ACTA ARITHMETICA
LVII (1991)

Локальные оценки в проблеме Лемера

Ф. Ф. Желудевич (Минск)

Памяти профессора В. Г. Спринджука

1. Введение. В недавние годы в связи с многочисленными приложениями получила широкую известность проблема оценки снизу мультипликативной высоты $M(\alpha)$ целого алгебраического α

$$M(\alpha) = \prod_{i=1}^{n} \max(1, |\alpha_i|),$$

где α_i — сопряженные с α комплексные числа ($i = 1, 2, \ldots, n$).

На основе анализа множества численных примеров Лемер [9] поставил вопрос, разве если $M(\alpha) \neq 1$, то $\ln M(\alpha) \geqslant C > 0$, где C — абсолютная постоянная. Классическая теорема Кронекера [6] утверждает, что $\ln M(\alpha) > 0$, если $M(\alpha) \neq 1$. Этот результат уточняется оценками вида $\ln M(\alpha) \geqslant c(n)$, где $c(n)$ обозначает явную функцию > 0. В частности принципиальное улучшение получил Добровольский, который доказал [4], что при условии $M(\alpha) \neq 1$ можно взять $c(n) = (1-\varepsilon)(\ln\ln n/\ln n)^3$, где $n \geqslant n_0(\varepsilon)$, $\varepsilon > 0$ — произвольное. Наиболее точные значения величины $c(n)$ были получены в работах [3], [10], [12].

Известны также оценки вида $\ln M(\alpha) \geqslant c(k)$, зависящие от числа k ненулевых коэффициентов определяющего α полинома $g(x)$. Например, в работе [5] при условии $M(\alpha) \neq 1$ установлено, что можно взять $c(k) = (\ln(2e)/2e)\cdot(k+1)^{-k}$.

Подобного рода результаты находят применение в таких, например, вопросах, как мультипликативная зависимость в числовых полях [11], оценка числа неизоморфных алгебраических полей фиксированной степени и ограниченного регулятора [13] и ряде других.

Наша работа касается вопроса получения оценок вида $\ln M(\alpha) \geqslant c(p, n)$ в зависимости от характера разложения в кольце целых $\boldsymbol{Z}_{\boldsymbol{K}}$ поля $\boldsymbol{K} = \boldsymbol{Q}(\alpha)$ простого рационального числа p. При этом мы будем стремиться получать наиболее точную зависимость от p значений $c(p, n)$. Такого рода оценки, на наш взгляд, могут найти применение в задаче о погружении любого поля алгебраических чисел в поле с малым регулятором [13, стр. 237], если дополнительно привлечь результаты по эффективизации теоремы плотности Артина–Чеботарева [7].

Заметим, что первые значения константы $c(p, n)$ получены уже в работе [2]:

если простое $p \nmid \Delta_K$, Δ_K — дискриминант поля $\boldsymbol{K}$ и для простых идеалов $\mathfrak{p} | p$ из кольца $\boldsymbol{Z}_K$ с нормой $N(\mathfrak{p}) = p^{f_\mathfrak{p}}$ число $f = \text{НОК}\{f_\mathfrak{p}\}$, то $M(\alpha) \neq 1$ влечет, что $c(p, n) = n \ln(p/2)/(p^f - 1)$.

Наш подход базируется на p-адическом методе арифметико-аналитического продолжения Гельфонда–Шнейдера.

В этой работе доказана

Теорема. *Если простое* $p \nmid \Delta_K$ *и число идеалов* $\mathfrak{p}$ *из кольца* $\boldsymbol{Z}_K$

$$|\{\mathfrak{p} | p\colon f_\mathfrak{p} = 1\}| = r = c \cdot n, \qquad 0 < c \leqslant 1, \ c \text{ не зависит от } n,$$

то $M(\alpha) \neq 1$ *влечет, что*

$$c(p, n) = p^{-2(1+\varepsilon)}(\ln n \cdot (\ln \ln n)^\varepsilon)^{-1},$$

иными словами имеет место оценка

$$\ln M(\alpha) \geqslant p^{-2(1+\varepsilon)}(\ln n \cdot (\ln \ln n)^\varepsilon)^{-1} \tag{1}$$

при $n \geqslant n_1(\varepsilon)$, $\varepsilon > 0$ — *произвольное*.

