МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени М. В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

ОТЗЫВ НА ИТОГОВУЮ КВАЛИФИКАЦИОННУЮ (ДИПЛОМНУЮ) РАБОТУ

студента 6-го курса 605-й группы Семенюка Павла Игоревича

Научный руководитель доцент Е. А. Уланский

ТЕМА О доказательстве Галкина корректности и остановки сигнатурного алгоритма Фожера

В дипломной работе П. И. Семенюка изучается алгоритм Фожера F5 построения базиса Грёбнера заданного идеала кольца многочленов. Построение базиса Грёбнера требуется во многих прикладных задачах, в том числе при решении задачи дискретного логарифмирования на эллиптических кривых методом Семаева. От скорости нахождения базиса Грёбнера существенно зависит скорость нахождения дискретного логарифма, а F5 считается наиболее эффективным алгоритмом построения базиса Грёбнера на сегодняшний день.

В существующей на сегодняшний день достаточно обширной литературе, посвящённой описанию алгоритма Фожера, не обнаруживается внятного доказательства как его корректности, так и остановки. Павел провёл объёмное исследование и привёл в своей работе максимально подробное описание алгоритма, указывая явно этапы его работы, а также приводя обоснование остановки алгоритма, руководствуясь при этом доказательством Галкина. К сожалению, в полной мере не удалось привести доказательство корректности алгоритма, а также не до конца удалось реализовать идею синтезирования на основе имеющихся описаний наиболее удобного языка изложения.

Автор продемонстрировал достаточное знакомство с базисами Грёбнера и алгоритмами их построения. Проведённая им работа будет полезна для дальнейших исследований в этой области.

Считаю, что дипломная работа П. И. Семенюка «О доказательстве Галкина корректности и остановки сигнатурного алгоритма Фожера» должна быть оценена «хорошо».

_____ /Е. А. Уланский/ *18 мая 2019 г.*