УДК 519.642.8

01.00.00 Физико-математические науки

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ И НЕКОТОРЫЕ ЕЕ ПРИЛОЖЕНИЯ

Лаптев Владимир Николаевич
к.т.н., доцент
Кубанский государственный аграрный университет, Краснодар, Россия

Сергеев Александр Эдуардович
к.ф.-м.н, доцент

Сергеев Эдуард Александрович
к.ф.-м.н, доцент
Кубанский государственный университет, Краснодар, Россия

В статье приводится основная теорема арифметики и ее роль. Рассматриваются различные кольца, в которых она выполняется

Ключевые слова: КОЛЬЦО, ОБЛАСТЬ, ТЕОРЕМА АРИФМЕТИКИ

UDC 519.642.8

Physics and Math

FUNDAMENTAL THEOREM OF ARITHMETIC AND SOME OF ITS ASPECTS

Laptev Vladimir Nikolaevich
Cand.Tech.Sci., associate professor
Kuban State Agrarian University, Krasnodar, Russia

Sergeev Alexander Eduardovich
Cand.Phys.-Math.Sci., associate professor

Sergeev Eduard Alexandrovich
Cand.Phys.-Math.Sci., associate professor
Kuban State University, Krasnodar, Russia

In this article, we present the fundamental theorem of arithmetic and its role. We consider various rings for its performance

Keywords: RING, DOMAIN, THEOREM OF ARITHMETIC

Идея изучения математических объектов путём факторизации (разбиения) их на более простые математические объекты – одна из плодотворных идей современной математики. Она первоначально возникла при изучении натуральных чисел, в форме так называемой «основной теоремы арифметики».

Частный случай основной теоремы арифметики был сформулирован и доказан Евклидом в восьмой книге его «Начал» ещё в третьем веке до нашей эры. По-видимому, впервые в полной общности основная теорема арифметики была сформулирована и доказана К.Ф. Гауссом в 1801 году в его знаменитом сочинении «Арифметические исследования». Она формулируется следующим образом: Каждое натуральное число $n>1$ можно представить в виде произведения конечного числа простых чисел и такое представление единственно с точностью до порядка следования простых сомножителей.

Если $n = p_1 p_2 \dots p_s$ и все p_i – простые числа, то объединяя в этом произведении равные сомножители, получаем каноническое представление числа: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, где $\alpha_i \geq 1$ и p_i – различные простые числа.

Из канонического представления числа n легко получить, что число $\tau(n)$ различных натуральных делителей числа n вычисляется по формуле

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\dots(\alpha_r + 1).$$

Однако найти каноническое представление больших натуральных чисел найти непросто, а порой это превышает вычислительные возможности современной математики. Например, каноническая факторизации числа $2^{1093} - 1$ по-видимому, неизвестна, хотя это число составное, так как делится на 1093^2.

Среди составных натуральных чисел имеются такие, что $\tau(n) < \tau(m)$ для всех натуральных $m < n$. Этим свойством обладают числа 4,6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840. Такие натуральные числа Раманудж назвал сильно составными и исследовал их распределение в натуральном ряде чисел.

Со временем аналог основной теоремы арифметики был сформулирован для кольца целых чисел и кольца полиномов $K[x]$, где K – произвольное поле. Аналог основной теоремы арифметики для кольца полиномов $K[x]$: каждый полином из $K[x]$ степени больше или равной единицы раскладывается (факторизуется) в произведение неприводимых полиномов из этого кольца, и такое разложение однозначно с точностью до ассоциированности.

Напомним, что два полинома $f(x)$ и $g(x)$ из кольца $K[x]$ называются ассоциированными, если существует не равная нулю константа α из поля K такая, что $g(x) = \alpha f(x)$.

Приведение теоремы послужили примерами для формирования более общего понятия евклидова кольца, в котором выполняется аналог основной теоремы арифметики.

Коммутативное, ассоциативное кольцо A с единицей, в котором из $a,b\in A,\ a\neq 0,\ b\neq 0$ всегда выполняется $a\cdot b\neq 0$ (то есть в кольце A нет делителей нуля), называется областью целостности (или просто областью). Область A называется евклидовым кольцом, если существует ненулевая функция $\lambda: A\to \mathbb{N}\cup\{0\}$ такая, что для любых $a,b\in A,\ b\neq 0$ существуют такие $q,r\in A,$ что $a=bq+r$ и $r=0$ или $\lambda(r)<\lambda(b).$ Функцию λ в этом случае называют евклидовой.

