ГРАФИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ПРОСТЫХ И СОСТАВНЫХ ЧИСЕЛ

К.П. Вишневский, В.И. Чижиков

Кубанский государственный университет, г. Краснодар

Работа посвящена доказательству малой теоремы Ферма. В ней предлагается простой в понимании вариант доказательства. Для доказательства используется графическая интерпретация простых и составных чисел как наиболее простой способ наглядного представления чисел.

Сначала приведем ряд свойств деления целых чисел по модулю. Для произвольных целых чисел a и n справедливо очевидное соотношение

$$a = cn + b. \quad (1)$$

Здесь a – делимое, n – делитель, c – частное и b – остаток от деления целого числа a на целое число n. Если $a < n$, то $c = 0$ и $b = a$, в противном случае b находится на отрезке $[0, n\text{-}1]$. Если же остаток $b = 0$, то говорят, что целое число a делится на целое число n нацело, то есть без остатка. Представление числа a по формуле (1) является единственным. В дальнейшем мы в основном будем использовать только натуральные числа и 0. Поэтому прилагательное целое будем опускать.

Определение. Два числа a и b называются конгруэнтными по модулю n, если они имеют равные остатки при их делении на n.

Для конгруэнтных чисел будем использовать обозначение

$$a \equiv_n b, \quad (2)$$

вместо определяющего соотношения

$$a \bmod n = b \bmod n. \quad (3)$$

Конгруэнтность чисел по модулю обладает следующими свойствами. Если

$$a \equiv_n b, \text{ и } c \equiv_n d, \quad (4)$$

то из представления чисел (1) следуют простые правила:

$$(a + c) \equiv_n (b + d), \quad (5)$$

$$ac \equiv_n b \ , \ . \quad (6)$$

В случае произвольных целых чисел a и c имеем

$$(a + c) \equiv_n ({}_n a +_n c), \quad (7)$$

$$(ac) \equiv_n ({}_n a \,{}_n c), \quad (8)$$

$$a^m \equiv_n ({}_n a^m). \quad (9)$$

Если взять одну и ту же конгруэнтность, то из формул (6) и (8) следует, что обе части конгруэнтности можно возвести в одну и ту же степень, или умножить на одно и тоже целое число. Можно также умножать на одно и то же число обе части конгруэнтности и модуль, то есть, если $a \equiv_n b,$ то и $ak \equiv_{nk} bk,$. Очевидно также, что если $a \equiv_n b,$ то $b \equiv_n a$; если $a = b,$ то $a \equiv_n b,$ а обратное утверждение неверно. Кроме того, разность чисел a и b, удовлетворяющих (2), всегда делится нацело на n:

$${}_n(a - b) = 0. \quad (10)$$

В общем же случае ${}_n(a - b) \equiv_n ({}_n a -_n b).$ Наконец, отметим еще одно свойство конгруэнтности. Если два числа a и b конгруэнтны по модулю $n = pq$, то они конгруэнтны по модулю p и по модулю q, и вообще по модулю d, равному любому делителю числа n.

Теорема 1. Если $a \neq 0, ar \equiv_p as$ и a и p являются взаимно простыми числами, то $r =_p s$.

Доказательство этого утверждения можно дать следующим образом. Из условия теоремы и (10) следует, что $a(r - s) = cp$ или $(r - s) = (c/a)p$. Поскольку разность двух целых чисел является целым числом, а числа a и p – взаимно простые, то отношение (c/a) должно быть целым числом. Следовательно, $(r - s)$ делится на p нацело и $r =_p s$. Обратное утверждение очевидно, так как обе части конгруэнтности можно умножать на любое число.

Таким образом, получение конгруэнтности $r =_p s$ из $ar =_p as$ путем умножения на a^{-1} возможно только в том случае, когда a и p взаимно простые числа.

Теорема 2. Для любого целого числа $a \neq 0$ и простого числа p справедливо соотношение $a^p =_p a$.

