Math-Net.Ru

Общероссийский математический портал

М. О. Авдеева, В. А. Быковский, Верхние и нижние оценки константы Вороного–Минковского, *Матем. заметки*, 2010, том 87, выпуск 4, 483–491

DOI: <https://doi.org/10.4213/mzm4886>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.234.156.22

26 апреля 2023 г., 15:50:05

Верхние и нижние оценки константы Вороного–Минковского

М. О. Авдеева, В. А. Быковский

В работе изучено поведение константы $C(s)$ при $s \rightarrow \infty$, которая возникает при оценке количества относительных минимумов s -мерных целочисленных решеток Γ через $\log_2 N$ в степени $s - 1$, где $N = D(\Gamma)$ – определитель Γ .

Библиография: 9 названий.

1. Введение. Напомним, что элементы (узлы) $\gamma = (\gamma_1, \dots, \gamma_s)$ любой полной s -мерной решетки Γ являются целочисленными комбинациями

$$m_1 \gamma^{(1)} + \dots + m_s \gamma^{(s)}, \quad m_i \in \mathbb{Z},$$

некоторых базисных линейно независимых узлов $\gamma^{(i)} = (\gamma_1^{(i)}, \dots, \gamma_s^{(i)})$, $i = 1, \dots, s$ (см., например, [1]). При этом $D(\Gamma) = |\det(\gamma_j^{(i)})|$ – определитель Γ . В работе рассматриваются только полные решетки и поэтому в дальнейшем слово “полная” мы будем опускать.

Следуя Вороному [2] (см. также [3]), назовем ненулевой узел γ *относительным минимумом* решетки Γ , если не существует другого ненулевого узла η из Γ , для которого $|\eta_j| \leq |\gamma_j|$ при $j = 1, \dots, s$ и $|\eta_i| < |\gamma_i|$ хотя бы при одном $j = i$. Множество всех относительных минимумов решетки Γ обозначим через $\mathfrak{M}(\Gamma)$. Речь идет о многомерном обобщении теории классических непрерывных дробей, восходящем к Вороному и Минковскому.

Назовем две решетки Γ_1 и Γ_2 *подобными*, если для некоторых вещественных $\alpha_1, \dots, \alpha_s$, отличных от нуля,

$$\Gamma_2 = \{(\alpha_1 \gamma_1, \dots, \alpha_s \gamma_s) \mid (\gamma_1, \dots, \gamma_s) \in \Gamma_1\}.$$

Из определения немедленно следует, что

$$\mathfrak{M}(\Gamma_2) = \{(\alpha_1 \gamma_1, \dots, \alpha_s \gamma_s) \mid (\gamma_1, \dots, \gamma_s) \in \mathfrak{M}(\Gamma_1)\}.$$

В [4] было доказано, что множество $\mathfrak{M}(\Gamma)$ конечно тогда и только тогда, когда решетка Γ подобна целочисленной.

Так как множество целочисленных решеток с фиксированным определителем конечно, то для любого натурального N определена величина $T_s(N)$ – максимум

Работа выполнена при поддержке Российского фонда фундаментальных исследований (гранты №№ 09-01-12129-офи_м, 10-01-98002-р_сибирь_а) и Дальневосточного отделения РАН (проект № 09-I-ОМН-09).

$\#\mathfrak{M}(\Gamma)$ (количество элементов множества $\mathfrak{M}(\Gamma)$) по всем целочисленным решеткам Γ с $D(\Gamma) = N$. В работе [5] (см. также [6]) было доказано, что $T_s(N) = O_s(\log_2^{s-1} N)$ при $N \geq 2$. По этой причине определено число

$$C(s) = \overline{\lim}_{N \rightarrow \infty} \frac{T_s(N)}{\log_2^{s-1} N}$$

(речь идет о верхнем пределе), которое мы назовем *константой Вороного–Минковского*.

