Владикавказский математический журнал
Январь–март, 1999, Том 1, Выпуск 1

УДК **511.3**

О МНОЖЕСТВЕ ЗНАЧЕНИЙ ФУНКЦИИ ЭЙЛЕРА

Б. Г. Тасоев

Как известно, (см. например, [1]), функция Эйлера $\varphi(m)$, где $m > 1$ — целое положительное число, выражает число целых положительных чисел отрезка $[1, m]$, взаимно простых с m.

Известно, что если $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение m на простые множители, то

$$\varphi(m) = m \cdot \prod_{p_i} \left(1 - \frac{1}{p_i}\right) = (p_1 - 1)(p_2 - 1) \dots (p_k - 1) p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1}. \quad (1)$$

Насколько нам известно, по настоящее время не изучено множество

$$\{\varphi(m) \mid \ m \in \mathbb{N}\}. \quad (2)$$

Теорема 1. *Существуют сколь угодно большие четные числа $2n$, для которых уравнение*

$$\varphi(x) = 2n, \quad x \in \mathbb{N} \quad (3)$$

не имеет решения.

Предварительно докажем три вспомогательных предложения.

Лемма 1. *Если p — простое число такое, что $2p + 1$ — составное, то уравнение*

$$\varphi(x) = 2p, \quad x \in \mathbb{N} \quad (4)$$

неразрешимо.

Доказательство. Пусть

$$x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

— каноническое разложение x на простые множители. Тогда, согласно (1) и (4), имеем:

$$(p_1 - 1)(p_2 - 1) \dots (p_k - 1) p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1} = 2p. \quad (5)$$

Поскольку 2 и p — простые числа и $p \geqslant 7$, то $k \leqslant 2$. Пусть $k = 2$. Тогда равенство (5) примет вид:

$$(p_1 - 1)(p_2 - 1) p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} = 2p, \quad (5_1)$$

что при $p_1 > 2$ невозможно, так как левая часть (5_1) делится на 4, в то время как правая часть не делится на 4. Положим $p_1 = 2$. Тогда α_1 должно равняться 1 и равенство (5_1) примет вид:

$$(p_2 - 1) \cdot p_2^{\alpha_2 - 1} = 2p, \tag{5_2}$$

откуда следует, что $\alpha_2 \leqslant 2$. Пусть $\alpha_2 = 2$. Тогда из (5_2) следует, что

$$(p_2 - 1)p_2 = 2p.$$

Но, поскольку $p_2 > p_1 = 2$ — простое число, то p_2 делит p, и, следовательно, $p_2 = p$ и $p_2 - 1 = 2$, т. е. $p_2 = 3$. Откуда следует, что $p = 3$, что невозможно.

Пусть теперь $\alpha_2 = 1$. Тогда равенство (5_2) примет вид: $p_2 - 1 = 2p$, откуда $p_2 = 2p + 1$, что, по условию, невозможно, т. к. $2p + 1$ — составное.

Остается рассмотреть случай: $k = 1$. Тогда из (5) следует:

$$(p_1 - 1) \cdot p_1^{\alpha_1 - 1} = 2p. \tag{5_3}$$

Очевидно, $\alpha_1 - 1 \leqslant 1$ при $p_1 > 2$. Предположим, что $\alpha_1 = 2$. Тогда

$$(p_1 - 1)p_1 = 2p,$$

откуда следует, что p делится на p_1, т. е. $p = p_1$ и $p_1 = 3$. А это означает, что $p = 3$, что невозможно.

Пусть теперь $\alpha_1 = 1$, $p_1 > 2$. Тогда из (5_3) имеем: $p_1 - 1 = 2p$, откуда $p_1 = 2p + 1$, что невозможно, т. к. по условию, $2p + 1$ — составное число.

Положим теперь $p_1 = 2$. Тогда равенство (5_3) примет вид:

$$2^{\alpha_1 - 2} = p.$$

Но, поскольку, p — простое число, то $\alpha_1 = 3$ и $p = 2$, что также невозможно. Лемма доказана.

Лемма 2. *Нечетное число $2l + 1$, $l \in \mathbb{N}$ тогда и только тогда является составным, когда $l = 2uv + u + v$, где u и v — целые положительные числа.*

Доказательство. Пусть $2l+1$ — составное. Тогда его можно представить в виде

$$2l + 1 = (2u + 1)(2v + 1),$$

или, что то же самое,

$$2l + 1 = 2(2uv + u + v) + 1,$$

откуда следует, что $l = 2uv + u + v$.

Обратно, пусть $l = 2uv + u + v$. Тогда

$$2l + 1 = 2(2uv + u + v) + 1 = (2u + 1)(2v + 1)$$

— составное число.

Лемма 3. *Множество простых чисел p, таких, что $2p+1$ — составное, бесконечно.*

Доказательство. Пусть p — простое число. Рассмотрим число $2p+1$. Согласно лемме 2, для того, чтобы оно было составным, необходимо и достаточно, чтобы простое число p было вида $2uv + u + v$, т. е. $p = (2u + 1)v + u$. Придавая u значения $1, 2, 3, \ldots$, получим бесконечное число арифметических прогрессий

$$3v + 1,\ 5v + 2,\ 7v + 3,\ 9v + 4,\ \ldots,$$

каждая из которых, в силу теоремы Дирихле (см. [2]), содержит бесконечное число простых чисел.

Доказательство теоремы следует из лемм 1 и 3.

Литература

1. *Бухштаб А. А.* Теория чисел.—М.: Просвещение, 1966.
2. *Дэвенпорт Г.* Мультипликативная теория чисел.—М.: Наука, 1971.