ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

В. В. ЖИКОВ

Владимирский государственный педагогический университет

THE BASIC THEOREM OF ARITHMETIC

V. V. ZHIKOV

Any integer greater than one can be uniquely represented as a product of prime divisors. These results are called "the basic theorem of arithmetic". Apart from its many applications in secondary school mathematics, the idea of the division theory of polynomials is given – Gaussian integers, and Euclidean rings, in general. Examples of rings of algebraic numbers admitting a factorization into prime divisors which is not unique are presented.

Всякое целое число, большее единицы, однозначно разлагается на простые делители. Эта основная теорема арифметики не только имеет многочисленные приложения в школьном курсе, но и служит образцом теории делимости для многочленов, целых гауссовых чисел и вообще евклидовых колец. Приведены примеры колец алгебраических чисел, в которых есть разложение на простые делители, но нет единственности разложения.

Арифметика изучает свойства натуральных чисел 1, 2, 3, ... Эти числа интересуют людей с древнейших времен, причем особое внимание всегда уделялось простым числам. Многие числа могут быть разложены на меньшие множители: $10 = 2 \cdot 5$, $111 = 3 \cdot 37$ и т.п. Числа, неразлагаемые таким образом, носят название простых. Точнее, простым называется такое натуральное число, большее единицы, которое не имеет других делителей, кроме единицы и самого себя. Значение простых чисел заключается в том, что любое натуральное число, большее единицы, является простым либо разлагается в произведение простых. В самом деле, если данное число непростое, то его можно последовательно разлагать на множители до тех пор, пока все множители не окажутся простыми, например $666 = 2 \cdot 333 = 2 \cdot 3 \cdot 111 = 2 \cdot 3 \cdot 3 \cdot 37 = 2 \cdot 3^2 \cdot 37$. Простое доказательство этого факта содержится в книге VII "Начал" Евклида и воспроизведено в настоящей работе.

Если какое-нибудь число мы разложили на простые множители, то эти множители можем располагать в каком угодно порядке, например в порядке возрастания. Мысль о возможности разложения этого же числа на другие простые даже не приходит в голову – интуитивно мы убеждены, что перестановками полученных множителей все исчерпывается. Между тем эта единственность разложения, на первый взгляд такая естественная, в действительности является глубоким свойством целых чисел и требует доказательства. Само по себе разложение на простые множители ничего не дает без единственности. В самом деле, пусть найдено разложение на простые делители: $n = 2 \cdot 5 \cdot 37 \cdot \ldots$ Часто требуется описать все делители числа n или хотя бы все простые делители. Нам хотелось бы, чтобы всякий простой делитель совпадал с одним из чисел 2, 5, 37, ... Но без свойства единственности установить это не представляется возможным. Школьникам известно, что такое наибольший общий делитель двух целых чисел, причем известен также метод его нахождения. Но, проанализировав этот метод, можно заметить, что он использует однозначность разложения чисел на простые множители.

В книге VII “Начал” доказана следующая теорема.

Теорема Евклида. *Если простое делит произведение двух целых чисел, то оно делит хотя бы одно из этих чисел.*

Из этой теоремы Евклида очень легко выводится свойство единственности разложения на простые множители. Но само это свойство единственности в “Началах” не сформулировано и, вероятно, поэтому в течение веков рассматривалось как самоочевидный факт. К.Ф. Гаусс первый отметил, что невозможность двух существенно различных разложений одного и того же числа на простые множители вовсе не очевидна и нуждается в доказательстве. Он же сформулировал и доказал в 1801 году следующую основную теорему арифметики: *Всякое натуральное число больше единицы представляется в виде произведения простых множителей, и это представление единственно* (*с точностью до порядка множителей*).

От натуральных чисел перейдем к множеству целых чисел $Z = \{0, \pm1, \pm2, ...\}$ и наряду с натуральным простым p число $-p$ также назовем простым. Разложению на простые подлежат все числа, отличные от 0 и ±1, например $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$. Видим, что разложение единственно с точностью до перестановки множителей и их знаков.

