Некоторые вычислительные задачи в полях простого порядка

С. В. Конягин

Пусть $\mathbb{F}_p$– поле вычетов по простому модулю p. Основное внимание будет сосредоточено на следующих задачах.

1. Дан многочлен над полем $\mathbb{F}_p$. С помощью детерминированного алгоритма найти все корни многочлена в $\mathbb{F}_p$ или какой-либо его корень.

2. Задано число e, делящее $p-1$. Имеется неизвестный элемент $s \in \mathbb{F}_p$. Оракул для любого $x \in \mathbb{F}_p$ сообщает $(x+s)^e$. Требуется определить s с помощью детерминированного алгоритма, используя возможно меньшее число обращений к Оракулу и арифметических операций.

Доклад основан на готовящихся к печати совместных работах докладчика с Ж. Бургеном, М. З. Гараевым и И. Е. Шпарлинским.