Функция Эйлера

Простые числа

Число, которое не имеет никаких делителей, кроме 1 и самого себя, называется простым числом. Примеры простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …

Любое число N может быть представлено в виде произведения степеней простых чисел (*каноническое* представление числа). Такое представление единственно (с точностью до перестановки сомножителей). Так, число

$$600 = 2^3 3^1 5^2.$$

Функция Эйлера

Функция Эйлера $\varphi(m)$ определяется для всех целых чисел m как количество чисел ряда 1, 2, 3, ..., m взаимно простых с m. Так, $\varphi(1) = 1$ (по определению), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ и т. д. Легко показать, что для $m = p$ (простых чисел) $\varphi(p) = p-1$. Для $m = p^n$ функция Эйлера $\varphi(p^n) = p^{n-1}(p-1)$. Для произвольного числа m, представленного в канонической форме $m = p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$, функция Эйлера определяется следующим образом: $\varphi(m) = m(1-1/p_1)(1-1/p_2)\ldots(1-1/p_s)$.

Например: $\varphi(11) = 10$; $\varphi(9) = 6$; $\varphi(18) = 6$.

Классы вычетов, получаемые в соответствии с функцией Эйлера, всегда образуют абелеву группу по умножению. А это, в частности, означает, что для любого представителя из этих классов можно найти обратный элемент из представителей этих же классов.

Теорема Ферма. Если p - простое число и НОД$(a, p)=1$, то

$$a^{p-1} \equiv 1 \bmod p.$$

Теорема Эйлера. Если $m>1$ и НОД$(a,m)=1$, то

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Эта теорема обобщает теорему Ферма, т.к. при $m=p$, $\varphi(m)=p-1$.