Задача вычисления $T_s(N)$ при $s = 2$ эквивалентна задаче о сложности нахождения максимального числа операций при вычислении НОД(A, N) для натурального A от 1 до N . Из хорошо известных результатов на эту тему (см., например, [7]) немедленно следует, что $C(2) = 2 \log_2 \Phi$. Здесь $\Phi = (1 + \sqrt{5})/2$ – золотое сечение. При $s \geq 3$ известны лишь оценки

$$C(s) \leq s \cdot 2^s \quad (\text{см. [8]}), \quad (1)$$

$$C(s) \geq \frac{1}{(s-1)!} \frac{1}{(2s)^s} \quad (\text{см. [9]}). \quad (2)$$

В настоящей работе доказывается следующий результат, позволяющий судить о поведении $C(s)$ при $s \rightarrow \infty$.

ТЕОРЕМА 1. *Для любого $\varepsilon > 0$ при $s \geq s_0(\varepsilon)$*

$$(s!)^{-1-\varepsilon} < C(s) < (s!)^{-1+\varepsilon}.$$

Доказательству этой теоремы посвящены п. 2 (верхняя оценка) и п. 3 (нижняя оценка).

Отметим, что неравенства (1) и (2) приводят к неправильным по порядку (в логарифмической шкале) оценкам

$$(s!)^{-2} < C(s) < (s!)^\varepsilon.$$

2. Верхняя оценка.

ЗАМЕЧАНИЕ 1. Из теоремы Минковского о линейных формах непосредственно следует, что для любого относительного минимума $\gamma = (\gamma_1, \dots, \gamma_s)$ решетки Γ выполняется неравенство $|\gamma_1 \cdots \gamma_s| < D(\Gamma)$.

Из теоремы о приведении целочисленных матриц к треугольному виду (см., например, [1]) непосредственно следует

ЗАМЕЧАНИЕ 2. Пусть Γ – целочисленная решетка размерности $s \geq 2$ с $D(\Gamma) = N$. Тогда для любого индекса j от 1 до s множество Γ_j , которое получается из элементов $\{(\gamma_1, \dots, \gamma_s) \in \Gamma \mid \gamma_j = 0\}$ вычеркиванием j -й нулевой координаты, является решеткой размерности $s-1$ с определителем $N_j = D(\Gamma_j)$ – делителем N .

Доказательство верхней оценки для $C(s)$ основано на следующем утверждении, которое справедливо для любой решетки в $\mathbb{R}^s$ (а не только целочисленной).

ЛЕММА 1. *Пусть $P_1, \dots, P_{s-1}$ – произвольные положительные числа. Тогда количество всех относительных минимумов γ s -мерной решетки Γ , удовлетворяющих неравенствам*

$$P_j \leq |\gamma_j| < 2P_j, \quad j = 1, \dots, s-1,$$

не превосходит 2^s .

ДОКАЗАТЕЛЬСТВО. Предположим, что имеется более 2^s интересных нас относительных минимумов. Тогда среди них найдутся два, γ и η , для которых γ_j и η_j при всех $j = 1, \dots, s$ не могут быть ненулевыми числами разных знаков. При этом можно считать, что $|\gamma_s| \leq |\eta_s|$. Но в таком случае

$$|\eta_j - \gamma_j| < P_j \leq |\eta_j|, \quad j = 1, \dots, s-1,$$

и $|\eta_s - \gamma_s| \leq |\eta_s|$. Таким образом, узел $\eta - \gamma$ нарушает условие минимальности η . Значит, наше предположение неверно и лемма 1 доказана.

ТЕОРЕМА 2. Для любого $s \geq 1$

$$C(s) \leq \frac{2^s}{(s-1)!}.$$

ДОКАЗАТЕЛЬСТВО. Проведем индукцию по s . При $s = 1$ решетка на прямой – последовательность точек вида $m_1 \gamma_1^{(1)}$, среди элементов которой ровно два относительных минимума $\gamma_1^{(1)}$ и $-\gamma_1^{(1)}$.

