E. P. Golubeva, On the class numbers of indefinite binary quadratic forms with discriminant dp^2, *Zap. Nauchn. Sem. POMI*, 2002, Volume 286, 40–47

Записки научных
семинаров ПОМИ
Том 286, 2002 г.

Е. П. Голубева

О ЧИСЛАХ КЛАССОВ НЕОПРЕДЕЛЕННЫХ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ ДИСКРИМИНАНТА dp^2

Вопрос о поведении чисел классов неопределенных бинарных квадратичных форм восходит к Гауссу. Все табличные данные свидетельствуют о том, что для подавляющего большинства дискриминантов это число мало (имеет логарифмический порядок роста при растущем дискриминанте). Существует целый ряд количественных гипотез на эту тему, имеющих совершенно определенный, с точностью до явных констант, вид и подкрепленных различными косвенными соображениями (см. [1–3]).

Тем не менее, этот вопрос дает яркий пример очень старой проблемы, в которой со времени возникновения нет заметного прогресса. Основная трудность при попытках получить продвижение состоит в необходимости найти или оценить наименьшее решение соответствующего уравнения Пелля

$$t^2 - du^2 = 1, \tag{1}$$

где d – определитель целочисленной неопределенной бинарной квадратичной формы, который не совпадает с квадратом целого числа.

Наилучшие на настоящий момент известные результаты имеют в общем случае следующий вид:

> пусть t и u – наименьшие положительные целые числа, удовлетворяющие уравнению (1), и $\varepsilon(d) = t + \sqrt{d}\,u$; пусть $0 < b < 3/2$ – произвольная постоянная. Тогда для почти всех d справедлива оценка $\varepsilon(d) > d^b$.

Этот результат был доказан в работе [1]. Для простых d справедлива лучшая оценка:

Работа выполнена при поддержке Математического института Макса Планка.

пусть δ – произвольная положительная постоянная. Количество простых p таких, что $p \leqslant x$, $p \equiv 3 (\operatorname{mod} 4)$ и $\varepsilon(p) \leqslant p^3/\log^{1+\delta} p$, не превосходит величины $C(\delta)x/\log^{1+\delta} x$, где $C(\delta)$ – постоянная.

Этот результат был доказан в работе [3].

Отметим, что по всем гипотезам для почти всех d должна быть справедлива оценка $\varepsilon(d) > \exp(\sqrt{d}/\log^{\lambda} d)$, где $\lambda > 0$ – постоянная.

Можно построить бесконечные серии примеров, когда значение $\varepsilon(d)$ явно вычисляется. Во всех этих случаях $\varepsilon(d)$ мало. Самыми рекордными из них на настоящий момент являются последовательности, для которых $\varepsilon(d) \gg \exp(\log^3 d)$ (см [4, 5]). Эти последовательности растут экспоненциальным образом и, хотя в них, по-видимому, должно быть бесконечно много бесквадратных и даже простых значений d, доказательство последнего факта само по себе является проблемой.

Если дискриминант формы делится на большой квадрат, то возникают дополнительные возможности для изучения числа классов, связанные с тем, что $\varepsilon(dp^2)$ является степенью $\varepsilon(d)$. До сих пор исследовались случаи последовательности dp^2 с небольшими фиксированными d (см. [4, 6, 7]). В этих случаях доказаны результаты, несравнимо более точные, чем в общем. Некоторые из них получены в предположении справедливости расширенной гипотезы Римана для ζ-функций некоторого набора алгебраических полей.

Решения уравнения Пелля тесно связаны с разложениями $\sqrt{d}$ в обыкновенную непрерывную дробь. Предположение о том, что это разложение в случае, когда d делится на большой квадрат, в среднем не обладает никакими особыми свойствами, представляется весьма правдоподобным. Соответственно, числа классов в этом случае должны вести себя в среднем так же как и в общем.

