О решении уравнений 2-й степени с двумя неизвестными в целых числах

Докладчик: Владислав Фатеев (11 класс, школа № 11, 2001/2002 уч. год)

Аннотация

В работе излагается один из методов решения диофантовых уравнений 2-й степени с двумя неизвестными. Предлагается новый подход к поиску базовых решений уравнения вида

$$x^2 - Ay^2 = B$$

и приводятся примеры, демонстрирующие преимущество этого подхода в сравнении с уже известными.

Введение

Решение уравнений в целых числах (или, иначе говоря, *диофантовых уравнений*) представляет собой одну из труднейших проблем теории чисел. Такие уравнения могут быть записаны в виде

$$P(x, y, \ldots, z) = 0, \qquad (*)$$

где x, y, …, z — неизвестные, $P(x, y, \ldots, z)$ — некоторый многочлен с целыми коэффициентами. Трудность проблемы состоит в том, что не существует никакого общего алгоритма, который позволил бы по произвольному уравнению $(*)$ выяснить, разрешимо ли оно в целых числах или нет (не говоря уже о том, чтобы найти или как-то описать все решения).

Однако для диофантовых уравнений некоторых специальных типов алгоритмы решения всё же есть. Самый простой тип уравнений $(*)$ — это уравнения 1-й степени или *линейные уравнения*. В случае двух неизвестных алгоритм решения линейного уравнения

$$ax + by + c = 0$$

по существу сводится к хорошо известному *алгоритму Евклида* нахождения НОД (a, b).

В данной работе описывается один из методов решения уравнений 2-й степени с двумя неизвестными. Теория таких уравнений создавалась усилиями многих великих математиков, среди которых следует отметить П. Ферма, Л. Эйлера, Ж. Лагранжа и К. Ф. Гаусса. Ключевым моментом в этой теории является исследование так называемого *уравнения Пелля*

$$x^2 - Ay^2 = 1,$$

где A — целое положительное число, не являющееся точным квадратом. Название «уравнение Пелля» не совсем корректно, однако является уже традиционным (правильнее было бы называть это уравнение «уравнением Ферма», поскольку именно Ферма впервые его детально исследовал).

В §1 мы показываем, как на основе теории уравнения Пелля можно решать уравнения более общего вида

$$x^2 - Ay^2 = B, \qquad (\dagger)$$

где B — целое ненулевое число. Здесь мы также предлагаем новый подход к поиску базовых решений. В §2 излагается один из способов сведения произвольного уравнения 2-й степени с двумя неизвестными к уравнению $(\dagger)$ (в том случае, когда исследование исходного уравнения невозможно более простыми методами). В Приложении мы доказываем основной факт теории уравнений Пелля — утверждение о существовании нетривиального решения.

§1. Решение уравнений вида $x^2 - Ay^2 = B$ в целых числах

В этом параграфе мы изложим алгоритм решения уравнения

$$x^2 - Ay^2 = B, \qquad (1)$$

в целых числах x, y. Здесь A — целое положительное число, не являющееся точным квадратом, B — целое число, отличное от 0. Основой алгоритма служит факт существования у *ассоциированного* уравнения Пелля

$$x^2 - Ay^2 = 1 \qquad (2)$$

решения в целых положительных числах x, y.[1] *Минимальное* из таких решений обозначим через (x_0, y_0).

Пусть (x, y) — произвольное решение уравнения (1), удовлетворяющее условию

$$x + y\sqrt{A} > 0.$$

Тогда существует такое целое число k, что

$$(x_0 + y_0\sqrt{A})^k \sqrt{|B|} \leqslant x + y\sqrt{A} < (x_0 + y_0\sqrt{A})^{k+1}\sqrt{|B|}. \tag{3}$$

Определим целые числа x_*, y_* равенством

$$x_* + y_*\sqrt{A} = (x + y\sqrt{A})(x_0 + y_0\sqrt{A})^{-k} = (x + y\sqrt{A})(x_0 - y_0\sqrt{A})^k.$$

Ясно, что (x_*, y_*) — решение уравнения (1), причем из (3) следует, что

$$\sqrt{|B|} \leqslant x_* + y_*\sqrt{A} < (x_0 + y_0\sqrt{A})\sqrt{|B|}. \tag{4}$$

