При этом свойство 3) функции Эйлера используется для анализа стойкости криптосистемы RSA против атаки повторного шифрования.

Понятие функции Эйлера можно обобщить и для многочленов над конечным полем следующим образом.

Пусть F_p – конечное поле, состоящее из p элементов, $g(x)$ – многочлен положительной степени над полем F_p. Обозначим через $\varphi(g)$ количество всех ненулевых многочленов над F_p, которые взаимно просты с многочленом $g(x)$ и степени которых меньше степени многочлена $g(x)$. Если же $g(x)$ – многочлен нулевой степени над полем F_p, то будем считать $\varphi(g) = 1$. Кроме того, введем следующее обозначение: $\tilde{g} = p^{\deg g}$, где $g(x) \in F_p[x]$.

Теорема 1. *Пусть* $f(x), g(x) \in F_p[x]$, $\deg(g) > 0$, $\text{НОД}\,(f, g) = 1$, *тогда* $f^{\varphi(g)} \equiv \equiv 1 (\mathrm{mod}\, g)$.

Теорема 2. *Имеют место следующие утверждения:*

1) пусть $f(x), g(x)$ – *ненулевые взаимно простые многочлены над* F_p, *тогда* $\varphi(f, g) = \varphi(f)\varphi(g)$;

2) пусть многочлен $g(x)$ *неприводим над* F_p, *тогда* $\varphi(g) = \tilde{g} - 1$;

3) пусть многочлен $g(x)$ *неприводим над* F_p, $m \in \mathbb{N}$, *тогда* $\varphi(g^m) = \tilde{g}^m - \tilde{g}^{m-1} = = \tilde{g}^m(1 - 1/\tilde{g})$;

4) пусть $g(x) = \prod_{i=1}^{k} g_i^{m_i}(x)$ – *каноническое разложение многочлена* $g(x)$ *на степени неприводимых над* F_p *многочленов* $g_1(x), \ldots, g_k(x)$, *тогда* $\varphi(g) = \tilde{g} \prod_{i=1}^{k}(1 - - 1/\tilde{g}_i)$, *в частности,* $\varphi(g) \equiv 0 (\mathrm{mod}(p-1)^k)$;

5) пусть $g(x)$ – *ненулевой многочлен над* F_p, *тогда* $\sum_{d|g} \varphi(d) = \tilde{g}$ *(суммирование проводится по всем унитарным делителям* $d(x) \in F_p[x]$ *многочлена* $g(x)$*).*

Полученные результаты показывают преемственность в изучении функции Эйлера в модулярной арифметики и в теории многочленов над конечными полями. Эти результаты могут быть использованы в учебном процессе по дисциплине «Криптографические системы с открытым ключом» для студентов высших учебных заведений, а также курсантов военных специальностей.

Литература

1. Бухштаб А.А. *Теория чисел.* М., 1960.

2. Агиевич С.В. *Математические и компьютерные основы криптологии.* Мн.: Новое издание, 2003.

ОПЫТ ПРОВЕРКИ ЗНАНИЙ СТУДЕНТОВ ПО АНАЛИТИЧЕСКОЙ ГЕОМЕТРИИ И ЛИНЕЙНОЙ АЛГЕБРЕ НА ФИЗИЧЕСКОМ ФАКУЛЬТЕТЕ И ФАКУЛЬТЕТЕ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Березкина Л.Л., Абрашина-Жадаева Н.Г., Тимощенко И.А., Филиппова Н.К.

Белорусский государственный университет, Минск, Беларусь
berezkina51@mail.ru; {zhadaeva@bsu.by,timoshchenkoia,filipava}@bsu.by

В организации учебного процесса в высших учебных заведениях мерами контроля результативности обучающихся являются наличие реальных систематических контрольных мероприятий, стимулирующих работу студентов в течение семестра, не включая зачетов и экзаменов.

На кафедре высшей математики и математической физики (ВМиМФ) физического факультета Белгосуниверситета оценка степени усвоения студентами изучаемого материала базировалась и базируется на регулярном тестировании. Такой метод апробирован в течение 30 лет. За это время составлен сборник тестов, включающий 9 частей (более 2000 вопросов) [1], и издано учебное пособие [2]. Эти материалы охватывают все разделы математического анализа, согласно учебным планам. Эффективность метода была налицо: тестирование проводилось регулярно по всем темам математического анализа; каждый студент выполнял индивидуальное задание и получал оценку, причем были минимизированы затраты времени преподавателя на проверку тестов.

В текущий момент, мы констатируем, что опыт внедрен и расширен в течение 15 лет по всем дисциплинам, которые читает кафедра ВМиМФ с применением электронных средств на образовательных порталах БГУ. В основу тестовых мероприятий по аналитической геометрии и линейной алгебре положены установки и принципы, заложенные преподавателями кафедры в трех частях учебного пособия «Высшая математика. Сборник задач», изданных в 2013–2015 гг. [3–5] и учебных пособий [6–8].

Созданный банк тестов имеет две части. I часть по курсу «Аналитическая геометрия», а II часть – «Линейная алгебра». Первая часть представляет собой набор тренировочных тестов по векторной алгебре, аналитической геометрии на плоскости и в пространстве, кривым и поверхностям второго порядка для студентов физических, радиофизических и математических специальностей. Они предназначены для оперативного контроля текущей успеваемости и промежуточной аттестации студентов с целью проверки их уровня подготовки по данной дисциплине и сформированности у них фундаментальных навыков.

