



УДК 531.38; 531.39

ПРЕДСТАВЛЕНИЕ МОДУЛЯРНЫХ ОПЕРАЦИЙ НАД ПОЛЕМ ВЕЩЕСТВЕННЫХ ЧИСЕЛ

*В.А. Есаулов, esaul_va@mail.ru, В.С. Токарев, vstokarev@mail.ru,
П.А. Павлов, mr.vip.pavlov@list.ru*

Южно-Российский государственный политехнический университет (НПИ)
имени М.И. Платова, г. Новочеркасск

В данной статье рассматривается возможность обобщения операций модулярной арифметики на случай вещественных чисел. Введено представление оператора остатка по модулю для произвольной величины основания над полем вещественных чисел. Установлено, что степень близости двух чисел косвенно может рассматриваться как степень близости их соответствующих остатков. Это позволяет обобщить операцию приращения, используемую в традиционном анализе. Введено понятие производной функции по модулю аргумента, установлена ее связь с классической производной функции по аргументу. Сформулированы принципы построения степенных рядов функций по остатку аргумента. Это позволило получить обобщение ряда Тейлора и Маклорена в рамках модулярного анализа.

Ключевые слова: математика, степенные ряды, модулярные операции, производная функции, математический анализ, операторная экспонента.

THE PERFORMANCE OF MODULAR OPERATIONS OVER THE FIELD OF REAL NUMBERS

V.A. Esaulov, V.S. Tokarev, P.A. Pavlov

Platov South-Russian State Polytechnic University (NPI), Novochoerkassk

This article discusses the possibility of generalization of modular arithmetic operations in the case of real numbers. We introduce a representation of the remainder operator modulo for an arbitrary value of the base over the field of real numbers. It is found that the degree of proximity of two numbers can be indirectly considered as the degree of proximity of their respective residues. This allows you to generalize the increment operation used in traditional analysis. The concept of a derived function modulo the argument is introduced, its connection with the classical derivative of the function by the argument is established. The principles of constructing power series of functions on the remainder of the argument are formulated. This allowed us to obtain a generalization of the Taylor and Maclaurin series in the framework of modular analysis.

Keywords: mathematics, power series, modular operations, derivative of a function, mathematical analysis, operator exponent.

Сравнение, или вычисление остатка по модулю натурального числа — отношение эквивалентности на множестве целых чисел, связанное с делимостью. На его основе можно построить систему чисел, обладающую высокой наглядностью и конструктивностью. Так, одним из важных результатов теории сравнений является модулярная арифметика, имеющая широкий круг приложений во многих областях математики [1,2].

Рассмотрим вопросы обобщения операции остатка на случай действительных чисел. Как известно, остаток по модулю n можно рассматривать как функцию вида

$$x \bmod n = \begin{cases} x, & x \in N_n \\ 0, & x = n \end{cases}, \quad N_n = 0..n-1 \quad (1)$$



В силу своих свойств операция может быть периодически продолжена за пределы конечного множества из чисел от 0 до $n-1$. В этой связи ее можно интерпретировать как треугольную функцию, имеющую период n . Это позволяет сделать вывод о том, что зависимость (1) может быть представлена рядом Фурье вида [3]

$$\psi_n(x) = x \bmod n = \sum_{m=0}^{n-1} a_m e^{\frac{2\pi j x m}{n}} \quad (2)$$

Неизвестные коэффициенты можно определить, решая систему уравнений вида:

$$\begin{cases} \psi_n(0) = \sum_{m=0}^{n-1} a_m = 0 \\ \psi_n(1) = \sum_{m=0}^{n-1} a_m e^{\frac{2\pi j m}{n}} = 1 \\ \dots \\ \psi_n(n-1) = \sum_{m=0}^{n-1} a_m e^{\frac{2\pi j m (n-1)}{n}} = n-1 \end{cases} \quad (3)$$

В силу структуры (2) решение системы (3) можно рассматривать как дискретное обратное преобразование от функции $\psi_n(x)$, заданной в узлах на множестве N_n . В таком случае функцию остатка в тензорной форме можно представить как

$$\psi_n(x) = x \bmod n = IFFT(N_n) \otimes \Psi_n(x), \quad \Psi_n(x) = \left\{ e^{\frac{2\pi j x k}{n}} \right\}_{k=0}^{n-1} \quad (4)$$

Таким образом, можно говорить о том, что операция взятия остатка имеет тригонометрическое представление. Этот результат существенно отличается от традиционных обобщений операций многозначной логики [1,2] или интерпретации операций булевой алгебры, потому что позволяет без ограничений использовать (4) для аргументов, выходящих за пределы области определения N_n .

