ОБ ИСПОЛЬЗОВАНИИ ЦЕПНЫХ ДРОБЕЙ ДЛЯ ВЫБОРА МНОГОЧЛЕНОВ В АЛГОРИТМЕ РЕШЕТА ЧИСЛОВОГО ПОЛЯ

О.В. Бабуль, Д.В. Васильев

Институт математики НАН Беларуси,

Сурганова 11, 220072 Минск, Беларусь

vasilyev@im.bas-net.by, oleg.babul@gmail.com

Нами получен алгоритм построения квадратичного многочлена со старшим коэффициентом равным единице, который может быть использован в алгоритме решета числового поля для решения задачи дискретного логарифмирования.

Задача нахождения целого числа x такого, что $g^x \equiv b(\mathrm{mod} p)$ называется задачей дискретного логарифмирования. Здесь p — простое число, g — первообразный корень по модулю p, $0 < b < p$. На сегодняшний день одним из самых эффективных методов решения задачи дискретного логарифмирования для больших p является метод решета числового поля. Одной из стадий данного метода является построение пары многочленов $f_1(x)$, $f_2(x)$, обладающих следующими свойствами.

1. $f_1(x), f_2(x) \in \mathbb{Z}[x]$ -- неприводимы над $\mathbb{Q}$.

2. Для заданного большого простого числа p существует $m \in \mathbb{Z}$, такое что $f_1(m) \equiv f_2(m) \pmod p$ и $f_i'(m) \not\equiv 0 \pmod p$ при $i = 1, 2$.

Обзор существующих методов построения многочленов можно найти в [1]. В случае задачи дискретного логарифмирования один из многочленов можно выбрать произвольным образом и свойство 2 сводится к задаче построения многочлена по заданному корню. Для последующих стадий алгоритма решета числового поля необходимо, чтобы коэффициенты многочленов имели малые по модулю значения.

Найденный алгоритм использует свойства цепных дробей и позволяет за $O(\log^3 p)$ шагов построить $f(x) \in Z[x]$, такой что $f(m) \equiv 0 \,(\mathrm{mod} p)$ и $\|f(x)\| \leqslant \min\limits_{k>1}\left(\max\left(\frac{q_k}{2}, \frac{p}{q_k}\right)\right)$, где $\|f(x)\|$ — высота многочлена $f(x)$, $\frac{p_k}{q_k}$ — k-я подходящая дробь к $\frac{m^{-1} \bmod p}{p}$.

Литература

1. *Murphy B.A.* Polynomial selection for the number field sieve integer factorisation algorithm // Ph.D. thesis, Australian National University, 1999.