На множестве целых чисел определены операции сложения, вычитания и умножения. В этом смысле Z есть коммутативное кольцо с единицей. Присмотримся внимательнее к операции умножения. Какой элемент кольца Z является обратимым? Другими словами, для какого целого u найдется целое υ, такое, что $u\upsilon = 1$? Ясно, что только для $u = \pm1$. Остальные целые не имеют обратных в Z, то есть необратимы. Обратимые элементы называются также делителями единицы или просто единицами. Очевидно также, что ненулевое целое является простым, если его нельзя записать в виде произведения двух необратимых. Все это дает возможность представить основную теорему арифметики в алгебраических терминах: *любой элемент, отличный от нуля и делителей единицы, можно разложить на простые множители, причем это разложение единственно* (*с точностью до порядка множителей и их умножения на делители единицы*).

В этой формулировке уже ничего не осталось от самих целых чисел, и можно пытаться рассмотреть другие коммутативные кольца, например кольцо многочленов с рациональными коэффициентами или кольцо гауссовых целых – комплексных чисел вида $m + in$, где m, n – обычные целые, $i^2 = -1$.

Еще при жизни Гаусса вопрос о единственности разложения на простые множители приобрел большую остроту. В связи с Великой теоремой Ферма оказались критически важными свойства делимости в кольцах так называемых круговых целых чисел. Вопреки многим ожиданиям выяснилось, что единственности разложения на простые в этих кольцах нет (пример Э. Куммера, 1847 год). В дальнейшем трудности, связанные с невыполнением основной теоремы арифметики, были успешно преодолены как самим Э. Куммером, так и Р. Дедекиндом, Е. Золотаревым, Л. Кронекером и др. Возникла новая область в математике – алгебраическая теория чисел, которая успешно развивается вплоть до наших дней.

ДОКАЗАТЕЛЬСТВО ЕВКЛИДА РАЗЛОЖЕНИЯ НА ПРОСТЫЕ ДЕЛИТЕЛИ

Начнем со следующей **леммы Евклида:**

Всякое целое число $n > 1$ имеет простой делитель.

Доказательство. Среди делителей числа n имеются числа, превосходящие 1 (например, само число n). Пусть p – наименьший из таких его делителей. Очевидно, что p есть простое число, ибо иначе оно имело бы такой делитель u, что $1 < u < p$. Но u, будучи делителем p, было бы и делителем числа n, что противоречит определению числа p, и лемма доказана.

Теперь для $n > 1$ по лемме Евклида имеем $n = p_1n_1$, где p_1 – простое число. Если $n_1 > 1$, то снова по лемме Евклида $n = p_1p_2n_2$. Поскольку $n > n_1 > n_2 > ...$, то за конечное число шагов получим $n = p_1p_2 ... p_k$ и все множители справа простые. Разложение на простые делители доказано. Проследив за доказательством, замечаем, что оно совсем не использовало операции сложения целых чисел. В связи с этим укажем принадлежащий Д. Гильберту пример “короткой” арифметики, в которой есть только умножение и нет единственности разложения на простые делители. Вместо множества натуральных чисел берем множество чисел $S = \{4k + 1, k = 0, 1, 2, ...\} = \{1, 5, 9, 13, ...\}$. Это множество замкнуто относительно обычного умножения, то есть $a, b \in S \Rightarrow a \cdot b \in S$.

Число $p \in S$ называем простым, если оно непредставимо в виде произведения $p = ab$, где $a, b \in S$ и $a, b > 1$. Числа 5, 9, 13, 17, 21 являются простыми, а 25 есть первое непростое число. Каждое число системы S либо само простое, либо может быть разложено на простые множители, – это доказывается так же, как и раньше. Ничто не мешает нам повторить доказательство леммы Евклида и затем установить разложение на простые множители. Но в этой системе разложение на простые множители не является однозначным; например, число 441 имеет два разложения: $441 = 21 \cdot 21 = 9 \cdot 49$, где все числа 21, 9 и 49 простые.

Посмотрим, как обстоит дело с разложением многочлена на простые делители. Условимся брать

многочлены с вещественными рациональными коэффициентами: $f(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$, где a_0, a_1, ..., a_m – рациональные числа. Последний из ненулевых коэффициентов называется старшим коэффициентом, а его номер – степенью многочлена. Ненулевая константа рассматривается как многочлен нулевой степени, $2 = 2x^0$. Нулевым называется многочлен, у которого все коэффициенты равны нулю. Степень нулевого многочлена не определяется (иногда считают ее равной $-\infty$). Обратим внимание, что при умножении многочленов их старшие коэффициенты перемножаются. Поэтому произведение ненулевых есть ненулевой многочлен и $cm(fg) = cmf + cmg$. Многочлен положительной степени называется простым, если он непредставим в виде произведения двух многочленов положительной степени. Многочлен первой степени $x - a$ всегда простой. Многочлен $x^2 - 2$ простой, так как разложение $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ содержит иррациональное число $\sqrt{2}$.