Заметим, что по теореме плотности Артина–Чеботарева существует бесконечное число простых p, удовлетворяющих условию теоремы. При этом известны оценки [7] для наименьшего такого p через Δ_L — дискриминант поля $\boldsymbol{L}$, где $\boldsymbol{L}$ — расширение Галуа поля $\boldsymbol{K}$.

Существенный момент доказательства теоремы состоит в том, что можно, как и в [8], построить систему вспомогательных сопряженных и одновременно маленьких функций.

2. Доказательство теоремы. Пусть Ω_p — пополнение по норме $|\ |_p$ алгебраического замыкания поля p-адических чисел $\boldsymbol{Q}_p$, где p — простое натуральное число, удовлетворяющее условию теоремы.

Пусть также $\varepsilon > 0$ — произвольное, $\delta = \varepsilon/5$, $S = [(\ln \ln n)^\delta]$, $m = [\ln n]$, $N = 6nmS^2$.

Используя „принцип ящиков" Дирихле, можно построить регулярную функцию $f\colon \Omega_p \to \Omega_p$ вида

$$0 \not\equiv f(z) = \sum_{k=1}^{N} a_k (\alpha^{p-1})^{kz}, \tag{2}$$

имеющую целые рациональные коэффициенты a_k с условием $|a_k| \leqslant N$ $(k = 1, 2, \ldots, N)$ и удовлетворяющую системе сравнений

$$(\ln \alpha)^{-s} f^{(s)}(jp) \equiv 0 \ (\mathrm{mod}\, \mathfrak{q}^g) \qquad (j = 0, 1, \ldots, m-1;\ s = 0, 1, \ldots, S), \tag{3}$$

где $\mathfrak{q}$ — простой идеал кольца $\boldsymbol{Z}_K$, причем

(4) $$N(\mathfrak{q}^g)^{m(S+1)} < (N+1)^N \leqslant N(\mathfrak{q}^{g+1})^{m(S+1)}, \quad \ln N(\mathfrak{q}) \leqslant n,$$

$N(\mathfrak{q})$ — число классов вычетов по модулю $\mathfrak{q}$, g — натуральное число.

Если среди чисел ряда (3) есть хотя бы одно, скажем; $\theta_j^{(s)} = (\ln\alpha)^{-s}\cdot f^{(s)}(jp)$, отличное от нуля, то заметим, что $\theta_j^{(s)} \in \boldsymbol{Z}_K$ а по формуле произведения [1, стр. 311] из (3) следует

(5) $$|Nm_{K/Q}\theta_j^{(s)}|\cdot N(\mathfrak{q}^g)^{-1} \geqslant 1.$$

С учетом (4) из (5) получаем, что

(6) $$\ln M(\alpha) \geqslant \frac{N-4nmS^2}{2Np^2m^2S}\ln N - \frac{n}{Np^2m} > (8p^2mS)^{-1}.$$

А из (6), в силу наших обозначений, следует требуемая оценка (1).

Пусть теперь

(7) $$f^{(s)}(jp) = 0 \quad (j = 0, 1, \ldots, m-1;\ s = 0, 1, \ldots, S).$$

По теореме Куммера [14, стр. 83] сравнение $g(x) \equiv 0 \pmod p$ имеет r решений и, используя вариант леммы Гензеля [1, стр. 305] получаем, что полином $g(x)$ имеет r целых радических нулей, скажем, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$. Тогда, в силу малой теоремы Ферма

(8) $$\alpha_i^{p-1} \equiv 1 \pmod p \quad (i = 1, 2, \ldots, r).$$

Теперь, с учетом сопряжений по α, из (7) получаем

(9) $$f_i^{(s)}(jp) = 0 \quad (i = 1,2, \ldots, r;\ j = 0, 1, \ldots, m-1;\ s = 0, 1, \ldots, S),$$

где

$$f_i(z) = \sum_{k=1}^{N} a_k(\alpha_i^{p-1})^{kz}, \quad (\alpha_i^{p-1})^{kz} = \exp(kz\ln(\alpha_i^{p-1})).$$

Заметим, что функция $f_i(z)$, $1 \leqslant i \leqslant r$, как линейная комбинация функций α_i^{kz} $(k = 1, 2, \ldots, N)$ регулярна в круге $|z|_p \leqslant R_i$, где $R_i > 1$. Действительно, функции $\alpha_i^{kz} = \exp(kz\ln\alpha_i)$ регулярны в круге

$$|z|_p \leqslant p^{-1/(p-1)}|\ln\alpha_i|_p^{-1} = p^{-1/(p-1)}|\alpha_i - 1|_p^{-1} = R_i > 1,$$

что следует из (8) и очевидного неравенства $|k|_p \leqslant 1$.

