

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:

$$(2^2)^5 = 2^{10} \equiv 1,$$

$$(2^4)^5 = 2^{20} \equiv 1,$$

$$(2^5)^2 \equiv 1,$$

$$(2^6)^5 \equiv 1,$$

$$(2^8)^5 \equiv 1 \pmod{11}.$$

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 Безу¹ можно сформулировать и до-

¹ Этьен Безу (1730–1783) – французский математик.

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

казать очень коротко. В равенство

$$f(x) = (x - a)g(x) + r,$$

где $g(x)$ – многочлен (неполное частное), а r – число (остаток), можно подставить вместо x число a . Получим

$$f(a) = (a - a)g(a) + r = r.$$

Значит, остаток r от деления $f(x)$ на $x - a$ равен $f(a)$. Это и есть теорема Безу.

А для остальных читателей теорему Безу можно сформулировать и доказать чуть более длинным, но не менее естественным способом.

Теорема 5. Число a является корнем многочлена $f(x)$ в том и только том случае, когда $f(x)$ делится на $x - a$, т.е. когда

$$f(x) = (x - a)g(x),$$

где g – некоторый многочлен.

Доказательство. Если

$$f(x) = (x - a)g(x),$$

то

$$f(a) = (a - a)g(a) = 0.$$

Обратно, пусть $f(a) = 0$. Подставим в многочлен

$$f(x) = k_n x^n + k_{n-1} x^{n-1} + \dots + k_2 x^2 + k_1 x + k_0$$

число a . Получим

$$0 = f(a) = k_n a^n + k_{n-1} a^{n-1} + \dots + k_2 a^2 + k_1 a + k_0.$$

Следовательно,

$$\begin{aligned} f(x) &= f(x) - f(a) = \\ &= k_n (x^n - a^n) + k_{n-1} (x^{n-1} - a^{n-1}) + \dots \\ &\quad \dots + k_2 (x^2 - a^2) + k_1 (x - a). \end{aligned}$$

Каждая из разностей

$$x - a,$$

$$x^2 - a^2 = (x - a)(x + a),$$

...

$$x^n - a^n =$$

$$= (x - a)(x^{n-1} + x^{n-2}a + \dots + xa^{n-2} + a^{n-1})$$

кратна $x - a$. Теорема доказана.

Переформулировка малой теоремы Ферма

Из теоремы Безу следует, что если a_1, a_2, \dots, a_m – различные корни

многочлена $f(x)$, то $f(x) = (x - a_1)(x - a_2)\dots(x - a_m)g(x)$, где g – некоторый многочлен.

Применив это соображение к многочлену $x^{p-1} - 1$, получим замечательную переформулировку малой теоремы Ферма:

$$x^{p-1} - 1 \equiv (x - 1)(x - 2)\dots(x - p + 1),$$

где знак сравнения означает, что если раскрыть все скобки в правой части и вычесть из нее левую, то получим многочлен, коэффициенты которого кратны p . Как вы помните, для частных случаев $p = 2, 3, 5, 7$ и 11 это разложение на множители встречалось в первой части статьи.

Упражнение 49. Подставив $x = 0$, докажите теорему Вильсона: $(p - 1)! \equiv -1 \pmod{p}$ для любого простого числа p .

Сравнение $x^k \equiv 1 \pmod{p}$

Если k – делитель числа $p - 1$, т.е. $p - 1 = km$, то

$$\begin{aligned} x^{p-1} - 1 &= \\ &= (x^k - 1)(x^{k(m-1)} + x^{k(m-2)} + \dots + x^k + 1). \end{aligned}$$

Значит, многочлен $x^k - 1$ является делителем многочлена $x^{p-1} - 1$. Поскольку $x^{p-1} - 1$ разлагается в произведение многочленов первой степени, то его делитель $x^k - 1$ является произведением k многочленов первой степени.

Немного подумав, можно сообразить, что мы доказали следующее утверждение.

