Н.А. Гурьянова, Т.В. Павлова

Ишимский педагогический институт им. П.П. Ершова (филиал)
Тюменского государственного университета, г. Ишим
УДК 511.172

ОБ УТОЧНЕНИИ ТЕОРЕМЫ ЭЙЛЕРА В ТЕОРИИ ЧИСЕЛ

Аннотация. В статье доказывается формула для вычисления показателя целого числа a по модулю m в случае существования первообразного корня по модулю m.

Ключевые слова: функция Эйлера, теорема Эйлера, первообразный корень, показатель числа по модулю.

Теория чисел, или высшая арифметика – раздел математики, изучающий целые числа и сходные объекты. В теории чисел в широком смысле рассматриваются как алгебраические, так и трансцендентные числа, а также функции различного происхождения, которые связаны с арифметикой целых чисел и их обобщений.

До XX века теория чисел считалась отвлеченной наукой, «чистым искусством от математики», не имеющим абсолютно никакого практического применения. В настоящее время ее роль значительно возросла, результаты теории чисел используют в криптографических протоколах, при расчете траекторий спутников и космических зондов, в программировании. Экономика, финансы, информатика, геология – сегодня все эти науки невозможны без теории чисел.

Большую роль в элементарной теории чисел играет теорема Эйлера. На языке теории сравнений она формулируется следующим образом: любое целое число a, взаимно простое с целым числом $m > 1$, в степени $\varphi(m)$ (где $\varphi(m)$ – функция Эйлера, которая определяется как количество натуральных чисел, не превосходящих m и взаимно простых с m),

сравнимо с единицей по модулю m, то есть

$$a^{\varphi(m)} \equiv 1 \ (mod \ m) \qquad (1)$$

Теорема Эйлера имеет многочисленные применения в математике. Непосредственно в теории чисел ее используют для возведения чисел в степень по некоторому модулю, нахождения остатков от деления, нахождения мультипликативных обратных по модулю. Применение теоремы Эйлера при решении перечисленных задач может быть неэффективным в силу того, что теорема Эйлера не утверждает, что число $\varphi(m)$ является наименьшим числом со свойством (1). Наименьшее натуральное число n, такое, что $a^n \equiv 1 \ (mod \ m)$, где числа a и m взаимно простые, называется *показателем*, или *мультипликативным порядком*, целого числа a по модулю m и обозначается как $P_m(a)$ [1].

Заметим, более точную оценку искомой степени дает теорема Кармайкла [1], которая утверждает, что если a, m взаимно просты, то $a^{\lambda(k)} \equiv 1 (mod \ n)$, где $\lambda(k)$ – функция Кармайкла, которая для степеней нечётных простых, а также для чисел 2 и 4, равна функции Эйлера $\varphi(k)$; а для степеней двойки, больших 4, равна половине функции Эйлера: $\lambda(k) = \frac{\varphi(k)}{2}$. Но, так же как и теорема Эйлера, теорема Кармайкла не утверждает, что число $\lambda(k)$ является показателем любого числа a, взаимно простого с m.

Несложно доказывается, что $P_m(a)$ является делителем числа $\varphi(m)$. При этом практические вычисления показывают, что $\varphi(m)$ может намного превосходить $P_m(a)$. Например, для $a = 13$ и $m = 21$, так как 13 и 21 взаимно простые, согласно теореме Эйлера, $13^{\varphi(21)} = 13^{12} \equiv 1 \ (mod \ 21)$, хотя уже $13^2 = 169 \equiv 1 \ (mod \ 21)$.

Поэтому представляет интерес найти формулу для вычисления показателя для любого числа a, взаимно простого с m. К примеру, для $a = m - 1$ является справедливым следующее утверждение:

Предложение 1. Для $m > 1$ *показатель* $m - 1$ *равен* $P_m(m-1) = 2$.