Докажем, что любой многочлен положительной степени есть произведение простых. Применим некоторую вариацию рассуждений Евклида. Хорошими многочленами назовем произведения любого числа простых. В частности, сами простые хорошие, а произведение хороших также хороший. Допустим, что существуют плохие многочлены положительной степени. Выберем из них многочлен наименьшей степени. Пусть это будет многочлен f. Он не может быть простым, и, значит, $f = f_1f_2$, где f_1 и f_2 имеют положительные степени, меньшие степени f. Но тогда f_1 и f_2 должны быть хорошими. Значит, f также хороший, что противоречит нашему допущению.

ВЫВОД СВОЙСТВА ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ ИЗ ТЕОРЕМЫ ЕВКЛИДА

В “Началах” свойство единственности разложения на простые делители не сформулировано, но от этого сама арифметика “Начал” ничего не потеряла: то, что можно вывести из основной теоремы арифметики, получено там на основе теоремы Евклида. Легко могло бы быть получено и само свойство единственности. Сейчас мы это сделаем.

Пусть имеем два разложения на простые делители

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k = \tilde{p}_1 \cdot \tilde{p}_2 \cdot ... \cdot \tilde{p}_l. \qquad (1)$$

Докажем, что число множителей в обоих разложениях одинаково и после подходящей перестановки множителей $p_1 = \tilde{p}_1$, $p_2 = \tilde{p}_2$, ... Можно предполагать, что $k \geq 1$. Если p_1 делится на $\tilde{p}_1$, то они равны. Если $p_1 \neq \tilde{p}_1$, то по теореме Евклида произведение $p_2 \cdot p_3 \cdot ... \cdot p_k$ делится на $\tilde{p}_1$. Продолжая и далее эти рассуждения, получим, что $\tilde{p}_1$ совпадает с одним из $p_1, p_2, ..., p_k$. Перестановкой множителей можно добиться того, что $p_1 = \tilde{p}_1$. После сокращения (1) на p_1 имеем равенство $p_2 \cdot p_3 \cdot ... \cdot p_k = \tilde{p}_2 \cdot \tilde{p}_3 \cdot ... \cdot \tilde{p}_l$ и, повторяя предыдущий шаг, получим $p_3 \cdot p_4 \cdot ... \cdot p_k = \tilde{p}_3 \cdot \tilde{p}_4 \cdot ... \cdot \tilde{p}_l$. После l таких шагов справа останется 1, а слева $k - l$ простых множителей. Поэтому $k = l$ и однозначность установлена.

Кроме теоремы Евклида мы использовали только определение простого числа и закон сокращения: $ab = ac$, $a \neq 0 \Rightarrow b = c$.

Чтобы доказать теорему Евклида, нам потребуется предварительно развить теорию наибольшего общего делителя двух целых чисел. Именно для этой цели будут востребованы самые существенные свойства целых чисел.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

Самое важное свойство целых чисел – это хорошо известное деление с остатком: *для любых целых a, b, $b \neq 0$, найдутся целые q и r, такие, что $a = qb + r$, $|r| < |b|$*. Число r называют остатком, а q – неполным частным. *Наибольшим общим делителем* (НОД) *двух целых чисел a и b* называется такой их общий делитель, который делится на любой другой общий делитель.

Например, НОД (12, 9) = ±3. Вообще наибольший общий делитель двух данных чисел определен однозначно с точностью до знака, поскольку (в силу самого определения) любые два НОД должны делиться друг на друга. Очевидно, что НОД не существует, если оба числа a и b равны нулю. Исключим этот случай из рассмотрения. Тогда найдутся целые u и υ, такие, что $au + b\upsilon > 0$, и, как мы сейчас увидим, НОД существует. Следующее замечательное утверждение принадлежит Гауссу: *наименьшее положительное число d, представимое в виде*

$$d = au + b\upsilon \text{ с целыми } u \text{ и } \upsilon, \qquad (2)$$

есть наибольший общий делитель чисел a и b.

