



# ПЕРВООБРА́ЗНЫЙ КО́РЕНЬ

ПЕРВООБРА́ЗНЫЙ КО́РЕНЬ по модулю  $m$ , натуральное число  $g$  такое, что наименьшее положительное число  $k$ , для которого разность  $g^k - 1$  делится на  $m$  ( $g^k$  сравнимо с 1 по модулю  $m$ ), совпадает с  $\varphi(m)$ , где  $\varphi(m)$  – число натуральных чисел, меньших  $m$  и взаимно простых с  $m$ . Напр., при  $m=7$  П. к. по модулю 7 является число 3. Действительно,  $\varphi(7)=6$ ; числа  $3^1-1=2$ ,  $3^2-1=8$ ,  $3^3-1=26$ ,  $3^4-1=80$ ,  $3^5-1=242$  не делятся на 7, лишь  $3^6-1=728$  делится на 7.

П. к. существуют, когда  $m=2$ ,  $m=4$ ,  $m=p^\alpha$ ,  $m=2p^\alpha$ , где  $p$  – простое нечётное число,  $\alpha \geq 1$  – целое, а для др. модулей их нет. Число П. к. в этих случаях равно  $\varphi(\varphi(m))$  (числа, разность которых кратна  $m$ , не считаются за различные). И. М. [Виноградов](#) установил (1926), что в интервале  $(1, 2^{\sqrt{2k}} \sqrt{p \ln p})$  существует П. к. по модулю  $p$ , где  $p$  – простое нечётное число,  $k$  – число разл. простых делителей числа  $p-1$ . См. также [Индекс](#) в теории чисел, [Чисел теория](#).

Loading [MathJax]/jax/output/HTML-CSS/fonts/TeX/fontdata.js