МЕТОДЫКА ВЫКЛАДАННЯ

МЕТОДЫКА ВЫКЛАДАННЯ МАТЭМАТЫКІ

Весці БДПУ. Серыя 3. 2023. № 2. С. 5–9

УДК 519.624

UDC 519.624

АЛЬТЕРНАТИВНЫЙ ПОДХОД К ПРЕПОДАВАНИЮ ТЕОРИИ ЧИСЕЛ В ПЕДАГОГИЧЕСКИХ УНИВЕРСИТЕТАХ

А. А. Черняк,
доктор физико-математических наук, профессор кафедры математики и методики преподавания математики Белорусского государственного педагогического университета имени Максима Танка;

А. П. Шкрабов,
студент физико-математического факультета Белорусского государственного педагогического университета имени Максима Танка

ALTERNATIVE APPROACH TO TEACHING NUMBERS THEORY IN PEDAGOGICAL UNIVERSITIES

A. Chernyak,
Doctor of Physics and Mathematics, Professor of the Department of Mathematics and Methods of Teaching Mathematics, Belarusian State Pedagogical University named after Maxim Tank;

A. Shkrabov,
Student of the Faculty of Physics and Mathematics, Belarusian State Pedagogical University named after Maxim Tank

Поступила в редакцию 20.04.23.

Received on 20.04.23.

Представлена оригинальная методика преподавания теории чисел в педагогических университетах в рамках новых учебных планов Республики Беларусь. В частности, на примере ряда классических результатов теории чисел (теоремы Эйлера, Ферма, Вильсона, китайской теоремы об остатках, признаках делимости и т. д.) продемонстрирована единая доказательная база на основе элементарных утверждений теории групп и колец. Такой подход позволит студентам легко освоить краткие доказательства нетривиальных теорем, в отличие от классических доказательств теории чисел, использующих элементарные, но громоздкие и разрозненные рассуждения.

Ключевые слова: теория чисел, группы, кольца, поля, новые учебные планы по алгебре.

An original methodology of teaching number theory in pedagogical universities within the framework of the new curricula of the Republic of Belarus is presented. In particular, on the example of a number of classical results of number theory (Euler, Fermat, Wilson theorems, Chinese theorem on residuals, signs of divisibility, etc.) a unified proof base on the basis of elementary statements of group and ring theory is demonstrated. This approach will allow students to easily master short proofs of nontrivial theorems, in contrast to classical proofs of number theory, which use elementary, but cumbersome and disjointed reasoning.

Keywords: numbers theory, groups, rings, fields, new algebra curricula.

Введение. Относительно недавний переход к 4-летнему циклу подготовки учителей в некотором смысле сыграл положительную роль. Университеты вынуждены были существенно уменьшить часовой фонд аудиторных занятий за счет сокращения разделов и дисциплин, не востребованных в деятельности школьного учителя. Это продиктовало необходимость совершенствовать учебные программы, отдавая предпочтение практической направленности изучаемых предметов.

Со следующего учебного года вновь обновляются учебные планы на физико-математических факультетах педагогических университетов в связи с обновлением номенклатуры специальностей.

При этом традиционный набор «надэлементарной» математики сохранился в качестве математического фундамента для всего спектра специальностей физико-математического образования. Он представлен в виде модуля государственного компонента «Высшая математика-1», куда вошли дисциплины «Высшая алгебра», «Математический анализ», «Аналитическая геометрия», «Теория вероятностей и математическая статистика».

Модуль «Высшая математика-2» включен как компонент учреждения образования и содержит, в частности, дисциплину «Алгебраические структуры и теория чисел». На данную дисциплину отведено 54 аудиторных часа, и она должна включать теорию основных структур алгебры (группы, кольца, поля) и теорию чисел. В пятилетних учебных планах «Теория чисел» была отдельной дисциплиной, на которую отводилось 66 аудиторных часов.

