поэтому

$$\sigma^{-1} = \tfrac{1}{2} + \big(\tau(2k)-5\big)/3.$$

4) $2 \nmid k$, $3 \mid k$. Аналогично предыдущему $\sigma(P_d) = 3$ при $d \neq 1, 2, 3, 6$, $\sigma(P_1 P_3) = \sigma(P_2 P_6) = 4$, что дает

$$\sigma^{-1} = \tfrac{1}{2} + \big(\tau(2k)-4\big)/3.$$

Теперь ясно, что в силу неравенств (40), (41) мы получаем Теорему 2.

5. Заключение. Если нет информации о величинах $R(f', f_a)$, $D_a, \ldots$, но известен дискриминант D_f многочлена $f(x)$ и $D_f \neq 0$, то величину B в неравенстве (4) можно заменить величиной

$$B' = |D_f|^{12s+8(d+d_1+d_2)}.$$

Это следует из того, что $R(f', f_a), D_a, \ldots$ являются делителями D_f: если $f(x) = f_a(x) g(x)$, то

$$D_f = D_a D_g R^2(f_a, g),$$

$$D_f = R(f', f_a) R(f', g).$$

Аналогично исследуется уравнение вида (2), где вместо y^2 стоит y^m с фиксированным натуральным $m \geqslant 3$. Такое уравнение в некотором отношении проще (2), так как оно допускает исследование в предположении, что $f(x)$ имеет два простых корня, для которых вместо (16) получается одно уравнение

$$\alpha_1 - \alpha = \gamma \xi^m - \gamma_1 \xi_1^m$$

относительно неизвестных целых чисел ξ, ξ_1, лежащих соответственно в полях $\boldsymbol{K}$ и $\boldsymbol{K}_1$. Это уравнение анализируется теми же приемами, что и обычное уравнение Туэ, а окончательный результат подобен неравенству (4).

Не требуется никаких новых приемов, чтобы исследовать уравнение (2) в предположении, что A и коэффициенты многочлена $f(x)$ являются целыми алгебраическими числами, а решения ищутся в кольце целых чисел фиксированного поля. Граница, получаемая описанным путем для $\max(|x|, |y|)$ имеет вид, аналогичный (4). Из этого следует эффективная оценка вида

$$\max(|x|, |y|) < \exp(c_{53} H^{c_{54}})$$

для целых точек на эллиптической кривой $f(x, y) = 0$, где c_{53} и c_{54} зависит только от степени многочлена $f(x, y)$, H — его высота. Для решений этого уравнения Бэйкер и Коутес [7] получили границу вида (3) (с другими величинами вместо n^{10n} и n^2).

Из рассуждений, примененных в доказательстве Теоремы 2, видно, что представляет интерес описание класса тех целочисленных многочленов, для которых уравнение (39) разрешимо в целочисленных многочленах $a(x)$, $b(x)$ при $g(x) = 1$. Эта задача восходит, вероятно, к Абелю, а последние известные автору результаты принадлежат Шинцелю [9], [10].

В силу сделанных выше замечаний об уравнении вида (2), в котором вместо y^2 стоит y^m с целым $m \geqslant 3$, можно оценивать неравенством вида (36) свободные от кубов делители многочленов. Рассуждения, описанные в доказательстве теоремы 2, позволяют строить такие целочисленные многочлены $f(x)$ что поля $\boldsymbol{K}_m = \boldsymbol{Q}\big(\sqrt[3]{f(m)}\big)$ имеют дискриминанты и числа классов идеалов, удовлетворяющие неравенс-

твам вида (40), (41). В этом случае неравенство (41) эффективно, что следует из недавних результатов Старка [18], и можно в явном виде найти все поля K_m с любым заданным числом классов.

Цитированная литература

[1] В. Г. Спринджук, *Об оценке решений уравнения Туэ*, Изв. АН СССР, сер. матем., 36 (1972), стр. 712–741.

[2] — *Свободные от квадратов делители многочленов и числа классов идеалов алгебраических числовых полей*, Acta Arith. 24 (1973), стр. 143–149.

[3] — *Поля алгебраических чисел с большим числом классов*, Изв. АН СССР, сер. матем., 38 (1974), стр. 971–982.

[4] N. C. Ankeny, R. Brauer and S. Chowla, *A note on the class-numbers of algebraic number fields*, Amer. J. Math. 78 (1956), стр. 51–61.

[5] A. Baker, *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. 43 (1968), стр. 1–9.

[6] — *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. 65 (1969), стр. 439–444.

[7] A. Baker and J. Coates, *Integer points on curves of genus* 1, Proc. Camb. Phil. Soc.67 (1970), стр. 595–602.

[8] L. J. Mordell, *Diophantine Equations*, London and New York 1969.

[9] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1961), стр. 393–413.

[10] — *On some problems of the arithmetical theory of continued fractions II*, Acta Arith. 7 (1962), стр. 287–298.

[11] C. L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc. (1926), стр. 66–68. Ges. Abhandlungen I, стр. 207–208.

[12] — *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen 9 (1969), стр. 71–86.

[13] — *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), стр. 83–86.

[14] V. G. Sprindžuk, *The distribution of the fundamental units of real quadratic fields*, Acta Arith. 25 (1974), стр. 405–409.

[15] — *"Almost every" algebraic number-field has a large class-number*, Acta Arith. 25 (1974), стр. 411–413.

[16] H. M. Stark, *Further advances in the theory of linear forms in logarithms*, Diophantine approx. and its applic., New York and London 1973.

[17] — *Effective estimates of solutions of some diophantine equations*, Acta Arith. 24 (1973), стр. 251–259.

[18] — *Some effective cases of the Brauer–Siegel theorem*, Inventiones Math. 23 (1974), стр. 135–152.

Поступило 20. 12. 1974 (650)