Доказательство. Будем далее утверждение «a делится на b» обозначать как $a \vdots b$. В первую очередь покажем, что для любого $m > 1$, числа m и $m - 1$ взаимно простые. Предположим, что это не так. Пусть НОД$(m, m-1) = d > 1$. Тогда m и $m - 1$ делятся на d. Следовательно, найдется целое число t такое, что $m - 1 = dt$, откуда $m - dt = 1$. Левая часть равенства делится на d, следовательно, правая часть также делится на d, то есть $1 \vdots d$, где $d > 1$. Что невозможно, поэтому $(m, m-1) = d > 1$. Покажем, что $(m-1)^2 \equiv 1\ (mod\ m)$. Так как $(m-1)^2 = m^2 - 2m + 1$ и $m^2 \equiv 0\ (mod\ m)$, $2m \equiv 0\ (mod\ m)$, то $(m-1)^2 = m^2 - 2m + 1 \equiv 0 + 0 + 1 = 1\ (mod\ m)$. ■

Основной результат работы (теорема 1) содержит формулу для вычисления $P_m(a)$ в случае, когда существует *первообразный корень* [1] по модулю m, т.е. натуральное число k, обладающее свойством: $k^{\varphi(m)} \equiv 1\ (mod\ m)$, но $k^n \not\equiv 1 (mod\ m)$ для всех натуральных чисел $n < \varphi(m)$. Это равносильно тому, что мультипликативная группа $\mathbb{Z}_m^*$ элементов кольца классов вычетов по модулю m является циклической группой, порожденной классом вычетов $\bar{k}$.

В общем случае структура группы $\mathbb{Z}_m^*$, описывается известной теоремой, доказанной К. Гауссом в 1801 году, согласно которой группа $\mathbb{Z}_m^*$ (см., например, [2]) является циклической группой тогда и только тогда, когда выполняется один из следующих случаев:

1) $m = p^\alpha$, где p – нечетное простое число, $\alpha \in \mathbb{N}$;

2) $m = 2p^\alpha$, где p – нечетное простое число, $\alpha \in \mathbb{N}$;

3) $m = 1, 2, 4$.

Прежде чем перейти к формулировке и доказательству основного результата, сформулируем и докажем вспомогательные утверждения, необходимые для его доказательства.

Лемма 1. *Для любых целых чисел* a, b, c, *число* $a \vdots b$ *и* $a \vdots c$ *тогда и только тогда, когда* $a \vdots НОК(b, c)$.

Доказательство. Рассмотрим канонические представления чисел a, b, c: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots p_n^{\beta_n}$, $c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots p_n^{\gamma_n}$, где $\alpha_i, \beta_i, \gamma_i \geq 0$ для всех $i = 1, \dots, n$. Если $a \vdots b$, то $\alpha_i \geq \beta_i$ для всех $i = 1, \dots, n$. Аналогично, если $a \vdots c$, то $\alpha_i \geq \gamma_i$ для всех $i = 1, \dots, n$. Получаем, $\alpha_i \geq max\{\beta_i; \gamma_i\}$. Это означает, что $a \vdots НОК(b, c)$. Ясно, что верно и обратное: *если* $a \vdots НОК(b, c)$, то $a \vdots b$ *и* $a \vdots c$. ■

Лемма 2. *Если* $k^a \equiv 1(mod\ m)$, *где* a – *наименьшее натуральное число с таким свойством и* $k^b \equiv 1(mod\ m)$, *то* $b \vdots a$

Доказательство. Разделим b на a с остатком: $b = an + r$, причем $n \in \mathbb{N}$, $0 \leq r < a$. Получаем, $k^b = k^{an+r} = k^{an} \cdot k^r$ и $k^{an} \cdot k^r \equiv 1\ (mod\ m)$.Так как $k^a \equiv 1(mod\ m)$, то и $k^{an} \equiv 1(mod\ m)$. Следовательно, $k^r \equiv 1\ (mod\ m)$. Так как $0 \leq r < a$ и a наименьшее со свойством $k^a \equiv 1(mod\ m)$, то $r = 0$, следовательно $b = an$, что означает, $b \vdots a$. ■

