

Упражнения

55. Выполнив еще пять шагов циклического метода, найдите решение $48842^2 - 67 \cdot 5967^2 = 1$.

56. а) Выполните вычисления для $d = 67$, применяя английский метод. б) Сравните английский и циклический методы для $d = 67$ и для нескольких других значений d , сформулируйте гипотезу о взаимосвязи этих двух методов.

Если вы решили эти два упражнения, то убедились, что индийский и английский методы позволяют найти решение для $d = 67$. Однако ни для английского, ни для индийского метода нет никаких очевидных причин, по которым равенство с правой частью 1 должно обязательно получиться в общем случае. Есть и много других вопросов. Например, если эти методы дадут нам какое-то решение уравнения Пелля, можно ли утверждать, что это решение – наименьшее из возможных?

Я уверен, что попытка самостоятельно разобраться в этих вопросах будет очень полезной. Любитель компьютеров может начать с написания английской и индийской программ, которые вычислят приведенную выше таблицу. А вот для обоснования циклического или английского метода (а лучше бы обоим!) вам придется создать чуть ли не целую теорию! Но даже если у вас ничего не получится (а у большинства, вы уж не обижайтесь, действительно ничего не получится, поскольку задача очень сложна даже для тех, кто успешно справляется с «Задачиком «Кванта»»), это будет очень полезно.

Доказательство существования**Приближения иррациональных чисел рациональными**

Теорему 10 можно доказать, рассматривая приближения числа \sqrt{d} рациональными числами. Для этого сначала сформулирую и докажу следующую лемму.

Лемма. Для любого вещественного числа ξ и любого натурального числа N существуют такие целое число a и натуральное число b , что $b \leq N$ и

$$|b\xi - a| \leq \frac{1}{N+1}.$$

Доказательство. Рассмотрим числа 0 и 1, а также дробные части чисел $\xi, 2\xi, \dots, N\xi$. Если бы все расстояния между этими $(N+2)$ -мя числами были больше $1/(N+1)$, то получилось бы противоречие. Значит, какое-то из расстояний не превосходит $1/(N+1)$. Если

$$|\{b_2\xi\} - \{b_1\xi\}| \leq \frac{1}{N+1},$$

где $1 \leq b_1 < b_2 \leq N$, то

$$|(b_2\xi - [b_2\xi]) - (b_1\xi - [b_1\xi])| \leq \frac{1}{N+1},$$

так что достаточно взять $b = b_2 - b_1$ и $a = [b_2\xi] - [b_1\xi]$. Остальные два случая столь же очевидны: если

$$\{b\xi\} - 0 \leq \frac{1}{N+1},$$

то годится $a = [b\xi]$; если же

$$1 - \{b\xi\} \leq \frac{1}{N+1},$$

то можно взять $a = [b\xi] + 1$. Лемма доказана.

Упражнения

57. Для любых чисел $\xi_1, \xi_2, \dots, \xi_k$ и любого натурального числа N существуют такие целые числа b_1, b_2, \dots, b_k и a , хотя бы одно из которых отлично от нуля, что абсолютные величины чисел b_1, b_2, \dots, b_k не превосходят N и

$$|b_1\xi_1 + b_2\xi_2 + \dots + b_k\xi_k - a| \leq \frac{1}{N^k + 1}.$$

Докажите это.

58. Для любых чисел $\xi_1, \xi_2, \dots, \xi_k$ и любого натурального числа N существует такое натуральное число b , что $b \leq N^k$ и дробные части чисел $b\xi_1, b\xi_2, \dots, b\xi_k$ не превосходят $1/N$. Докажите это.

Доказательство теоремы 10

Положим $\xi = \sqrt{d}$. Для любого натурального $n > 1$ в силу леммы существуют такие натуральные числа a_n и b_n , что $b_n < n$ и

$$|a_n - b_n\sqrt{d}| \leq \frac{1}{n}.$$

Очевидно,

$$\begin{aligned} |a_n^2 - db_n^2| &= |a_n - b_n\sqrt{d}| \cdot |a_n + b_n\sqrt{d}| \leq \\ &\leq \frac{1}{n} |a_n - b_n\sqrt{d} + 2b_n\sqrt{d}| \leq \frac{1}{n} \left(\frac{1}{n} + 2n\sqrt{d} \right) < 1 + 2\sqrt{d}. \end{aligned}$$

Итак, величина $a_n^2 - db_n^2$ может принимать лишь конечное число значений. Но n можно брать сколь угодно большим! И при этом в силу неравенства $|a_n - b_n\sqrt{d}| \leq \frac{1}{n}$ при $n \rightarrow \infty$ имеем $b_n \rightarrow \infty$. Значит, хотя бы для одного целого числа c , по модулю меньшего $1 + 2\sqrt{d}$, существует бесконечно много пар натуральных чисел (a_n, b_n) , для которых

$$a_n^2 - db_n^2 = c.$$

Зафиксируем одно из таких чисел c . Рассмотрим остатки от деления чисел a_n и b_n на $|c|$. Поскольку количество остатков конечно, то существуют такие две⁵ разные пары натуральных чисел $(a; b)$ и $(A; B)$, что

$$a^2 - db^2 = c = A^2 - dB^2$$

и

$$\begin{aligned} a &\equiv A \pmod{|c|}, \\ b &\equiv B \pmod{|c|}. \end{aligned}$$

(Продумайте это!) Рассмотрим частное

$$\begin{aligned} \frac{A + B\sqrt{d}}{a + b\sqrt{d}} &= \frac{(a - b\sqrt{d})(A + B\sqrt{d})}{a^2 - db^2} = \\ &= \frac{aA - bBd + (aB - Ab)\sqrt{d}}{c}. \end{aligned}$$

⁵ На самом деле даже не две, а бесконечно много, но нам это не нужно.