Малая теорема Ферма

В.СЕНДЕРОВ, А.СПИВАК

Напоминание

Малая теорема Ферма гласит: *если a – целое число, не делящееся на простое число p, то $a^{p-1} - 1$ делится на p.*

Функция Эйлера $\varphi(n)$ – это количество натуральных чисел от 1 до n, взаимно простых с n.

Функция Кармайкла $\lambda(n)$– это такое наименьшее натуральное число k, что для всякого целого числа a, взаимно простого с натуральным числом n, разность $a^k - 1$ делится на n.

Число g называют *первообразным корнем по модулю n*, если для всякого целого a, взаимно простого с n, существует такое натуральное число m, что $g^m \equiv a \pmod n$.

Подробно об этих и многих других понятиях и теоремах арифметики можно прочитать в предыдущих частях статьи. Там не было доказано существование первообразного корня по простому модулю. Пришла пора это сделать.

Первообразные корни

Первообразные корни по модулю 11

Число 2 – первообразный корень по модулю 11. Какие еще есть первообразные корни по этому модулю?

Для ответа не нужно перебирать все числа 3, 4, 5, …, 9, 10 и составлять для каждого из них таблицу. Некоторые степени двойки можно сразу отбросить:

$$\left(2^2\right)^5 = 2^{10} \equiv 1,$$
$$\left(2^4\right)^5 = 2^{20} \equiv 1,$$
$$\left(2^5\right)^2 \equiv 1,$$
$$\left(2^6\right)^5 \equiv 1,$$
$$\left(2^8\right)^5 \equiv 1 \pmod{11}.$$

А вот степени двойки $2^1 \equiv 2$, $2^3 \equiv 8$, $2^7 \equiv 7$ и $2^9 \equiv 6$, показатели которых взаимно просты с 10, являются первообразными корнями. (Обдумайте это!)

И вообще, если g – первообразный корень по простому модулю p, то g^s является первообразным корнем в том и только том случае, когда s и $p - 1$ взаимно просты.

Упражнения

44. Докажите это.

45. Для того чтобы число a было первообразным корнем по простому модулю p, необходимо и достаточно, чтобы a не делилось на p и ни для какого простого делителя q числа $p - 1$ разность $a^{(p-1)/q} - 1$ не делилась бы на p. Докажите это.

46. Найдите наименьшее натуральное число, являющееся первообразным корнем по модулю а) 23; б) 41; в) 257.

47. а) Проверьте, что 2 не является первообразным корнем по модулю 263, а -2 является.

б) Пусть $a^3 - a$ не делится на 83. Докажите, что ровно одно из чисел a и $-a$ является первообразным корнем по модулю 83.

48. а) Пусть p – простое число, $p \equiv 1 \pmod 4$. Докажите, что число $-a$ является первообразным корнем по модулю p тогда и только тогда, когда само число a – первообразный корень по модулю p.

б) Пусть p – простое число, $p \equiv 3 \pmod 4$. Докажите, что число a является первообразным корнем по модулю p тогда и только тогда, когда порядок числа $-a$ по модулю p равен $(p - 1)/2$.

Порядки классов вычетов

В таблице 5 для каждого ненулевого остатка $a \pmod{11}$ указан его порядок k.

Как и должно быть, порядки – делители числа 10. Давайте посчитаем, сколько раз в нижней строке

Таблица 5

a	1	2	3	4	5	6	7	8	9	10
k	1	10	5	5	5	10	10	10	5	2

таблицы 5 встречаются числа 1, 2, 5 и 10. Ответы запишем в виде таблицы 6.

Таблица 6

Порядок	1	2	5	10
Встречается	1	1	4	4

Видна закономерность? Если нет, посмотрите на таблицу 7, составленную для $p = 13$.

Таблица 7

a	1	2	3	4	5	6
k	1	12	3	6	4	12
a	7	8	9	10	11	12
k	12	4	3	6	12	2

В ней порядки – делители числа 12. Посчитаем, сколько раз встречаются в нижней строке таблицы 7 числа 1, 2, 3, 4, 6 и 12 (табл.8).

Таблица 8

Порядок	1	2	3	4	6	12
Встречается	1	1	2	2	2	4

Если вы все еще не догадались, составьте такие таблицы для нескольких других простых чисел p, и рано или поздно увидите, что в нижних строках этих таблиц – значения функции Эйлера: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(10) = 4$, $\varphi(12) = 4$.

Великий немецкий математик К.Ф.Гаусс (1777 – 1855) в «Арифметических исследованиях», опубликованных в 1801 году, доказал, что это не случайность, а общий закон.

Теорема 4. *Среди $p - 1$ ненулевых классов вычетов по простому модулю p порядок k, где k – делитель числа $p - 1$, имеют ровно $\varphi(k)$ классов вычетов. (В частности, для любого простого числа p существует $\varphi(p-1)$ первообразных корней по модулю p.)*

Для доказательства теоремы 4 мы используем теорему Безу и одно интересное свойство функции Эйлера.

Теорема Безу

Для тех, кто знаком с делением многочленов с остатком, теорему Безу[1] можно сформулировать и до-

Окончание. Начало см. в «Кванте» №1, 3.

[1] *Этьен Безу (1730–1783) – французский математик.*