ACTA ARITHMETICA
XXIV (1973)

Свободные от квадратов делители многочленов и числа классов идеалов алгебраических числовых полей

В. Г. Спринджук (Минск)

Профессору К. Л. Зигелю

1. Введение. Известная теорема Зигеля [4] утверждает конечность числа решений гиперэллиптического диофантова уравнения

$$f(x) = y^2, \tag{1}$$

где $f(x)$ — целочисленный многочлен, имеющий по крайней мере три простых корня. Следовательно, если $A(x) = A_f(x)$ — максимальный свободный от квадратов делитель[1] $f(x)$ при целом x, то $|A(x)| \to \infty$, если $|x| \to \infty$.

Рассуждения Зигеля не позволяют оценить скорость возрастания $|A(x)|$, так как они неэффективны. Недавно Бэйкер [2] установил, что рассуждения Зигеля, дополненные эффективными оценками величины решений обобщенного уравнения Туэ, позволяют получить явные границы для решений уравнения (1). На этом пути Бэйкер получил оценку:

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

где n — степень многочлена $f(x)$, H — его высота (наибольший по модулю коэффициент). Если эту оценку применить к уравнению

$$f(x) = Ay^2 \tag{3}$$

приведя его к виду $Af(x) = (Ay)^2$, то мы получим

$$|A(x)| > c_1(\log\log\log|x|)^{n-2},$$

где $c_1 > 0$ — величина, легко определяемая в явном виде и зависящая только от n и H. Эту оценку можно улучшить, заменив тройной логарифм на двойной, если применить рассуждения Бэйкера непосредственно к уравнению (3) и учесть, что $f(x)$ остается фиксированным, а изменяется A.

[1] Т.е. свободные от квадратов ядра.

В этой статье доказана

Теорема. *Наибольший свободный от квадратов делитель $A(x)$ целочисленного многочлена $f(x)$ степени $n \geqslant 3$, имеющего по крайней мере три простых корня, удовлетворяет неравенству*

$$|A(x)| > c_2(\log|x|)^{(2n)^{-9/3}}, \tag{4}$$

где $c_2 > 0$ — величина, эффективно определяемая по H и n.

Чтобы доказать теорему, мы выведем оценку сверху для решений уравнения (3) в зависимости от переменного числа A и при фиксированном многочлене $f(x)$, хотя не составляет труда учесть влияние высоты и степени многочлена на величину решений (см. 3-й раздел статьи). Применяемые нами рассуждения заметно отступают от схемы Зигеля–Бэйкера, так как мы не сводим уравнение (3) к обобщенному уравнению Туэ, а непосредственно анализируем получающиеся показательные уравнения. Таким путем достигается также улучшение оценки (2): вместо трех экспонент мы получаем две.

В третьем разделе статьи обсуждаются перспективы усиления теоремы и ее связь с проблемой величины числа классов идеалов полей алгебраических чисел.

2. Доказательство теоремы. В дальнейшем через $c_3, c_4, \ldots$ мы обозначаем положительные величины, эффективно определяемые по коэффициентам многочлена $f(x)$ и n.

Пусть α — один из простых корней $f(x)$, $\boldsymbol{K} = \boldsymbol{Q}(\alpha)$, где $\boldsymbol{Q}$ — поле рациональных чисел. Считаем, что старший коэффициент $f(x)$ равен единице, чего легко добиться.

Из уравнения (3) мы видим, что справедливо разложение на идеалы в $\boldsymbol{K}$: $(x-\alpha) = \mathfrak{a}\mathfrak{b}^2$, где $\mathfrak{a} \mid Af'(\alpha)$. Если $\mathfrak{a}'$, $\mathfrak{b}'$ — целые идеалы, лежащие в классах, противоположных $\mathfrak{a}$, $\mathfrak{b}$ соответственно и с нормами, не превосходящими $|D_{\boldsymbol{K}}|^{1/2}$, где $D_{\boldsymbol{K}}$ — дискриминант поля $\boldsymbol{K}$, то $\mathfrak{a}'(\mathfrak{b}')^2$ — главный идеал, и из равенства

$$\mathfrak{a}'(\mathfrak{b}')^2(x-\alpha) = \mathfrak{a}\mathfrak{a}'(\mathfrak{b}\mathfrak{b}')^2$$