Теперь обоснуем индуктивный переход от размерности $s-1$ к размерности s . Для этого разобьем $\mathfrak{M}(\Gamma)$ на два подмножества $\mathfrak{M}'(\Gamma)$ и $\mathfrak{M}^0(\Gamma)$. К первому отнесем все относительные минимумы с ненулевыми координатами, а ко второму – остальные. Пусть $k = (k_1, \dots, k_{s-1})$ – произвольный набор из $s-1$ неотрицательных целых чисел. Обозначим через $\mathfrak{M}'(\Gamma; k)$ подмножество в $\mathfrak{M}'(\Gamma)$, состоящее из всех относительных минимумов γ , для которых

$$2^{k_j} \leq |\gamma_j| < 2^{k_j+1}, \quad j = 1, \dots, s-1.$$

Так как координата γ_s – ненулевое целое, то с учетом замечания 1 получаем, что

$$2^{k_1+\dots+k_{s-1}} \leq |\gamma_1 \dots \gamma_{s-1}| \leq |\gamma_1 \dots \gamma_s| < D(\Gamma) = N.$$

Применяя лемму 1, находим

$$\begin{aligned} \#\mathfrak{M}'(\Gamma) &= \sum_{\substack{k_1+\dots+k_{s-1} \leq \log_2 N \\ k_j \geq 0}} \#\mathfrak{M}'(\Gamma; k_1, \dots, k_{s-1}) \leq 2^s C_{s-1}^{s-1} \log_2 N \\ &= \frac{2^s}{(s-1)!} \log_2^{s-1} N + O_s(\log_2^{s-2} N). \end{aligned}$$

Из замечания 2 следует, что

$$\#\mathfrak{M}^0(\Gamma) \leq \sum_{j=1}^s \#\mathfrak{M}(\Gamma_j)$$

с $(s-1)$ -мерными решетками Γ_j , у которых определители $N_j = D(\Gamma_j)$ – делители N . Поэтому по предположению индукции

$$\#\mathfrak{M}^0(\Gamma) = O_s(\log_2^{s-2} N).$$

В результате находим, что

$$\frac{T_s(N)}{\log_2^{s-1} N} \leq \frac{2^s}{(s-1)!} + O_s\left(\frac{1}{\log_2 N}\right).$$

Переходя в обоих частях неравенства к верхнему пределу при $N \rightarrow \infty$, получим утверждение теоремы 1.

ЗАМЕЧАНИЕ 3. Поскольку

$$\frac{2^s}{(s-1)!} = \frac{s \cdot 2^s}{s!}$$

и

$$\log(s \cdot 2^s) = O(s) = o(s \log s) = o(\log s!),$$

то при $s \geq s_0(\varepsilon)$ выполняется верхняя оценка в сформулированной во введении теореме 1.

3. Нижняя оценка. Пусть p – простое число и

$$\mathbb{Z}_p^s = \{a = (a_1, \dots, a_s) \in \mathbb{Z}^s \mid 1 \leq a_1, \dots, a_s \leq p\}.$$

Для каждого $a \in \mathbb{Z}_p^s$ определим s -мерную целочисленную решетку

$$\Gamma_p(a) = \{n = (n_1, \dots, n_s) \in \mathbb{Z}^s \mid a_1 n_1 + \dots + a_s n_s \equiv 0 \pmod{p}\}.$$

Если $a_1 = \dots = a_s = p$, то $\Gamma_p(a) = \mathbb{Z}^s$ и $D(\Gamma_p(a)) = 1$. Для остальных $a \in \mathbb{Z}_p^s$ определитель $\Gamma_p(a)$ равен p .

Обозначим через $\mathbb{Z}_+^s$ множество всех целочисленных наборов $k = (k_1, \dots, k_s)$ с натуральными $k_1, \dots, k_s$. Каждому натуральному l сопоставим в $\mathbb{Z}_+^s$ подмножество

$$\mathbb{Z}_+^s(l) = \{k \in \mathbb{Z}_+^s \mid k_1 + \dots + k_s = l\},$$

которое пусто для $1 \leq l < s$. Пусть $\lambda > 1$ и

$$\Omega_\lambda^s(k) = \{x \in \mathbb{R}^s \mid |x_i| \leq \lambda^{k_i} \text{ для } i = 1, \dots, s\}.$$

