Записки научных
семинаров ПОМИ
Том 383, 2010 г.

Е. П. Голубева

ОБ ОТРИЦАТЕЛЬНОМ УРАВНЕНИИ ПЕЛЛЯ

Как хорошо известно, уравнение Пелля

$$x^2 - dy^2 = 1$$

разрешимо при любом d, не являющемся полным квадратом.

Отрицательное уравнение Пелля

$$x^2 - dy^2 = -1 \tag{1}$$

может иметь решения только в том случае, когда d представимо в виде суммы двух квадратов (поскольку $d|x^2+1$). Это условие является достаточным, если d – простое число, и не является достаточным в общем случае. Существует ряд работ (см. [1]), где решаются частные случаи этой проблемы, но в общем виде она не решена.

В работе [3] (см. также [2]) доказано, что среди чисел, представимых в виде суммы двух квадратов, оба множества тех d, для которых уравнение (1) имеет решения (и, соответственно, не имеет решений), имеют положительную плотность.

В настоящей работе мы приводим один из алгоритмов, позволяющих выписать все значения d, для которых уравнение (1) разрешимо.

Теорема 1. *Пусть P, Q и C целые, удовлетворяющие условиям*

$$P - \text{нечетно}, \quad P > Q, \quad CP = Q^2 + 1. \tag{2}$$

Пусть d не является полным квадратом, тогда уравнение Пелля (1) *разрешимо в том и только том случае, когда $d = n^2+k$, где $1 \leqslant k \leqslant 2n$ и n, k удовлетворяют равенствам*

$$2n = CQ - 2Pt, \quad k = C^2 - 2Qt, \tag{3}$$

и t таково, что $k > 0$.

Из этой теоремы легко получить новую оценку наименьшего решения уравнения (1) для почти всех d (из тех, для которых уравнение (1) разрешимо). Эта оценка получена в теореме 2, являющейся основным результатом настоящей работы.

Ключевые слова: отрицательное уравнение Пелля, основная единица квадратичного поля, непрерывные дроби.

Теорема 2. *Пусть (U,T) – наименьшее решение уравнения* (1). *Тогда для всех d, удовлетворяющих условию $X<d<2X$, кроме $0(X/\log X)$ возможных исключений справедлива оценка $U+\sqrt{d}T>X^{3/2}/\log^{-2}X$.*

Последняя оценка улучшает для этого случая результат работы [4] (см. также [5]).

В заключительной части работы мы находим явное представление в виде суммы двух квадратов значений d, для которых уравнение 1 разрешимо, через параметры из теоремы 1 (см. Предложение ниже).

Доказательство теоремы 1

Докажем предварительно две леммы.

Лемма 1. *Пусть $P>Q$, $(P,Q)=1$ и разложение P/Q в непрерывную дробь имеет симметричный вид:*

$$P/Q=[r_1,\dots,r_w,r_w,\dots,r_1]. \tag{4}$$

Тогда $P/(Q^2+1)$ и выполнены равенства

$$P=A^2+A'^2 \tag{5}$$
$$Q=AB+A'B', \tag{6}$$
$$C=B^2+B'^2 \tag{7}$$
$$AB'-A'B=(-1)^w, \tag{8}$$

где

$$\begin{gathered} A/B=[r_1,\dots,r_w],\quad A/A'=[r_w,\dots,r_1]\\ A'/B'=[r_1,\dots,r_{w-1}],\quad B/B'=[r_{w-1},\dots,r_1],\\ PC=Q^2+1. \end{gathered} \tag{9}$$

Доказательство. Соотношения (8) и (9) следуют из известных свойств непрерывных дробей (см., например, [6]).

Докажем равенства (5) и (6).