Далее мы воспользуемся одним вспомогательным утверждением, доказанным в книге [13, стр. 46].

Лемма 1. *Пусть* $z_1, \ldots, z_{m-1}$, T, $R \in \Omega_p$, $T \neq 0$, $R \neq 0$, $\varrho > 0$ — *вещественное число,* $|T|_p < |z_i|_p < |R|_p < \varrho$, $|z_i - z_j|_p > |T|_p$ $(i \neq j;\ i, j = 1, 2, \ldots, m-1)$, $f(z)$—*регулярная в круге* $|z|_p < \varrho$ *функция,* $S \geqslant 0$—*целое,*

$$F(z) = [z(z-z_1)\ldots(z-z_{m-1})]^{S+1}.$$

Тогда для любого $z \in \Omega_p$ *с условием*

$$|z - z_i|_p > |T|_p \qquad (i = 1, 2, \ldots, m-1)$$

имеем $(z_0 = 0)$

$$f(z) = \int\limits_{0,R} \frac{F(z)}{F(\theta)} \cdot \frac{f(\theta)\theta}{\theta - z} d\theta - \sum_{k=0}^{S} \sum_{l=0}^{m-1} \frac{f^{(k)}(z_l)}{k!} \int\limits_{z_l,T} \frac{F(z)}{F(\theta)} \cdot \frac{(\theta - z_l)^{k+1}}{\theta - z} d\theta.$$

В правой части последнего равенства интегрирование ведется по Шнирельману.

В условиях леммы 1 положим

$$F(z) = \left[z(z-p)(z-2p)\ldots(z-(m-1)p)\right]^{S+1}, \qquad R = 1$$

и возьмем $T \in \Omega_p$ с условием

$$(2pm_1)^{-1} < |T|_p < (pm_1)^{-1},$$

где $m_1 = (p^2 \ln\ln n)^{\delta} \cdot \ln p \cdot \ln n$. Тогда для $z = jp$ $(m \leqslant j < m_1)$, с учетом (9), получаем

$$f_i(z) = \int\limits_{0,1} \frac{F(z)}{F(\theta)} \cdot \frac{f_i(\theta)\theta}{\theta - z} d\theta \qquad (i = 1, 2, \ldots, r).$$

Очевидно, в силу (8), что $|f_i(\theta)|_p \leqslant 1$ для $|\theta|_p \leqslant 1$ $(i = 1, 2, \ldots, r)$. По принципу максимума модуля

$$(10) \qquad |f_i(jp)|_p = \left| \int\limits_{0,1} \frac{F(jp)}{F(\theta)} \cdot \frac{f_i(\theta)\theta}{\theta - jp} d\theta \right|_p \leqslant \max \frac{|F(jp)|_p}{|F(\theta)|_p} \cdot \frac{|f_i(\theta)|_p |\theta|_p}{|\theta - jp|_p}$$
$$\leqslant |F(jp)|_p \leqslant p^{-(S+1)m} \qquad (i = 1, 2, \ldots, r),$$

если учесть, что из $|\theta|_p = 1$ следует, что $|\theta - jp|_p = 1$, $|F(\theta)|_p = 1$.

Предположим теперь, что $f(jp) \neq 0$ для какого-то j в интервале $m \leqslant j < m_1$. Тогда, учитывая (10) получаем

$$1 \leqslant |Nm_{K/Q} f(jp)| \, |Nm_{K/Q} f(jp)|_p = \prod_{i=1}^{n} |f_i(jp)| \cdot |f_i(jp)|_p$$
$$\leqslant \exp\left(Nm_1 p^2 \ln M(\alpha) - Smr \ln p\right).$$

Отсюда следует, что

$$(11) \qquad \ln M(\alpha) \geqslant \frac{Smr \ln p}{Nm_1 p^2},$$

что дает, в силу обозначений, неравенство (1).