мы видим, что $x-\alpha = \gamma\xi^2$, где γ и ξ — числа из $\boldsymbol{K}$, причем $|\mathrm{Nm}(\gamma)| \leqslant c_3|A|^n$, существует такое натуральное g, что $g\gamma$ — целое, $|g| \leqslant c_4$, ξ — целое. Умножая γ на подходящую единицу поля $\boldsymbol{K}$, добиваемся того, что можно считать

$$\overline{|\gamma|} = \max\ |\text{сопряженные с } \gamma| < c_5|A|. \tag{5}$$

Если α_1, α_2 — два других простых корня многочлена $f(x)$, то аналогично предыдущему $x-\alpha_1 = \gamma_1\xi_1^2$, $x-\alpha_2 = \gamma_2\xi_2^2$, где $\gamma_1, \xi_1, \gamma_2, \xi_2$ лежат соответственно в полях $\boldsymbol{K}_1 = \boldsymbol{Q}(\alpha_1)$, $\boldsymbol{K}_2 = \boldsymbol{Q}(\alpha_2)$ и удовлетворяют условиям: $g_1\gamma_1$, $g_2\gamma_2$ — целые, $\max(|g_1|, |g_2|) \leqslant c_6$, ξ_1, ξ_2 — целые,

$$\max(\overline{|\gamma_1|}, \overline{|\gamma_2|}) < c_7|A|. \tag{6}$$

Из полученных соотношений находим

$$\begin{gathered} a_1 - a = \gamma\xi^2 - \gamma_1\xi_1^2, \qquad a_2 - a = \gamma\xi^2 - \gamma_2\xi_2^2, \\ a_1 - a_2 = \gamma_2\xi_2^2 - \gamma_1\xi_1^2. \end{gathered} \tag{7}$$

Пусть теперь $\boldsymbol{L}$ — поле алгебраических чисел, содержащее числа $a, a_1, a_2, \sqrt{\gamma}, \sqrt{\gamma_1}, \sqrt{\gamma_2}$ и степень которого ограничена величиной c_8. Из работы Зигеля [5] следует, что в поле $\boldsymbol{L}$ существует система независимых единиц $\eta_i\ (i = 1, 2, \ldots, k)$ с условием: все элементы матрицы

$$(\log|\eta_i^{(j)}|)_{i,j=1,2,\ldots,k}$$

по абсолютной величине не превосходят c_9R, где R — регулятор поля $\boldsymbol{L}$; элементы обратной матрицы не превосходят c_{10}. Кроме того, справедливо неравенство Ландау

$$R < c_{11}|D_{\boldsymbol{L}}|^{1/2}(\log|D_{\boldsymbol{L}}|)^{m-1} \tag{8}$$

где $D_{\boldsymbol{L}}$ — дискриминант поля $\boldsymbol{L}$, m — его степень.

Из (7) мы видим, что числа $\xi\sqrt{\gamma} - \xi_1\sqrt{\gamma_1}$, $\xi\sqrt{\gamma} - \xi_2\sqrt{\gamma_2}$, $\xi_2\sqrt{\gamma_2} - \xi_1\sqrt{\gamma_1}$ лежат в поле $\boldsymbol{L}$, а их нормы равны фиксированным числам. Следовательно, используя указанные выше единицы, находим

$$\xi\sqrt{\gamma} - \xi_1\sqrt{\gamma_1} = \varepsilon_1\lambda_1, \quad \xi\sqrt{\gamma} - \xi_2\sqrt{\gamma_2} = \varepsilon_2\lambda_2, \quad \xi_2\sqrt{\gamma_2} - \xi_1\sqrt{\gamma_1} = \varepsilon_3\lambda_3, \tag{9}$$

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

$$\max(\overline{|\lambda_1|}, \overline{|\lambda_2|}, \overline{|\lambda_3|}) < c_{12}\exp(c_{13}R) \tag{10}$$

(детали см. [6], лемма 4.5).