Заметим, что имеется лишь *конечное число* решений (x_*, y_*) уравнения (1), удовлетворяющих условию (4). Действительно, так как

$$x_* - y_*\sqrt{A} = \frac{B}{x_* + y_*\sqrt{A}},$$

то, очевидно,

$$x_* = \frac{1}{2}\left(x_* + y_*\sqrt{A} + \frac{B}{x_* + y_*\sqrt{A}}\right), \quad y_* = \frac{1}{2\sqrt{A}}\left(x_* + y_*\sqrt{A} - \frac{B}{x_* + y_*\sqrt{A}}\right), \tag{5}$$

откуда ввиду (4) и следует ограниченность чисел x_* и y_*.

Более точно, неравенства (4) равносильны неравенствам

$$\sqrt{B} \leqslant x_* < x_0\sqrt{B}, \quad 0 \leqslant y_* < y_0\sqrt{B},$$

если $B > 0$, и неравенствам

$$0 \leqslant x_* < y_0\sqrt{A}\sqrt{|B|}, \quad \frac{\sqrt{|B|}}{\sqrt{A}} \leqslant y_* < \frac{x_0\sqrt{|B|}}{\sqrt{A}},$$

если $B < 0$.[2] Поэтому на практике можно перебирать все целые значения y_* в указанных пределах, проверяя при этом, является ли число $x_* = \sqrt{Ay_*^2 + B}$ целым.

Пусть (x_j, y_j) $(1 \leqslant j \leqslant r)$ — все попарно различные решения уравнения (1), удовлетворяющие условию (4) (в дальнейшем такие решения называются *базовыми*). Для $1 \leqslant j \leqslant r$ обозначим через $\pm S_j$ множество всех пар $(x_j^{(k)}, y_j^{(k)})$, где k пробегает множество целых чисел $\mathbb{Z}$, а числа $x_j^{(k)}$, $y_j^{(k)}$ определяются из равенства

$$x_j^{(k)} + y_j^{(k)}\sqrt{A} = \pm(x_j + y_j\sqrt{A})(x_0 + y_0\sqrt{A})^k.$$

[1] В Приложении мы приведем одно из доказательств этого факта.

[2] Для доказательства этого утверждения нужно воспользоваться равенствами (5), а также монотонным возрастанием функции $t + B/t$ при $t \geqslant \sqrt{|B|}$.

Множество $\pm S_j$ $(1 \leqslant j \leqslant r)$ будем называть *серией* решений уравнения (1). Всего имеется, таким образом, $2r$ серий. Из сказанного выше следует, что множество всех решений уравнения (1) в целых числах представляется в виде

$$\bigcup_{j=1}^{r} \pm S_j.$$

Легко видеть, что различные серии не имеют общих решений. Кроме того, в любой серии $+S_j$ одновременное выполнение неравенств

$$x_j^{(k)} \geqslant 0, \quad y_j^{(k)} \geqslant 0$$

возможно тогда и только тогда, когда $k \geqslant 0$. Если $+S_j^+$ — «укороченные» этим условием серии $+S_j$, то множество всех решений уравнения (1) в целых неотрицательных числах есть

$$\bigcup_{j=1}^{r} +S_j^+.$$

Ещё раз скажем, что нахождение всех серий $\pm S_j$ $(1 \leqslant j \leqslant r)$ может быть осуществлено (во всяком случае, принципиально) за конечное число шагов. Возможен случай $r = 0$, он означает, что уравнение (1) неразрешимо в целых числах.

Обычно базовые решения уравнения (1) определяются условием

$$1 \leqslant x_* + y_*\sqrt{A} < \varepsilon, \quad \varepsilon = x_0 + y_0\sqrt{A} \tag{4*}$$