Предположим теперь противное: пусть $f(jp) = 0$ для всех j: $m \leqslant j < m_1$. Тогда, вместе с (7), это дает систему равенств

$$(12) \qquad f(0) = f(p) = f(2p) = \ldots = f([m_1]p) = 0.$$

Полагая далее

$$m = [(p^2 \ln\ln n)^\delta \cdot \ln p \cdot \ln n], \qquad m_1 = (p^2 \ln\ln n)^{2\delta} \cdot \ln p \cdot \ln n,$$

мы, как и выше, получим (1) или (12). Пусть $\delta = 1/\Delta$, где Δ — большое натуральное число, тогда за $\Delta+4$ шага мы получим (1) или систему уравнений

$$(13) \qquad f(jp) = \sum_{k=1}^{N} a_k(\alpha^{p(p-1)})^{jk} = 0 \qquad (j = 0, 1, \ldots, m-1),$$

где уже $m = [(p^2 \ln\ln n)^{1+4\delta} \cdot \ln p \cdot \ln n]$.

Воспользуемся, наконец, двумя утверждениями, доказанными в статье Добровольского [4].

Лемма 2. *Пусть* α — *алгебраическое число,* $\deg\alpha = n$. *Тогда множество*

$$P = \{q \text{ — простое}, \deg(\alpha^q) < n\}$$

имеет мощность

$$|P| \leqslant \ln n/\ln 2.$$

Лемма 3. *Если для чисел* α_1 *и* α_2, *сопряженных с* α, *выполняется равенство* $\alpha_1^k = \alpha_2^l$ *с целыми* $k \neq l$, *то* α — *корень из единицы*: $M(\alpha) = 1$.

Введем обозначения: $\beta = \alpha^{p(p-1)}$, $\deg\beta = n_p$, β_i $(i = 1, 2, \ldots, n_p)$ — сопряженные с $\beta = \beta_1$ числа.

По лемме 2 число простых чисел $j = q$, для которых $\deg(\beta^q) < n_p$, не превосходит $\ln n_p/\ln 2 \leqslant \ln n/\ln 2$, так как $n/p^2 < n_p \leqslant n$. По неравенству Чебышева $\pi(x) \gg x/\ln x$ при $x \geqslant x_0$, поэтому от системы уравнений (13) мы можем перейти, с учетом сопряжений по β, к системе

$$(14) \qquad \sum_{k=1}^{N} a_k(\beta_i^q)^k = 0 \qquad (i = 1, 2, \ldots, n_p;\ q \in Q_1 = Q \backslash P,\ |Q_1| = N/n_p),$$

где P — множество из леммы 2.

Система (14) — это система с определителем Вандермонда, который, согласно леммам 2 и 3, отличен от нуля. Отсюда следует, что $a_1 = a_2 = \ldots = a_N = 0$. Мы получили противоречие, тем самым теорема доказана.

В заключение заметим, что для больших значений p, а именно при $p > 2^{n/r}$, по формуле произведения для целого $\prod_{i=1}^{n}(\alpha_i^{p-1} - 1) \neq 0$ в силу (8), получаем оценку $\ln M(\alpha) > (r \ln p - n \ln 2)/(p-1)$, что сильнее, чем (1).

Литература

[1] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Наука, Москва 1985.
[2] Th. Callachan, W. Newman and M. Sheingorn, *Fields with large Kronecker constants*, J. Number Theory 9 (1977), 182–186.

[3] D. Cantor and E. G. Straus, *On a question of D. H. Lehmer*, Acta Arith. 42 (1982), 97–100; Correction, ibid. 325.

[4] E. Dobrowolski, *On a question of D. H. Lehmer and the number of irreducible factors of a polynomial*, ibid. 34 (1979), 391–401.

[5] — *On a question of Lehmer*, Mém. Soc. Math. France 2 (1980), 35–39.

[6] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), 173–175.

[7] J. C. Lagarias, H. L. Montgomery, A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. 54 (1979), 271–296.

[8] M. Laurent, *Sur la mesure de Mahler de certaines d'entiers algébriques*, C. r. a. Journées de St. Et., 1983, exp. 33.

[9] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. (2) 34 (1933), 461–479.

[10] R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*, CR Acad. Sci. Paris, Sér. I, 296 (1983), 707–708.

[11] J. H. Loxton and A. J. van der Poorten, *Multiplicative dependence in number fields*, Acta Arith. 42 (1982), 291–302.

[12] U. Rausch, *On a theorem of Dobrowolski about the product of conjugate numbers*, Colloq. Math. 50 (1985), 137–142.

[13] В. Г. Спринджук, *Классические диофантовы уравнения от двух неизвестных*, Наука, Москва 1982.

[14] Г. Вейль, *Алгебраическая теория чисел*, ГИИЛ, Москва 1947.

Поступило 6.1.1989 (1899)

Editorial note: The paper was intended to Sprindžuk's memorial volume and it was delayed due to the fault of the editors.