3.4.1. Простейшие диофантовы уравнения и сравнения первой степени

Предположим, что $\frac{P_k}{Q_k}$ — последняя подходящая дробь в представлении непрерывной дробью рационального числа $\frac{a}{b}$, где НОД$(a, b) = 1$. Тогда $a = P_k$, $b = Q_k$. Перепишем выражение (3.6) для соседних подходящих дробей: $a \cdot (-1)^{k-1} Q_{k-1} - b \cdot (-1)^{k-1} P_{k-1} = 1$. Получаем одно решение диофантова уравнения $ax - by = 1$: $x_0 = (-1)^{k-1} Q_{k-1}$, $y_0 = (-1)^{k-1} P_{k-1}$.

Остальные решения имеют вид

$$x = (-1)^{k-1} Q_{k-1} + bt, y = (-1)^{k-1} P_{k-1} + at, \; t \in \mathbb{Z}.$$

В общем случае диофантово уравнение $ax - by = c$ разрешимо, если число c делится на НОД(a, b); решение имеет вид

$$x = (-1)^{k-1} \frac{c}{\text{НОД}(a,b)} Q_{k-1} + bt, \quad y = (-1)^{k-1} \frac{c}{\text{НОД}(a,b)} P_{k-1} + at, \quad t \in \mathbb{Z}.$$

Пример 3.12. Решим диофантово уравнение $31x - 23y = 11$. Поскольку 11 делится на НОД$(31, 23) = 1$, решение существует. Заполняем таблицу:

k	-1	0	1	2	3
a_k		1	2	1	7
P_k	1	1	3	4	31
Q_k	0	1	2	3	23

Значит, $k = 3$, $\frac{P_2}{Q_2} = \frac{4}{3}$. Находим решение: $x = (-1)^2 \cdot 11 \cdot 3 + 23t = 33 + 23t, y = (-1)^2 \cdot 11 \cdot 4 + 31t = 44 + 31t$, где $t \in \mathbb{Z}$.

Проверка: $31 \cdot (33 + 23t) - 23 \cdot (44 + 31t) = 31 \cdot 33 + 31 \cdot 23t - 23 \cdot 44 - 23 \cdot 31t = 31 \cdot 33 - 23 \cdot 44 = 11$. □

Пример 3.13. Решим диофантово уравнение $655x - 115y = 700$. Поскольку 700 делится на НОД(655, 115) = 5, решение существует. Заполняем таблицу:

k	–1	0	1	2	3	4
a_k		5	1	2	3	2
P_k	1	5	6	17	57	131
Q_k	0	1	1	3	10	23

Значит, $k = 4$, $\frac{P_3}{Q_3} = \frac{57}{10}$. Находим решение:

$$x = (-1)^3 \cdot 140 \cdot 10 + 115t = -1400 + 115t,$$

$$y = (-1)^3 \cdot 140 \cdot 57 + 655t = -7980 + 655t,$$

где $t \in \mathbb{Z}$.

Проверка: $655 \cdot (-1400 + 115t) - 115 \cdot (-7980 + 655t) = -655 \cdot 1400 + 655 \cdot 115t + 115 \cdot 7980 - 115 \cdot 655t = -917000 + 917700 = 700$. □

Аналогично решаются сравнения первой степени вида $ax \equiv b \pmod m$. Для этого достаточно взять обе части диофантова уравнения $ax - my = b$ по модулю m. Как уже говорилось в главе 1, это сравнение разрешимо только тогда, когда b делится на НОД(a, m). Решение имеет вид

$$x \equiv (-1)^{k-1} \frac{b}{\text{НОД}(a, m)} Q_{k-1} \pmod m.$$

3.4.2. Уравнение Пелля

Определение 3.7. *Уравнением Пелля* называется диофантово уравнение вида

$$x^2 - Ny^2 = 1, \tag{3.10}$$

где натуральное число N свободно от квадратов.

Теорема 3.7. Для данного иррационального числа α существует бесконечно много пар таких взаимно простых целых чисел x, y, что $\left|\frac{x}{y}-\alpha\right|<\frac{1}{y^2}, y>0.$

Лемма 3.8. Если натуральное число N свободно от квадратов, то существует такое число $c>0$, что неравенство $\left|x^2-Ny^2\right|<c$ имеет бесконечно много целочисленных решений (x, y).

