АДЫГЕЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ТОЧНЫХ НАУК И ЦИФРОВЫХ ТЕХНОЛОГИЙ
в рамках
КАВКАЗСКОГО МАТЕМАТИЧЕСКОГО ЦЕНТРА
состоится мини-курс

5, 6 и 7 апреля 2023 года с 14.45 по 16.20 –
ауд. 312 главного корпуса АГУ

«КОНЕЧНАЯ АЛГЕБРА И ЕЕ ПРИМЕНЕНИЯ»

Лектор: **Григорий Анатольевич Кабатянский**,
доктор физико-математических наук, вице-президент по академическому сотрудничеству Сколковского института науки и технологий (Сколтех),
G.Kabatyansky@skoltech.ru

Аннотация

Конечные поля были открыты Эваристом Галуа 190 лет назад и в течении долгого времени они даже среди математиков (кроме алгебраистов) были «вещью в себе» и вдруг где-то полвека назад они очень понадобились радиоинженерам, и стали их настольным инструментом! А затем они вдруг понадобились специалистам по криптографии, в простейшем случае как способ строить конечные логарифмы. Слово «вдруг» здесь играет важную роль, так как эти применения были неожиданными и, даже можно сказать, революционными.

В этом кратком курсе лекций я постараюсь объяснить математические понятия и результаты конечной алгебры через призму приложений.

Лекция 1. От поиска фальшивых монет к смартфону

Начнем с олимпиадной задачи. Имеется M монет и известно, что одна из них фальшивая. Также известно, что вес всех настоящих монет одинаков, и равен, скажем, 10 грамм, а вес фальшивой монеты равен 9 грамм. Имеются точные весы, но за каждое измерение надо платить, и, более того, план взвешиваний должен быть составлен заранее (например, точные весы находятся в другом городе). Сколько нужно взвешиваний, чтобы найти все фальшивые монеты?

Для одной монеты ответ двоичный $\log_2(M+1)$.

А что если, тот кто взвешивает монеты, может один раз соврать? (Более простой вариант – один раз не ответить).

Это уже не олимпиадная, а вполне серьезная задача, которую решили сравнительно недавно и понадобилось 10 лет, чтобы доказать, что 25 взвешиваний для миллиона монет достаточно, а 24 – нет.

Мы докажем этот результат совсем просто с помощью кода Хэмминга. Двоичный код Хэмминга – это такое максимальное множество двоичных -мерных векторов, что любые два вектора различаются как минимум в трех позициях. Можно задаться более общим вопросом – как устроены максимальные множества двоичных -мерных векторов таких, что любые два вектора различаются как минимум в d позициях. И если случай $d=3$, то есть коды Хэмминга, можно построить, не выходя за рамки привычной арифметики по модулю 2, то уже случай $d=5$ требует конечных полей. Например, для тех же миллиона монет понадобится поле из 2^{20} элементов.

Ну и конечно мы поговорим о том как с помощью кодов исправлять ошибки. А тут уже и смартфон рядом, и не только!

Лекция 2. Дележ секрета

Можно задаться довольно абстрактным вопросом: как определить линейную независимость векторов аксиоматически? А можно задаться вполне практическим вопросом о том, как «разделить» секрет между n участниками таким образом, что разрешенные множества (коалиции) участников могли бы найти секрет, а любые неразрешенные коалиции не узнавали о секрете ничего «дополнительного». Самый популярный и изученный пример – это пороговые (n,k)-схемы, когда разрешенные коалиции состоят из k или более участников. Мы расскажем элегантное решение этой подзадачи, придуманное Ади Шамиром, которое опирается на конечные поля. А еще мы обсудим задачу о построении семейств -мерных подпространств в n-мерном пространстве со свойством «все или ничего», то есть линейная оболочка любого множества этих подпространств пересекается с фиксированным k-мерным подпространством либо по вектору θ, либо содержит это фиксированное подпространство целиком. Отсюда мы вернемся к абстрактному определению независимости, известному как теория матроидов, и установим ее связь с задачей разделения секрета.

Лекция 3. Коды, чтобы запутать, а не исправить

Для большинства людей «код» это такой способ записать информацию, что никто, кроме легального получателя, не сможет эту информацию извлечь. На самом деле разработкой таких «кодов» занимается криптография – наука, хотя и родственная теории кодирования, но все-таки довольно далекая от нее. Однако есть один хорошо известный пример, когда можно построить «код тайнописи» с помощью кода, исправляющего ошибки. Это система МакЭлиса. Мы изложим ее, а также более традиционные криптографические системы, основанные на теории чисел и конечных полей, и объясним почему систему МакЭлиса любят называть «постквантовой».

Г.А.Кабатянский, 30.03.2023 г.

Регистрация на мини-курс здесь → https://goo.su/gLJsP. Просьба записаться до 17.00 4-го апреля 2023 года.

ПРИГЛАШАЮТСЯ СТУДЕНТЫ, ПРЕПОДАВАТЕЛИ И ВСЕ ЖЕЛАЮЩИЕ!!!