Позитивны или негативны эти изменения – не предмет обсуждения в данной статье (оценку этих изменений можно найти в [1]). Здесь же мы предлагаем оригинальный методический подход, альтернативный традиционному изложению классических теорем теории чисел, который, на наш взгляд, решает следующую триединую задачу:

– единая доказательная база: мощный аппарат теории групп позволяет получать элегантные и краткие доказательства практически всех теорем теории чисел, в отличие от классических доказательств, использующих элементарные, но громоздкие и разрозненные рассуждения (см. например, [2–4]);
– мотивация к изучению: абстрактные и нетривиальные понятия группы, кольца, поля становятся востребованными студенческой аудиторией, поскольку могут быть напрямую использованы в их будущей профессиональной деятельности на факультативных занятиях и в профильных классах;
– связь с другими дисциплинами: все теоремы теории чисел, играющие ключевую роль при изучении дисциплин «Алгебра многочленов и расширения полей», «Алгебраические методы защиты информации», предусмотренных в новых учебных планах, формулируются в терминах колец целых чисел по натуральному модулю.

Единая доказательная база открывает возможности к совершенствованию учебных программ и настраивает на ускоренное освоение общего понятийного аппарата, а также исключает громоздкие формулировки, используемые в процессе изучения доказательной базы. При этом значительно возрастает мотивация студентов к изучению нетривиального математического материала. Связь с другими разделами алгебры позволяет взглянуть на математику более глобально, что, в свою очередь, улучшает и ускоряет процесс получения новых знаний.

Основная часть. Для демонстрации конкретных возможностей нашего подхода приведем ключевые теоремы и их доказательства, без которых невозможно представить себе курс теории чисел для будущих учителей. Для комфорта восприятия текста предлагаем примеры сопутствующих вычислительных процедур.

Теорема 1 *(теоремы Эйлера и Ферма)*. Пусть a – элемент мультипликативной группы кольца $(\mathbb{Z}_n,+,\cdot)$. Тогда $a^{(\varphi(n))} = 1$. В частности, если n – простое, то $a^{(n-1)} = 1$ (здесь равен $\varphi(n)$ – функция Эйлера, $\mathbb{Z}_n$ – кольцо целых чисел по модулю n).

Доказательство. Утверждение прямо следует из того, что порядок мультипликативной группы $\mathbb{Z}_n^*$ кольца $\mathbb{Z}_n$ равен $\varphi(n)$, а порядки всех элементов группы являются делителями порядка группы.

Теорема 2 *(о сумме всех делителей)*. Для любого $n \in \mathbb{N}$ $\sum_{n|r} \varphi(r)$, где сумма берется по всем натуральным делителям r числа n.

Доказательство. Группа $(\mathbb{Z}_n,+)$ − циклическая порядка n с образующим элементом 1. Согласно свойству порядков элементов циклических групп, для каждого натурального делителя r числа n в группе $(\mathbb{Z}_n,+)$ существует ровно $\varphi(r)$ элементов порядка r. Но порядок каждого элемента из $(\mathbb{Z}_n,+)$ является натуральным делителем n. Поэтому количество всех элементов в группе $(\mathbb{Z}_n,+)$ равно $\sum_{n|r} \varphi(r)$.

Теорема 3 *(теорема Вильсона)*. Пусть n – натуральное число, отличное от 1. Тогда в кольце $(\mathbb{Z}_n,+,\cdot)$ $(n-1)!+1=0$, если и только если n простое.

Доказательство. Если n составное и $n = k \cdot m$, то в кольце $(\mathbb{Z}_n,+,\cdot)$ $(n-1)! = 0$ и значит, равенство $(n-1)!+1=0$ не выполняется.