Положим

$$\mathcal{L}_p^{(s)}(k; \lambda) = \sum_{a \in \mathbb{Z}_p^s} \#(\mathfrak{M}(\Gamma_p(a)) \cap \Omega_\lambda^s(k)).$$

ЛЕММА 2. Пусть $s < \lambda$ и $\lambda^l < p$. Тогда для любого набора k из $\mathbb{Z}_+^s(l)$ выполняется неравенство

$$\mathcal{L}_p^{(s)}(k; \lambda) \leq 2^{s+1} \lambda^l p^{s-1}.$$

ДОКАЗАТЕЛЬСТВО. Обозначим через $\Gamma'_p(a)$ множество всех ненулевых узлов решетки $\Gamma_p(a)$. Так как $\mathfrak{M}(\Gamma_p(a)) \subset \Gamma'_p(a)$, то

$$\begin{aligned} \mathcal{L}_p^{(s)}(k; \lambda) &\leq \sum_{a \in \mathbb{Z}_p^s} \#(\Gamma'_p(a) \cap \Omega_\lambda^s(k)) \\ &= \sum_{a_1, \dots, a_s=1}^p \sum_{n \in \Omega_\lambda^s(k) \cap \mathbb{Z}^s}^l \delta_p(a_1 n_1 + \dots + a_s n_s) = \sum_{n \in \Omega_\lambda^s(k) \cap \mathbb{Z}^s}^l T_p(n). \end{aligned}$$

Здесь штрих означает, что слагаемое с $n = (0, \dots, 0)$ опускается,

$$\delta_p(r) = \begin{cases} 1, & \text{если } r \equiv 0 \pmod{p}, \\ 0, & \text{если } r \not\equiv 0 \pmod{p}, \end{cases}$$

а $T_p(n)$ – число решений сравнения $a_1 n_1 + \dots + a_s n_s \equiv 0 \pmod{p}$ относительно неизвестных $a_1, \dots, a_s \in \mathbb{Z}_p^1 = \mathbb{Z}_p$. Так как для $(n_1, \dots, n_s) \in \Omega_\lambda^s(k)$ выполняются неравенства

$$|n_i| \leq \lambda^{k_i} < \lambda^{k_1 + \dots + k_s} = \lambda^l < p, \quad i = 1, \dots, s,$$

то для каждого такого ненулевого набора найдется координата $n_j \not\equiv 0 \pmod{p}$ и в этом случае $T_p(n) = p^{s-1}$. Следовательно,

$$\begin{aligned} \mathcal{L}_p^{(s)}(k; \lambda) &\leq p^{s-1} \#(\Omega_\lambda^s(k) \cap \mathbb{Z}^s) = p^{s-1} \prod_{i=1}^s (2[\lambda^{k_i}] + 1) \\ &\leq 2^s \lambda^{k_1 + \dots + k_s} p^{s-1} \prod_{i=1}^s \left(1 + \frac{1}{2\lambda^{k_i}}\right) \leq \left(1 + \frac{1}{2s}\right)^s 2^s \lambda^l p^{s-1} < 2^{s+1} \lambda^l p^{s-1}. \end{aligned}$$

Лемма 2 полностью доказана.

Обозначим через $\tilde{\mathbb{Z}}^s$ множество всех целочисленных наборов $(n_1, \dots, n_s)$, у которых $n_i \neq 0$ при всех $i = 1, \dots, s$ и $\text{НОД}(n_1, \dots, n_s) = 1$. Пусть также $\tilde{\Gamma}_p(a) = \tilde{\mathbb{Z}}^s \cap \Gamma_p(a)$. Для $k \in \mathbb{Z}_+^s$ положим

$$\mathcal{M}_p(k; \lambda) = \sum_{a \in \mathbb{Z}_p^s} \#(\tilde{\Gamma}_p(a) \cap \Omega_\lambda^s(k)).$$