В работе [4] было показано, что

$$\sum_{p \leqslant X} h(5p^2) = O\bigl(X^{3/2}/\log X\bigr), \tag{2}$$

где $h(m)$ – число классов целочисленных бинарных квадратичных форм дискриминанта m.

Заметим, что здесь и всюду в дальнейшем фигурируют только оценки сверху для чисел классов. Поэтому не имеет значения, в каком смысле понимается эквивалентность форм – в узком или широком. Также не имеет значения, в каком смысле понимается целочисленность форм – в смысле Гаусса или как в большинстве современных работ.

Из оценки (2) следует, что для почти всех p справедливо соотношение $\varepsilon(p) \gg \exp(\sqrt{p})$.

В настоящей работе мы получаем аналогичную оценку для последовательности dp^2 с произвольным d.

Предложение 1. *Имеет место оценка*

$$\sum_{X \leqslant p \leqslant 2X} h(dp^2) = O\big(h(d)\sqrt{\log \varepsilon(d)}\, X^{3/2}/\log X\big).$$

Естественно предположить, что в действительности при больших X и фиксированном d должна иметь место асимптотическая формула

$$\sum_{p \leqslant X} h(dp^2) \sim C(d)h(d)X,$$

где функция $C(d)$ удовлетворяет неравенствам $\log^{-\lambda_1} d < C(d) < \log^{\lambda_2} d$ при некоторых положительных постоянных λ_1 и λ_2.

Основной результат настоящей работы говорит в пользу этого предположения.

Теорема 1. *Пусть* $d = 4n^2 + 1$, *тогда*

$$\sum\nolimits_1 = \sideset{}{'}\sum_{1 \leqslant n \leqslant X} \frac{1}{h(d)} \sum_{2X \leqslant p \leqslant 3X} h(dp^2) = O(X^2), \tag{3}$$

где $\sum'$ *означает, что суммирование ведется только по бесквадратным* d.

Поскольку $h(dp^2) \geqslant h(d)$, сумма $\sum_1$ из последней формулы удовлетворяет, очевидно, оценке

$$\sum\nolimits_1 \geqslant CX^2/\log X,$$

где C – абсолютно постоянная. В действительности, неравенство (3) является, по-видимому, правильным по порядку.

Аналогично можно рассмотреть и другие последовательности значений d. Это может быть, например, последовательность вида $d = n^2 + k$, где $k \mid 2n$. Это могут быть и другие квадратичные последовательности, для которых удается уследить за значениями $\varepsilon(d)$.

К сожалению, общий случай, когда значения d берутся подряд из некоторого интервала, не поддается изучению таким образом. Это вызвано тем, что в этом случае мы не можем указать решений основного уравнения Пелля и, соответственно, не знаем, как распределены вычеты этих решений по простым модулям.

Из теоремы 1 в качестве следствия легко вытекает

Теорема 2. *В условиях теоремы* 1 *справедлива оценка*

$$\sum\nolimits_1 = \sum_{1\leqslant n\leqslant X}{}' \sum_{2X\leqslant p\leqslant 3X} h(dp^2) = O\big(X^3 \log\log X/\log X\big).$$

Можно предположить, что должна иметь место асимптотическая формула

$$\sum\nolimits_2 \sim CX^3/\log X,$$

где C – постоянная.

Доказательство предложения 1. В силу известной формулы Гаусса (см., например, [8]),

$$h(dp^2) = O\left(h(d)\frac{p-\chi_d(p)}{i_d(p)}\right), \tag{4}$$

где $\chi_d(p) = \left(\frac{d}{p}\right)$, $i_d(p)$ – наименьший из показателей m таких, что

$$\varepsilon^m(d) \equiv 1 \,(\mathrm{mod}\, p). \tag{5}$$

Таким образом,

$$\sum_{X\leqslant p\leqslant 2X} h(dp^2)\log p = O\left(h(d)\sum_{X\leqslant p\leqslant 2X}\frac{X\log p}{i_d(p)}\right).$$