Очевидно, что при $_p a = 0$ теорема верна. Поэтому пусть $b =_p a \in [1, p-1]$. Формула (9) позволяет заменить доказательство конгруэнтности $a^p =_p a$ доказательством $b^p =_p b$, b принадлежит отрезку $[1, p- 1]$. Совокупность $p - 1$ элементов, значения которых $1, 2, \ldots, p - 1$, обозначим B. Все элементы этого множества не конгруэнтны друг другу по модулю p. Однако произведение двух любых элементов конгруэнтно некоторому элементу этого множества. Кроме того, они взаимно просты с p.

Рассмотрим последовательность $1, b, b^2, b^3, \ldots, b^k, \ldots$. $\forall m$ и $\forall b$ элемент $_p b^m$ всегда принадлежит B. В силу конечности числа элементов в B один из членов этой последовательности должен появиться второй раз после определенного числа степеней. Пусть первый повторяющийся элемент есть $b^m =_p b^l$. При этом $m > l$. Очевидно, что степень $l = 0$ и $b^m \equiv_p 1$, так как при $l > 0$ согласно теореме 1 мы имели бы очевидное соотношение $b^{m-1} =_p b^{l-1}$, то есть элемент b^{m-1}, конгруэнтный b^{l-1}, появился еще раньше в последовательности, и b^m не был бы первым повторяющимся элементом, что противоречит допущению. Следовательно, первым повторяющимся элементом будет элемент, конгруэнтный единице.

Обозначим посредством n_i остаток деления b^i по модулю p, т.е. $n_i = b^i \bmod p$. Тогда $b^i =_p n_i$ и $b^k =_p n_k$. Следовательно, согласно формуле (8) имеем

$$b^i b^k = b^{i+k} \equiv_p n_i n_k \text{ или } n_i n_k \equiv_p b^{i+k} =_p b^i b^k . \qquad (11)$$

Кроме того, каждому элементу n_i соответствует обратный элемент $n_i^{-1} \equiv_p b^{-i}$, удовлетворяющий согласно (12) определению $n_i n_i^{-1} \equiv_p 1$. Множество с такими свойствами элементов называется группой, а число элементов – порядком группы.

Наименьшее число m, при котором $b^m \equiv_p 1$, называется порядком элемента b, а последовательность $1, b, b^2, b^3, \ldots, b^{m-1}$ его периодом. Все элементы периода обозначим F. При дальнейшем увеличении степени m элементы F начинают повторяться. Легко также видеть, что $b^{m-1} \equiv_p b^{-1}, b^{m-2} \equiv_p b^{-2}$ и т.д. Период любого элемента b образует циклическую группу, которая является подмножеством множества B. Более того, порядок элемента (порядок подгруппы) является делителем числа элементов множества B, т.е. $p - 1 = ms$. Действительно, возьмем элемент $c_1 \in B$, но не принадлежащий периоду F. Образуем всевозможные произведения $c_1 b^i$, $i \in [0, m - 1]$. Таких элементов будет m. Обозначим их $c_1 F$. Множества F и $c_1 F$ не имеют общих элементов. В противном случае мы имели бы соотношение $c_1 b^i \equiv_p b^k$, умножая которое на b^{-i} и применяя теорему 1, получили бы соотношение $c_1 \equiv_p b^{k-i}$, т.е. и элемент c_1 принадлежал бы F. Далее возьмем $c_2 \in B$, но $c_2 \notin F$ и $c_2 \notin c_1 F$. Аналогично доказываем, что F, $c_1 F$ и $c_2 F$ не имеют общих элементов. Продолжая этот процесс, пока не исчерпаем всех элементов группы B, мы получим, что множество B будет разбито на s непересекающихся подмножеств F, $c_1 F$, $c_2 F$, …, $c_{s-1} F$ и, очевидно, $p - 1 = ms$. При простом p число $(p - 1)$ – четное и поэтому составное. Использование теоремы 1 позволяет получить $b^{p-1} \equiv_p b^{-1}$ и $b^p \equiv_p b$. Таким образом, теорема доказана.

Очевидно, что множество B также является группой. Однако любое другое множество остатков относительно операции деления по модулю n в общем случае не является группой. Поскольку все приведенные рассуждения об обратном элементе, порядке элемента и его цикле базируются на теореме 1, которая доказана для взаимно простых чисел b и p.