Поскольку A/B является подходящей дробью к P/Q и A/A' – соответствующее неполное частное в разложении (4), имеем

$$P/Q-A/B=\frac{(-1)^{w-1}}{B(BA/A'+B')}.$$

Следовательно,

$$PB - AQ = (-1)^{w-1}A'Q/(AB + A'B')$$

или

$$(AB + A'B')(PB - AQ) = (-1)^{w-1}A'Q.$$

Последнее равенство можно переписать в виде

$$(AB + A'B')PB - A^2BQ = A'Q(AB' + (-1)^{w-1}).$$

С учетом (8) имеем отсюда

$$(AB + A'B')P = Q(A^2 + A'^2).$$

Поскольку $(P, Q) = 1$,

$$AB + A'B' = Qt, \quad A^2 + A'^2 = Pt.$$

Докажем, что $t = 1$. Действительно,

$$\begin{aligned} Q^2t^2 + 1 &= (AB + A'B')^2 + (AB' - A'B)^2 \\ &= (AB)^2 + (A'B')^2 + (AB')^2 + (A'B)^2 \\ &= (A^2 + A'^2)(B^2 + B'^2) = PtC. \end{aligned}$$

Отсюда следует, что $t = 1$ и лемма доказана.

Лемма 2. *Пусть* $P/(Q^2 + 1)$, $P > Q$ *и*

$$P/Q = [r_1, \ldots, r_{v-1}, r_v] = [r_1, \ldots, r_{v-1}, r_v - 1, 1].$$

Тогда то из последних разложений, которое имеет четную длину, является симметричным.

Доказательство. Пусть

$$P/Q = [a_1, \ldots, a_{2w}] \tag{10}$$

Выберем Q' так, что $Q' < P$ и $QQ' \equiv -1 \pmod{P}$, тогда

$$P/Q' = [a_{2w}, \ldots, a_1]. \tag{11}$$

Но $Q^2 \equiv -1 \pmod{P}$. Следовательно, $Q' \equiv Q \pmod{P}$ и $Q' = Q$. Отсюда следует, что разложения (10) и (11) совпадают и лемма доказана.

Доказательство теоремы 1. Пусть уравнение Пелля (1) имеет решение. Тогда, как известно, разложение $\sqrt{d}$ в непрерывную периодическую дробь имеет вид

$$\sqrt{d} = [n, \overline{r_1, \dots, r_w, r_w, \dots, r_1, 2n}]. \tag{12}$$

Найдем P и Q из условия

$$P/Q = [r_1, \dots, r_w, r_w, \dots, r_1].$$

В силу результата леммы 1, $PC = Q^2 + 1$.

Покажем, что P – нечетно.

Из (12) следует, что Q/C является последней подходящей дробью к P/Q.

Так как P/Q является подходящей дробью к $(n + \sqrt{d})/k$, имеем

$$(n + \sqrt{d})/k - P/Q = -1/(Q(n + \sqrt{n + \sqrt{d}}) + Q_{-1}),$$

где Q_{-1} – знаменатель последней подходящей дроби к P/Q, т.е. $Q_{-1} = C$.

Таким образом,

$$nQ - Pk + \sqrt{d}Q = -k/(Qn + C + \sqrt{d}Q)$$

и, значит,

$$Pk - nQ = nQ + C$$

или

$$2nQ - kP = -C, \quad (Qn + C)^2 - dQ^2 = k \tag{13}$$

В действительности, последнее равенство эквивалентно предыдущему, поскольку его можно записать в виде

$$2nQC + C^2 = k(Q^2 + 1).$$

Из (13) следует, в частности, что P – нечетно, так как при четном P мы имели бы четное C, а $PC = Q^2 + 1 \not\equiv 0 \pmod{4}$. Заметим также, что CQ является четным.

При заданных P, Q и C диофантово уравнение (13) имеет решение $k = C^2$ и $2n = CQ$, поскольку при подстановке этих значений имеем

$$CQ^2 - C^2P = C(Q^2 - CP) = -C.$$

Таким образом, все решения этого уравнения имеют вид

$$k = C^2 - 2Qt, \quad n = CQ/2 - Pt \tag{14}$$

при некотором t.