Из вида (4) можно сделать вывод, что при $x \rightarrow 0$ будет справедливо соотношение $\Psi_n(x) \rightarrow 0$. Это позволяет сделать вывод о том, что при близких значениях некоторых переменных x_1 и x_2 значения их остатков $\psi_n(x_1)$ и $\psi_n(x_2)$ также будут близки, а для остатка разности будет выполняться свойство $\psi_n(x_1 - x_2) \xrightarrow{|x_1 - x_2| \rightarrow 0} 0$. В этой связи можно поставить вопрос о обобщении традиционного понятия производной функции. Как известно, производной функции $f(x)$ в точке x_0 называется предел отношения приращения функции к вызвавшему его приращению аргумента, когда приращение аргумента стремится к нулю, т.е. выполняется соотношение [4]

$$f'(x_0) = \lim_{\Delta x \rightarrow 0} \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x} \quad (5)$$



Можно модифицировать соотношение (5), рассматривая отношение приращения функции к приращению остатков $\Psi_n(x_0 + \Delta x)$ и $\Psi_n(x_0)$ остатку от приращения аргумента, т.е., ввести определение производной по остатку аргумента

$$\frac{d_{\Psi_n} f(x)}{dx} = \lim_{\Delta x \rightarrow 0} \frac{f(x_0 + \Delta x) - f(x_0)}{\Psi_n(x_0 + \Delta x) - \Psi_n(x_0)} \quad (6)$$

Между производными и производными по остатку аргумента легко установить связь. Для этого сократим числитель и знаменатель, например (6), на Δx . Тогда будем иметь

$$\frac{d_{\Psi_n} f(x_0)}{dx} = \lim_{\Delta x \rightarrow 0} \frac{\frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}}{\frac{\Psi_n(x_0 + \Delta x) - \Psi_n(x_0)}{\Delta x}} \quad (7)$$

Из (7) непосредственно вытекает [4,5]

$$\frac{d_{\Psi_n} f(x_0)}{dx} = \lim_{\Delta x \rightarrow 0} \frac{\frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}}{\frac{\Psi_n(x_0 + \Delta x) - \Psi_n(x_0)}{\Delta x}} = \frac{\lim_{\Delta x \rightarrow 0} \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}}{\lim_{\Delta x \rightarrow 0} \frac{\Psi_n(x_0 + \Delta x) - \Psi_n(x_0)}{\Delta x}} \quad (8)$$

Как видно, из (8), числитель удовлетворяет (5). Знаменатель дает неопределенность вида $\frac{0}{0}$, однако ее легко раскрыть по правилу Лопиталья. В этом смысле будем иметь

$$\frac{d_{\Psi_n} f(x_0)}{dx} = \frac{f'(x_0)}{\Psi_n'(x_0)} \quad (9)$$

Легко видеть, что производная в смысле (6) может существовать при условии дифференцируемости $f(x)$ в точке x_0 , а также существования соотношения (9). Из соотношения (9) можно сформулировать свойство понижения степени остатка

$$\frac{d_{\Psi_n} (\Psi_n(x))^m}{dx} = \frac{((\Psi_n(x))^m)'}{\Psi_n'(x)} = \frac{m(\Psi_n(x))^{m-1} \Psi_n'(x)}{\Psi_n'(x)} = m(\Psi_n(x))^{m-1} \quad (10)$$

Очевидно, что определение производной (9) удовлетворяет соотношениям:

$$\begin{cases} \frac{d_{\Psi_n} (f(x) + g(x))}{dx} = \frac{d_{\Psi_n} f(x)}{dx} + \frac{d_{\Psi_n} g(x)}{dx} \\ \frac{d_{\Psi_n} (f(x)g(x))}{dx} = g(x) \frac{d_{\Psi_n} f(x)}{dx} + f(x) \frac{d_{\Psi_n} g(x)}{dx} \end{cases} \quad (11)$$