Теорема 3.9. Уравнение (3.10) имеет бесконечно много решений в целых числах. Кроме того, существует такое решение (x_1, y_1), что каждое другое решение (x_k, y_k) задается соотношением

$$x_k+y_k\sqrt{N}=\pm(x_1+y_1\sqrt{N})^k. \qquad (3.11)$$

Упорядочим множество решений уравнения Пелля: будем говорить, что решение (x, y) больше, чем решение (u, v), если $x+y\sqrt{N}>u+v\sqrt{N}$. Пусть (x_1, y_1) — наименьшее решение с положительными x_1, y_1 (оно называется *фундаментальным*). Покажем, что для любого другого решения (u, v) с положительными u, v выполняется равенство $u+v\sqrt{N}=(x_1+y_1\sqrt{N})^k$ для некоторого целого числа k. Выберем целое число k так, чтобы

$$(x_1+y_1\sqrt{N})^k<u+v\sqrt{N}<(x_1+y_1\sqrt{N})^{k+1}.$$

Тогда

$$1<(x_1-y_1\sqrt{N})^k(u+v\sqrt{N})<x_1+y_1\sqrt{N},$$

поскольку $x_1-y_1\sqrt{N}=\frac{1}{x_1+y_1\sqrt{N}}$.

Обозначим $U+V\sqrt{N}=(x_1-y_1\sqrt{N})^k(u+v\sqrt{N})$. Пара (U, V) является решением уравнения Пелля, причем $1<U+V\sqrt{N}<x_1+y_1\sqrt{N}$. Так как $U+V\sqrt{N}>0$ и $U-V\sqrt{N}=\dfrac{1}{U+V\sqrt{N}}>0$, получаем $U>0$. Кроме того, $U-V\sqrt{N}=\dfrac{1}{U+V\sqrt{N}}<1$, то есть $V\sqrt{N}>U-1\geq 0$ и $V>0$. Получили решение (U, V) с положительными U, V, меньшее, чем фундаментальное. Противоречие.

Если решение (u, v) уравнения Пелля таково, что $u>0$, $v<0$, то

$$\frac{1}{u+v\sqrt{N}}=u-v\sqrt{N}=(x_1+y_1\sqrt{N})^k$$

для некоторого целого k (поскольку $-v>0$) и $u+v\sqrt{N}=(x_1+y_1\sqrt{N})^{-k}$.

При $u<0$, $v>0$ и $u<0$, $v<0$ получаем $-(x_1+y_1\sqrt{N})^{\pm k}$ для $k\in\mathbb{Z}$. □

Фундаментальное решение можно найти, раскладывая $\sqrt{N}$ в непрерывную дробь (*метод Браункера*) [2]: если $\frac{P_k}{Q_k}$ — подходящие дроби для непрерывной дроби

$$\sqrt{N} = [a_0; \{a_1, a_2, \ldots, a_n, 2a_0\}],$$

то при нечетном n решением будет пара (P_n, Q_n), при четном n — пара (P_{2n+1}, Q_{2n+1}).

Пример 3.14. Решим уравнение $x^2 - 34y^2 = 1$. Раскладываем число $\sqrt{34}$ в непрерывную дробь:

$$\sqrt{34} = 5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{10 + \ddots}}}},$$

то есть $a_0 = 5$, $a_1 = 1$, $a_2 = 4$, $a_3 = 1$ и $n = 3$ — нечетное число. Вычисляем подходящие дроби: $\frac{P_0}{Q_0} = \frac{5}{1}$, $\frac{P_1}{Q_1} = \frac{6}{1}$, $\frac{P_2}{Q_2} = \frac{29}{5}$, $\frac{P_3}{Q_3} = \frac{35}{6}$. Значит, $x_1 = 35$, $y_1 = 6$.

Проверка: $35^2 - 34 \cdot 6^2 = 1225 - 1224 = 1$.

Решениями будут также пары (2449, 420), (171395, 29394), (11995201, 2057160), (839492675, 143971806), …, определяемые из соотношения (3.11). □

Пример 3.15. Решим уравнение $x^2 - 29y^2 = 1$. Раскладываем число $\sqrt{29}$ в непрерывную дробь:

$$\sqrt{29} = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \ddots}}}}},$$

то есть $a_0 = 5$, $a_1 = 2$, $a_2 = a_3 = 1$, $a_4 = 2$ и $n = 4$ — четное число, $2n + 1 = 9$.

Вычисляем подходящие дроби:

$$\frac{P_0}{Q_0} = \frac{5}{1}, \quad \frac{P_1}{Q_1} = \frac{11}{2}, \quad \frac{P_2}{Q_2} = \frac{16}{3}, \quad \frac{P_3}{Q_3} = \frac{27}{5}, \quad \frac{P_4}{Q_4} = \frac{70}{13}, \quad \frac{P_5}{Q_5} = \frac{727}{135},$$

$$\frac{P_6}{Q_6} = \frac{1524}{283}, \quad \frac{P_7}{Q_7} = \frac{2251}{418}, \quad \frac{P_8}{Q_8} = \frac{3775}{701}, \quad \frac{P_9}{Q_9} = \frac{9801}{1820}.$$

Значит, $x_1 = 9801$, $y_1 = 1820$.

Проверка: $9801^2 - 29 \cdot 1820^2 = 96059601 - 96059600 = 1$.

Решениями будут также пары

(192119201, 35675640),

(3765920568201, 699313893460),

(73819574785756801, 13707950903927280),

(1447011301184484245001, 268703252919468649100), …,

определяемые из соотношения (3.11). □