Функция Эйлера

Определение 2.3. Функция $\varphi:\mathbb{N}\to\mathbb{N}$, ставящая в соответствие каждому натуральному числу m количество $\varphi(m)$ натуральных чисел, меньших m и взаимно простых с m, называется *функцией Эйлера*. При этом полагают $\varphi(1)=1$.

Таким образом, функция Эйлера $\varphi(m)$ задает число элементов приведенной системы вычетов по модулю m.

Пример 2.4. $\varphi(2)=1$ (единственное число, меньшее 2 и взаимно простое с ним, — это 1); $\varphi(3)=2$ (числа 1, 2), $\varphi(6)=2$ (числа 1, 5), $\varphi(9)=6$ (числа 1, 2, 4, 5, 7, 8). □

Функция Эйлера обладает свойством *мультипликативности*: если НОД$(m, n)=1$, то $\varphi(mn)=\varphi(m)\varphi(n)$.

Пример 2.5. Пусть $m=3$, $n=4$. Вычислим $\varphi(3)$, $\varphi(4)$ и $\varphi(3\cdot 4)=\varphi(12)$. Имеем: $\varphi(3)=2$ (числа 1, 2); $\varphi(4)=2$ (числа 1, 3); $\varphi(12)=4$ (числа 1, 5, 7, 11), то есть, действительно, $\varphi(12)=\varphi(3)\cdot\varphi(4)$. □

Теорема 2.1 (Эйлер). Пусть число $m>1$ натуральное. Тогда для любого целого числа a, взаимно простого с m, выполняется сравнение $a^{\varphi(m)}\equiv 1 \pmod m$.

Пример 2.6. Пусть $a=2$, $m=35$. Вычислим функцию Эйлера: $\varphi(35)=\varphi(5\cdot 7)=\varphi(5)\cdot\varphi(7)=4\cdot 6=24$. Тогда $2^{24}=(2^5)^4\cdot 2^4\equiv 3^4\cdot 2^4\equiv$ $\equiv(6^2)^2\equiv 1 \pmod{35}$. □

Замечание. Умножив обе части сравнения $a^{\varphi(m)}\equiv 1 \pmod m$ на a, получим сравнение

$$a^{\varphi(m)+1} \equiv a \pmod{m},$$

которое будет выполняться уже для любого числа a, не обязательно взаимно простого с m.

Пример 2.7. Пусть $a = 18$, $m = 42$. Вычислим функцию Эйлера:

$$\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = \varphi(2) \cdot \varphi(3) \cdot \varphi(7) = 1 \cdot 2 \cdot 6 = 12.$$

Тогда

$$18^{13} = (18^3)^4 \cdot 18 \equiv (2 \cdot 18)^4 \cdot 18 = 2^4 \cdot 18^3 \cdot 18^2 \equiv 2^5 \cdot 18^3 \equiv 2^6 \cdot 18 =$$

$$= 2^7 \cdot 9 \equiv 2 \cdot 9 = 18 \pmod{42}. \qquad \square$$

Если число p простое, то $\varphi(p) = p - 1$. Отсюда получаем частный случай теоремы Эйлера.

Теорема 2.2 (малая теорема Ферма). Пусть число p простое, число a целое, a не делится на p. Тогда $a^{p-1} \equiv 1 \pmod{p}$.

Пример 2.8. Используя малую теорему Ферма, найдем младший разряд числа $7^{1000000}$ в системе счисления с основанием 13.

В этой системе счисления $7^{1000000} = a_n \cdot 13^n + a_{n-1} \cdot 13^{n-1} + \ldots + a_1 \cdot 13 + a_0$, где $0 \le a_i < 13$, для всех $i = 0, 1, \ldots, n$. Тогда $7^{1000000} \equiv a_0 \pmod{13}$, то есть для решения задачи нужно вычислить $7^{1000000} \pmod{13}$. Числа 7 и 13 взаимно просты, поэтому в обозначениях малой теоремы Ферма $a = 7$, $p = 13$ и $7^{12} \equiv 1 \pmod{13}$. Используя теорему о делении с остатком, находим представление $1000000 = 12 \cdot 83333 + 4$. Отсюда $7^{1000000} = 7^{12 \cdot 83333 + 4} = (7^{12})^{83333} \cdot 7^4 \equiv 7^4 \equiv 9 \pmod{13}$, то есть $a_0 = 9$. $\square$

Рассмотрим способ вычисления функции Эйлера.

Теорема 2.3. Если число p простое, число n натуральное, то $\varphi(p^n) = p^n - p^{n-1}$.

Из свойства мультипликативности функции Эйлера и теоремы 2.3 следует, что если число $n > 1$ и $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ — его каноническое разложение, то

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_s^{\alpha_s}) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_s}\right).$$

Эту формулу называют *формулой Эйлера*. С ее помощью можно дать еще одно доказательство первой теоремы Евклида о простых числах (теорема 1.12). Как и ранее, предположим, что $p_1, p_2, \dots, p_s$ — все простые числа, и составим число $N = p_1 p_2 \dots p_s$. Тогда должно выполняться равенство $\varphi(N) = 1$ (все числа, не превосходящие N, должны делиться хотя бы на одно из простых чисел $p_1, p_2, \dots, p_s$). Но по формуле Эйлера

$$\varphi(N) = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_s}\right) = (p_1-1)(p_2-1)\dots(p_s-1) \neq 1.$$

Пример 2.9. Вычислим $\varphi(283500)$. Находим каноническое разложение: $283500 = 2^2 \cdot 3^4 \cdot 5^3 \cdot 7$. Тогда по формуле Эйлера:

$$\varphi(283500) = 283500 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) =$$

$$= 283500 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 64800.$$ □