Пусть теперь n простое. Тогда кольцо $(\mathbb{Z}_n,+,\cdot)$ является полем с мультипликативной группой $\mathbb{Z}_n^* = \{1,...,n-1\}$. Пусть для некоторого элемента $a \in \mathbb{Z}_n^*$ верно $a^2 = 1$. Тогда $(a-1)(a+1)=0$, а так как в поле нет делителей нуля, то либо один из элементов $a-1=0$ (и в этом случае a = 1), либо a + 1 = 0 (и в этом случае $a = n-1$). Следовательно, каждый элемент, отличный от 1 и n – 1, не совпадает со своим обратным элементом. Поэтому множество элементов {2,…,n – 2} можно разбить на пары взаимно обратных элементов, произведение которых равно 1. Отсюда $2 \cdot 3 \cdot ... \times (n-2) = 1 \Rightarrow (n-1)! = n-1 \Rightarrow (n-1)!+1=0$.

Теорема 4 *(мультипликативность функции Эйлера)*. Для любых взаимно простых натуральных чисел n и m $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Доказательство. Возьмем произвольные циклические группы $(G,\cdot)$ и $(H,\cdot)$ порядков m и n. Тогда группа $(G \times H,\cdot)$ – циклическая порядка mn. Группы G, H и $G \times H$ имеют соответственно $\varphi(m)$, $\varphi(n)$ и $\varphi(mn)$ образующих. А поскольку элемент (a,b) является образующим в $(G \times H,\cdot)$, если и только если элементы a и b – образующие в G и H соответственно, то $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Теорема 5 *(китайская теорема об остатках)*. Пусть даны попарно взаимно простые натуральные числа $n_1,...,n_r$, отличные от 1, и $a_1,...,a_r$ – произвольные натуральные числа, меньшие $n_1,...,n_r$ соответственно. Положим $m_i = n_1 \cdot n_2 \cdot ... \cdot n_{i-1} \cdot n_{i+1} \times \times ... \cdot n_r$ $i = 1,2,...,r$. В каждом кольце $(\mathbb{Z}_{n_i},+,\cdot)$ найдем элемент $t_i = m_i^{-1}$. Вычислим натуральное число $x = \sum_{i=1}^{r} a_i m_i t_i$. Тогда $x = a_i$ в кольце $(\mathbb{Z}_{n_i},+,\cdot)$ для каждого i =1, 2, …, r.

Кроме того, любое натуральное число y с аналогичными свойствами имеет вид $y = x + tN$ при некотором целом t и $N = n_1 \cdot ... \cdot n_r$.

Доказательство. Сразу отметим, что элемент m_i обратим в кольце $\mathbb{Z}_{n_i}$, поскольку m_i и n_i взаимно просты. Зафиксируем произвольное натуральное k, где 1 ≤ k ≤ r. Тогда $m_k t_k$ = 1 в $\mathbb{Z}_{n_k}$. Так как m_i делится на n_k для всех $i \neq k$, то m_i = 0 в кольце $\mathbb{Z}_{n_k}$ и, следовательно, $x = \sum_{i=1}^{r} a_i m_i t_i = a_k m_k t_k = a_k$ в кольце $\mathbb{Z}_{n_k}$.

Пусть $y = a_i$ в кольце $\mathbb{Z}_{n_i}$. Тогда $y - x$ кратно n_i =1, 2, …, r, и следовательно, $y - x$ кратно N, поскольку n_1,… , n_r, попарно взаимно простые.

Пример применения теоремы 5.

Найти все натуральные числа, удовлетворяющие системе уравнений

$$\begin{cases} x = 4 \text{ в кольце } \mathbb{Z}_5, \\ x = 3 \text{ в кольце } \mathbb{Z}_6, \\ x = 4 \text{ в кольце } \mathbb{Z}_7. \end{cases}$$

В обозначениях теоремы 5 имеем: N = = 210, m_1 = 42, m_2 = 35, m_3 = 30. Обратные элементы в кольцах $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_7$ находим с помощью полиномиального алгоритма из [5]: t_1 = 3, t_2 = 5, t_3 = 4. Отсюда $x = 4 \cdot 42 \cdot 3 + + 3 \cdot 35 \cdot 5 + 5 \cdot 30 \cdot 4 + 210t = 1629 + 210t$ или $x = 159 + 210t$, $t \in \mathbb{N} \cup \{0\}$.