(см., например, [1, с. 342]). Однако применение условия (4) вместо (4*) иногда может оказаться более целесообразным. Так, например, можно сразу, без дополнительного исследования указать все решения уравнения (1) в целых неотрицательных числах. Вообще же, базовые решения уравнения (1) можно искать, исходя из условия

$$q \leqslant x_* + y_*\sqrt{A} < q\varepsilon \tag{4**},$$

где $q > 0$ — некоторое фиксированное число. Можно показать, что наиболее узкий промежуток возможных значений y_* получается при

$$q = \sqrt{\frac{|B|}{\varepsilon}}.$$

При так выбранном q в случае $B > 0$ будем иметь

$$\frac{\sqrt{B}}{2\sqrt{A}}\,(\varepsilon^{-1/2} - \varepsilon^{1/2}) \leqslant y_* < \frac{\sqrt{B}}{2\sqrt{A}}\,(\varepsilon^{1/2} - \varepsilon^{-1/2}), \quad x_* = \sqrt{Ay_*^2 + B},$$

а при $B < 0$ — соответственно

$$\frac{\sqrt{|B|}}{\sqrt{A}} \leqslant y_* < \frac{\sqrt{|B|}}{2\sqrt{A}}\,(\varepsilon^{1/2} + \varepsilon^{-1/2}), \quad x_* = \pm\sqrt{Ay_*^2 + B},$$

а также

$$y_* = \frac{\sqrt{|B|}}{2\sqrt{A}}\,(\varepsilon^{1/2} + \varepsilon^{-1/2}), \quad x_* = -\sqrt{Ay_*^2 + B}.$$

Рассмотрим несколько примеров, иллюстрирующих предложенный выше алгоритм.

Пример 1. Пусть $B = 1$ (уравнение Пелля). В этом случае условие (4), как нетрудно заметить, выполнено только для одного решения уравнения (1), а именно $(x_*, y_*) = (1, 0)$. Таким образом, здесь $r = 1$.

Пример 2. Пусть $B = -1$. Тогда любое решение (x_*, y_*) уравнения (1), для которого выполнено условие (4), удовлетворяет равенству

$$(x_* + y_*\sqrt{A})^2 = x_0 + y_0\sqrt{A}, \tag{6}$$

при этом $x_* > 0$, $y_* > 0$. Обратно, если целые положительные числа x_*, y_* удовлетворяют равенству (6), то (x_*, y_*) — решение уравнения (1), удовлетворяющее условию (4). Таким образом, либо $r = 1$, либо $r = 0$ (в зависимости от разрешимости уравнения (6) в целых положительных числах x_*, y_*). Оба варианта реализуются: первый, например, при $A = 2$ (имеем $x_0 = 3$, $y_0 = 2$ и $x_* = 1$, $y_* = 1$), второй — при $A = 3$.

Пример 3. Рассмотрим уравнение

$$x^2 - 2y^2 = 17.$$

Здесь $A = 2$, $B = 17$ и $x_0 = 3$, $y_0 = 2$. Условие (4) принимает вид

$$\sqrt{17} \leqslant x_* + y_*\sqrt{2} < (3 + 2\sqrt{2})\sqrt{17}$$

или, в эквивалентной форме,

$$\sqrt{17} \leqslant x_* < 3\sqrt{17}, \quad 0 \leqslant y_* < 2\sqrt{17}.$$

Перебирая пары целых чисел x_*, y_* в указанных пределах, найдем два базовых решения ($r = 2$):

$$(x_1, y_1) = (5, 2), \quad (x_2, y_2) = (7, 4).$$

Таким образом, данное уравнение имеет четыре серии решений $\pm S_1$, $\pm S_2$. Все решения (x, y) можно найти из формул

$$x + y\sqrt{2} = \pm(5 + 2\sqrt{2})(3 + 2\sqrt{2})^k, \quad x + y\sqrt{2} = \pm(7 + 4\sqrt{6})(3 + 2\sqrt{2})^k,$$

где $k \in \mathbb{Z}$.[3)]

В следующих двух примерах исследуются *параметрические* уравнения (1) — с коэффициентами A и B, зависящими от некоторого целочисленного параметра.

Пример 4. Для каждого целого $d \geqslant 2$ решим уравнение

$$x^2 - (d^2 - 1)y^2 = d$$

в целых числах x, y.

Имеем $A = d^2 - 1$, $B = d$. Легко видеть, что $x_0 = d$, $y_0 = 1$, поэтому

$$\varepsilon = d + \sqrt{d^2 - 1}.$$

[3)] Между прочим, из полученных формул вытекает, что для любого решения (x, y) в целых положительных числах имеет место одно из сравнений $x \equiv 5 \pmod 8$ или $x \equiv 7 \pmod 8$. В частности, число x *не может быть точным квадратом*, а значит, уравнение $x^4 - 2y^2 = 17$ неразрешимо в целых числах — факт, который без этой теории получить не так-то просто.

