порядок по модулю p, причем этот порядок – делитель числа k. Осталось вспомнить теорему 7 – и становится ясно, что классов порядка k существует ровно $\varphi(k)$ штук. Теорема 4 доказана.

Упражнения

56. Пусть p – простое число, $p > 3$. Найдите остаток от деления на p произведения тех из чисел 1, 2, …, $p-1$, которые являются первообразными корнями по модулю p.

57. а) Если порядки чисел a и b по модулю p равны m и n соответственно, то порядок произведения ab – делитель числа НОК$[m, n]$. Докажите это.

б) Покажите, что порядок числа ab равен mn, если числа m и n взаимно просты, и не обязательно равен числу НОК$[m, n]$, если m и n не взаимно просты.

58. а) Пусть p – простое число, $p > 2$, $p-1 = q_1^{a_1} q_2^{a_2} \dots q_s^{a_s}$ – разложение числа $p-1$ в произведение степеней различных простых чисел. Пусть $g_1, g_2, \dots, g_s$ – такие не кратные p числа, что $g_i^{(p-1)/q_i} \not\equiv 1 \pmod p$ при $i = 1, 2, \dots, s$. Докажите, что число $g = g_1^{(p-1)/q_1^{a_1}} g_2^{(p-1)/q_2^{a_2}} \dots g_s^{(p-1)/q_s^{a_s}}$ – первообразный корень по модулю p. (Заметьте: мы получили еще одно доказательство существования первообразного корня по простому модулю!)

б) Для любого натурального n существует взаимно простое с n целое число a, порядок которого по модулю n равен $\lambda(n)$. Докажите это.

в) Если $n = 2, 4, p^m$ или $2p^m$, где p – нечетное простое, m – натуральное, то существует первообразный корень по модулю n. Докажите это.

Гипотеза Артина

Как мы только что доказали, для каждого простого числа p существует первообразный корень по модулю p. Интересно: какие целые числа бывают первообразными корнями, а какие не бывают?

Очевидно, -1 является первообразным корнем только по модулю 2 или 3. Далее, из равенства $\left(a^2\right)^{(p-1)/2} = a^{p-1}$ следует, что точный квадрат не может быть первообразным корнем ни по какому нечетному простому модулю p.

Немецкий алгебраист Эмиль Артин (1898–1962) предположил, что для любого целого числа $g \neq -1$, не являющегося квадратом целого числа, существует бесконечно много таких простых p, что g – первообразный корень по модулю p.

Более того, некоторые вероятностные соображения привели Артина к следующему уточнению его гипотезы: если k есть наибольшее такое число, что g является k-й степенью, то отношение количества $\pi_g(n)$ простых чисел, не превосходящих n, по модулю которых g является первообразным корнем, к количеству $\pi(n)$ всех простых чисел, не превосходящих n, стремится при $n \to \infty$ к зависящему только от k пределу

$$\lim_{n\to\infty} \frac{\pi_g(n)}{\pi(n)} = \prod_{k:q} \left(1 - \frac{1}{q-1}\right) \cdot \prod_{k \text{ не } \vdots q} \left(1 - \frac{1}{q(q-1)}\right),$$

где первое произведение распространено на все простые числа q, являющиеся делителями k, а второе – на все простые числа q, не являющиеся делителями k.

К настоящему времени гипотеза Артина не доказана, хотя некоторый ее аналог, относящийся к полю рациональных функций от одной переменной над конечным полем, доказать удалось.

Числа Кармайкла

В силу малой теоремы Ферма, $2^{p-1} \equiv 1 \pmod p$ для любого нечетного простого числа p. Существуют ли составные числа с тем же свойством? Да, существуют:

$$2^{340} \equiv 1 \pmod{341}.$$

В самом деле, $341 = 11 \cdot 31$, причем $2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$. (Можно проверить, что число 341 – наименьшее составное число n со свойством $2^{n-1} \equiv 1 \pmod n$.)

Упражнение 59. а) Если $n = \left(4^p - 1\right)/3$, где p – простое число, $p > 3$, то $2^{n-1} \equiv 1 \pmod n$. Докажите это.