Теорема 6 *(линейные уравнения в кольце по модулю n)*. Пусть дано линейное уравнение

$$ax = b \text{ в кольце } (\mathbb{Z}_n,+,\cdot). \qquad (1)$$

Обозначим d = НОД(a,n). Если b не делится на d, то уравнение (1) не имеет решений. В противном случае положим $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $n_1 = \frac{n}{d}$ и вычислим в кольце $\mathbb{Z}_{n_1}$ элементы a_1^{-1} и $a_1^{-1}b_1$. В этом случае уравнение (1) имеет точно d решений $x = a_1^{-1}b_1 + n_1 t \quad t = 0,1,...,d-1$.

Доказательство. Сразу отметим, что элемент a_1 обратим в кольце $\mathbb{Z}_{n_1}$, поскольку a_1 и n_1 взаимно простые. Поэтому $x_1 = a_1^{-1}b_1$ – решение уравнения $a_1x_1 = b_1$ в кольце $\mathbb{Z}_{n_1}$, и следовательно, в кольце $\mathbb{Z}_n$ $da_1x_1 = db_1 \Rightarrow ax_1 = b$, т. е. x_1 – решение уравнения (1).

Пусть уравнение (1) имеет еще одно решение y. Тогда $a(y-x_1) \mid n \Leftrightarrow a_1(y-x_1) \mid n_1 \Leftrightarrow (y-x_1) \mid n_1 \Leftrightarrow y = x + n_1 t$, для некоторого целого t, причем $t < d$ ввиду $y < n$.

Пример применения теоремы 6.

Решить уравнение $21x = 9$ в кольце $(\mathbb{Z}_{30},+,\cdot)$. В обозначениях теоремы 6 имеем: $d = 3$, $a_1 = 7$, $b_1 = 3$, $n_1 = 10$. Обратный элемент d = 7^{-1} в кольце $\mathbb{Z}_{10}$ находим с помощью полиномиального алгоритма из [5]: t = 3. Отсюда $x = 3 \cdot 3 + 10t = 9 + 10t$, $t = 0,1,2$, и уравнение $21x = 9$ имеет следующие три решения: 9, 9 + 10 = 19, 9 + 20 = 29.

Обоснование метода решения нелинейных уравнений в кольцах по простому модулю p (которые являются полями) основывается на следующем простом утверждении теории групп: если элемент a имеет порядок k, то для любых целых l и m $a^l = a^m$ равносильно $(l-m) \mid k$. Рассмотрим этот метод, который сводит решение нелинейных уравнений к решению линейных уравнений.

Пусть g и c – элементы мультипликативной группы $\mathbb{Z}_m^*$ кольца $(\mathbb{Z}_m,+,\cdot)$. Дискретным логарифмом $ind_g c$ с элемента c по основанию g называется наименьшее неотрицательное целое число s, что $g^s = c$ По определению $g^{ind_g c} = c$. Если группа $\mathbb{Z}_m^*$ циклическая, но g не является ее образующим, то дискретные логарифмы существуют не для всех $c \in \mathbb{Z}_m^*$. Если g является образующим элементом циклической группы $\mathbb{Z}_m^*$, то каждый элемент $c \in \mathbb{Z}_m^*$ является степенью g и потому число $ind_g c$ существует.

Если $m = p$ – простое число, то $\mathbb{Z}_p$ – поле и его мультипликативная группа $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ циклическая, причем она имеет ровно $\varphi(p-1)$ образующих элементов. Если g – один из них, то $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\} = \{1, 2, \ldots, p-1\}$. Таким образом, каждому элементу c из $\{1, 2, \ldots, p-1\}$ соответствует один и только один дискретный логарифм $ind_g c$ из множества целых чисел $\{0, 1, \ldots, p-2\}$.

