

вить значения  $X$  и  $Y$  вместо  $x$  и  $y$ . А именно,

$$\begin{aligned}(x+2y)^2 - 2(x+y)^2 &= \\ &= x^2 + 4xy + 4y^2 - 2(x^2 + 2xy + y^2) = \\ &= 2y^2 - x^2 = -(x^2 - 2y^2).\end{aligned}$$

Как видите, если  $x^2 - 2y^2 = \pm 1$ , то  $X^2 - 2Y^2 = \mp 1$ . Теорема 1 доказана, мы научились строить «новое» решение из «старого».

А вот доказательство теоремы 2 хотя и не очень сложно, но требует привлечения идеи, которая слишком важна, чтобы говорить о ней мимоходом. Поэтому мы займемся этим позже, а пока посмотрим, как для решения уравнения Пелля можно использовать иррациональные числа.

### Упражнения

1. Рассмотрим последовательности  $x_0 = 1$ ,  $x_1 = 1$ ,  $x_2 = 3$ ,  $x_3 = 7$ ,  $x_4 = 17$ , ... и  $y_0 = 0$ ,  $y_1 = 1$ ,  $y_2 = 2$ ,  $y_3 = 5$ ,  $y_4 = 12$ , ..., заданные своими первыми членами  $x_0 = 1$ ,  $y_0 = 0$  и рекуррентными соотношениями  $x_{n+1} = x_n + 2y_n$  и  $y_{n+1} = x_n + y_n$ .

2. Докажите, что  $x_{n+2} = 2x_{n+1} + x_n$  и  $y_{n+2} = 2y_{n+1} + y_n$ . По правилам нового танца надо делать либо шаг вперед, либо два шага вперед, либо два шага вперед и сразу же шаг назад. Сколькими способами танцор может за несколько таких па сдвинуться на 7 шагов от исходного рубежа?

### Степени числа $1 + \sqrt{2}$

Если  $d$  не является квадратом натурального числа, то в разложении

$$x^2 - dy^2 = (x - y\sqrt{d})(x + y\sqrt{d})$$

участвует иррациональное число  $\sqrt{d}$ . Казалось бы, мы решаем уравнения в целых числах; зачем нам иррациональности?

Но заметьте:

$$\begin{aligned}(1 + \sqrt{2})^2 &= 1 + 2\sqrt{2} + 2 = 3 + 2\sqrt{2}, \\ (1 + \sqrt{2})^3 &= 1 + 3\sqrt{2} + 3 \cdot 2 + 2\sqrt{2} = 7 + 5\sqrt{2}.\end{aligned}$$

Узнали? Это же решения (3; 2) и (7; 5) уравнения  $x^2 - 2y^2 = \pm 1$ ! Если вас не убедили эти два примера, вот еще один:

$$\begin{aligned}(1 + \sqrt{2})^4 &= (1 + \sqrt{2})^3 (1 + \sqrt{2}) = \\ &= (7 + 5\sqrt{2})(1 + \sqrt{2}) = 17 + 12\sqrt{2}.\end{aligned}$$

Впрочем, это всего лишь примеры. Чтобы получить доказательство, посмотрим, что происходит при переходе от  $n$ -й степени числа  $1 + \sqrt{2}$  к  $(n+1)$ -й. А именно, пусть

$$(1 + \sqrt{2})^n = x_n + y_n \sqrt{2},$$

где  $x_n$  и  $y_n$  — натуральные числа. Тогда

$$\begin{aligned}(1 + \sqrt{2})^{n+1} &= (1 + \sqrt{2})^n (1 + \sqrt{2}) = (x_n + y_n \sqrt{2})(1 + \sqrt{2}) = \\ &= x_n + y_n \sqrt{2} + x_n \sqrt{2} + 2y_n = (x_n + 2y_n) + (x_n + y_n) \sqrt{2},\end{aligned}$$

так что  $x_{n+1} = x_n + 2y_n$  и  $y_{n+1} = x_n + y_n$ . Знакомые формулы, не правда ли?

Что будет, если возводить в степень не  $1 + \sqrt{2}$ , а  $1 - \sqrt{2}$ ? Смотрите:

$$\begin{aligned}(1 - \sqrt{2})^2 &= 3 - 2\sqrt{2}, \\ (1 - \sqrt{2})^3 &= 7 - 5\sqrt{2}, \\ (1 - \sqrt{2})^4 &= 17 - 12\sqrt{2},\end{aligned}$$

и вообще,

$$(1 - \sqrt{2})^n = x_n - y_n \sqrt{2}.$$

Это легко доказать по индукции:

$$\begin{aligned}(1 - \sqrt{2})^{n+1} &= (1 - \sqrt{2})^n (1 - \sqrt{2}) = (x_n - y_n \sqrt{2})(1 - \sqrt{2}) = \\ &= x_n - y_n \sqrt{2} - x_n \sqrt{2} + 2y_n = (x_n + 2y_n) - (x_n + y_n) \sqrt{2}.\end{aligned}$$

А можно обойтись и без индукции, заметив, что при возведении числа  $1 + \sqrt{2}$  в степень мы используем равенство  $(\sqrt{2})^2 = 2$ ; но число  $(-\sqrt{2})^2$  тоже равно 2.

Подобные соображения в алгебре используют часто, есть даже термин: *сопряженные числа*. В полной общности это важное понятие нам не понадобится. Поэтому пока просто скажем, что для каждого числа вида  $a + b\sqrt{2}$ , где  $a, b$  — рациональные числа, сопряженным числом называют  $a - b\sqrt{2}$ . Если вы знаете, что такое комплексные числа, и помните, что для любого комплексного числа  $a + bi$  сопряженное — это  $a - bi$ , не удивляйтесь использованию одного и того же слова для разных целей: если бы мы подробно рассказали о сопряженных числах, то все стало бы абсолютно ясно. Но это, к сожалению, слишком отвлекло бы нас от основной темы.

Тем не менее, для нас важно следующее свойство: *сопряженное к сумме (разности, произведению, частному) двух чисел равно сумме (разности, произведению, частному) сопряженных к ним*. Например, вот как выглядит это для сложения:

$$(a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}).$$

Чуть больших усилий потребует от нас проверка этого свойства для умножения.<sup>1</sup> Прежде всего вычислим произведение

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Значит, сопряженное к произведению равно  $(ac + 2bd) - (ad + bc)\sqrt{2}$ . Осталось вычислить произведение сопряженных:

$$(a - b\sqrt{2})(c - d\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2}.$$

Как видите, результат получился тот же самый.

Отображение  $a + b\sqrt{2} \mapsto a - b\sqrt{2}$  называют *автоморфизмом поля  $\mathbb{Q}[\sqrt{2}]$* . А произведение

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

<sup>1</sup> Строго говоря, надо бы еще разобраться с разностью и частным, но не будем тратить на это силы: при желании вы легко сделаете это самостоятельно.