При диктанте не организуется жесткого контроля за переговорами студентов (пусть помогают друг другу, если знают как) за использованием вспомогательного материала (если за короткое время студент найдет то, что надо, то это и требуется). Можно даже пользоваться конспектом, но только своим. Быстро выясняется, далеко не у всех он имеется и далеко не всегда там написано то, что требуется для ответа на вопросы. Это допускается по той причине, что цель математического диктанта чаще всего не контроль знаний, а закрепление полученных знаний Обычно диктант состоит из 12 вопросов и рассчитан на 35 минут учебного времени. Последние 10 минут студенты обязаны прочитать свои работы, а затем сдать на проверку. Иногда, чтобы студенты были не только писателями, но и читателями проверка случайным образом поручается студентам. Проверяющий должен поставить плюс при правильном ответе и исправить неправильный ответ, либо внести уточнения при неполной формулировке ответа.

Литература

1. Асмыкович И.К. *Реалии и перспективы электронного обучения математике* // «Современный педагогический процесс: содержание, методы, приемы, формы». Сб. тр. конф. – Астана: ТОО «Астанинский учебно-методический центр». 2019. С. 42–48.

2. Адуло Т.И., Асмыкович И. К. *Математическая компетентность индивида – необходимое условие инновационного развития общества* // Тр. БГТУ. Физ.-мат. науки и информатика. 2020. № 2 (236). С. 18–25.

3. Асмыкович И.К. *Математические диктанты как средство активизации работы студентов на практических занятиях* // В сб. «Новая технология обучения при двухступенчатой системе образования». Мн., 1992. Ч. I. С. 27–28.

МНОГОЧЛЕНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ В КУРСЕ «КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ»

Базылев Д.Ф.

Белорусский государственный университет, Минск, Беларусь
bazylev@bsu.by

В современном информационном пространстве одной из важнейших задач является обеспечение информационной безопасности, которая, в частности, включает в себя задачу обеспечения конфиденциальности переданной информации. В целях формирования фундаментальных знаний в области защиты информации курсанты военных специальностей должны быть ознакомлены с основными направлениями этой области знаний.

Обеспечение конфиденциальности достигается, например, путем использования криптосистемы RSA. Как известно, алгоритм криптосистемы RSA основан на свойствах функции Эйлера, в частности, используется формула Эйлера $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, справедливая для любого целого значения a и любого натурального значения m, взаимно простого с числом a. Функция Эйлера обладает следующими свойствами:

1) $\varphi(mn) = \varphi(m)\varphi(n)$ для взаимно простых натуральных чисел m и n;

2) $\varphi(m) = m \prod_{i=1}^{k}(1 - 1/p_i)$, где $p_1, p_2, \ldots, p_k$ – различные простые делители числа m;

3) $\sum_{d|m} \varphi(d) = m$.

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.