Лемма. Пусть g – образующий элемент циклической группы $\mathbb{Z}_m^*$ кольца $(\mathbb{Z}_m,+,\cdot)$. Тогда:

а) $a = b$ в кольце $\mathbb{Z}_m \Leftrightarrow ind_g a = ind_g b$ в кольце $\mathbb{Z}_{\varphi(m)}$

б) в кольце $\mathbb{Z}_{\varphi(m)}$ $ind_g(ab) = ind_g a + ind_g b$ и $ind_g a^n = n \cdot ind_g a$.

Доказательство.

а) Пусть $a = g^s$, $b = g^r$. Тогда $a = b \Leftrightarrow g^s = g^r \Leftrightarrow (s-r) \mid \varphi(m) \Leftrightarrow s = r$ в кольце $\mathbb{Z}_{\varphi(m)}$. Утверждение доказано, так как $s = ind_g a$ $r = ind_g b$.

б) $g^{ind_g(ab)} = ab = g^{ind_g a} \cdot g^{ind_g b} = g^{ind_g a + ind_g b} \Leftrightarrow g^{ind_g a^n} = a^n = (g^{ind_g a})^n = g^{n \cdot ind_g a} \Leftrightarrow \left(ind_g(ab) - (ind_g a + ind_g b)\right) \mid \varphi(m)$.

Теорема 7 *(нелинейные уравнения в кольце по простому модулю)*. Пусть p – простое нечетное число, g – образующий элемент мультипликативной группы $\mathbb{Z}_p^*$ и дано уравнение

$$ax^n = b \text{ в кольце } (\mathbb{Z}_p^*,+,\cdot). \qquad (2)$$

Тогда x является решением уравнения (2), если и только если $y = ind_g x$ – решение линейного уравнения

$$ny = ind_g b - ind_g a \text{ в кольце } (\mathbb{Z}_{p-1}^*,+,\cdot). \qquad (3)$$

При этом различным решениям x уравнения (2) соответствуют различные ре-

шения $y = ind_g x$ уравнения (3) (все дискретные логарифмы определяются в группе $\mathbb{Z}_p^*$).

Доказательство. Учитываем, что $\varphi(p) = p - 1$ и все дискретные логарифмы принадлежат множеству $\{0, 1,...., p-2\}$. Уравнение (2) в силу леммы равносильно уравнению $ind_g a + n \cdot ind_g x = ind_g b$ или $ny = ind_g b - ind_g a$ в кольце $(\mathbb{Z}_{p-1}^*, +, \cdot)$.

Таким образом, x – решение (2), меньше p, если и только если $y = ind_g x$ – решение (3).

Пример применения теоремы 7.

Решить уравнение $4x^{11} = 3$ в кольце $\mathbb{Z}_7$. Так как $ind_2 3 = 5$, как $ind_2 4 = 2$, то исходное уравнение сводится к решению линейного уравнения $5y = 3$ в кольце $\mathbb{Z}_6$. Так как $5^{-1} = 5$ в кольце $\mathbb{Z}_6$, то уравнение $5y = 3$ в кольце $\mathbb{Z}_6$ имеет единственное решение $y = 3$. С помощью таблиц дискретных логарифмов находим x = 6, при котором $3 = ind_5 x$. Таким образом, x = 6 – единственное решение уравнения $4x^{11} = 3$ в кольце $\mathbb{Z}_7$.

Теорема 8 *(признаки делимости)*.

1. Признак делимости на 13: натуральное число делится на 13, если и только если разность сумм его цифр в 1000-ичной системе счисления, расположенных соответственно на четных и нечетных позициях, делится на 13.

2. Признак делимости на 11: натуральное число делится на 11, если и только если сумма его цифр в 100-ичной системе счисления делится на 11.

Доказательство.