Следствие 1. Для любого $a \neq 0$ и ${}_p a \neq 0$ справедлива конгруэнтность

$$a^{p-1} \equiv_p 1 \text{ (малая теорема Ферма).} \qquad (12)$$

Действительно, из теорем 1 и 2 следует, что $a^p = a \cdot a^{p-1} \equiv_p a = a \cdot 1$ и $a^{p-1} \equiv_p 1$.

Следствие 2. Для любого числа $a \neq 0$ и простого числа p существуют такие $1 \le x \le p-1$ и $1 \le b \le p-1$, что выполняется соотношение

$$a^x \equiv_p b\,. \qquad (13)$$

При заданном простом числе p и выбранном b число a, которое удовлетворяет (13), называется примитивным корнем p, а x – дискретным логарифмом b. Никаких эффективных методов вычисления примитивных корней и дискретных логарифмов не предложено.

Следствие 3. Если $x \equiv_{(p-1)} y$, то

$$a^x \equiv_p a^y\,. \qquad (14)$$

Соотношение (14) легко получить, если учесть, что имеет место очевидное соотношение $x = y + c(p-1)$ и $a^x \equiv_p a^y \cdot (a^{p-1})^c$.

Следствие 4. Если d положительное наименьшее число, такое что $a^d \equiv_p 1$, то для любого $c \neq 0$ и $a^c \equiv_p 1$ d делит c без остатка.

Положим $c = de + r$. Тогда $a^c \equiv_p (a^d)^e a^r \equiv_p a^r$ и заключаем, что конгруэнтность $a^c \equiv_p 1$ будет иметь место только, если $r = 0$, т.е. если d делит c без остатка.

Следствие 5. Множества c_1F, c_2F, …, $c_{s\text{-}1}F$ не являются подгруппами, так как они не содержат элемента, конгруэнтного единице. Их называют смежными классами для элементов c_i. Циклическая группа F представляет класс смежности для единичного элемента.

Как ранее мы отмечали, что множество остатков деления чисел по произвольному модулю n не образует группы. Это обусловлено тем, что элементы этого множества не являются взаимно простыми с модулем n. Од-нако на базе этих элементов все-таки можно образовать группу. С этой целью поступают следующим образом. Вводят понятие чисел, конгруэнтных одному и тому же остатку. Такие числа образуют класс по модулю n. Они представимы в форме $cn + b$ с числом c, принимающим значения всех возможных целых чисел. Соответственно n различным значениям b имеем n различных классов по модулю n. Далее любое число класса называется вычетом по модулю n по отношению ко всем числам того же класса. Вычет, получаемый при $c = 0$, равный остатку b, называется наименьшим неотрицательным вычетом. Взяв от каждого класса по одному вычету, получаем полную систему вычетов по модулю n. Очень часто в качестве полной системы вычетов используют наименьшие неотрицательные вычеты $0, 1, \ldots, n-1$.

Числа одного и того же класса по модулю n имеют с модулем один и тот же наибольший общий делитель. Особенно важны классы, для которых этот делитель равен единице, т.е. классы, содержащие числа, взаимно простые с модулем. Взяв от каждого такого класса по одному вычету, получим приведенную систему вычетов по модулю n. Очевидно, что приведенную систему вычетов можно получить из полной системы $0, 1, \ldots, n-1$, оставив в ней взаимно простые элементы с модулем n. Число элементов в приведенной системе вычетов зависит от модуля n. Его обозначают $\varphi(n)$ и эту зависимость называют функцией Эйлера. Если p простое число, то $\varphi(n) = p - 1$ и $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Последнее равенство можно доказать прямым вычислением, то есть исключением из полной системы вычетов p^α чисел, крат-

ных p: p, $2p$, …, $p^{\alpha-1}p$.. Очевидно, что таких чисел $p^{\alpha-1}$. В общем случае для любого целого числа a, представленного в каноническом виде $a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_k^{\alpha k}$; $\varphi(a) = a(1-1/p_1) \cdot a(1-1/p_2) \cdot \ldots \cdot a(1-1/p_k)$. Множество элементов приведенной системы вычетов обладает всеми свойствами множества B.

