

Центральная часть рассматриваемой дисциплины должна быть посвящена описанию наиболее известных и востребованных криптосистем с открытым ключом: криптосистемы RSA, Рабина, Блюма — Гольдвассера, основанные на вычислительной сложности задачи факторизации больших чисел, криптосистемы Мэсси — Омуры и Эль-Гамала, основанные на сложности задачи дискретного логарифмирования в конечных полях большой мощности, криптосистема Мак-Элиса, основанная на сложности декодирования двоичных кодов, криптосистема рюкзака способа шифрования. Особое внимание следует уделить схеме электронной цифровой подписи на основе криптосистем RSA и Эль-Гамала, а также следует остановиться на задачах, связанных с созданием пороговой схемы разделения секрета на основе модулярной арифметики, и задачах, связанных с реализацией протоколов с нулевым разглашением.

Важной составляющей криптосистем, основанных на сложности факторизации больших натуральных чисел, являются современные методы проверки на простоту, а также методы генерации больших простых чисел, в том числе простых чисел специального вида. Эти методы позволяют сформулировать вероятностные и детерминированные тесты на простоту. Немаловажной задачей при этом является задача построения больших простых чисел, как общего вида, так и простых чисел, пригодных для использования в системе RSA.

Задача проверки чисел на простоту тесно связана с задачей факторизации больших простых чисел. Здесь стоит отметить такие методы, как методы факторизации Ферма и факторных баз, метод цепных дробей, методы Полларда и Вильямса, а также метод квадратичного решета и метод решета числового поля.

Отдельно следует остановиться на методах дискретного логарифмирования в полях большой размерности: методы сведения к собственным подгруппам, индекс-метод, методы Полларда и Гельфонда — Шенкса.

В заключение могут быть рассмотрены аналоги известных криптосистем на основе эллиптических кривых над конечными полями, а также приложения эллиптических кривых к тестированию натуральных чисел на простоту и к решению задачи факторизации больших простых чисел, поскольку в ряде случаев криптосистемы, основанные на эллиптических кривых, обладают более высокой стойкостью по сравнению с их числовыми аналогами.

Литература

1. Коблиц Н. *Курс теории чисел и криптографии*. М.: ТВП, 2001.

О ВЫДЕЛЕНИИ УРОВНЕЙ УСВОЕНИЯ СТУДЕНТАМИ СОДЕРЖАНИЯ МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН

Н.В. Бровка

Белгосуниверситет, механико-математический факультет, Минск, Беларусь
n_br@mail.ru

Изучение имеющихся классификаций уровней усвоения материала (Б. Блум, В. П. Беспалько, В. И. Загвязинский, О. Е. Лисейчиков и др.), практический опыт педагогической деятельности в вузе, и учет деятельностного характера математического знания позволили прийти к заключению о целесообразности выделения четырех уровней усвоения студентами содержания математического образования.

Первый — *уровень ознакомления и осмысления*. В силу таких особенностей математики, как абстрактность и опора на символичный математический язык, а также по причине насыщенности содержания математической подготовки новыми понятиями, на этом этапе важно не только ознакомление с новым материалом, но и содержательное, осознанное его осмысление, без которого невозможно его применение в дальнейшей деятельности. Результатом

деятельности студентов на этом уровне является *неформальное, содержательное распознавание и воспроизведение основных опорных понятий изучаемого материала*. Деятельность преподавателя является излагающей и руководящей.

Второй — уровень *репродукции*, достигается при заучивании материалов лекций, выполнении заданий по образцу, по алгоритму, в знакомой ситуации на практических занятиях, в процессе самостоятельной работы с учебником (деятельность по заучиванию и использованию понятий и их свойств в знакомой ситуации по образцу).

Результатом деятельности студентов под руководством преподавателя на этом уровне являются *знания опорных понятий и их свойств, способов решения типовых задач, доказательств основных теорем, умения определять, сравнивать, формировать, объяснять, доказывать, повторять*.

Третий уровень — *продуктивный*, предполагает *деятельность по использованию знаний в незнакомой, нестандартной ситуации, творческий перенос знаний под постоянным руководством и контролем преподавателя*. Студенты используют изученные материалы лекций, основной и дополнительной литературы, материалов спецкурсов, Интернет для выполнения индивидуальных заданий, написания рефератов, докладов, курсовых работ, добывают субъективно новую информацию (новую для себя).

Четвертый уровень — *уровень творческого применения знаний*, предполагает *деятельность по самостоятельному добыванию знаний и их применению для новых выводов и обобщений под идейным руководством преподавателя* [1].