ЛЕММА 3. Пусть $s \geq 3$ и $l \geq s$. Тогда для любого набора k из $\mathbb{Z}_+^s(l)$ выполняется оценка

$$\mathcal{M}_p(k; \lambda) \geq 2^{s-1} \left(1 - \frac{4s}{\lambda}\right) \lambda^l p^{s-1}.$$

ДОКАЗАТЕЛЬСТВО. По определению

$$\begin{aligned} \mathcal{M}_p(k; \lambda) &= \sum_{a \in \mathbb{Z}_p^s} \sum_{n \in \tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)} \delta_p(a_1 n_1 + \dots + a_s n_s) \\ &= \sum_{n \in \tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)} \sum_{a \in \mathbb{Z}_p^s} \delta_p(a_1 n_1 + \dots + a_s n_s) = \#(\tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)) p^{s-1}. \end{aligned}$$

По формуле обращения Мёбиуса

$$\#(\tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)) = \sum_{d=1}^{\infty} \mu(d) \sum_{\substack{0 < |dn_i| \leq \lambda^{k_i} \\ i=1, \dots, s}} 1 = 2^s \sum_{1 \leq d \leq \lambda^{k_0}} \mu(d) \prod_{i=1}^s \left[\frac{\lambda^{k_i}}{d} \right],$$

где $k_0 = \min\{k_1, \dots, k_s\}$. Воспользовавшись очевидным тождеством

$$x_1 \cdots x_s - y_1 \cdots y_s = \sum_{i=1}^s \left(\prod_{j < i} x_j \right) (x_i - y_i) \left(\prod_{j > i} y_j \right),$$

получим, что

$$\begin{aligned} 0 &\leq \prod_{i=1}^s \frac{\lambda^{k_i}}{d} - \prod_{i=1}^s \left[\frac{\lambda^{k_i}}{d} \right] \leq \sum_{i=1}^s \left\{ \frac{\lambda^{k_i}}{d} \right\} \cdot \frac{d}{\lambda^{k_i}} \cdot \frac{\lambda^{k_1 + \dots + k_s}}{d^s} \\ &\leq \frac{\lambda^l}{d^{s-1}} \sum_{i=1}^s \frac{1}{\lambda^{k_i}} \leq \frac{s}{\lambda^{k_0}} \cdot \frac{\lambda^l}{d^{s-1}} \leq \frac{s}{\lambda} \cdot \frac{\lambda^l}{d^{s-1}}. \end{aligned}$$

Поэтому

$$\#(\tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)) \geq 2^s \lambda^l \left(\sum_{1 \leq d \leq \lambda^{k_0}} \frac{\mu(d)}{d^s} - \frac{s}{\lambda} \sum_{1 \leq d \leq \lambda^{k_0}} \frac{1}{d^{s-1}} \right).$$

Так как

$$\sum_{1 \leq d \leq \lambda^{k_0}} \frac{\mu(d)}{d^s} \geq 1 - \sum_{d=2}^{\infty} \frac{1}{d^s} > 1 - \frac{1}{2} \sum_{d=2}^{\infty} \frac{1}{d(d-1)} = \frac{1}{2},$$

а также

$$\sum_{1 \leq d \leq \lambda^{k_0}} \frac{1}{d^{s-1}} < \sum_{d=1}^{\infty} \frac{1}{d^2} = \frac{\pi^2}{6} < 2,$$

то

$$\mathcal{M}_p(k; \lambda) \geq 2^s \lambda^l \left(\frac{1}{2} - \frac{2s}{\lambda} \right) p^{s-1}.$$

Лемма 3 полностью доказана.

