КЛАССИФИКАЦИЯ ТОЧЕЧНЫХ ОБРАЗОВ. ИСТОРИЯ И СОВРЕМЕННОСТЬ

В.А. ЛИПНИЦКИЙ, А.И. СЕРГЕЙ, Н.В. СПИЧЕКОВА

Распознавание образов — актуальнейшая проблема в практике видеонаблюдений и в теории обработки двумерных массивов информации. Один из ее предельных дискретных аналогов выглядит следующим образом. На множестве P_n квадратных (0,1)-матриц порядка n и с n единицами действует симметрическая группа S_n — переставляет строки и/или столбцы этих матриц. Требуется дать описание возникающих классов эквивалентности (орбит) и определить их количество a_n.

В таком виде задача возникла в поле зрения белорусской школы кодирования как частная задача обработки кодов-произведений. Несомненна ее связь с проблемами радиолокации, микробиологии, генетики. Установлена связь данной задачи с классической проблемой разбиения чисел, известной с XVIII века. Развитая в XIX веке теория конечных групп предоставляет леммой Бернсайда общую формулу для количества орбит при действии любой конечной группы на множестве.

По электронному адресу http://oeis.org/ размещается информационный ресурс «The On-Line Encyclopedia of Integer Sequences». Здесь последовательность a_n представлена под №A049311. Добавлена она на данный ресурс в 1999 г. П. Кэмероном со значениями a_1, a_2, …, a_7. Йовович В. нашел a_8. В 2003 г. добавлено еще 10 значений. В 2009 г. М. Алексеев нашел еще 10 значений.

В 2006 г. П. Кэмерон переформулировал задачу на языке теории графов. Им же сформулированы 27 открытых проблем теории подстановок. Проблема вычисления a_n стоит в этом списке под № 3.

На основе леммы Бернсайда вторым из авторов данного доклада в 2013 г. получены все из известных значений a_n и список продолжен до n=34.

XTR-КРИПТОСИСТЕМА. СПЕЦИФИКА И РЕАЛИЗАЦИЯ

В.А. ЛИПНИЦКИЙ, Е.В. СЕРЕДА

Первые криптосистемы, создавшие лицо современной криптографии — криптосистемы RSA, Рабина, Эль-Гамаля — основаны на вычислениях в кольцах классов вычетов. Криптографическая стойкость первых двух базируется на сложности задачи факторизации целых чисел, третья свою криптостойкость находила в изящной и внешне более простой проблеме дискретного алгоритма. Криптосистема Эль-Гамаля оказалась плодотворной в идейном плане. Она породила разнообразные модификации, вроде шнорровской. Появились и более далекие аналоги — на некоммутативных брейд-группах, на эллиптических кривых — требующие применения новейших результатов современной математики.

А. Ленстра и Е. Верхейл создали свою XTR-криптосистему на промежуточном материале — квадратичных расширениях K полей классов вычетов Z/pZ. Аббревиатура XTR очень точно отражает суть криптосистемы — эффективное вычисление в поле K следов элементов поля F — расширение Z/pZ шестой степени. Здесь также наблюдается упор на проблему дискретного логарифма.

XTR-криптосистема была представлена общественности авторами в 2000 г. Следовательно, её можно считать целиком продуктом XXI века. Отсутствие иных публикаций и наличие спорадических сообщений, из которых явствует, что XTR-криптосистема далеко не хуже иных ныне действующих, свидетельствует о деловом интересе к ней реальных разработчиков средств защиты информации.

Авторами данного доклада XTR-криптосистема тщательно изучена, разработана собственная ее программная реализация для достаточно широкого спектра параметров.