Теорема 6. Если p – простое число, k – делитель числа $p - 1$, то сравнению $x^k \equiv 1 \pmod{p}$ удовлетворяют ровно k классов вычетов по модулю p .

Упражнения

50. Решите сравнения

а) $x^4 \equiv 1 \pmod{13}$; б) $x^{1604} \equiv 1 \pmod{17}$. (Указание. 2 и 3 – первообразные корни, соответственно, по модулю 13 и по модулю 17.)

51. Зная, что 2 – первообразный корень по модулю 29, решите сравнение $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{29}$.

52. Пусть p – простое число. При каких k сумма $1^k + 2^k + \dots + (p-1)^k$ кратна p ?

53. а) Сколько существует таких пар (a, b) натуральных чисел, что $a, b \leq 1717$ и $a^8 + b^8$ кратно 17?

б) Сколько существует таких троек (a, b, c) натуральных чисел, что

$a, b, c \leq 289$ и $a^{1000} + b^{3000} + c^{9000}$ кратно 17?

Сумма значений функции Эйлера

Рассмотрим 100 дробей: $1/100, 2/100, \dots, 100/100$. Если каждую из них привести к несократимому виду, то получим $\phi(100) = 40$ дробей со знаменателем 100, $\phi(50) = 20$ дробей со знаменателем 50, и так далее: для каждого делителя d числа 100 получим $\phi(d)$ дробей со знаменателем d . (Почему? Потому что $\phi(d)$ – это количество несократимых правильных дробей со знаменателем d .)

Мы получили замечательное равенство:

$$\begin{aligned} 100 &= \phi(100) + \phi(50) + \phi(25) + \phi(20) + \\ &+ \phi(10) + \phi(5) + \phi(4) + \phi(2) + \phi(1). \end{aligned}^2$$

Если бы мы рассмотрели не дробь со знаменателем 100, а дробь со знаменателем n , то точно так же доказали бы следующее утверждение.

Теорема 7. Для любого натурального числа n сумма значений функции Эйлера $\phi(d)$ по всем делителям d числа n равна n .

Упражнения

54. Если d – делитель числа n , то существует ровно $\phi(n/d)$ таких натуральных чисел k , что $k \leq n$ и $\text{НОД}(k, n) = d$. Докажите это.

55. Пусть $n > 1$. Найдите сумму всех несократимых правильных дробей, знаменатели которых равны n .

Доказательство теоремы 4

Мы должны доказать, что если k – делитель числа $p - 1$, то среди ненулевых классов вычетов по простому модулю p существует ровно $\phi(k)$ классов порядка k .

Применим индукцию. *База.* Для $k = 1$ утверждение верно.

Переход. Рассмотрим некоторый делитель k числа $p - 1$. Предположим, что для любого делителя d числа k , где $d < k$, существует ровно $\phi(d)$ классов вычетов порядка d . Найдем количество классов вычетов порядка k .

В силу теоремы 6, сравнению $x^k \equiv 1 \pmod{p}$ удовлетворяют ровно k классов вычетов. Каждое решение x этого сравнения имеет некоторый

² Для Фомы неверующего: $40 + 20 + 20 + 8 + 4 + 4 + 2 + 1 + 1 = 100$.

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 $1, 2, \dots, p-1$, 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 $\text{НОК}[m, n]$. Докажите это.

б) Покажите, что порядок числа ab равен mn , если числа m и n взаимно просты, и не обязательно равен числу $\text{НОК}[m, n]$, 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 $(a^2)^{(p-1)/2} = a^{p-1}$ 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 явля-

ется 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 $n \rightarrow \infty$ к зависящему только от k пределу

$$\lim_{n \rightarrow \infty} \frac{\pi_g(n)}{\pi(n)} = \prod_{k:q} \left(1 - \frac{1}{q-1}\right) \cdot \prod_{k \neq q} \left(1 - \frac{1}{q(q-1)}\right),$$

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 со свойством $2^{n-1} \equiv 1 \pmod{n}$.)