1. Порядок мультипликативной группы кольца $(\mathbb{Z}_{13}, +, \cdot)$ равен 12. Поэтому порядок элемента 10 должен быть делителем числа 12. Среди делителей числа 12 найдем такое наименьшее натуральное число k, что либо $10^k - 1 = 0$, либо $10^k + 1 = 0$. В нашем случае $10^3 + 1 = 0$. Итак, k = 3 и 1000 = –1.

Запишем натуральное число a в 1000-ичной системе счисления: $a_{k-1}(1000)^{k-1} + ... + a_1(1000)^1 + a_0$. И так как $a_i(1000)^i = a(-1)^i$, то $a = a_{k-1}(1000)^{k-1} + ... + a_1(1000)^1 + a_0 = a_{k-1}(-1)^{k-1} + ... + a_1(-1)^1 + a_0$.

2. Порядок мультипликативной группы кольца $(\mathbb{Z}_{11}, +, \cdot)$ равен 10. Поэтому порядок элемента 10 должен быть делителем числа 10. Среди делителей числа 12 найдем такое наименьшее натуральное число k, что либо $10^k - 1 = 0$, либо $10^k + 1 = 0$. В нашем случае $10^2 = 1$. Итак, k = 2 и 100 = 1.

Запишем натуральное число a в 100-ичной системе счисления: $a = a_{k-1}(100)^{k-1} + ... + a_1(100)^1 + a_0$. И так как $a_i(1000)^i = a_i \cdot 1^i$, то $a = a_{k-1}(100)^{k-1} + ... + a_1(100)^1 + a_0 = a_{k-1} + ... + a_1 + a_0$.

Заключение. В заключение добавим, что идея унификации доказательной базы вполне может быть распространена на другие традиционные разделы университетских дисциплин высшей математики, в частности на линейную алгебру. Планируем продемонстрировать имеющуюся в нашем распоряжении данную методику по линейной алгебре в следующей статье данного цикла.

Литература

1. *Черняк, А. А.* Перестройка обучения математике в вузах и ссузах Беларуси / А. А. Черняк, И. В. Кирюшин // Вышэйшая школа. – № 2. – 2022. – С. 26–31.
2. *Виноградов, И. М.* Основы теории чисел: учебник для вузов / И. М. Виноградов. – М. : Издательство Лань, 2023. – 176 с.
3. *Жмурова, И. Ю.* Теория чисел : учебное пособие для вузов / И. Ю. Жмурова, А. В. Игнатова. – М. : Издательство Юрайт, 2023. – 52 с.
4. *Нестерова, Л. Ю.* Теория чисел: учебник и практикум для вузов / Л. Ю. Нестерова, С. В. Напалков. – Москва: Издательство Юрайт, 2023. – 150 с.
5. *Виноградов, И. М.* Основы теории чисел / И. М. Виноградов. – М. : Издательство Юрайт, 2023. – 123 с.

References

1. *Chernyak, A. A.* Perestrojka obucheniya matematike v vuzah i ssuzah Belarusi / A. A. Chernyak, I. V. Kiryushin // Vyshejshaya shkola. – № 2. – 2022. – S. 26–31.
2. *Vinogradov, I. M.* Osnovy teorii chisel: uchebnik dlya vuzov / I. M. Vinogradov. – M. : Izdatel'stvo Lan', 2023. – 176 s.
3. *Zhmurova, I. Yu.* Teoriya chisel : uchebnoe posobie dlya vuzov / I. Yu. Zhmurova, A. V. Ignatova. – M. : Izdatel'stvo Yurajt, 2023. – 52 s.
4. *Nesterova, L. Yu.* Teoriya chisel: uchebnik i praktikum dlya vuzov / L. Yu. Nesterova, S. V. Napalkov. – Moskva: Izdatel'stvo Yurajt, 2023. – 150 s.
5. *Vinogradov, I. M.* Osnovy teorii chisel / I. M. Vinogradov. – M. : Izdatel'stvo YUrajt, 2023. – 123 s.