Например, кольцо целых чисел $\mathbb{Z}$ - евклидово кольцо, так как в качестве евклидовой функции $\lambda:\mathbb{Z}\to\mathbb{N}\cup\{0\}$ можно взять функцию, определенную формулой $\lambda(a)=|a|,$ где $|a|$ – модуль числа $a.$

Кольцо полиномов $K[x]$ над полем K также является евклидовым: в качестве его евклидовой функции $\lambda: K[x]\to\mathbb{N}\cup\{0\}$ можно взять $\lambda(f(x))=\deg(f)$ – степень полинома $f.$

Пусть m – натуральное число, целые числа a и b называются сравнимыми по модулю $m,$ т.е. $a\equiv b(\mathrm{mod}\, m),$ если m делит $a-b.$

Если $K=\mathbb{Q}(\sqrt{d})=\left\{a+b\sqrt{d}\,\middle|\, a,b\in\mathbb{Q}\right\}$ – квадратичное расширение поля $\mathbb{Q}$, т.е. d – целое число, не являющееся квадратом целого числа, то кольцо целых алгебраических чисел A_K поля K определяется по следующим правилам:

$$A_K=\mathbb{Z}+\sqrt{d}\mathbb{Z}=\left\{a+b\sqrt{d}\,\middle|\, a,b\in\mathbb{Z}\right\},\ \text{если}\ d\equiv 2,3(\mathrm{mod}\ 4);$$

$$A_K=\mathbb{Z}+\frac{1+\sqrt{d}}{2}\mathbb{Z}=\left\{a+\frac{1+\sqrt{d}}{2}b\,\middle|\, a,b\in\mathbb{Z}\right\},\ \text{если}\ d\equiv 1(\mathrm{mod}\ 4).$$

Поиск различных евклидовых колец – один из моментов исследований в теории колец. Существует всего шестнадцать

вещественных квадратичных евклидовых колец над кольцом [2]: это кольца целых алгебраических чисел квадратичных полей $K = \mathbb{Q}(\sqrt{d})$ для $d =$ 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.

Постепенно математики пришли к понятию факториального кольца (факториальной области). Сформулируем это понятие. Пусть A – область, $U(A)$ – мультипликативная группа обратимых элементов области A, т.е. элемент a из A принадлежит $U(A)$ только если существует такой элемент $b \in A$, что $a \cdot b = 1_A$, где 1_A – единица области A. Необратимый элемент $d \in A$ называется неприводимым элементом области A, если его нельзя представить в виде произведения $d = a \cdot b$, где a и b также необратимые элементы.

Область A называется факториальной областью (областью с однозначной факторизацией), если каждый её необратимый элемент можно представить в виде конечного произведения неприводимых элементов из A, и это представление единственно с точностью до порядка следования сомножителей и с точностью до ассоциированности неприводимых сомножителей.

Таким образом, каждая евклидова область есть факториальная область, однако существуют факториальные области, не являющиеся евклидовыми. Например, хорошо известно, что если K – поле, то кольцо полиномов $K[x, y]$ от двух переменных x, y является факториальным, но неевклидовым кольцом.

Пусть A – коммутативное кольцо, J – непустое подмножество элементов из A, обладающее свойствами: для любых $d \in A$ и a, $b \in A$ имеем включения $a + b \in J$, $a - b \in J$, $d \cdot a \in J$. Тогда такое подмножество J называют идеалом кольца A.

Если для идеала J существует такой элемент $t \in J$, что множество $(t) = \{t \cdot a | a \in A\}$ совпадает с J, то J называют главным идеалом кольца A. Область целостности A называется областью главных идеалов, если каждый идеал в ней главный. Например, как легко проверить, всякая евклидова область является областью главных идеалов. Имеет место теорема [3].

Теорема 1. *Всякая область главных идеалов является областью с однозначной факторизацией.*

Существуют области с однозначной факторизацией, не являющиеся областями главных идеалов, например, кольцо от двух переменных $K[x, y]$ над полем K.

С помощью теоремы об однозначной факторизации в кольце целых чисел можно найти все решения в целых числах некоторых неопределенных (диофантовых) уравнений. Например, с помощью этой теоремы можно доказать, что неопределенное уравнение $x^2 + y^2 = z^2$ имеет решения $x = a^2 - b^2,\ y = 2ab,\ z = a^2 + b^2$, где a и b – произвольные целые числа.

Аналогично можно доказать, что уравнение $x^4 + y^4 = z^4$ не имеет нетривиальных решений в целых числах.

Используя теорему об однозначной факторизации в произведение неприводимых элементов в кольце целых гауссовых чисел $\mathbb{Z}[i]$, можно найти все решения в целых числах неопределенного уравнения $x^2 + 4 = y^3$: такими целыми решениями будут только числа $x = \pm 2,\ y = 2$ и $x = \pm 1,\ y = 5$. Этот результат был известен ещё П. Ферма (1601 – 1665), но его доказательства он не привёл.

Используя теорему об однозначной факторизации в кольце $\mathbb{Z}[\rho]$, где $\rho = \frac{-1 + i\sqrt{3}}{2}$ можно доказать, что уравнение $x^3 + y^3 = z^3$ не имеет

нетривиальных решений в целых числах. Это утверждение П. Ферма впервые доказал именно таким путём Л. Эйлер (1707 – 1783).

Таким образом, мы видим, что кольца с однозначной факторизацией позволяют находить в целых числах все решения некоторых диофантовых уравнений. Эти кольца имеют и другие приложения [1], [2], [3].

ЛИТЕРАТУРА

1. Хассе Г. Лекции по теории чисел, М. 1953.

2. Боревич З.И., Шафаревич И.Р., Теория чисел, М. 1972.

3. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел, М. 1987.

References

1. Hasse G. Lekcii po teorii chisel, M. 1953.

2. Borevich Z.I., Shafarevich I.R., Teorija chisel, M. 1972.

3. Ajerljend K., Rouzen M. Klassicheskoe vvedenie v sovremennuju teoriju chisel, M. 1987.