Пример 1. Возьмем дифференциальное уравнение

$$y' = -\frac{y}{x} \quad \text{или} \quad \frac{dy}{dx} = -\frac{y}{x},$$

Данное уравнение является уравнением с разделяющимися переменными. Переносим переменные в разные стороны, записываем уравнение в виде

$$\frac{dy}{y} = -\frac{dx}{x}$$

Интегрирование левой и правой частей уравнения дает общее решение вида $\ln|y| = -\ln|x| + \ln c$, где постоянная взята в виде $\ln c$, $c > 0$. Далее несложно преобразовать данное уравнение к виду $yx = c''$ или $y = \bar{c}/x$ где постоянная $\bar{c}$ уже не имеет ограничений на знак. Как видно, получилось семейство гипербол.

знание	понимание	применение
анализ	синтез	оценка

В результате я наблюдала, что 30% учителей расположили вопросы в колонке «знание»; 25% — «понимание»; 20% — «применение»; 15% — «анализ»; 5% — «синтез»; 5% — «оценка». Можно утверждать, что использование правильных глаголов - это ключ к успешному написанию результатов обучения. Учителям предлагается проверить работу коллеги. Когда учителя комментируют работы друг друга, они не оценивают работы, а определяют и указывают на два положительных момента — *«две звезды»* — и на один момент, который заслуживает доработки, — *«желание»*. Данное оценивание проходит позитивно по отношению друг к другу, эффективно показывает, над чем работать учителю в дальнейшем.

Опыт — единство умений и знаний. Чем его больше, шире перспективы. Это то, что «вынесу из проделанной работы».

Задача школ на сегодняшний день заключается не только в достижении высоких результатов, но и в подготовке обучающихся к непрерывному образованию. Чтобы сохранялась перманентность образования, поскольку человек должен учиться всю свою жизнь.

Литература

1. *Руководство для тренера.* АОО «Назарбаев Интеллектуальные школы», 2012.

2. *Руководство для учителя.* АОО «Назарбаев Интеллектуальные школы», 2012.

3. Шакиров Р. Х., Буркитова А. А., Дудкина О. И., Сидоров В. В., Якин Я. Я. *Оценивание учебных достижений учащихся.* Б.: Билим, 2012.

4. Мирсеитова С., Иргебаева А. *Успехи и вызовы сегодняшнего дня RWCT.* Б.: Билим, 2012.

5. *Программа курсов повышения квалификации педагогов общеобразовательных школ РК.* www.cpm.kz

О ПРЕПОДАВАНИИ ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ»

Д.Ф. Базылев, М.М. Васьковский, Г.В. Матвеев

Белгосуниверситет, факультет прикладной математики и информатики, Минск, Беларусь

bazylev@bsu.by, vaskovskii@bsu.by, matveev@bsu.by

Современная криптография основана как на классических областях арифметики и алгебры, таких, как модулярная арифметика, теория конечных полей, так и на самых современных разделах, включающих теорию и приложения эллиптических кривых, помехозащитное кодирование.

Центральная часть рассматриваемой дисциплины должна быть посвящена описанию наиболее известных и востребованных криптосистем с открытым ключом: криптосистемы RSA, Рабина, Блюма — Гольдвасеер, основанные на вычислительной сложности задачи факторизации больших чисел, криптосистемы Мэсси — Омуры и Эль-Гамаля, основанные на сложности задачи дискретного логарифмирования в конечных полях большой мощности, криптосистема Мак-Элиса, основанная на сложности декодирования двоичных кодов, криптосистема рюкзачного способа шифрования. Особое внимание следует уделить схеме электронной цифровой подписи на основе криптосистем RSA и Эль-Гамаля, 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, та к 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 символьный 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