Доказательство. Проверим, что a и b делятся на d. Сделаем это, скажем, для a. Делим a на d с остатком: $a = qd + r$, $0 \leq r < d$. Тогда $r = a - qd = a - q(au + b\upsilon) = a(1 - qu) + bq\upsilon = au' + b\upsilon'$, u' и υ' целые. Так как $r < d$, а d есть по определению наименьшее положительное число, представимое в форме $au + b\upsilon$ с целыми u и υ, то r не может быть положительным. Следовательно, $r = 0$, то есть a делится на d. Мы проверили, что число d есть общий делитель чисел a и b. Остается заметить, что из самого соотношения (2) непосредственно ясно, что d делится на любое число, служащее общим делителем

чисел a и b. Мы доказали не только что НОД(a, b) существует, но и что его можно выразить линейно через сами эти числа: *если* d = НОД(a, b), *то найдутся такие целые числа* u *и* υ, *что* $d = au + b\upsilon$.

Последнее обстоятельство сейчас будет использовано для доказательства теоремы, родственной теореме Евклида, и самой теоремы Евклида. Числа a и b называются взаимно простыми, если у них нет других общих делителей, кроме ±1. В этом случае d = НОД(a, b) = 1 и линейное представление принимает следующий вид:

найдутся целые u *и* υ, *такие, что* $au + b\upsilon = 1$. (3)

Теорема 1. *Если некоторое число делит произведение двух чисел и взаимно просто с одним из сомножителей, то оно делит другой сомножитель.*

Доказательство. Пусть ac делится на b и b взаимно просто с a. Тогда из (3) имеем $c = acu + cb\upsilon$. Правая часть этого равенства делится на b, значит, и c делится на b, что и требовалось доказать.

Из теоремы 1 следует теорема Евклида. Действительно, пусть ab делится на простое p. Если a делится на p, то доказывать нечего. В противном случае a и p взаимно просты и по теореме 1 множитель b делится на p. Теорема Евклида и вместе с ней основная теорема арифметики доказаны.

Замечание. Из основной теоремы арифметики можно получить множество следствий. Кроме школьного правила нахождения НОД можно получить, например, теорему 1. Но вывести линейное представление НОД нам не удастся: линейное представление есть более глубокое свойство, чем сама основная теорема.

АЛГОРИТМ ЕВКЛИДА

Укажем процедуру нахождения НОД, которая в геометрической форме описана еще в “Началах”. Даны числа a и b, $b \neq 0$. Делим a на b и получаем остаток r_1, $|r_1| < |b|$. Далее делим b на r_1 и получаем остаток r_2, $|r_2| < |r_1|$. Продолжаем далее до тех пор, пока не получим нулевой остаток. Утверждается, что последний ненулевой остаток есть НОД(a, b). Для доказательства рассмотрим цепочку равенств

1) $a = q_1 b + r_1$,

2) $b = q_2 r_1 + r_2$,

3) $r_1 = q_3 r_2 + r_3$,

4) $r_2 = q_4 r_3 + r_4$,

5) $r_3 = q_5 r_4 + r_5$,

6) $r_4 = q_6 r_5 + 0$,

в которой для определенности шестой остаток равен нулю, а пятый отличен от нуля. Проверим, что r_5 = НОД(a, b). Сначала убедимся, что r_5 есть общий делитель чисел a и b. Из (6) видно, что r_4 делится на r_5. Тогда из (5) заключаем, что r_3 делится на r_5. Поднимаясь по цепочке, видим, что a и b делятся на r_5. Далее пусть δ – какой-нибудь общий делитель чисел a и b. Равенство (1) показывает, что остаток r_1 делится на δ. Тогда из (2) заключаем, что r_2 делится на δ. Спускаясь по цепочке, находим, что и r_5 делится на δ, что и требовалось.

С помощью алгоритма Евклида легко установить линейное представление НОД. Действительно, равенство (5) показывает, что $r_5 = d$ можно линейно выразить через r_3 и r_4. Но из (4) видно, что r_4 можно выразить через r_2 и r_3. Поднимаясь по цепочке вверх, находим, что окончательно d выражается через a и b.

КОЛЬЦА С НОРМОЙ И ЕВКЛИДОВЫ КОЛЬЦА

Предположим, что элементы некоторого множества K можно складывать, вычитать и перемножать, причем умножение ассоциативно, коммутативно и имеется единичный элемент 1, такой, что $a \cdot 1 = a$ для любого a. К этим свойствам присоединим также закон сокращения. Тогда мы говорим о коммутативном кольце с единицей или для краткости просто о кольце. Примерами служат кольцо Z целых чисел и кольцо многочленов с рациональными коэффициентами.