Зная определение (9), можно ввести понятие дифференциала функции. Так, под дифференциалом функции будем понимать следующее соотношение

$$D_{\Psi_n} (f(x)) = \frac{d_{\Psi_n} f(x)}{dx} D_{\Psi_n} x = \frac{d_{\Psi_n} f(x)}{dx} \Psi_n'(x) dx = f'(x) d\Psi_n(x) \quad (12)$$

Пользуясь свойством (10), можно вывести понятие ряда Тейлора для случая остатков. Пусть дана функция $f(x)$. Предположим, что она является бесконечно



дифференцируемой в смысле (9) в некоторой окрестности точки x_0 . Будем искать ее представление в виде ряда следующего вида

$$f(x) = \sum_{m=0}^{\infty} a_m (\psi_n(x-x_0))^m \quad (14)$$

Очевидно, что для функции остатка будет выполняться $\psi_n(0) = 0$. Таким образом, $a_0 = f(x_0)$. Применяя к (12) почленное дифференцирование в смысле (9) и учитывая при этом соотношение понижения степени (10), для коэффициентов разложения будем иметь представление

$$a_m = \frac{1}{m!} \left. \frac{d^m f(x)}{dx^m} \right|_{x=x_0} \quad (15)$$

Тогда ряд Тейлора в смысле дифференцирования по остатку с учетом (16) будет иметь вид [3-5]:

$$f(x) = \sum_{m=0}^{\infty} \frac{1}{m!} \left. \frac{d^m f(x)}{dx^m} \right|_{x=x_0} (\psi_n(x-x_0))^m \quad (16)$$

Остаточный член разложения можно оценить как

$$R_n = \frac{1}{(m+1)!} \left. \frac{d^{m+1} f(x)}{dx^{m+1}} \right|_{x=\xi} (\psi_n(x-x_0))^{m+1}, \quad x_0 < \xi < x.$$

При этом можно говорить о сходимости ряда (12), если выполняется $\lim_{n \rightarrow \infty} R_n = 0$.

Важным частным случаем ряда Тейлора является ряд Маклорена. С учетом приведенных соображений он будет иметь следующий вид:

$$f(x) = \sum_{m=0}^{\infty} \frac{1}{m!} \left. \frac{d^m f(x)}{dx^m} \right|_{x=0} (\psi_n(x))^m \quad (17)$$

Рассмотрим некоторые важные частные случаи разложения в ряд Тейлора. Разложим экспоненту $f(x) = e^{j\pi nx}$ с целочисленным показателем n в ряд Тейлора по степеням остатка по модулю два $\psi_2(x) = \frac{1 - e^{j\pi x}}{2}$. Соотношение для производной порядка m будет иметь вид:

$$\frac{d^m e^{j\pi nx}}{dx^m} = \frac{n!}{(n-m)!} (-2)^m e^{j\pi(n-m)x} \quad (18)$$

Подставляя соотношение (18) в (17), получим разложение вида

$$e^{j\pi nx} = \sum_{m=0}^n \frac{1}{m!} \frac{n!}{(n-m)!} (-2)^m (\psi_2(x))^m = \sum_{m=0}^n \frac{1}{m!} \frac{n!}{(n-m)!} (-1)^m (1 - e^{j\pi x})^m \quad (19)$$

Полученное соотношение можно рассматривать как формулу понижения степени для экспонент с любым натуральным показателем. С другой стороны, полиномы в правой части (18) можно рассматривать как ортогональные на отрезке



$x \in [0, 2]$. Это свойство непосредственно вытекает из свойства системы комплексных экспонент в левой части (18).

Рассмотрим разложение в ряд по $\Psi_2(x)$ функции $f(x) = x$. Действуя аналогично тому, как это сделано выше, получим степенной ряд следующего вида:

$$f(x) = x = \frac{1}{\pi j} \sum_{m=1}^{\infty} \frac{1}{m} (1 - e^{j\pi x})^m \quad (20)$$

Разложение (20) представляет интерес тем, что дает связь между переменной и разложением по ее степеням ее остатка по модулю два. Ряд будет сходиться при выполнении условия $|1 - e^{j\pi x}| < 1$.