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

б) (M672) 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 $n = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$, 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 $\lambda(p_i^{m_i}) = p_i^{m_i-1}(p_i-1)$, 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 ?

в) (M1510) Докажите, что существует бесконечно много таких составных чисел n , что $3^{n-1} - 2^{n-1}$ кратно n .

63. Докажите, что если n – составное число и $1^{n-1} + 2^{n-1} + \dots + (n-1)^{n-1} \equiv -1 \pmod{n}$, то n – число Кармайкла. (Воспользовавшись списком чисел Кармайкла, не превосходящих 10^{16} , можно при помощи компьютера проверить, что не существует ни одного удовлетворяющего этому сравнению числа, не превосходящего 10^{16} . Существуют ли такие числа, большие 10^{16} , мы не знаем.)

Приложения

Бином Ньютона

Малую теорему Ферма легко доказать по индукции, если использовать формулу бинома Ньютона. Мы сделаем это для натуральных чисел a , оставив случай отрицательных чисел читателю.

Пусть сначала $p = 3$. *База индукции:* $1^3 - 1 = 0$ делится на 3. *Переход:* если для некоторого числа a уже доказали, что $a^3 - a$ кратно 3, то

$$\begin{aligned} (a+1)^3 - (a+1) &= a^3 + 3a^2 + 3a + 1 - (a+1) \equiv \\ &= a^3 + 3a^2 + 3a - a \equiv \\ &= a^3 + 1 - a - 1 = a^3 - a \equiv 0 \pmod{3}. \end{aligned}$$

Аналогично для $p = 5$: база очевидна ($1^5 - 1 \equiv 0 \pmod{5}$), а для перехода используем формулу

$$(a+1)^5 = a^5 + 5a^4 + 10a^3 + 10a^2 + 5a + 1.$$

Видите, коэффициенты при a^4, a^3, a^2 и a кратны 5. Поэтому

$$(a+1)^5 \equiv a^5 + 1 \pmod{5},$$

откуда и следует возможность индукционного перехода:

$$\begin{aligned} (a+1)^5 - (a+1) &\equiv \\ &\equiv a^5 + 1 - a - 1 = a^5 - a \pmod{5}. \end{aligned}$$

Упражнение 64. Докажите индукцией по a малую теорему Ферма для а) $p = 2$; б) $p = 7$.

Займемся общим случаем. Формула бинома имеет вид

$$\begin{aligned} (a+1)^p &= a^p + pa^{p-1} + \frac{p(p-1)}{2} a^{p-2} + \\ &+ \frac{p(p-1)(p-2)}{3!} a^{p-3} + \dots \\ &\dots + \frac{p(p-1)}{2} a^2 + pa + 1. \end{aligned}$$

Коэффициенты

$$\begin{aligned} C_p^1 &= p, C_p^2 = p(p-1)/2, \dots \\ \dots C_p^k &= p(p-1)\dots(p-k+1)/k!, \dots \\ \dots C_p^{p-1} &= p \end{aligned}$$

кратны простому числу p . Поэтому $(a+1)^p \equiv a^p + 1 \pmod{p}$, что и требова-

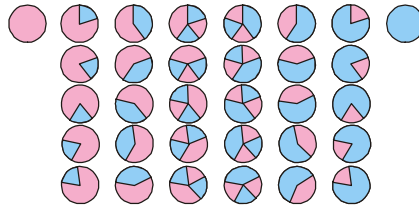
лось:

$$\begin{aligned} (a+1)^p - (a+1) &\equiv \\ &\equiv a^p + 1 - a - 1 = a^p - a \pmod{p}. \end{aligned}$$

Упражнение 65. Если n составное, то хотя бы один из биномиальных коэффициентов $C_n^{n-2}, C_n^2, \dots, C_n^k, \dots, C_n^{n-1}$ не кратен n . Докажите это.