В данном случае условие (4) непригодно для поиска базовых решений. Если же воспользоваться условием ($4^{\star\star}$), то нетрудно получить при любом $d \geqslant 2$ оценку $|y_*| < 1$. Значит, $y_* = 0$. Но тогда $x_*^2 = d$, т. е. число d должно быть точным квадратом.

Таким образом, при $d = l^2$ приходим к двум сериям решений:

$$x + y\sqrt{l^4 - 1} = \pm l(l^2 + \sqrt{l^4 - 1})^k,$$

где $k \in \mathbb{Z}$. Если d не является точным квадратом, то решений нет.

Пример 5. Покажем, что при целом $d \geqslant 2$ уравнение

$$x^2 - (d^2 + 2)y^2 = -3$$

неразрешимо в целых числах x, y.

Прежде всего заметим, что пара чисел $(d^2 + 1, d)$ является одним из решений ассоциированного уравнения Пелля. Более того, это решение является минимальным. Действительно, если $\varepsilon < d^2 + 1 + d\sqrt{d^2 + 2}$, то будем иметь

$$d^2 + 1 + d\sqrt{d^2 + 2} = \varepsilon^k = (x_0 + y_0\sqrt{d^2 + 2})^k \geqslant (x_0 + y_0\sqrt{d^2 + 2})^2 > y_0^2(d^2 + 2).$$

Значит, $y_0 = 1$, но тогда $x_0^2 - d^2 = 3$, что при $d \geqslant 2$ невозможно. Итак,

$$\varepsilon = d^2 + 1 + d\sqrt{d^2 + 2}.$$

Нетрудно понять, что применение условий (4) и ($4^{\star}$) здесь окажется неэффективным. Если же воспользоваться наиболее сильным условием ($4^{\star\star}$), то получим $y_* = 1$ при любом $d \geqslant 2$. Однако, как легко проверить, это невозможно.

§2. Общее уравнение $au^2 + buv + cv^2 + du + ev + f = 0$

Опишем теперь метод решения в целых числах произвольного уравнения 2-й степени с двумя неизвестными (метод *выделения полных квадратов по Лагранжу*, см. [2, с. 402]). Общее уравнение 2-й степени с двумя неизвестными

$$au^2 + buv + cv^2 + du + ev + f = 0 \tag{7}$$

при условии $a \neq 0$, $b^2 - 4ac \neq 0$ может быть приведено к виду (1), где

$$A = b^2 - 4ac, \quad B = (bd - 2ae)^2 - (b^2 - 4ac)(d^2 - 4af),$$

при этом $x = (b^2 - 4ac)v + bd - 2ae$, $y = 2au + bv + d$. Таким образом, любое решение (u, v) уравнения (7) находится по формулам

$$u = \frac{-bx + (b^2 - 4ac)y - 2a(be - 2dc)}{2a(b^2 - 4ac)}, \quad v = \frac{x - bd + 2ae}{b^2 - 4ac},$$

где (x, y) — решение уравнения (1), удовлетворяющее системе сравнений

$$\begin{cases} x \equiv bd - 2ae \pmod{b^2 - 4ac}, \\ -bx + (b^2 - 4ac)y \equiv 2a(be - 2dc) \pmod{2a(b^2 - 4ac)}. \end{cases} \tag{8}$$

Далее мы будем считать, что $a > 0$, $b^2 - 4ac > 0$, причем $b^2 - 4ac$ не является точным квадратом (остальные случаи либо сводятся к этому, либо исследуются более простым образом). Обозначим

$$m = 2a(b^2 - 4ac).$$

Система сравнений (8) эквивалентна совокупности m пар сравнений

$$x \equiv bd - 2ae + (b^2 - 4ac)p \pmod{m}, \quad y \equiv d + bp + 2aq \pmod{m},$$

где $0 \leqslant p < 2a$, $0 \leqslant q < b^2 - 4ac$. Для отбора нужных решений (x, y) в сериях $\pm S_j$ можно воспользоваться *периодичностью* последовательности пар остатков

$$(x_j^{(k)} \bmod m, y_j^{(k)} \bmod m)$$

от деления чисел $x_j^{(k)}$ и $y_j^{(k)}$ на m. Этот факт периодичности основан на следующем утверждении.