Из (9) получаем

$$\delta_1\lambda_1 - \delta_2\lambda_2 = \lambda_3, \quad \delta_1 = \varepsilon_1\varepsilon_3^{-1}, \quad \delta_2 = \varepsilon_2\varepsilon_3^{-1}. \tag{11}$$

Положим

$$\delta_1 = \eta_1^{x_1}\ldots\eta_k^{x_k}, \quad \delta_2 = \eta_1^{y_1}\ldots\eta_k^{y_k},$$

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

Из (11), переходя к сопряженным величинам, получаем

$$\frac{|\lambda_1^{(j)}|}{|\lambda_3^{(j)}|}|(\eta_1^{(j)})^{x_1}\ldots(\eta_k^{(j)})^{x_k}| = \left|\left(-\frac{\lambda_2^{(j)}}{\lambda_3^{(j)}}\right)(\eta_1^{(j)})^{y_1}\ldots(\eta_k^{(j)})^{y_k} - 1\right| \quad (j = 1, 2, \ldots, k).$$

К правой части этого равенства можно применить оценку Бэйкера [3], и мы получим число, не меньшее $e^{-\delta Y}$, если только $Y > c_{14}(\delta^{-1}R)^{\nu}$, $\nu = (2k+3)^2$, где δ — любое вещественное число из интервала $0 < \delta \leqslant 1$.

Это показывает, что тогда, в силу (10),

$$\sum_{i=1}^{k} x_i \log|\eta_i^{(j)}| > -\delta Y - c_{15}R \quad (j = 1, 2, \ldots, k). \tag{12}$$

Аналогично, из (11) находим

$$\frac{|\lambda_3^{(j)}|}{|\lambda_1^{(j)}|}|(\eta_1^{(j)})^{-x_1} \ldots (\eta_k^{(j)})^{-x_k}| = \left|\left(\frac{\lambda_2^{(j)}}{\lambda_1^{(j)}}\right)(\eta_1^{(j)})^{y_1-x_1} \ldots (\eta_k^{(j)})^{y_k-x_k} - 1\right| \quad (j = 1, 2, \ldots, k),$$

что при $Z > c_{16}(\delta^{-1}R)^{\nu}$ дает

$$\sum_{i=1}^{k} x_i \log|\eta_i^{(j)}| < \delta Z + c_{17}R \quad (j = 1, 2, \ldots, k). \tag{13}$$

Из неравенств (12) и (13) следует $X < c_{19}\,\delta \max(Y, Z)$, откуда получаем $X \leqslant \frac{1}{2}Y$, полагая $\delta = (3c_{19})^{-1}$.

Подобным же образом мы найдем $Y \leqslant \frac{1}{2}X$ в предположении, что $X > c_{20}R^{\nu}$. Мы должны заключить из этого, что хотя бы одно из трех чисел X, Y, Z должно оцениваться сверху величиной $c_{21}R^{\nu}$. Но из уравнения (11) мы видим, что эти числа с точностью до множителя R — одного порядка. Поэтому

$$\max(X, Y) < c_{22}R^{\nu+1},$$

откуда получаем

$$\max\left(\left|\overline{\delta_1}\right|, \left|\overline{\delta_2}\right|\right) < \exp(c_{23}R^{\nu+2}). \tag{14}$$

Полагая $\mu_1 = \delta_1\lambda_1$, $\mu_2 = \delta_2\lambda_2$, из (9) находим

$$\xi\sqrt{\gamma} - \xi_1\sqrt{\gamma_1} = \mu_1\varepsilon_3, \qquad \xi\sqrt{\gamma} - \xi_2\sqrt{\gamma_2} = \mu_2\varepsilon_3, \tag{15}$$

причем из (10), (14) следует

$$\max\left(\left|\overline{\mu_1}\right|, \left|\overline{\mu_2}\right|\right) < c_{12}\exp(c_{24}R^{\nu+2}). \tag{16}$$

Исключая ε_3 из соотношения (15), получаем

$$\xi_2 = \sigma\xi + \tau\xi_1, \quad \sigma = \frac{\mu_1 - \mu_2}{\mu_1\sqrt{\gamma_2}}, \quad \tau = \frac{\mu_2\sqrt{\gamma_1}}{\mu_1\sqrt{\gamma_2}}. \tag{17}$$

В силу оценок (5), (6), (16) высоты $h(\sigma)$, $h(\tau)$ чисел σ и τ удовлетворяют неравенствам

$$\max\left(h(\sigma), h(\tau)\right) < |A|^{c_{25}}\exp(c_{26}R^{\nu+2}). \tag{18}$$

Теперь первые два из уравнений (7) имеют вид:

$$a_1 - a = \gamma\xi^2 - \gamma_1\xi_1^2,$$
$$a_2 - a = \gamma\xi^2 - \gamma_1(\sigma\xi + \tau\xi_1)^2.$$