Пусть теперь при заданных P, Q и C, удовлетворяющих условиям теоремы, числа k и n задаются равенствами (14) и $t \leqslant [CQ/2P]$. Покажем прежде всего, что $k \leqslant 2n$. Очевидно, что k и $2n$ удовлетворяют соотношению

$$kP - 2nQ = C.$$

Отсюда следует, что

$$(k - 2n)P + 2n(P - Q) = C.$$

Так как $P > Q > C$, из последнего равенства видно, что $k \leqslant 2n$.

Положим $d = n^2 + k$. Так как $1 \leqslant k \leqslant 2n$, значение d не является полным квадратом. Покажем, что P/Q является подходящей дробью к $(n + \sqrt{d})/k$. Действительно,

$$\begin{aligned}\frac{n+\sqrt{d}}{k} - \frac{P}{Q} &= \frac{nQ - kP + Q\sqrt{d}}{kQ} = \frac{-C - nQ + Q\sqrt{d}}{kQ} \\ &= \frac{Q^2d - C^2 - 2nCQ - n^2Q^2}{kQ(C + nQ + Q\sqrt{d})} = \frac{k(Q^2 - CP)}{kQ(Q(n + \sqrt{d} + C)} \\ &= -\frac{1}{Q(Q(n + \sqrt{d}) + C)}. \end{aligned} \tag{15}$$

Таким образом,

$$\left| \frac{n+\sqrt{d}}{k} - \frac{P}{Q} \right| < \frac{1}{2Q^2}$$

и P/Q действительно является подходящей дробью к $(n+\sqrt{d})/k$. Следовательно,

$$\frac{n+\sqrt{d}}{k} - \frac{P}{Q} = -\frac{1}{Q(Q\alpha + Q_{-1})},$$

где α – приведенная иррациональность определителя d. С учетом (15) имеем $n+\sqrt{d}-\alpha = U$, где U – целое рациональное. Значит, $\alpha = n+\sqrt{d}$ и теорема доказана.

Замечание. Очевидно, что P и Q определяются по d неоднозначно. Если

$$\sqrt{d} = [n, \overline{r_1, \dots, r_w, r_w, \dots, r_1, 2n}]$$

и

$$P/Q = [r_1, \dots, r_w, r_w, \dots, r_1],$$

то те же значения d мы будем иметь и при

$$P_i/Q_i = [r_1, \dots, r_w, r_w, \dots, r_1, 2n, r_1, \dots, r_w, \\ r_w, \dots, r_1, 2n, \dots, r_1, \dots, r_w, r_w, \dots, r_1]$$

где i – нечетно и группа элементов $[r_1, \dots, r_w, r_w, \dots, r_1]$ повторяется i раз.

Доказательство теоремы 2. Пусть $d = n^2 + k$ $(1 \leqslant k \leqslant 2n)$ и

$$\sqrt{d} = [n, \overline{r_1, \dots, r_w, r_w, \dots, r_1, 2n}],$$

где период является наименьшим. Как хорошо известно,

$$U/T = [n, r_1, \dots, r_w, \dots, r_1].$$

Из равенства (10) имеем

$$U = nP + Q, \quad T = nQ + C,$$

где P, Q, C удовлетворяют условиям теоремы 1.

Пусть $X < 2 < 2X$, тогда $\sqrt{X/2} < n < \sqrt{2X}$. Если $U + \sqrt{d}T < X^{3/2}\log^{-2} X$, то $nQ < nP < U < X^{3/2}\log^{-2} X$ и, значит, $Q = O(X\log^{-2} X)$.

Пусть $\mathcal{N}\#(d \leqslant X, Q = O(X\log^{-2} X))$. По теореме 1, каждому значению Q отвечает не более чем $\tau(Q^2+1)$ значений P (и, соответственно, C), где $\tau(m)$ – число различных делителей m.