Лемма 1. *Пусть m — произвольное натуральное число, а числа X_k, Y_k определены равенством*

$$X_k + Y_k\sqrt{A} = (x_0 + y_0\sqrt{A})^k \quad (k \in \mathbb{Z}).$$

Тогда последовательность пар остатков $(X_k \bmod m, Y_k \bmod m)$ является чисто периодической с наименьшим периодом k_0, где k_0 — наименьшее из натуральных чисел k, удовлетворяющих сравнениям

$$X_k \equiv 1 \pmod{m}, \quad Y_k \equiv 0 \pmod{m}. \tag{9}$$

Доказательство. Поскольку пар остатков при делении на m имеется в точности m^2, найдутся такие неравные числа k', k'' из $\{0, 1, \ldots, m^2\}$, что

$$X_{k'} \equiv X_{k''} \pmod{m}, \quad Y_{k'} \equiv Y_{k''} \pmod{m}.$$

Считая $k' > k''$, докажем, что условие (9) выполнено при $k = k' - k''$. Действительно, так как

$$X_{k'-k''} + Y_{k'-k''}\sqrt{A} = (X_{k'} + Y_{k'}\sqrt{A})(X_{-k''} + Y_{-k''}\sqrt{A}) = (X_{k'} + Y_{k'}\sqrt{A})(X_{k''} - Y_{k''}\sqrt{A}) =$$
$$= X_{k'}X_{k''} - AY_{k'}Y_{k''} + (-X_{k'}Y_{k''} + X_{k''}Y_{k'})\sqrt{A},$$

то имеем

$$X_{k'-k''} = X_{k'}X_{k''} - AY_{k'}Y_{k''} \equiv X_{k'}^2 - AY_{k'}^2 = 1 \pmod{m},$$
$$Y_{k'-k''} = -X_{k'}Y_{k''} + X_{k''}Y_{k'} \equiv 0 \pmod{m}.$$

Итак, существуют натуральные числа k, удовлетворяющие условию (9). Пусть k_0 — наименьшее из таких k. Осталось убедиться в том, что

$$X_{k+k_0} \equiv X_k \pmod{m}, \quad Y_{k+k_0} \equiv Y_k \pmod{m}$$

для любого целого k. В самом деле,

$$X_{k+k_0} = X_kX_{k_0} + AY_kY_{k_0} \equiv X_k \pmod{m}, \quad Y_{k+k_0} = X_kY_{k_0} + X_{k_0}Y_k \equiv Y_k \pmod{m},$$

поскольку $X_{k_0} \equiv 1 \pmod{m}$, $Y_{k_0} \equiv 0 \pmod{m}$. □

Замечание 1. Для наименьшего периода k_0 очевидно неравенство $k_0 \leqslant m^2$.

Продемонстрируем на нескольких примерах указанную выше схему решения уравнения (7). Первый из этих примеров взят из «Арифметических исследований» К. Ф. Гаусса (см. [2, с. 405] или [3]).

Пример 6. Уравнение

$$u^2 + 8uv + v^2 + 2u - 4v + 1 = 0$$

приводится к уравнению

$$x^2 - 60y^2 = 576 \tag{10}$$

подстановкой $u = (-2x + 15y + 18)/30$, $v = (x - 24)/60$. Вычисления дают $(x_0, y_0) = (31, 4)$,

$$(x_1, y_1) = (24, 0), \quad (x_2, y_2) = (96, 12),$$

так что уравнение (10) имеет четыре серии решений $\pm S_1$, $\pm S_2$. Нас интересуют те решения (x, y), которые удовлетворяют хотя бы одной паре сравнений

$$x \equiv 24 + 60p \pmod{120}, \quad y \equiv 2 + 8p + 2q \pmod{120},$$

где p, q — целые числа, $0 \leqslant p \leqslant 1$, $0 \leqslant q \leqslant 59$. Это, как можно проверить, имеет место для всех решений из серий $+S_1$ и $-S_2$, а в сериях $-S_1$ и $+S_2$ таких решений нет.

