О ПРОБЛЕМЕ «ДВОЙКИ» В КРИПТОЛОГИИ

А.А. ЧАРУШИНА, В.А. ЛИПНИЦКИЙ

Современная криптология в основном является «вычетной» — наиболее популярные алгоритмы в защите информации от несанкционированного доступа так или иначе связаны с вычислениями в кольцах классов вычетов. Важной составляющей формирования криптосистем типа Эль-Гамаля является проблема определения примитивного элемента (первообразного корня) в кольце классов вычетов по простому модулю. Задача достаточно громоздкая.

Предельно минимальным выражением этой проблемы и является известная в теории чисел проблема «двойки» — конечно или бесконечно количество простых p, для которых 2 есть первообразный корень?

Как и по большинству проблем теории чисел (проблема «близнецов», проблема Гольдбаха, проблема нулей дзета-функции и много других) специалисты уверенно высказываются о неразрешимости проблемы «двойки» и сулят премию Неванлинны за ее решение.

В докладе приводятся первые результаты исследования проблемы «двойки». Все простые числа можно разделить на 4 непересекающихся класса, принадлежащие последовательностям $8n+1$, $8n+3$, $8n+5$ и $8n+7$. Каждая из названных последовательностей — арифметических прогрессий — содержит, согласно теореме Дирихле, бесконечно много простых чисел. Доказано, что в первой и последней последовательностях ни одно из простых чисел не может иметь 2 в качестве первообразного корня.

В математическом пакете «Mathematica» разработана компьютерная программа, позволяющая эффективно вычислять первообразный корень по простому модулю, в частности, проверять первообразность двойки. С помощью данной программы была исследована 2 на примитивность для каждого из первых 50 000 простых чисел из последовательностей $8n+3$ и $8n+5$. Выяснилось, что в каждой из этих двух последовательностей примерно для 75% простых чисел 2 является первообразным корнем.