Зафиксируем Q, P и C. Если $P \leqslant \sqrt{X}$, то поскольку

$$\frac{1}{2}\sqrt{X} \leqslant n = CQ - 2Pt \leqslant \sqrt{2X},$$

каждой тройке (Q,P,C) отвечает $O(\sqrt{X}/P)$ значений t.

Если $P>\sqrt{X}$, то, очевидно, каждой тройке (Q,P,C) отвечает не более чем одно значение t.

Таким образом,

$$\mathcal{N}=O\left(\sum_{Q<\sqrt{X}}\frac{\sqrt{X}}{Q}\tau(Q^2+1)+\sum_{Q<X\log^{-2}X}\tau(Q^2+1)\right)=O(X\log^{-1}X),$$

и теорема доказана.

Негативное уравнение Пелля (1) не может иметь решение, если d не является суммой двух квадратов. Найдем явное представление в таком виде значений d, найденных в теореме 1.

Предложение. *В обозначениях теоремы* 1) имеем

$$d=(\alpha t-\beta)^2+(\gamma t-\delta)^2, \tag{16}$$

где

$$\alpha=A^2-A'^2,\gamma=2AA',\beta=(AB^3-A'B'^3+3BB')/2,\quad \delta=A'B^3+AB'^3.$$

Доказательство. Из теоремы 1 следует, что

$$d=\left(\frac{CQ}{2}-Pt\right)^2+C^2-2Q=P^2t^2-Q(2+CP)t+C^2+\frac{(CQ)^2}{4} \tag{17}$$

(заметим, что поскольку P – нечетно, то CQ является четным числом).

Обозначим через Δ дискриминант этого многочлена относительно t. Тогда

$$\begin{aligned}\Delta=&Q^2(2+CP)^2-C^2(Q^2+4)P^2=Q^2(Q^2+3)^2-(Q^2+4)(Q^2+1)^2\\&=4Q^2+4Q^2CP-4C^2P^2=4Q^2-4CP=-4.\end{aligned}$$

Будем искать представление многочлена (17) в виде (16). Тогда α,γ,β и δ удовлетворяют системе уравнений

$$\alpha^2+\gamma^2=P^2,\quad \alpha\beta+\gamma\delta=\frac{Q(CP+2)}{2},\quad C^2+\frac{(CQ)^2}{4}=\beta^2+\gamma^2. \tag{18}$$

Из последних равенств имеем

$$(\alpha^2+\gamma^2)(\beta^2+\delta^2)-(\alpha\beta+\gamma\delta)^2=(\alpha\delta-\beta\gamma)^2$$
$$=\frac{C^2P^2(Q^2+4)}{4}-\frac{Q^2(CP+2)^2}{4}=\frac{4C^2P^2-4Q^2-4CPQ^2}{4}=1$$

Таким образом система (18) относительно α,β,γ и δ равносильна системе

$$\alpha^2+\gamma^2=P^2, \tag{19}$$
$$\alpha\beta+\gamma\delta=\frac{(CP+2)Q}{2}, \tag{20}$$
$$\alpha\delta-\beta\gamma=\pm1. \tag{21}$$

Уравнение (19) имеет, очевидно, как минимум одно решение

$$\alpha=A^2-A'^2,\quad \gamma=2AA'.$$

Покажем, что при таких α и γ линейная система уравнений (20) и (21) относительно β и δ имеет целочисленное решение при одном из знаков $\pm b$ (21). Определитель этой системы равен $\alpha^2+\gamma^2=P^2$. Пусть для определенности $AB'-A'B=1$ (что соответствует четному w в разложении (12)). Тогда

$$\delta=\begin{vmatrix}\alpha & (CP+2)Q/2\\ -\gamma & 1\end{vmatrix}/P^2=(\alpha+\gamma(CP+2)Q/2)/P^2$$
$$-\gamma CQ/2P+(\gamma Q+\alpha)/P^2.$$