Исключая из этой системы ξ_1, мы получим для ξ уравнение

$$\zeta_1\xi^4 + \zeta_2\xi^2 + \zeta_3^2 = 0, \tag{19}$$

где

$$\zeta_1 = 4\sigma^2\tau^2\gamma_1\gamma - (\gamma - \tau^2\gamma - \sigma^2\gamma_1)^2,$$
$$\zeta_2 = 4\sigma^2\tau^2\gamma_1(a - a_1) + 2(\gamma - \tau^2\gamma - \sigma^2\gamma_1)\left(\tau^2(a - a_1) - a + a_2\right),$$
$$\zeta_3 = \tau^2(a - a_1) - a + a_2.$$

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 (17), влечет $a_1 = a_2$. Следовательно, уравнение (19) нетривиально. На основе (5), (6), (18) получаем оценку для $|\xi|$, из которой выводим

$$|x| < |A|^{c_{27}}\exp(c_{28}R^{\nu+2}). \tag{20}$$

Для доказательства теоремы остается оценить R через A. Будем считать, что $\boldsymbol{L} = \boldsymbol{L}_0$, где

$$\boldsymbol{L}_0 = \boldsymbol{Q}(a, a_1, a_2, \sqrt{\gamma}, \sqrt{\gamma_1}, \sqrt{\gamma_2}).$$

В силу (8) достаточно оценить $|D_{\boldsymbol{L}_0}|$ через $|A|$. Для этого заметим, что дифферента поля $\boldsymbol{L}_0$ делит число

$$f'(a)f'(a_1)f'(a_2)2g\sqrt{\gamma}2g_1\sqrt{\gamma_1}2g_2\sqrt{\gamma_2},$$

а дискриминант, как норма дифференты, делит норму этого числа. Следовательно, в силу (5), (6),

$$|D_{\boldsymbol{L}_0}| < c_{29}|A|^{12n(n-1)(n-2)}.$$

Теперь из (8) получаем

$$R^{\nu+2} < c_{30}|A|^{3(2n)^9},$$

так как $k < 8n(n-1)(n-2)$, и оценка (20) принимает вид

$$|x| < \exp(c_{31}|A|^{3(2n)^9}), \tag{21}$$

что соответствует неравенству (4).

3. Обсуждение. Показатель степени $3(2n)^9$ в оценке (21) можно уменьшить, применив вместо теоремы Бэйкера [3] о линейной форме от логарифмов алгебраических чисел новые результаты [6]. Однако добиться таким путем существенного усиления неравенства (21), повидимому, нельзя. Существенным усилением была бы оценка

$$|x| < \exp(c_{32}|A|^{\varepsilon}), \tag{22}$$

где $\varepsilon > 0$ — сколь угодно малое число (c_{32} зависит от ε). Это неравенство следовало бы из (20), если бы мы знали, что над $\boldsymbol{L}_0$ существует поле $\boldsymbol{L}$ с условием $R < c_{33}|D_{\boldsymbol{L}_0}|^{\varepsilon}$ и, как мы предполагали ранее, $[\boldsymbol{L}:\boldsymbol{Q}] \leqslant c_8$. Однако мы не знаем, существует ли такое надполе.

Интересно заметить, что оценка (22) сама приводит к некоторым утверждениям о полях с „малыми" регуляторами. Возьмем, например, $f(x) = x^4 - 1$. Тогда уравнение (3) равносильно $x^4 - Ay^2 = 1$, и мы видим, что основная единица η поля $Q(\sqrt{A})$ удовлетворяет неравенству $\log \eta < c_{34} A^{\varepsilon}$.

Более глубокий пример связан с работой Анкени, Брауэра и Чоула [1]. Они доказали, в частности, что если $a_1, a_2, \ldots, a_{n-1}$ — произвольные различные целые числа, $n \geqslant 3$, то для бесконечного множества натуральных чисел N многочлены

$$g_N(x) = (x-a_1)(x-a_2)\ldots(x-a_{n-1})(x-N)+1$$

генерируют поля алгебраических чисел с условием $R < c_{35}|D|^{\varepsilon}$. Из оценки (22) следует, что *все* многочлены $g_N(x)$ обладают этим свойством. Действительно, дискриминант D поля G_N, порожденного корнем многочлена $g_N(x)$, отличается от дискриминанта $d(N)$ многочлена $g_N(x)$ квадратом целого рационального числа, т.е. $d(N) = Dy^2$. Очевидно, $d(N)$ — многочлен от N степени $2n-2$. Можно доказать что этот многочлен имеет только простые корни. Поэтому из (22) получаем: $\log N < c_{36}|D|^{\varepsilon}$. В работе [1] доказано, что $R < c_{37}(\log N)^{n-1}$. Следовательно, при любом N имеем $R < c_{35}|D|^{\varepsilon}$, и мы видим, что все поля G_N имеют „малый" регулятор.