Положим

$$\mathcal{D}_p(k; \lambda) = \sum_{a \in \mathbb{Z}_p^s} (\#(\tilde{\Gamma}_p(a) \cap \Omega_\lambda^s(k)))^2.$$

ЛЕММА 4. Пусть $k \in \mathbb{Z}_+^s(l)$ и $\lambda^{k_i} < \sqrt{p/2}$ при всех $i = 1, \dots, s$. Тогда

$$\mathcal{D}_p(k; \lambda) \leq 2^{2s} p^{s-2} \lambda^{2l} + 2^{s+1} p^{s-1} \lambda^l.$$

ДОКАЗАТЕЛЬСТВО. Легко заметить, что

$$\mathcal{D}_p(k; \lambda) = \sum_{(n, m) \in (\tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k))^2} T(n, m),$$

где $T(n, m)$ – количество решений системы из двух сравнений

$$\begin{cases} a_1 n_1 + \dots + a_s n_s \equiv 0 \pmod{p}, \\ a_1 m_1 + \dots + a_s m_s \equiv 0 \pmod{p} \end{cases}$$

относительно неизвестных $a_i \in \mathbb{Z}_p$. Если хотя бы для одной пары индексов i и j выполняется условие

$$d_{ij}(n, m) = \det \begin{pmatrix} n_i & n_j \\ m_i & m_j \end{pmatrix} \not\equiv 0 \pmod{p},$$

то $T(n, m) = p^{s-2}$. Для остальных пар (n, m) таких, что при всех i и j имеют место равенства $d_{ij}(n, m) = p \cdot r_{ij}(n, m)$ с целыми $r_{ij}(n, m)$, всегда $T(n, m) = p^{s-1}$. Заметим, что в последнем случае для всех i и j

$$|r_{ij}(n, m)| = \frac{1}{p} |n_i m_j - n_j m_i| < \frac{1}{p} \left(\frac{p}{2} + \frac{p}{2} \right) = 1,$$

а поэтому $d_{ij}(n, m) = 0$. Но тогда для некоторых ненулевых целых u и v выполняется равенство $un = vm$. Поскольку

$$\text{НОД}(n_1, \dots, n_s) = \text{НОД}(m_1, \dots, m_s) = 1,$$

то $u = \pm 1$ и $v = \pm 1$. Следовательно, $m = \pm n$. Таким образом, окончательно находим, что

$$\begin{aligned} \mathcal{D}_p(k; \lambda) &\leq p^{s-2} (\#(\tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)))^2 + 2p^{s-1} \#(\tilde{\mathbb{Z}}^s \cap \Omega_\lambda^s(k)) \\ &\leq p^{s-2} \left(\prod_{i=1}^s 2\lambda^{k_i} \right)^2 + 2p^{s-1} \prod_{i=1}^s 2\lambda^{k_i} = p^{s-2} 2^{2s} \lambda^{2l} + 2^{s+1} p^{s-1} \lambda^l. \end{aligned}$$

Лемма 4 доказана.

Обозначим через $N_p(k; \lambda)$ количество всех $a \in \mathbb{Z}_p^s$, для которых $\tilde{\Gamma}_p(a) \cap \Omega_\lambda^s(k)$ – непустое множество.

ЛЕММА 5. Пусть $\lambda \geq 8s$, $\lambda^l \geq p2^{-s}$ и $l \geq s$, а также $k \in \mathbb{Z}_+^s(l)$ с $\lambda^{k_i} < \sqrt{p/2}$ при $i = 1, \dots, s$. Тогда

$$N_p(k; \lambda) \geq \frac{p^s}{48}.$$

ДОКАЗАТЕЛЬСТВО. Воспользовавшись неравенством Коши–Буняковского, получим

$$\mathcal{M}_p^2(k; \lambda) \leq N_p(k; \lambda) \mathcal{D}_p(k; \lambda).$$

Применяя оценки лемм 3 и 4, отсюда находим, что для $G = \lambda^l 2^s p^{-1} \geq 1$

$$N_p(k; \lambda) \geq \frac{(Gp^s/4)^2}{p^s(G^2 + 2G)} = \frac{p^s}{16} \cdot \frac{G}{G+2} \geq \frac{p^s}{48}.$$

Лемма 5 доказана.