Основные результаты модульного деления чисел можно получить простым графическим способом. Для этого представим число p как число, состоящее из цепочки p элементов (рис.1).

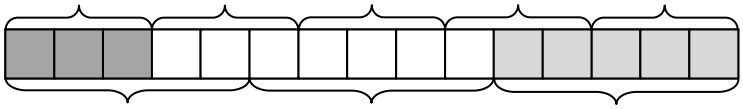

Рис. 1. Запись числа 15 в виде цепочки и его делители 3 и 5.

Будем называть «волной» отдельный сегмент цепочки, соответствующий делителю числа p. Очевидно, что если число составное, то мы можем наложить на цепочку целое число «волн», представляющих какой-нибудь множитель. Для простого число можно совместить лишь две «волны», ответственных за деление числа на себя и на 1.

Теперь представим это же число в виде замкнутой цепочки (рис. 2).

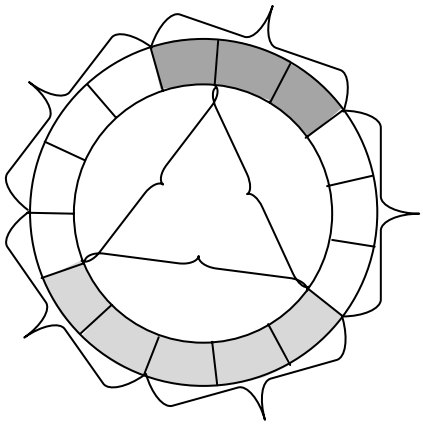

Рис. 2. Запись числа 15 в виде замкнутой цепочки и его делители 3 и 5.

Снова в случае простого числа можно уложить в замкнутую цепочку единственную «волну» p различными способами, полученными путем сдвига на один элемент начала «волны». Однако если же число будет составным, то число способов укладывания «волны», соответствующей какому-либо делителю, будет равно k, причем $k \le p$.

Далее для простоты представим «волну» в виде некоторого двоичного числа, то есть элемент цепочки может принимать только два значения (0 или 1). Так при $p = 7$ можно взять произвольный вариант двоичной записи числа длиной 7 бит, например 0000001, и записать его 7 различными способами (применяя циклический сдвиг): 0000001, 0000010, 0000100, 0001000, 0010000, 0100000 и 1000000. Если число составное, например 6, то вариант 001001, соответствующий делителю 2, используя сдвиг, можно записать 3 способами: 001001, 010010 и 100100. Вариант 010101, который соответствует делителю 3, можно записать лишь 2 способами: 010101 и 101010.

Теперь обобщим представление «волны» для всех вариантов двоичной записи числа длиной p. Учтем, что варианты 0000..0 и 1111..1 всегда неизменны при любых сдвигах. Они отвечают за деление на 1. Поэтому их необходимо исключить. В случае простого числа общее количество всех сдвигов для любого варианта «волны» будет равно p. Если же число p будет составным, то для некоторых вариантов «волны», соответствующей одному из множителей p, количе-

ство сдвигов будет меньше p. Следовательно, среднее количество сдвигов любой «волны» для простого числа будет целым, а для составного – дробным. Всего существует 2^p вариантов сдвигов. Таким образом, учитывая варианты 0000..0 и 1111..1, получаем выше доказанную теорему в случае простого числа p

$$2^p \equiv_p 2. \tag{15}$$

Приведенные рассуждения со сдвигами и укладыванием «волн» остаются справедливыми и в случае, когда элемент цепочки принимает не два, а a значений. В этой ситуации конгруэнтность (15) записывается в виде

$$a^p \equiv_p a. \tag{16}$$

Graphic interpretation of prime and compound numbers

K.P.Vishnevsky, V.I.Chizhikov

Work is devoted to the proof of the small Farm theorem. In it the variant of the proof is offered simple in understanding. For the proof graphic interpretation of prime and compound numbers as most a simple way of evident representation of numbers is used.

