Итерации функции Эйлера

К. С. Зюбин

Настоящая статья содержит решение задачи 2.3′ («Математическое просвещение», сер. 3, вып. 28, с. 237):

Пусть (a_i) *— бесконечная последовательность попарно различных натуральных чисел, удовлетворяющая условию*:

для каждого номера $i > 0$ *выполняется равенство* $\varphi(a_i) = a_{i-1}$. $(*)$

Опишите все такие последовательности. (*К. С. Зюбин*)

В статье доказывается, что всякая такая последовательность, начинающаяся с $a_0 = 1$, является либо последовательностью степеней двойки $1, 2, 4, \ldots$, либо последовательностью вида $1, 2, 4, \ldots, 2^{l-1}, 2^l, 2^l \cdot 3, 2^l \cdot 3^2, \ldots$, где l — некоторое натуральное число.

Напомним, что значение функции Эйлера $\varphi(n)$ по определению равно количеству натуральных чисел, не превосходящих данное натуральное n и взаимно простых с ним. При этом $\varphi(1) = 1$.

Функция Эйлера мультипликативна для взаимно простых n и m: в этом случае $\varphi(nm) = \varphi(n)\varphi(m)$. Пусть $n = p_1^{b_1} \ldots p_m^{b_m}$ — разложение на простые множители. Тогда [5, глава 10, теорема 116]

$$\varphi(n) = p_1^{b_1-1} \ldots p_m^{b_m-1}(p_1 - 1) \ldots (p_m - 1). \qquad (1)$$

Изучались различные вопросы, связанные с функцией Эйлера и её обратной, см. обзор в разделе B36 книги [3]. В той же книге, в разделе B39, обсуждается гипотеза Кармайкла, утверждающая, что уравнение $\varphi(x) = m$ либо не имеет решений, либо имеет более одного решения. На веб-странице [4] обсуждается задача о поиске наименьшего решения уравнения $\varphi(x) = m$. Следует также упомянуть результаты К. Форда и Х. Гупты. В статье [1] К. Форд доказывает, что для каждого целого $k \geqslant 2$ существует такое натуральное m, что уравнение $\varphi(x) = m$ имеет ровно k решений. В статье Х. Гупты [2] описывается метод нахождения множества всех решений уравнения $\varphi(x) = m$.

В настоящей статье рассматриваются последовательности попарно различных натуральных чисел $(a_0, a_1, \ldots)$, такие что для каждого $i > 0$ выполняется $\varphi(a_i) = a_{i-1}$, и изучается вопрос о их бесконечности.

Можно заметить, что $\varphi(a) = a$ только при $a = 1$. Во всех остальных случаях значение функции Эйлера меньше аргумента. Поэтому, если многократно применить её к какому-нибудь числу, то в некоторый момент будет получена единица. Например, $\varphi(12) = 4$, $\varphi(4) = 2$, $\varphi(2) = 1$, $\varphi(1) = 1$. Члены последовательности $(1, 2, 4, 12)$ удовлетворяют равенству $\varphi(a_i) = a_{i-1}$. Её можно продолжить, добавив, например, число 13. Полученную последовательность продолжить уже нельзя, потому что значение функции Эйлера в силу формулы (1) не может быть равно никакому нечётному числу, кроме 1.

Рассмотрим бесконечные последовательности, члены которых удовлетворяют равенству $\varphi(a_i) = a_{i-1}$ и первый член которых равен 1. Будем называть последовательностью вида I последовательность, в которой $a_i = 2^i$ для каждого номера i начиная с 0. К последовательностям вида II будем относить последовательности, в которых $a_i = 2^i$ при $i \leqslant l$ и $a_i = 2^l 3^{i-l}$ при всех $i > l$ для некоторого натурального l. Приведём примеры последовательностей вида II:

$$(1, 2, 4, 12, 36, 108, \ldots), \quad l = 2;$$
$$(1, 2, 4, 8, 16, 48, \ldots), \qquad l = 4.$$

Поскольку

$$\varphi(2^i) = 2^{i-1}, \quad \varphi(2^l \cdot 3) = 2^l \quad \text{и} \quad \varphi(2^l \cdot 3^{i-l}) = 2^l \cdot 3^{(i-1)-l},$$

члены последовательностей вида I или II удовлетворяют равенству

$$\varphi(a_i) = a_{i-1}.$$

Теорема. *Пусть* (a_i), $i = 0, 1, \ldots$, — *бесконечная последовательность попарно различных натуральных чисел, удовлетворяющая условию*:

для каждого номера $i > 0$ *выполняется равенство* $\varphi(a_i) = a_{i-1}$. $\quad (*)$