Пример 7. Уравнение

$$3u^2 + 11uv + 9v^2 + u + v = 0$$

подстановкой

$$u = \frac{-11x + 13y + 42}{78}, \quad v = \frac{x - 5}{13} \tag{11}$$

сводится к уравнению

$$x^2 - 13y^2 = 12.$$

Имеем $(x_0, y_0) = (649, 180)$,

$$\begin{array}{lll} (x_1, y_1) = (5, 1), & (x_2, y_2) = (8, 2), & (x_3, y_3) = (47, 13), \\ (x_4, y_4) = (83, 23), & (x_5, y_5) = (512, 142), & (x_6, y_6) = (905, 251). \end{array}$$

В сериях $\pm S_j$ $(1 \leqslant j \leqslant 6)$ нужно отобрать решения, удовлетворяющие хотя бы одной паре сравнений

$$x \equiv 5 + 13p \pmod{78}, \quad y \equiv 1 + 11p + 6q \pmod{78}$$

где p, q — целые числа, $0 \leqslant p \leqslant 5$, $0 \leqslant q \leqslant 12$. Серии $\pm S_2$, $\pm S_4$, $\pm S_6$ указанных решений не содержат, а в каждой из серий $\pm S_1$, $\pm S_3$, $\pm S_5$ такие решения есть (см. таблицу).

Серия	$k \bmod 2$
$+S_1$	0
$-S_1$	1
$+S_3$	1
$-S_3$	0
$+S_5$	0
$-S_5$	1

Найдём какое-нибудь частное решение рассматриваемого уравнения. Для этого возьмём, например, решение

$$(x, y) = (-181431272927, 50319981347)$$

из серии $-S_3$, имеющее номер $k = -4$. По формулам (11) получим решение

$$(u, v) = (33973125125, -13956251764)$$

исходного уравнения.

Замечание 2. На практике целесообразно сначала определить наименьший период k_0 (см. лемму 1), а затем для каждой из серий $\pm S_j$ выписать решения

$$(x_j^{(k)}, y_j^{(k)}), \quad k = 0, 1, \ldots, k_0 - 1,$$

и отобрать среди них те, которые удовлетворяют системе сравнений (8). В приведённых выше примерах $k_0 = 30$ (пример 5) и $k_0 = 26$ (пример 7).

Список литературы

[1] *Хассе Г.* Лекции по теории чисел. М.: ИЛ, 1953.

[2] *Эдвардс Г.* Последняя теорема Ферма. М.: Мир, 1980.

[3] *Гаусс К.Ф.* Труды по теории чисел. М.: Изд-во АН СССР, 1959.

[4] *Бугаенко В.О.* Уравнения Пелля. М.: МЦНМО, 2001.

[5] *Гельфонд А.О.* Решение уравнений в целых числах. М.: Наука, 1983.

[6] *Виноградов И.М.* Основы теории чисел. М.: Наука, 1981.

[7] *Боревич З.И., Шафаревич И.Р.* Теория чисел. М.: Наука, 1985.

Приложение

Исследование уравнения (7) существенным образом опирается на утверждение о существования решения уравнения (2) в целых положительных числах. Ниже мы приводим доказательство этого факта, основанное на так называемой *лемме Минковского о выпуклом теле.*[4)] Сформулируем её для случая плоских множеств.

Лемма 2. *Пусть $X \subset \mathbb{R}^2$ — выпуклое ограниченное центрально-симметричное множество площади $S(X)$. Пусть также $L \subset \mathbb{R}^2$ — решётка с площадью фундаментального параллелограмма Δ, имеющая одним из своих узлов центр множества X. Если $S(X) > 4\Delta$, то множество X содержит ещё хотя бы один узел решетки L.*

[4)] Имеется и другое доказательство, которое связано с разложением числа $\sqrt{A}$ в *непрерывную дробь* (см. [1, с. 317], [5, с. 37], а также [6, с. 83]). Впрочем, говоря о различных доказательствах, мы имеем в виду лишь различие в доказательстве следующей далее леммы 3.

Доказательство. Оно состоит в том, чтобы, рассуждая от противного, рассмотреть всевозможные сдвиги множества X на векторы $v \in 2L$ и заметить, что все эти множества попарно не пересекаются. (См., например, [4, с. 18], а также [7, с. 129], где доказательство дано в n-мерном случае.) □

Нам понадобится еще одно вспомогательное утверждение.