Разобьем последнюю сумму на две,

$$\sum_{X\leqslant p\leqslant 2X}\frac{X\log p}{i_d(p)} = \sum_{\substack{X\leqslant p\leqslant 2X\\ i_d(p)\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}}}\frac{X\log p}{i_d(p)} + \\ + \sum_{\substack{X\leqslant p\leqslant 2X\\ i_d(p)>\sqrt{X}/\sqrt{\log\varepsilon(d)}}}\frac{X\log p}{i_d(p)} = \sum\nolimits_3 + \sum\nolimits_4.$$

Для второй суммы имеем тривиальную оценку:

$$\sum\nolimits_4 = O\Big(\sqrt{X}\sqrt{\log\varepsilon(d)}\sum_{X\leqslant p\leqslant 2X}\log p\Big) = O\Big(X^{3/2}\sqrt{\log\varepsilon(d)}\Big).$$

Чтобы оценить $\sum_3$, мы опускаем условием $X\leqslant p\leqslant 2X$, тогда

$$\sum\nolimits_3 = O\bigg(\sqrt{X}\sqrt{\log\varepsilon(d)}\sum_{\substack{p\\ i_d(p)\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}}}\log p\sqrt{\frac{X}{\log\varepsilon(d)}}\,\frac{1}{i_d(p)}\bigg).$$

Поскольку для любого числа $\alpha>1$, очевидно, $\alpha<2[\alpha]$, имеем

$$\sum\nolimits_3 = O\bigg(\sqrt{X}\sqrt{\log\varepsilon(d)}\sum_{\substack{p\\ i_d(p)\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}}}\log p\bigg[\sqrt{\frac{X}{\log\varepsilon(d)}}\Big/i_d(p)\bigg]\bigg) =$$

$$= O\bigg(\sqrt{X}\sqrt{\log\varepsilon(d)}\,\log\prod_{\substack{p\\ i_d(p)\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}}}p^{\left[\sqrt{X}/\sqrt{\log\varepsilon(d)}/i_d(p)\right]}\bigg).$$

Пусть $\varepsilon^k(d)=P_k+\sqrt{d}\,Q_k$ и $\overline{\varepsilon}^k(d)=P_k-\sqrt{d}\,Q_k$. Если $\varepsilon^k(d)\equiv 1\,(\mathrm{mod}\,p)$, то $\overline{\varepsilon}^k(d)\equiv 1\,(\mathrm{mod}\,p)$. Следовательно, $Q_k\equiv 0\,(\mathrm{mod}\,p)$. Если $Q_k\equiv 0\,(\mathrm{mod}\,p)$, то для любого m имеем $Q_{mk}\equiv 0\,(\mathrm{mod}\,p)$. Таким образом, любое число p, удовлетворяющее условию $i_d(p)\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}$, входит в произведение

$$\prod_{n\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}}Q_n$$

в степени не меньшей, чем $\left[\sqrt{X}/\sqrt{\log\varepsilon(d)}/i_d(p)\right]$. Следовательно,

$$\sum\nolimits_3 = O\Big(\sqrt{X}\sqrt{\log\varepsilon(d)}\,\log\prod_{n\leqslant\sqrt{X}/\sqrt{\log\varepsilon(d)}}Q_n\Big) =$$

$$= O\Big(\sqrt{X}\sqrt{\log\varepsilon(d)}\,\log\Big(\varepsilon(d)^{X/\sqrt{\log\varepsilon(d)}}\Big)\Big) = O\Big(X^{3/2}\sqrt{\log\varepsilon(d)}\Big).$$

Сравнивая последнее выражение с оценкой для $\sum_4$, мы получаем требуемое утверждение.

Для доказательства теоремы 1 нам понадобится вспомогательный результат.