Основной результат работы формулируется следующим образом:

Теорема 1. *Если существуют первообразные корни по модулю* m *и* k *– такой корень, то для данного целого числа* a *и* $m > 1$, *взаимно простого с* a, *показатель числа* a *по модулю равен*

$$n = P_m(a) = \frac{НОК\big(l, \varphi(m)\big)}{l} = \frac{\varphi(m)}{НОД\big(l, \varphi(m)\big)},$$

где число l *такое, что* $a \equiv k^l\ (mod\ m)$.

Доказательство. Для краткости наименьшее общее кратное чисел

a, b будем обозначать как $[a, b]$. Покажем, что для $n = \frac{[l,\varphi(m)]}{l}$, $a^n \equiv 1(mod\ m)$. Имеем, $a^n = (k^l)^n = k^{ln} = k^{\frac{l[l,\varphi(m)]}{l}} = k^{[l,\varphi(m)]}$. Так как $[l, \varphi(m)] \vdots \varphi(m)$, то $[l, \varphi(m)] = \varphi(m) \cdot t$, где $t \in \mathbb{N}$, поэтому $k^{[l,\varphi(m)]} = k^{\varphi(m)t} = (k^{\varphi(m)})^t$. Число k – первообразный корень, то есть $k^{\varphi(m)} \equiv 1(mod\ m)$. Окончательно получим,

$$a^n = (k^{\varphi(m)})^t \equiv 1^t = 1\ (mod\ m).$$

Докажем, что n – наименьшее натуральное число, такое, что $a^n \equiv 1(mod\ m)$.

Предположим, что это не так, то есть найдется натуральное число $n_1 < n$ такое, что $a^{n_1} \equiv 1(mod\ m)$. Тогда $a^{n_1} = (k^l)^{n_1} = k^{ln_1} \equiv 1\ (mod\ m)$. Так как k – первообразный корень, то $\varphi(m)$ – наименьшая возможная степень для k такая, что $k^{\varphi(m)} \equiv 1\ (mod\ m)$. Тогда по лемме 1, из условия $k^{ln_1} \equiv 1\ (mod\ m)$, следует, что $ln_1 \vdots \varphi(m)$. Из этой делимости и того, что $ln_1 \vdots l$, по лемме 2 получаем, $ln_1 \vdots [l, \varphi(m)] = ln$. Таким образом, $ln_1 \vdots ln$, где $1 \leq ln_1 < ln$, что невозможно. Полученное противоречие окончательно доказывает минимальность числа n. Равенство $n = \frac{\varphi(m)}{\text{НОД}(l,\varphi(m))}$ следует из свойства $\text{НОК}(a, b) = \frac{a \cdot b}{\text{НОД}(a,b)}$. ■

Например, для нечетного простого числа $m = 19$, первообразные корни существуют и равны 10, 13, 14 и 15. Для $a = 11$ и $k = 10$ выполняется

$11 \equiv 10^6\ (mod\ 19)$, поэтому $P_{19}(11) = \frac{\varphi(19)}{\text{НОД}(6,\varphi(19))} = \frac{18}{\text{НОД}(6,18)} = 3$. И, действительно,

$$11^3 \equiv 11^2 \cdot 11 \equiv (121 - 19 \cdot 6) \cdot 11 \equiv 77 - 19 \cdot 4 = 1\ (mod\ 19).$$

СПИСОК ЛИТЕРАТУРЫ

1. Бухштаб, А.А. Теория чисел : учебное пособие / А.А. Бухштаб. – Москва : Просвещение, 1966. – 384 с.
2. Кострикин, А.И. Введение в алгебру. В 3-х ч. Часть 3. Основные структуры / А.И. Кострикин. – Москва : Физматлит, 2004. – 272 с.