Тогда если $a_0 = 1$, *то эта последовательность имеет либо вид I, либо вид II.*

Для доказательства теоремы потребуется

Лемма 1. *Пусть бесконечная последовательность* (a_i) *удовлетворяет условию* $(*)$, *начинается с* $a_0 = 1$ *и не является последовательностью вида I. Тогда существует такой член последовательности, что в разложении этого и всех последующих членов на простые множители степень двойки одинакова.*

Доказательство леммы 1. Пусть последовательность (a_i) не имеет вида I. Тогда существует наибольшее k, для которого a_k является

степенью двойки (возможно, $k = 0$ и $a_k = 1$). Рассмотрим члены последовательности a_i при $i \geqslant k$. Покажем, что степень двойки в разложении на простые множители этих чисел не может возрастать. Предположим противное. Пусть степень двойки в разложении на простые множители числа a_i меньше, чем в разложении a_{i+1}.

Согласно (1), если

$$a_{i+1} = 2^b p_1^{b_1} \dots p_m^{b_m},$$

где p_i — нечётные простые, то

$$\varphi(a_{i+1}) = 2^{b-1} p_1^{b_1-1} \dots p_m^{b_m-1} (p_1 - 1) \dots (p_m - 1).$$

Так как все числа p_i нечётные, получаем, что $p_i - 1$ чётны. Поэтому $a_i = \varphi(a_{i+1})$ делится на 2^{b-1+m}. Однако по нашем предположению $b - 1 + m < b$, что возможно только при $m = 0$, когда a_{i+1} является степенью двойки. Так как $i + 1 > k$, это противоречит выбору k.

Степень двойки в разложении члена последовательности может уменьшиться лишь конечное число раз. Следовательно, начиная с какого-то члена степень двойки в разложении на простые множители остаётся постоянной. □

Напомним, что простые числа p, такие что число $2p + 1$ также является простым, называются *простыми числами Софи Жермен*. Примером служат числа 2 и 3, так как $2 \cdot 2 + 1 = 5$ и $3 \cdot 2 + 1 = 7$ — простые числа.

Определение. *Последовательностью Софи Жермен* назовём последовательность натуральных чисел, каждый член которой, кроме первого, имеет вид $2^l(2p + 1)$, где $2^l p$ — предыдущий член, p — число Софи Жермен и l — некоторое фиксированное для данной последовательности натуральное число.

Пример последовательности Софи Жермен при $l = 1$:

$$(4, 10, 22, 46, 94).$$

Лемма 2. *Не существует бесконечной последовательности Софи Жермен.*

Доказательство леммы 2. Пусть первое число в последовательности Софи Жермен равно $2^l p$. Докажем по индукции, что m-й член последовательности имеет вид $2^l(2^m p + 2^m - 1)$. База индукции $m = 0$ очевидна. Шаг индукции: пусть $(m - 1)$-й член последовательности имеет вид $2^l(2^{m-1} p + 2^{m-1} - 1)$. Тогда следующий член имеет вид

$$2^l(2(2^{m-1} p + 2^{m-1} - 1) + 1) = 2^l(2^m p + 2^m - 2 + 1) = 2^l(2^m p + 2^m - 1),$$

что и требовалось. Значит, $(p-1)$-й член последовательности равен $2^l(2^{p-1}p+2^{p-1}-1)$. По малой теореме Ферма [5, глава 11, теорема 119] если $p \neq 2$, то $2^{p-1}-1 \vdots p$. Следовательно, число $2^{p-1}p+2^{p-1}-1$ делится на p и не является простым. Итак, последовательность Софи Жермен, начинающаяся не с $2^l \cdot 2$, конечна. В последовательности же, начинающейся с $2^l \cdot 2$, шестой член равен $2^l \cdot 95$, а $95 = 5 \cdot 19$ не является простым. □

Доказательство теоремы. Предположим противное: пусть бесконечная последовательность (a_i) удовлетворяет $(*)$, начинается с $a_0 = 1$ и не имеет ни вида I, ни вида II.

По лемме 1 существует такой член a_s, что степень двойки в разложении на простые множители a_s и всех последующих членов последовательности одинакова. Обозначим эту степень l.