Разложение (20) можно интерпретировать следующим образом. Как известно, справедливо следующее тождество [4,5]:

$$\ln(1 - x) = - \sum_{m=1}^{\infty} \frac{1}{m} x^m, \quad |x| < 1 \quad (21)$$

Тогда, с учетом (21), соотношение (20) может иметь вид:

$$x = - \frac{1}{\pi j} \sum_{m=1}^{\infty} \frac{1}{m} (1 - e^{j\pi x})^m = - \frac{1}{\pi j} \ln(1 - (1 - e^{j\pi x})) = - \frac{1}{\pi j} \ln(1 - 2\Psi_2(x)) \quad (22)$$

Соотношение (22) говорит о эквивалентности разложения (21) логарифмической функции от остатка аргумента. Легко видеть, что правая или левая части (22) являются эквивалентными. Это подтверждает верность (20).

Соотношение (20), помимо прочего, можно обобщить на случай операторов. Так, рассмотрим дифференциальный оператор вида $h \frac{d}{dx}$, где h – достаточно малое число. В таком случае разложение (20) примет вид

$$h \frac{d}{dx} = - \frac{1}{\pi j} \sum_{m=1}^{\infty} \frac{1}{m} \left(I - e^{j\pi h \frac{d}{dx}} \right)^m \quad (23)$$

В отношении конкретной функции справедлива формула Хевисайда, выражающая приращение функции через операторную экспоненту [4]:

$$f(x + h) = e^{h \frac{d}{dx}} f(x) \quad (24)$$

Таким образом, с учетом (24), представление можно переписать следующим образом:

$$h \frac{df(x)}{dx} = - \frac{1}{\pi j} \sum_{m=1}^{\infty} \frac{1}{m} \left(I - e^{j\pi h \frac{d}{dx}} \right)^m f(x) = - \frac{1}{\pi j} \sum_{m=1}^{\infty} \frac{1}{m} (-1)^m \Delta^m f(x) \quad (25)$$

где Δ – оператор приращения, действующий по правилу $\Delta f(x) = f(x + h) - f(x)$.

С учетом (21), соотношение (25) можно переписать в следующем виде:

$$h \frac{df(x)}{dx} = \ln(I + \Delta) f(x) \quad (26)$$



Соотношение (26) задает соотношение, которое можно трактовать как обращение формулы (24). Действительно, из (24) можно получить:

$$\Delta f(x) = \left(e^{h \frac{d}{dx}} - I \right) f(x) \quad (27)$$

Перенеся единичный оператор в правую часть и логарифмируя обе части, получим соотношение (26).

Аппроксимируя логарифмический оператор в составе (26) по параметру Δ , можно получить разные конечно-разностные аппроксимации оператора производной. Это может послужить методологической основой для построения конечно-разностных схем различного рода.

Приведенные соображения позволяют сделать вывод о корректности введения понятия модулярной операции над вещественными числами. Полученные на основании ее формализма для случая порядка 2 остатка результаты показывают свою непротиворечивость с уже существующими представлениями, что видно на примере соотношений (22)-(27). Это позволяет говорить о возможности конструктивного применения введенных обобщений при построении алгоритмов различных численных методов.

Список цитируемой литературы

1. Ландо С.К. Введение в дискретную математику. МНЦМО, 2012. – 272 с.
2. Коблиц Н. Курс теории чисел и криптографии / пер. с англ. М. А. Михайловой и В. Е. Тараканова, под ред. А. М. Зубкова. – М.: Научное изд-во ТВП, 2001. – 254 с.
3. Эдвардс Р. Ряды Фурье в современном изложении. Т. 2. М.: Мир, 1985. – 400 с.
4. Зорич В.А. Математический анализ. Т.1. – Изд. 4-е, испр. – М.: МЦНМО, 2002. – 664 с.
5. Дадаян А.А., Дударенко В.А. Математический анализ. Минск: Вышэйшая школа, 1990. – 432 с.