Лемма 1. *Пусть $d_1>1$ и $d_2>1$ – нечетные, бесквадратные целые, ε_1 является единицей поля $\mathbb{Q}(\sqrt{d_1})$, ε_2 – единицей поля $\mathbb{Q}(\sqrt{d_2})$; пусть $\varepsilon_1=(A_1+B_1\sqrt{d_1})/2$, $\varepsilon_2=(A_2+B_2\sqrt{d_2})/2$ и $N(\varepsilon_1)=N(\varepsilon_2)=\pm 1$. Пусть K – произвольное поле, содержащее оба поля $\mathbb{Q}(\sqrt{d_1})$ и $\mathbb{Q}(\sqrt{d_2})$. Пусть $\mathfrak{p}$ – простой идеал и $N_K(\mathfrak{p})=p^r$, где p – нечетное простое число. Пусть $\varepsilon_1\equiv\varepsilon_2 \pmod{\mathfrak{p}}$, тогда $A_1\equiv A_2 \pmod{p}$.*

Доказательство. Так как $\varepsilon_1\equiv\varepsilon_2 \pmod{\mathfrak{p}}$, то

$$A_1-A_2+B_1\sqrt{d_1}\equiv B_2\sqrt{d_2} \pmod{\mathfrak{p}}.$$

Возводя обе части этого сравнения в квадрат, получаем

$$A_1^2-2A_1A_2+A_2^2+B_1^2d_1+2(A_1-A_2)B_1\sqrt{d_1}-B_2^2d_2\equiv 0 \pmod{\mathfrak{p}}.$$

Поскольку

$$A_1^2-d_1B_1^2=A_2^2-d_2B_2^2=\pm 4,$$

имеем

$$A_1^2-A_1A_2+(A_1-A_2)B_1\sqrt{d_1}\equiv 0 \pmod{\mathfrak{p}}.$$

Следовательно,

$$(A_1-A_2)(A_1+B_1\sqrt{d_1})\equiv 0 \pmod{\mathfrak{p}}.$$

Поскольку $A_1+B_1\sqrt{d_1}\not\equiv 0 \pmod{\mathfrak{p}}$, имеет место сравнение $A_1\equiv A_2 \pmod{\mathfrak{p}}$. Значит, $A_1\equiv A_2 \pmod{p}$ и лемма доказана.

Доказательство теоремы 1. При $d=4n^2+1$ $\varepsilon_1(d)$ – основная единица поля $\mathbb{Q}(\sqrt{d_1})$ и $\varepsilon(d)$ связаны соотношением $\varepsilon(d)=\varepsilon_1^6(d)$. Следовательно, в формуле (4) можно заменить $i_d(p)$ на показатель $e_d(p)$, который определяется с помощью сравнения $\varepsilon_1^m(d)\equiv 1 \pmod{p}$ вместо (5).

Таким образом,

$$\sum\nolimits_1 = O\Big(X{\sum_{n\leqslant X}}' \sum_{2X\leqslant p\leqslant 3X}\frac{1}{e_d(p)}\Big).$$

Меняя порядок суммирования, получаем

$$\sum\nolimits_1 = O\Big(X\sum_{2X\leqslant p\leqslant 3X} {\sum_{n\leqslant X}}'\frac{1}{e_d(p)}\Big).$$

Рассмотрим произвольное поле K, содержащее все поля $\mathbb{Q}(\sqrt{d})$, где d пробегает все значения, участвующие в $\sum_1$. Пусть

$\mathfrak{p}$ – произвольный простой идеал K. Как известно, сравнение $\alpha^m \equiv 1 \,(\operatorname{mod} \mathfrak{p})$ имеет в поле K не более, чем m различных решений $(\operatorname{mod} \mathfrak{p})$.

Поскольку $\varepsilon_1(d_i) \equiv (n_i + \sqrt{d_i})/2$ и в условиях теоремы $n_i \not\equiv n_j$ $(\operatorname{mod} p)$ при любом p и $i \neq j$, из леммы 1 следует, что $\varepsilon_1(d_i) \not\equiv \varepsilon_1(d_j)$ $(\operatorname{mod} \mathfrak{p})$ для любого $\mathfrak{p} \mid p$ при $2X \leqslant p \leqslant 3X$.