Элемент u кольца K называется обратимым, если $u \cdot \upsilon = 1$ для некоторого $\upsilon \in K$. Произведение обратимых – обратимый (элемент). Произведение необратимого и обратимого необратим (в самом деле, если $au = b$ обратим, то $a = au\upsilon = b\upsilon$ обратим как произведение обратимых). Обратимые элементы называются также делителями единицы или просто единицами. В кольце Z обратимые элементы – это ±1, в кольце многочленов – это многочлены нулевой степени. Элемент p называется простым, если его нельзя представить в виде произведения двух необратимых. Если u обратим, то pu также простой. Очевидно, что если простой делится на простой, то они отличаются обратимым множителем.

Доказательство основной теоремы для целых чисел и многочленов использовало, конечно, не только алгебраические операции. Например, мы рассматривали некоторое множество ненулевых многочленов и выбирали в нем многочлен наименьшей степени. Желательно и в общем случае элементу кольца приписать размер, норму – некоторое целое неотрицательное число.

Скажем, что на кольце K задана норма, если каждому его элементу a сопоставлено целое неотрицательное число $N(a)$, такое, что: 1) $N(a) = 0 \Leftrightarrow a = 0$; 2) $N(ab) = N(a)N(b)$; 3) $N(a) = 1 \Leftrightarrow a$ обратим.

В кольце Z можно взять $N(a) = |a|$ – модуль целого числа. В кольце многочленов $N(f) = 2^{cmf}$, если $f \neq 0$, и

$N(f) = 0$, если f нулевой. Может показаться, что наличие нормы дает очень много. Так, разложение на простые делители достигается легко – нужно буквально повторить наше рассуждение с "плохими" и "хорошими" многочленами, заменив слово "степень" на слово "норма". Однако дальше разложения продвинуться нельзя – пример, который мы приведем позже, показывает, что единственности разложения нет. Читатель уже догадался, что норма еще не обеспечивает алгоритма деления с остатком, на котором было ранее основано доказательство единственности.

Кольцо с нормой называется евклидовым, если в нем имеется алгоритм деления с остатком: для любых $a, b \in K$, $b \neq 0$, найдутся $q, r \in K$ такие, что $a = qb + r$ и $N(r) < N(b)$. Теперь мы попадаем в знакомую обстановку и без труда можем повторить все сделанное для целых чисел и многочленов, включая гауссово доказательство существования НОД для любых одновременно не равных нулю элементов, линейное представление, алгоритм Евклида и т.д. Другими словами, в евклидовом кольце основная теорема арифметики имеет место.

КОЛЬЦО ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ

Гауссовым числом называется комплексное число $a = m + in$, где $m, n \in Z$. Гауссовы числа складываются и умножаются как комплексные числа. Кольцо гауссовых чисел обозначается $Z(i)$. Норма гауссова числа $N(a) = m^2 + n^2 = |a|^2$– квадрат модуля комплексного числа. Проверим выполнение свойств нормы. Очевидно, $N(a) = 0$ эквивалентно $a = 0$. Равенство $N(ab) = N(a)N(b)$ верно для любых комплексных чисел. Далее из $N(a) = m^2 + n^2 = 1$ находим, что в кольце $Z(i)$ четыре единицы $\{1, -1, i, -i\}$.

Для дальнейшего полезно представить себе расположение гауссовых чисел на комплексной плоскости. По определению гауссовы числа представляются точками с целочисленными координатами. Они лежат в вершинах сетки квадратов со стороной, равной 1, покрывающей комплексную плоскость. Геометрические соображения помогут нам сейчас доказать, что в кольце $Z(i)$ есть алгоритм деления с остатком. Для любых $a, b \in Z(i)$, $b \neq 0$, рассматриваем комплексное число $z = \frac{a}{b}$. Оно попадает в некоторый квадрат с целочисленными вершинами. Возьмем в качестве q ближайшую к z вершину, расстояние до которой не превышает $\frac{1}{\sqrt{2}}$. Поэтому $\frac{a}{b} = q + \alpha$,

$$|\alpha|^2 = N(\alpha) \le \frac{1}{2}, \qquad a = qb + r, \qquad r = b\alpha,$$