Конечно, вместо полей с „малыми" регуляторами можно говорить о полях с „большими" числами классов (формула Зигеля–Брауэра), хотя при этом мы рискуем потерять эффективность выводов.

Нетрудно оценить влияние высоты многочлена H на величину c_{31} в неравенстве (21), или, что почти то же самое, на величину c_2 в (4). Просматривая оценки через H величин $c_3, c_4, \ldots$, мы видим, что прежде всего влияние H сильно сказывается на c_5 и c_7, которые оцениваются как

$$\exp\{c_{38}(H\log H)^{n-1}\},$$

где c_{38} зависит только от n. Это приводит к тому, что $c_{26}, c_{28}, c_{29}, c_{30}, c_{31}$ оцениваются аналогичной величиной, а неравенство (21) принимает вид

$$|x| < \exp\left\{|A|^{3(2n)^9} \exp\left(c_{39}(H\log H)^{n-1}\right)\right\},$$

где c_{39} зависит только от n. В частности, для уравнения (1) мы получаем

$$\max(|x|, |y|) < \exp\exp\{c_{39}(H\log H)^{n-1}\}$$

вместо (2). Если бы поля K, K_1, K_2 можно было погрузить в поле с „малым" регулятором, подобно погружению L_0 в L, как мы обсуждали выше, то последнюю оценку можно было бы улучшить, заменив ее на $\exp\exp(c_{40}H^{\varepsilon})$.

Мы видим, таким образом, что весьма полезным было бы решение (в положительном смысле) следующей проблемы:

Всякое поле алгебраических чисел K степени $n \geqslant 2$ можно погрузить в такое поле алгебраических чисел L, что $[L:K] < c(n)$, $R_L < c(n,\varepsilon)|D_K|^{\varepsilon}$, где $\varepsilon > 0$ — произвольное число, $c(n)$ зависит только от n, $c(n,\varepsilon)$ зависит только от n и ε (R_L — регулятор L, D_K — дискриминант K).

Двойственная формулировка этой проблемы в силу теоремы Зигеля–Брауэра требует, чтобы вместо условия на R_L число классов h_L поля L удовлетворяло неравенству $h_L > c(n,\varepsilon)|D_L|^{1/2-\varepsilon}$ и чтобы отношение логарифмов величин $|D_L|$ и $|D_K|$ было ограничено величиной, зависящей только от n.

В качестве следствия из теоремы и проведенного обсуждения перспектив доказательства оценки (22) отметим следующий факт:

Если хотя бы для одного многочлена $f(x)$, удовлетворяющего предпосылкам теоремы, существует бесконечное число решений неравенства $|A(x)| < (\log|x|)^B$, где B не зависит от x, то существует бесконечное множество полей алгебраических чисел L степени не более $8n^3$, числа классов идеалов которых h_L удовлетворяют неравенству $h_L < |D_L|^{1/2-\delta}$, где $\delta = (6B(2n)^9)^{-1}$.

Мы видим, что если теорема допускает существенное усиление, т.е. если верна оценка (22), то наличие полей алгебраических чисел с „большим" числом классов — стандартное явление. Если же принципиальное усиление теоремы невозможно, то тогда бесконечно часто встречаются поля с „относительно малым" числом классов.

Конечно, вместо свободных от квадратов делителей многочленов можно рассматривать аналогичным образом свободные от кубов делители, и вообще делители, свободные от m-х степеней, где $m \geqslant 2$ — фиксированное натуральное число. Получаемые результаты вполне аналогичны.

Цитированная литература

[1] 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.

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

[3] — *Linear forms in the logarithms of algebraic numbers (IV)*, Mathematika 15 (1968), стр. 204–216.

[4] 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.

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

[6] В. Г. Спринджук, *Об оценке решений уравнения Туэ*, Известия АН СССР, сер. матем., 36, № 4 (1972), стр. 712–741.

Получено 22. 8. 1972