Положим

$$\mathcal{L}_p^{(s)} = \sum_{a \in \mathbb{Z}_p^s} \# \mathfrak{M}(\Gamma_p(a)).$$

ЛЕММА 6. Пусть $s < l$, $s \leq \lambda$, $\lambda^l < p$. Тогда

$$\mathcal{L}_p^{(s)} \geq \sum_{k \in \mathbb{Z}_+^s(l)} \mathcal{L}_p^{(s)}(k; \lambda) - \frac{s}{\lambda} 2^{s+1} \frac{\lambda^l}{p} C_{l-2}^{s-1} p^s.$$

ДОКАЗАТЕЛЬСТВО. Для каждого $k \in \mathbb{Z}_+^s(l)$ определим подмножество $E(k)$ в $\Omega_\lambda^s(k)$, состоящее из всех $x \in \mathbb{R}^s$, для которых

- 1) $\lambda^{k_i-1} < |x_i| \leq \lambda^{k_i}$, если $k_i > 1$;
- 2) $|x_i| \leq \lambda$, если $k_i = 1$.

Они попарно не пересекаются, и поэтому

$$\# \mathfrak{M}(\Gamma_p(a)) \geq \sum_{k \in \mathbb{Z}_+^s(l)} \# (\mathfrak{M}(\Gamma_p(a)) \cap E(k)). \quad (3)$$

Каждое множество $E(k)$, участвующее в суммировании, получается удалением из $\Omega_\lambda^s(k)$ всех подмножеств $\Omega_\lambda^s(k')$, отвечающих наборам $k' \in \mathbb{Z}_+^s(l-1)$, которые возникают из набора k уменьшением одной компоненты, большей единицы, на 1. Поэтому

$$\# (\mathfrak{M}(\Gamma_p(a)) \cap E(k)) \geq \# (\mathfrak{M}(\Gamma_p(a)) \cap \Omega_\lambda^s(k)) - \sum_{\substack{(k) \\ k' \in \mathbb{Z}_+^s(l-1)}} \# (\mathfrak{M}(\Gamma_p(a)) \cap \Omega_\lambda^s(k')),$$

где знак (k) означает суммирование по всем k' вышеуказанного вида. Поскольку набор k' при этом может возникать из элементов $\mathbb{Z}_+^s(l)$ ровно s способами, то при суммировании правой части последнего неравенства по $k \in \mathbb{Z}_+^s(l)$ получается выражение

$$\sum_{k \in \mathbb{Z}_+^s(l)} \#(\mathfrak{M}(\Gamma_p(a)) \cap \Omega_\lambda^s(k)) - s \cdot \sum_{k' \in \mathbb{Z}_+^s(l-1)} \#(\mathfrak{M}(\Gamma_p(a)) \cap \Omega_\lambda^s(k')).$$

Воспользовавшись неравенством (3), леммой 2 и комбинаторным тождеством

$$\#\mathbb{Z}_+^s(l-1) = C_{l-2}^{s-1},$$

а также выполнив суммирование по a , получаем утверждение леммы 6.

ТЕОРЕМА 3. Пусть $\Delta = 128s$. Тогда для любого $s \geq 16$ при $p \geq p_0(s)$

$$\mathcal{L}_p^{(s)} \geq \frac{1}{100} \frac{p^s}{(s-1)!} \log_\Delta^{s-1} p.$$

ДОКАЗАТЕЛЬСТВО. Пусть $l = \lceil \log_\Delta(p \cdot 2^{-s}) \rceil \geq s$ и λ определяется из равенства $\lambda^l = 2^{-s}p$. Легко проверить, что $\lambda = \Delta + O_s(\log^{-1} p)$ при $p \rightarrow \infty$. Если $\tilde{\Gamma}_p(a) \cap \Omega_\lambda^s(k)$ — непустое множество, то в $\mathfrak{M}(\Gamma_p(a)) \cap \Omega_\lambda^s(k)$ найдутся по крайней мере два относительных минимума γ и $-\gamma$ решетки $\Gamma_p(a)$. Применяя леммы 5 и 6, получим, что

$$\mathcal{L}_p^{(s)} \geq \sum_{\substack{k \in \mathbb{Z}_+^s(l) \\ \lambda^{k_i} < \sqrt{p/2}}} 2 \cdot \frac{p^s}{48} - \frac{2s}{\lambda} C_{l-2}^{s-1} p^s = \frac{p^s}{24} (C_{l-1}^{s-1} - T) - \frac{2s}{\lambda} C_{l-2}^{s-1} p^s,$$