Целью такого тестирования является подготовка и проверка степени усвоения материала студентами по данной дисциплине. Студент допускается к сдаче экзамена лишь в случае положительного результата тестирования. Уровень сложности заданий и их содержание полностью соответствуют требованиям государственного образовательного стандарта по высшей математике для физических специальностей вузов РБ.

Список вопросов конкретного теста формируется из перечня вопросов из банка тестов по данной теме. Вопросы выбираются случайным образом из разных разделов, что позволяет создать уникальный тест для каждого студента. Выбор разделов устанавливается преподавателем. Ввод персональных данных студент производит самостоятельно. Запуск теста осуществляет автоматически в установленное время администратором компьютерного класса. Количество вопросов в тестовом задании – 20. Время выполнения теста – 30 минут. В конце тестирования студент получает итоговый результат в процентах и возможность проверить правильность выполнения заданий. Для сдачи теста необходимо ответить не менее, чем на половину вопросов, а именно, набрать не менее 50%.

Таким же образом составлена и вторая часть тестовых заданий по всем темам, которые в совокупности охватывают все разделы курса «Линейная алгебра», изучаемые во втором семестре.

База данных тестов, сгруппированных по ключевым темам курса постоянно пополняется.

Литература

1. Жадаева Н.Г., Чупригин О.А. *Математический анализ: Задания коллоквиумов*. Ч. 5–6. Мн., 2001.

2. Чупригин О. А. *Математический анализ: Теория в тестах*. Мн.: БГУ, 2019.

3. Ахраменко В.К. [и др.]. *Высшая математика. Сборник задач*: учеб. пособие. В 3-х ч. Ч. 1. Аналитическая геометрия. Анализ функции одной переменной / под ред. Н.Г. Абрашиной-Жадаевой, В.Н. Русака. Мн.: БГУ, 2013.

4. Ахраменко В.К. [и др.]. *Высшая математика. Сборник задач*: учеб. пособие. В 3-х ч. Ч. 2. Линейная алгебра. Анализ функций многих переменных / под ред. Н.Г. Абрашиной-Жадаевой, В.Н. Русака. Мн.: БГУ, 2014.

5. Глецевич М.А. [и др.]. *Высшая математика. Сборник задач*: учеб. пособие. В 3-х ч. Ч. 3. Дифференциальные уравнения.Аналитические функции. Элементы функционального анализа / под ред. Н.Г. Абрашиной-Жадаевой, В.Н. Русака. Мн.: БГУ, 2015.

6. Абрашина-Жадаева Н.Г., Березкина Л.Л., Глецевич М.А., Филиппова Н.К. *Аналитическая геометрия*: учеб. пособие.

7. Абрашина-Жадаева Н.Г. [др]. *Аналитическая геометрия в примерах и задачах*. Мн.: РИВШ, 2008.

8. Березкина Л.Л. *Аналитическая геометрия и линейная алгебра*: учеб. пособие. Мн.: РИВШ, 2015.

ОБ ОДНОМ ЭКСПОНЕНЦИАЛЬНОМ НЕРАВЕНСТВЕ

Булатов В.И., Голухов В.Г., Кастрица О.А.

Белорусский государственный университет, Минск, Беларусь
bulatov@bsu.by; V.Goloukhov@gmail.com; kastritsa@bsu.by

Целью данной работы является обоснование для любого $t \neq 0$ хорошо известного неравенства

$$e^t > 1 + t, \tag{1}$$

не использующее исследование функций на монотонность и выпуклость методами дифференциального исчисления.

Очевидно, что (1) справедлива для $\forall t \leqslant -1$. Рассмотрим вначале случай $t = r \in \in \mathbb{Q}$, где $r \in (-1, 0) \bigcup (0, +\infty)$.

Во-первых, если $r \in (-1, 0)$, $r \in \mathbb{Q}$, то $\exists m, n \in \mathbb{N}$ такие, что $r = -m/(n+1)$, где $m < n + 1$. Учитывая далее неравенство $e < (1 + 1/n)^{n+1}$, $\forall n \in \mathbb{N}$, получим

$$e^r > \left(1 + \frac{1}{n}\right)^{-m} = \left(1 - \frac{1}{n+1}\right)^m = \prod_{k=1}^{m} \left(1 - \frac{1}{n+1}\right) \geqslant$$

$$\left[1 - \frac{1}{n+1} \geqslant 1 - \frac{1}{n-k+2} = \frac{n-k+1}{n-k+2} > 0, \quad 1 \leqslant k \leqslant m < n+1\right]$$

$$\geqslant \prod_{k=1}^{m} \left(\frac{n-k+1}{n-k+2}\right) = \frac{n-m+1}{n+1} = 1 - \frac{m}{n+1} = 1 + r.$$

Во-вторых, если $r > 0$, $r \in \mathbb{Q}$, то $\exists m, n \in \mathbb{N}$ такие, что $r = m/n$. Поэтому в силу неравенства $e > (1 + 1/n)^n$, $\forall n \in \mathbb{N}$, имеем

$$e^r > \left(1 + \frac{1}{n}\right)^m = \prod_{k=1}^{m} \left(1 + \frac{1}{n}\right) \geqslant \left[1 + \frac{1}{n} \geqslant 1 + \frac{1}{n+k-1} = \frac{n+k}{n+k-1} > 0, \quad \forall k \in \mathbb{N}\right] \geqslant$$

$$\geqslant \prod_{k=1}^{m} \frac{n+k}{n+k-1} = \frac{n+m}{n} = 1 + \frac{m}{n} = 1 + r.$$