Пусть a_r — член последовательности с наибольшим номером, являющийся произведением степеней двойки и тройки. Такой член существует, иначе последовательность будет иметь вид II: если некоторый член является произведением степеней двойки и тройки, то каждый из предыдущих членов также таков либо является степенью двойки. Выберем номер t такой, что $t > s$ и $t > r$. В членах $a_t, a_{t+1}, \ldots$ степень двойки в разложении на простые множители остаётся неизменной. Пусть

$$a_{t+2} = 2^l p_1^{b_1} \ldots p_m^{b_m},$$

где p_i — нечётные простые. Тогда

$$a_{t+1} = \varphi(a_{t+2}) = 2^{l-1} p_1^{b_1-1} \ldots p_m^{b_m-1}(p_1-1)\ldots(p_m-1) \vdots 2^{l-1+m}.$$

Положим $a_{t+1} = 2^l a'_{t+1}$, где a'_{t+1} — нечётное число. Тогда $l-1+m \leqslant l$ и $m \leqslant 1$. Поскольку $t > r$, число a_{t+2} не является степенью двойки и, значит, $m = 1$. Таким образом, $a_{t+2} = 2^l p^b$ и $a_{t+1} = \varphi(a_{t+2}) = 2^{l-1}p^{b-1}(p-1)$.

Предположим, что $b > 1$. Пусть $p-1 = 2^s d$, где d — нечётное число. Имеем

$$a_{t+1} = \varphi(a_{t+2}) = 2^{l-1}p^{b-1}(p-1) = 2^{l-1+s}p^{b-1}d.$$

Поскольку двойка входит в разложение a_{t+1} в степени l, получаем, что $s = 1$. Номер $t+2$ больше r, поэтому $p > 3$, $d > 1$ и $\varphi(d) \vdots 2$. Число $p-1$ взаимно просто с p, следовательно, d взаимно просто с p. Имеем:

$$a_t = \varphi(a_{t+1}) = \varphi(2^l p^{b-1} d) = 2^{l-1}p^{b-2}(p-1)\varphi(d).$$

Так как $(p-1) \vdots 2$, получаем, что $a_t \vdots 2^{l-1} \cdot 2 \cdot 2 = 2^{l+1}$, что противоречит неизменности степени двойки в разложении на простые множители чисел a_t, a_{t+1} и a_{t+2}. Таким образом, $0 < b \leqslant 1$, т. е. $b = 1$ и $a_{t+2} = 2^l p$.

Повторяя проведённые рассуждения для a_{t+3}, получим, что $a_{t+3} = 2^l q$, где q — некоторое простое число. Имеем $\varphi(a_{t+3}) = a_{t+2}$, т. е. $\varphi(2^l q) = 2^l p$, $2^{l-1}(q-1) = 2^{l-1} \cdot 2p$. Отсюда $2p + 1 = q$.

Положим $a_{t+2} = 2^l p_1$ и $a_{t+3} = 2^l p_2$. Повторим рассуждения, применённые к a_{t+2}, двигаясь дальше по последовательности (a_i). Получаем $a_{t+j} = 2^l p_{j-1}$ при $j = 4, \ldots$ Все p_j являются числами Софи Жермен, т. е. бесконечная последовательность $a_{t+3}, a_{t+4}, \ldots$ является последовательностью Софи Жермен. Но это противоречит лемме 2. Теорема доказана. □

Следствие. *Каждую бесконечную последовательность* (c_i), $i = 0, 1, \ldots$ *попарно различных натуральных чисел, удовлетворяющую условию* $(*)$, *можно достроить до последовательности вида I или II, добавляя в начало последовательности значения итераций функции Эйлера от первого члена* c_0.

Доказательство. Если первый член $c_0 = 1$, то по доказанной теореме (c_i) имеет вид I или II. Пусть $c_0 \neq 1$. Тогда $\varphi(c_0) < c_0$. Многократно применяя функцию Эйлера к c_0, рано или поздно получим единицу: $\varphi^k(c_0) = 1$ для некоторого k. Возьмём наименьшее такое k. Последовательность $(\varphi^k(c_0),\ \varphi^{k-1}(c_0),\ \ldots,\ \varphi(c_0),\ c_0, c_1, c_2, \ldots)$ по доказанной теореме имеет вид I или II. □

Список литературы

[1] *Ford K.* The Number of Solutions of $\varphi(x) = m$ // Annals of Math. 1999. Vol. 150, № 1. P. 283–311.

[2] *Gupta H.* Euler's Totient Function and its Inverse // Indian J. Pure Appl. Math. 1981. Vol. 12, № 1. P. 22–29.

[3] *Guy R. K.* Unsolved Problems in Number Theory. N. Y.: Springer, 2004.

[4] Inversion of the Euler totient function `https://math.stackexchange.com/questions/265397/inversion-of-the-euler-totient-function/265700`

[5] *Бухштаб А. А.* Теория чисел. М.: Лань, 2015.

Константин Сергеевич Зюбин, ученик МАОУ СОШ № 32, Томск
`kostya.zyubin@gmail.com`