где T — число наборов $k \in \mathbb{Z}_+^s(l)$, у которых $\max k_j \geq \log_\lambda(p/2)/2$. Поскольку переменные k_j входят в набор k равноправно, то $T \leq s \cdot T'$, где T' — число наборов $k \in \mathbb{Z}_+^s(l)$, у которых

$$k_s \geq \frac{1}{2} \log_\lambda \frac{p}{2} > \frac{1}{2} \log_\lambda(2^{-s}p) = \frac{1}{2} l.$$

Заметим, что

$$T' = \sum_{l/2 < k_s \leq l} C_{l-k_s-1}^{s-2} \leq l C_{\lfloor l/2 \rfloor}^{s-2} \leq \frac{l^{s-1}}{(s-2)! 2^{s-2}} + O_s(l^{s-2}).$$

Поэтому

$$\mathcal{L}_p^{(s)} \geq \left(\frac{1}{24} - \frac{4s(s-1)}{2^s} - \frac{1}{64} + O_s\left(\frac{1}{\log p}\right) \right) \frac{l^{s-1}}{(s-1)!} p^s.$$

Поскольку при $s \geq 16$

$$\frac{4s(s-1)}{2^s} \leq \frac{(2s)^2}{2^s} \leq \frac{(2^5)^2}{2^{16}} = \frac{1}{2^6} = \frac{1}{64},$$

то при $p \geq p_0(s)$

$$\mathcal{L}_p^{(s)} \geq \frac{1}{100} \cdot \frac{1}{(s-1)!} p^s \log_\Delta^{s-1} p.$$

Теорема 3 полностью доказана.

Из теоремы 3 следует, что при $s \geq 1$

$$C(s) \geq \lim_{p \rightarrow \infty} \frac{T_s(p)}{\log_2^{s-1} p} \geq \frac{1}{100} \cdot \frac{1}{s!} \cdot \frac{s}{\log_2^{s-1} \Delta}.$$

Так как при $s \rightarrow \infty$

$$\log \left(100 \frac{\log_2^{s-1} \Delta}{s} \right) = O(s \log \log s) = o(s \log s) = o(\log(s!)),$$

то при $s \geq s_0(\varepsilon)$ выполняется нижняя оценка сформулированной во введении теоремы 1.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Дж. В. С. Касселс, *Введение в геометрию чисел*, Мир, М., 1965.
- [2] Г. Ф. Вороной, *Собрание сочинений: В 3-х т.*, т. 1, Изд-во АН УССР, Киев, 1952.
- [3] Н. Minkowski, “Généralization de la théorie des fractions continues”, *Ann. Sci. École Norm. Sup.* (3), **13**:2, (1896), 41–60.
- [4] О. А. Горкуша, “Критерий конечности множества локальных минимумов решетки”, *Чебышевский сб.*, **5**:3, (2004), 15–17.
- [5] В. А. Быковский, “О погрешности теоретико-числовых квадратурных формул”, *Докл. РАН*, **382**:2, (2003), 154–155.
- [6] Н. М. Коробов, *Теоретическо-числовые методы в приближенном анализе*, МЦНМО, М., 2004.
- [7] Д. Кнут, *Искусство программирования*, т. 2, Получисленные алгоритмы, Мир, М., 2000.
- [8] О. А. Горкуша, Н. М. Добровольский, “Об оценках гиперболической дзета-функции решеток”, *Чебышевский сб.*, **6**:2, (2005), 129–137.
- [9] М. О. Авдеева, “О нижних оценках количества локальных минимумов целочисленных решеток”, *Фундамент. и прикл. матем.*, **11**:6, (2005), 9–14.

М. О. Авдеева

Хабаровское отделение Института прикладной математики
ДВО РАН

E-mail: avdeeva@iam.khv.ru

Поступило

28.04.2008

В. А. Быковский

Хабаровское отделение Института прикладной математики
ДВО РАН

E-mail: vab@iam.khv.ru