Комбинаторное доказательство

На рисунке изображены все 32 способа раскраски в два цвета круга, который разделен на 5 равных секторов. Среди



них выделяются два способа – когда весь круг синий и когда он весь красный. А остальные разбиты на 6 групп по 5 раскрасок, получающихся одна из другой поворотом.

Задача. Сколькими способами можно раскрасить a разными красками круг, разбитый на p одинаковых секторов, где p – простое число? (Каждый сектор окрашивается одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаются одинаковыми.)

Решение. Очевидно, можно все секторы покрасить одной краской. Таких способов столько же, сколько красок, т.е. a способов.

А вот из любой другой раскраски поворотами можно получить p разных раскрасок (считая и саму эту раскраску: она получается поворотом на 0°). Значит, ответ таков:

$$a + \frac{a^p - a}{p}.$$

Поскольку количество способов не бывает дробным, число $a^p - a$ обязано нацело делиться на p .

Упражнение 66. Сколькими способами можно раскрасить a разными красками круг, разбитый а) на p^2 секторов, где p – простое число? б) на pq секторов, где p, q – простые числа, $p \neq q$? (Каждый сектор окрашиваем одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаем одинаковыми.)

Как строят большие простые числа?

Как помнит читатель первой части статьи, для криптографической системы RSA нужны большие (лучше всего – длиной в несколько сот цифр) простые числа.

Наиболее эффективным средством построения таких чисел сейчас является метод, основанный на следующей лемме.

Лемма. Пусть q – нечетное простое число, r – четное натуральное, $n = qr + 1$. Если существует такое целое число a , что $a^{n-1} \equiv 1 \pmod{n}$ и $\text{НОД}(a^r - 1, n) = 1$, то каждый простой делитель p числа n удовлетворяет сравнению $p \equiv 1 \pmod{2q}$.

Доказательство. Обозначим порядок числа a по модулю p буквой k . Поскольку $a^{n-1} \equiv 1 \pmod{p}$ и $a^{(n-1)/q} \not\equiv 1 \pmod{p}$, то k делится на q . В силу теоремы 3, $p - 1$ делится на k . Следовательно, $p - 1$ делится на q . Кроме того, $p - 1$ четно. Лемма доказана.

Следствие. Если выполнены условия леммы и $r \leq 4q + 2$, то n – простое число.

Доказательство. Пусть n равняется произведению не менее чем двух простых чисел. Поскольку каждое из них не меньше $2q + 1$, получаем противоречие:

$$(2q+1)^2 \leq n = qr + 1 \leq 4q^2 + 2q + 1.$$

Покажем теперь, как, имея большое простое число q , можно пытаться строить существенно большее простое число n . Выберем случайным образом четное число r на промежутке $q < r \leq 4q + 2$ и положим $n = qr + 1$. Затем проверим n на отсутствие малых простых делителей, перепробовав малые простые числа.³ Если при этом выяснится, что n – составное, то следует выбрать новое значение r и повторить вычисления.

Если же есть надежда, что n простое, то можно случайным образом выбрать число a и проверить, выполнены ли для него соотношения $a^{n-1} \equiv 1 \pmod{n}$ и $\text{НОД}(a^r - 1, n) = 1$. Если выполнены, то можно утверждать, что n простое (заметьте: $n > q^2$, так что число n записывается примерно вдвое большим количеством цифр, чем q). Если же нет, то можно взять другое значение a , и так далее.

В настоящий момент нет доказательства того, что этот алгоритм сработает и тем более – что он сработает достаточно быстро. Однако на практике он позволяет строить большие (порядка 10^{300}) простые числа.

³ В этом месте мы чуть лукавим: следует не только делить на малые простые числа, но и применять более хитрые методы проверки на простоту. Хотя эти методы основаны на малой теореме Ферма и по сути сводятся к тому, что если для некоторого a , взаимно простого с n , число a^{n-1} не сравнимо с 1 по модулю n , то n составное, подробное обсуждение завело бы нас слишком далеко в бурно развивающуюся область теории чисел и вычислительной математики.