Следовательно, при заданном p фиксированное значение $e_d(p) = m(p)$ принимается при различных d не более, чем $m(p)$ раз. Таким образом,

$$\sum\nolimits_1 = O\Big(X \sum_{2X\leqslant p\leqslant 3X} \sum_{m(p)} 1\Big),$$

где во внутренней сумме $m(p)$ принимает по одному разу все возможные значения для $e_d(p)$.

Так как $e_d(p) \mid 2(p+1)$ или $e_d(p) \mid 2(p-1)$, то

$$\sum\nolimits_1 = O\Big(X \sum_{2X\leqslant p\leqslant 3X} \tau(p+1) + \tau(p-1)\Big) = O(X^2)$$

и теорема доказана.

Для доказательства теоремы 2 нам понадобится информация о количестве L-функций Дирихле с характерами $(\operatorname{mod} d)$, которые, возможно, не удовлетворяют условию $L_d(1) \ll \log\log d$.

Такой результат содержится в работе [9], хотя в ней идет речь о характерах мнимого квадратичного поля. В действительности, точно такие же оценки справедливы и в случае вещественных квадратичных полей.

Лемма 2. *Для любого $\delta > 0$ найдется вещественное число A, зависящее только от δ, и для каждого $X > 3$ найдется множество $E(X)$ (возможно пустое) со следующими свойствами:*

(i) *Пусть D – целое, $D \leqslant X$ и D не принадлежит $E(X)$. Тогда равномерное соотношение*

$$L_D(1) = \Big(1 + O\big((\log X)^{-1}\big)\Big) \prod_{p\leqslant H} \Big(1 - \chi_D(p)p^{-1}\Big)^{-1}$$

справедливо для всех вещественных H, удовлетворяющих условию $H \geqslant (\log X)^A$, и для всех примитивных характеров $\chi \,(\operatorname{mod} D)$.

(ii) *Число целых D, принадлежащих $E(X)$, равно $O(X^\delta)$.*

Доказательство см. в [9].

Доказательство теоремы 2. Утверждение теоремы мгновенно следует из теоремы 1 и леммы 2, поскольку при $d = 4n^2+1$ $h(d) \asymp \sqrt{d}\, L_d(1)/\log d$.

Литература

1. C. Hooley, *On the Pellian equation and the class number of indefinite binary quadratic forms,* J. reine und angew. Math. **353** (1984), 98–131.
2. P. C. Sarnak,, *Class numbers of indefinite binary quadratic forms. II,* J. Number Theory **21**, No. 3 (1985), 333–346.
3. Е. П. Голубева, *О числах классов вещественных квадратичных полей дискриминанта 4p,* Зап. научн. семин. ПОМИ **204** (1993), 11–36.
4. Е. П. Голубева, *О длинах периодов разложения в непрерывную дробь квадратичных иррациональностей и числах классов вещественных квадратичных полей. I,* Зап. научн. семин. ЛОМИ **160** (1987), 72–81.
5. Y. Yamamoto, *Real quadratic number fields with large fundamental units,* Osaka J. Math. **8**, No. 2 (1971), 261–270.
6. Е. П. Голубева, *О длинах периодов разложения в непрерывную дробь квадратичных иррациональностей и числах классов вещественных квадратичных полей. II,* Зап. научн. семин. ЛОМИ **168** (1988), 11–22.
7. О. М. Фоменко, *Числа классов неопределенных бинарных квадратичных форм,* Зап. научн. семин. ПОМИ **276** (2001), 312–333.
8. Б. А. Венков, *Элементарная теория чисел,* М.-Л., (1937).
9. P. D. T. A. Elliott, *The distribution of the quadratic class numbers,* Литовск. мат. сб. **10**, No. 1 (1970), 189–197.

Государственный
университет
телекоммуникаций
им. М. А. Бонч-Бруевича
E-mail:elena_golubeva@mail.ru

Поступило 25 декабря 2001 г.