$$N(r) = N(b)N(\alpha) \le \frac{1}{2}N(b).$$

КОЛЬЦО С НЕЕДИНСТВЕННОСТЬЮ РАЗЛОЖЕНИЯ

Рассматриваем комплексные числа вида $a = m + in\sqrt{3}$, где m, n целые. Замечаем, что сумма и произведение снова будут числом такого же вида. Имеем кольцо, обозначаемое $Z(i\sqrt{3})$. Норма определяется равенством $N(a) = m^2 + 3n^2 = |a|^2$. Из $N(a) = 1$ находим две единицы ± 1. Оказывается, что в нашем кольце основная теорема арифметики неверна: единственности разложения на простые множители нет. Например,

$$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3}) \qquad (4)$$

и вместе с тем числа 2 и $1 \pm i\sqrt{3}$ простые. Докажем, что 2 – простой элемент. Допустим, что $2 = (m + in\sqrt{3}) \times (k + il\sqrt{3}) = ab$, $N(a), N(b) > 1$. Тогда $4 = (m^2 + 3n^2) \times (k^2 + 3l^2) \Rightarrow m^2 + 3n^2 = k^2 + 3l^2 = 2$. Но в нашем кольце нет элементов с нормой 2! Аналогично $1 \pm i\sqrt{3}$ простые.

Для сравнения опишем другое кольцо, по виду очень похожее на $Z(i\sqrt{3})$, но являющееся евклидовым. Рассмотрим комплексные числа

$$a = m + n\omega, \qquad m, n \text{ целые}, \qquad \omega = \frac{1}{2}(-1 + i\sqrt{3}). \qquad (5)$$

Число ω – это комплексный корень третьей степени из 1, $\omega^3 = 1$. Поскольку $\omega \neq 1$, то $\omega^2 + \omega + 1 = 0$. Пользуясь этим равенством, легко проверяем, что множество чисел вида (5) образует кольцо K_3. Найдем элементы с единичной нормой. Пусть $\bar{a} = m + n\bar{\omega}$, $\bar{\omega} = -\frac{1}{2}(1 + i\sqrt{3})$ – комплексно-сопряженные числа. Тогда

$$N(a) = a\bar{a} = (m + n\omega)(m + n\bar{\omega}) = m^2 + n^2 + mn(\omega + \bar{\omega}) =$$
$$= m^2 + n^2 - mn = 1.$$

Перебором находим, что $a = \pm 1, \pm\omega, \pm(1 + \omega)$. Видно, что все эти элементы обратимы. Можно показать, что для кольца K_3 имеет место алгоритм деления с остатком. Посмотрим на разложение (4) с точки зрения кольца K_3. Элементы 2, $1 \pm i\sqrt{3}$ и здесь просты, так как и в K_3 нет элементов с нормой 2 (уравнение $m^2 + n^2 - mn = 2$ не имеет целочисленных решений). Не противоречит ли тогда (4) единственности разложения? Нет, так как

элементы $2,\ 1+i\sqrt{3}$ и $1-i\sqrt{3}$ отличаются друг от друга лишь обратимыми множителями, например $1-i\sqrt{3} = (-\omega)\cdot 2,\ 1+i\sqrt{3} = (1+\omega)\cdot 2$.

Числа вида (5) – это простейший пример круговых целых. В общем случае для любого простого $p \geq 3$ рассматриваются числа

$$a_0 + a_1\omega + \ldots + a_{p-2}\omega^{p-2}, \quad \omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}, \qquad (6)$$

где $a_0, a_1, \ldots, a_{p-2}$ – обычные целые числа. Поскольку $\omega^p = 1$ и $\omega \neq 1$, то $\omega^{p-1} + \omega^{p-2} + \ldots + 1 = 0$. Пользуясь этим равенством, легко проверяем, что множество чисел (6) образует кольцо K_p. Путем искусных вычислений Куммер обнаружил, что в кольце K_{23} нет единственности разложения на простые делители. Для простых $p < 100$ единственность разложения имеет место только для $p = 3, 5, 7, 11, 13, 17, 19$.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. *Курант Р., Роббинс Г.* Что такое математика? М.: Просвещение, 1967. 558 с.

2. *Постников М.М.* Введение в теорию алгебраических чисел. М.: Наука, 1982. 240 с.

3. *Эдвардс Г.* Последняя теорема Ферма. М.: Мир, 1980. 520 с.

Рецензент статьи Ю.П. Соловьев

* * *

Василий Васильевич Жиков, доктор физико-математических наук, профессор Владимирского государственного педагогического университета. Область научных интересов – уравнения с частными производными, почти-периодические функции, выпуклый анализ, усреднение дифференциальных операторов. Автор более 85 работ, в том числе четырех больших обзоров в “Успехах математических наук” и трех монографий.