Лемма 3. *Для любого натурального числа A, не являющегося точным квадратом, существует такое целое число $B \neq 0$, что уравнение $x^2 - Ay^2 = B$ имеет бесконечно много решений в целых неотрицательных числах x, y.*

Доказательство. Рассмотрим решётку

$$L = \{(x + y\sqrt{A}, x - y\sqrt{A}) \in \mathbb{R}^2 : (x, y) \in \mathbb{Z}^2\}.$$

Её фундаментальный параллелограмм образован векторами $(1, 1)$ и $(\sqrt{A}, -\sqrt{A})$ и имеет площадь $\Delta = 2\sqrt{A}$. Пусть $s > 0$ и Π_k $(k = 1, 2, \dots)$ — прямоугольник

$$\{(\xi, \eta) \in \mathbb{R}^2 : |\xi| < (s/4)^k, |\eta| < (s/4)^{1-k}\}.$$

Имеем $S(\Pi_k) = s$ для любого k. Выберем число s так, чтобы $s > 4\Delta$. По лемме 2 в каждом из прямоугольников Π_k найдётся отличный от $(0, 0)$ узел

$$\beta_k = (x_k + y_k\sqrt{A}, x_k - y_k\sqrt{A})$$

решётки L. Нетрудно видеть, что $\beta_k \neq \beta_l$ при $k \neq l$. Действительно, если какой-то узел $\beta = (x + y\sqrt{A}, x - y\sqrt{A}) \neq (0, 0)$ решетки L принадлежит сразу двум прямоугольникам Π_k и Π_l, причём $k > l$, то $|x + y\sqrt{A}| < (s/4)^l$, $|x - y\sqrt{A}| < (s/4)^{1-k}$, откуда

$$|x^2 - Ay^2| = |x + y\sqrt{A}| \cdot |x - y\sqrt{A}| < (s/4)^{l+1-k} \leqslant 1,$$

т. е. $|x^2 - Ay^2| < 1$. Но это невозможно, так как число $|x^2 - Ay^2|$ — целое положительное.

Итак, для любого k найдётся пара (x_k, y_k) целых чисел с условием

$$|x_k^2 - Ay_k^2| = |x_k + y_k\sqrt{A}| \cdot |x_k - y_k\sqrt{A}| < (s/4)^k \cdot (s/4)^{1-k} = s/4,$$

при этом разным k соответствуют разные пары (x_k, y_k). Теперь очевидно, что существует целое число B, удовлетворяющее условию $0 < |B| < s/4$ и обладающее свойством: равенство $x_k^2 - Ay_k^2 = B$ имеет место для бесконечно многих k. Тем самым утверждение леммы доказано. □

Для доказательства интересующего нас факта заметим, что если при некотором $B \neq 0$ уравнение $x^2 - Ay^2 = B$ имеет бесконечно много решений в целых неотрицательных числах (что гарантируется леммой 3), то среди них найдутся два таких, скажем, (x', y') и (x'', y''), для которых имеют место сравнения

$$x' \equiv x'' \pmod{|B|}, \quad y' \equiv y'' \pmod{|B|}. \tag{i}$$

Рассмотрим пару чисел (z, w), определённую равенством

$$z + w\sqrt{A} = \frac{x' + y'\sqrt{A}}{x'' + y''\sqrt{A}}.$$

Ясно, что $z^2 - Aw^2 = 1$. Кроме того, числа z, w являются целыми. В самом деле, имеем

$$z = \frac{x'x'' - Ay'y''}{B}, \quad w = \frac{-x'y'' + x''y'}{B},$$

а из сравнений (i) следует, что

$$x'x'' - Ay'y'' \equiv (x')^2 - A(y')^2 = B \equiv 0 \pmod{|B|}, \quad -x'y'' + x''y' \equiv 0 \pmod{|B|}.$$

Наконец, замечая, что пара (z, w) отлична от $(\pm 1, 0)$ и заменяя при необходимости z на $|z|$, а w — на $|w|$, мы получим решение уравнения $x^2 - Ay^2 = 1$ в целых положительных числах.