Необходимо подчеркнуть, что мы считаем достаточным формирование у студентов навыков и умений субъективного творчества. Оно может находить свое выражение в самостоятельном оригинальном решении или доказательстве заданной задачи, теоремы, в получении и обобщении некоторых сведений или математических результатов, в применении таких средств интеграции теории и практики обучения, как различные виды межпредметных связей при выполнении индивидуальных творческих, курсовых и дипломных работ, докладов и рефератов на занятиях и научных студенческих конференциях. Таким образом, желание вывести студентов на уровень творчества позволяет нам планировать формирование лишь основ интегративных умений, которые опираются на межпредметные связи и являются составляющей умений творческих [2].

Результатом деятельности студентов на этом уровне являются умения обобщать, анализировать, выбирать, импровизировать, интегрировать, выделять, доказывать, алгоритмизировать, классифицировать, совершенствовать, использовать межпредметные и трансдисциплинарные связи; моделировать, исследовать.

Отсутствие объективной надежной диагностики уровня творчества в режиме оперативного оценивания вынуждает нас остановиться на уровне основ творческого применения усвоенного материала, изучаемого с использованием интеграции теории и практики обучения студентов математическому анализу. Результатом деятельности студентов на этом уровне являются умения студентов внедрять изученное, выделять главное, обосновывать и доказывать, использовать внутри-дисциплинарные знания для решения задач изучаемой темы; типизировать, планировать, систематизировать, решать стандартные и нестандартные задачи.

Построение системы заданий в процессе обучения и разработка контрольно-диагностических материалов мониторинга результатов их выполнения в соответствии с выделенными уровнями усвоения позволяет:

- 1) придать учебному процессу развивающий характер;
- 2) обеспечить преемственность изучения материала на различных этапах (ступенях) обучения;
- 3) сделать более продуктивным процесс усвоения знаний;
- 4) создать условия для поддержания и закрепления стремления к познанию и саморазвитию [2].

Литература

1. Бровка Н. В. *Уровни усвоения содержания при обучении студентов педагогической специальности математике* // Изв. Южного федерального университета. Педагогические науки. 2008. № 10. С. 21–28.
2. Бровка Н. В. *Обучение студентов математике на основе интеграции теории и практики*. Saarbrücken: Lap Lambert Academic Publishing, 2015. 273 с.

ОБ ОДНОМ АНАЛОГЕ НЕРАВЕНСТВА БЕРНУЛЛИ И НЕКОТОРЫХ ЕГО ПРИЛОЖЕНИЯХ

В.И. Булатов

Белгосуниверситет, факультет прикладной математики и информатики, Минск, Беларусь
Bulatov@bsu.by

Используя двойное неравенство

$$1 + (n+1)x + \frac{n(n+1)}{2}x^2 + \frac{n(n^2-1)}{6}x^3 \leq (1+x)^{n+1} \leq 1 + (n+1)x + \frac{n(n+1)}{2}x^2, \quad (1)$$

являющегося аналогом классического неравенства Бернулли и справедливость которого для $\forall n \in N_0$ и $x \in [-1; 0]$ обосновывается методом математической индукции, исследуем на монотонность и сходимости числовые последовательности

$$a_n = \sqrt{\frac{n+2}{n+1}} \left(1 + \frac{1}{n}\right)^n, \quad (2)$$

$$b_n = \left(1 + \frac{1}{n}\right)^{n+1/2}, \quad (3)$$

$$c_n = \frac{\sqrt{n}}{n!} \left(\frac{n}{e}\right)^n, \quad (4)$$

$$d_n = \frac{\sqrt{n+1}}{n!} \left(\frac{n}{e}\right)^n. \quad (5)$$

Теорема Последовательность (2) является возрастающей, а последовательность (3) убывающей.

Доказательство. Для $\forall n \in N$ в силу левой части (1) при $x = -1/(n+1)^2 \in [-1; 0]$ после элементарных преобразований имеем

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{(n+1)\sqrt{(n+1)(n+3)}}{n(n+2)} \left(1 - \frac{1}{(n+1)^2}\right)^{n+1} \geq \frac{(n+1)\sqrt{(n+1)(n+3)}}{n(n+2)} \left(1 - \frac{1}{n+1} + \right. \\ &\quad \left. + \frac{n}{2(n+1)^3} - \frac{n(n-1)}{6(n+1)^5}\right) = \sqrt{1 - \frac{1}{(n+2)^2}} \left(1 + \frac{1}{2(n+1)^2} - \frac{1}{6(n+1)^3} + \frac{1}{3(n+1)^4}\right) \geq \\ &\geq \left(1 - \frac{1}{2(n+1)^2} + \frac{1}{6(n+1)^3}\right) \left(1 + \frac{1}{2(n+1)^2} - \frac{1}{6(n+1)^3} + \frac{1}{3(n+1)^4}\right) = \\ &= 1 + \frac{1}{12(n+1)^4} + \frac{6n^2 + 5n + 1}{36(n+1)^7} \geq 1. \end{aligned}$$