б) (М672) Пусть a – такое натуральное число, что $2^a - 2$ кратно a (например, $a = 3$). Определим последовательность $x_1, x_2, x_3, \dots$ условиями $x_1 = a$, $x_{n+1} = 2^{x_n} - 1$. Докажите, что $2^{x_n} - 2$ кратно x_n при любом n.

Но почему мы заинтересовались именно случаем $a = 2$? Наверное, разумнее спросить: существуют ли такие составные числа n, что для любого a, взаимно простого с n, выполнено сравнение $a^{n-1} \equiv 1 \pmod n$? Такие числа тоже существуют! Их называют *числами Кармайкла*. Наименьшее число – это

$$561 = 3 \cdot 11 \cdot 17,$$

за ним идут

$$1105 = 5 \cdot 13 \cdot 17,\ 1729 = 7 \cdot 13 \cdot 19,$$
$$2465 = 5 \cdot 17 \cdot 29,\ 2821 = 7 \cdot 13 \cdot 31,$$
$$6601 = 7 \cdot 23 \cdot 41,\ 8911 = 7 \cdot 19 \cdot 67,$$
$$10585 = 5 \cdot 29 \cdot 73,\ 15841 = 7 \cdot 31 \cdot 73,$$
$$29341 = 13 \cdot 37 \cdot 61,$$
$$41041 = 7 \cdot 11 \cdot 13 \cdot 41, \dots$$

В 1994 году в журнале Annals of Mathematics (т. 139, с. 703–722) три математика – Альфорд, Гренвилль и Померанц – опубликовали (абсолютно недоступное для школьника) доказательство бесконечности множества чисел Кармайкла.

Упражнение 60. а) Докажите, что $a^{561} - a$ кратно числу 561 при любом целом a.

б) Докажите при $n = 1105$ сравнения $2^{n-1} \equiv 1 \equiv 3^{n-1} \pmod n$. (Можно доказать, что число 1105 – наименьшее составное число с таким свойством.)

Очевидно, составное число n является числом Кармайкла тогда и только тогда, когда $n-1$ делится на $\lambda(n)$.

Теорема 8. *Составное число* $n = p_1^{m_1} p_2^{m_2} \cdot \dots \cdot p_s^{m_s}$, *где* $p_1, p_2, \dots, p_s$ – *различные простые числа,* $m_1, m_2, \dots, m_s$ – *натуральные числа, является числом Кармайкла в том и только том случае, когда* $m_1 = m_2 = \dots = m_s = 1$ *и* $n-1$ *кратно каждому из чисел* $p_1 - 1, p_2 - 1, \dots, p_s - 1$.

Следствие. *Если* n – *число Кармайкла, то для любого целого числа* a *верно сравнение* $a^n \equiv a \pmod n$.

Доказательство теоремы 8. Пусть n – число Кармайкла. Поскольку при $n > 2$ значение функции Кармайкла $\lambda(n)$ четно, то $n-1$ должно быть четным. Следовательно, n нечетно.

Поскольку $\lambda(n)$ делится на $\lambda\left(p_i^{m_i}\right) = p_i^{m_i-1}\left(p_i - 1\right)$, а $n-1$ не делится на p_i, то в случае $m_i > 1$ получаем противоречие. Следовательно, $m_1 = m_2 = \dots = m_s = 1$. Завершение доказательства теоремы 8 предоставляем читателю.

Упражнения

61. а) Докажите, что $2^{161038} \equiv 2 \pmod{161038}$. (При помощи компьютера легко проверить, что $n = 161038 = 2 \cdot 73 \cdot 1103$ – наименьшее четное составное число, для которого $2^n \equiv 2 \pmod n$. Следующее такое четное число $215326 = 2 \cdot 23 \cdot 31 \cdot 151$.)

б) Для любого целого числа $a \neq -1$ существует такое четное число $n > 2$, что $a^n \equiv a \pmod n$. Докажите это.

в*) Для любого натурального числа a существует бесконечно много таких четных чисел n, что $a^n \equiv a \pmod n$. Докажите это. (*Указание*. Используйте теорему Биркгофа–Вандивера, сформулированную в упражнении 32.)

62. а) Пусть $n = 3^m - 2^m$. Докажите, что если $n-1$ кратно m, то число $3^{n-1} - 2^{n-1}$ кратно n.

б) Существует ли составное число n, для которого $3^{n-1} - 2^{n-1}$ кратно n?