Поскольку

$$\gamma Q+\alpha=P+2AA'Q-2A'^2=P+2A'(A^2B+AB'A'-A')=P+2A'BP,$$

имеем

$$\delta=\frac{\gamma CQ+2+4A'B}{2P}=\frac{AA'CQ+1+2A'B}{P}$$
$$=\frac{C(A^2A'B+AA'^2B')+1+2A'B}{P}$$
$$=\frac{CA'B(A^2+A'^2)+CA'^2+1+2A'B}{P}$$
$$=CA'B+\frac{A'^2B^2+2A'B+1+B'^2A'^2}{P}=CA'B+\frac{A^2B'^2+B'^2A'^2}{P}$$
$$=CA'B+B'^2=A'B^3+A'BB'^2+B'^2=A'B^3+AB'^3.$$

Аналогично,

$$\beta = \begin{vmatrix} (CP+2)Q/2 & \gamma \\ 1 & \alpha \end{vmatrix} / P^2 = \alpha CQ/2P + \frac{\alpha Q - \gamma}{P^2}.$$

Так как

$$\begin{aligned} \frac{\alpha Q - \gamma}{P^2} &= \frac{PQ - 2AA' - 2A'^2 Q}{P^2} = \frac{Q}{P} - \frac{2A'(A + ABA' + A'^2 B')}{P^2} \\ &= \frac{Q}{P} - \frac{2A'(A + A^2 B' - A + A'^2 B')}{P^2} = \frac{Q - 2A'B'}{P} = \frac{AB - A'B'}{P}, \end{aligned}$$

имеем

$$\begin{aligned} \beta &= \frac{\alpha CQ + 2(AB - A'B')}{2P} = \frac{CQ}{2} + \frac{-A'^2 CQ + AB - A'B'}{P} \\ &= \frac{CQ}{2} + \frac{-C(A'^2 AB + A'^3 B') + AB - A'B'}{P} \\ &= \frac{CQ}{2} + \frac{-C(A^2 A'B' + A'^3 B' - AA') + AB - A'B'}{P} \\ &= \frac{CQ}{2} - CA'B' + \frac{CAA' + AB - A'B'}{P} \\ &= \frac{C(AB - A'B')}{2} + \frac{AB(A'B + 1) + A'B'(AB' - 1)}{P} \\ &= \frac{C(AB - A'B')}{2} + \frac{A^2 BB' + A'^2 BB'}{P} = \frac{C(AB - A'B')}{2} + BB' \\ &= \frac{AB^3 + ABB'^2 - A'B'B^2 - A'B'^3 + 2BB'}{2} = \frac{AB^3 - A'B'^3 + 3BB'}{2} \end{aligned}$$

Заметим, что последнее число является целым, так как P – нечетно и, следовательно, A и A' имеют разную четность.

Случай, когда $AB' - A'B = -1$, разбирается аналогично.

Литература

1. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*. Warszawa (1974).
2. V. Blomer, *On the negative Pell equation*. Preprint (2006).
3. E. Fouvry and J. Küners, *On the negative Pell equation*. — To appear in Annals of Mathematics.

4. C. Hooley, *On the Pellian equation an the class number of indefinite binary quadratic forms*. — J. reine und angew. Math. **353** (1984), 98–131.
5. Е. П. Голубева, *О числах классов вещественных квадратичных полей дискриминанта* $4p$. — Зап. научн. семин. ПОМИ **204** (1993), 11–36.
6. Б. А. Венков, *Элементарная теория чисел*. М.–Л. (1937).

Golubeva E. P. On the negative Pell equation.

Let ε be the fundamental unit of a field $Q(\sqrt{d})$. In the paper it is proved that $\varepsilon > d^{3/2}/\log^2 d$ for almost all d such that $N(\varepsilon) = -1$.

Государственный университет
телекоммуникаций им. М. А. Бонч-Бруевича
Наб. Мойки, 61,
191186 С.-Петербург, Россия

E-mail: elena_golubera@mail.ru

Поступило 27 октября 2010 г.