«УТВЕРЖДАЮ»
РЕКТОР
ФГБОУ ВПО «МОСКОВСКИЙ ПЕДАГОГИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
академик РАН, академик РАО
_____ / А.Л. Семёнов /
«__7__» апреля 2014г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

о диссертации Копьева Дмитрия Викторовича
«Квадратичные вычеты и невычеты и их приложения», представленной на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06- математическая логика, алгебра и теория чисел

Диссертация посвящена исследованию квадратичных вычетов невычетов и их приложениям. Это направление относится к аналитической теории чисел. Понятие квадратичного вычета было введено Л.Эйлером и исследовалось К. Гауссом, К. Якоби. И.М. Виноградов получил оценку наименьшего квадратичного невычета по простому модулю. Эту оценку впоследствии уточняли Г. Дэвенпорт, П.Эрдёш, Ю.В. Линник. Важную роль играет задача о распределении квадратичных вычетов и невычетов на коротком интервале. Здесь результаты получены И.М. Виноградовым, Г. Полиа, Д. Бёрджессом. Интерес к упомянутым выше и близким задачам проявили такие известные математики, как А.А. Карацуба , В.Н. Чубариков, Р.Н. Бояринов и др. Ими в последние годы получены многие важные результаты в этом направлении.

Теоретико-числовые методы играют важную роль в криптографии с открытым ключом. В работах Р. Ривеста, А. Шамира и Л. Адельмана разработан протокол, названный «Ментальный покер».

Диссертационная работа состоит из введения, трёх глав и заключения.

Автор диссертации Д.В. Копьев получил ряд новых важных результатов. Основными результатами работы являются:

- Законы распределения символов Якоби в последовательностях по системе различных попарно взаимно простых модулей по непрерывному промежутку и по последовательности бесквадратных чисел
- Оценка суммы Гаусса специального вида
- Обнаружение уязвимости одного криптографического протокола арифметическим методом
- Вычисление точного значения многомерной суммы Гаусса
- Нахождение закона распределения очень коротких усреднённых сумм Гаусса

Результаты диссертации актуальны, они относятся к современной области исследований, развивающей классическую теорию. Их получение потребовало привлечения ряда новых идей.

Основные результаты работы прошли надлежащую апробацию и опубликованы в пяти работах, в том числе в двух работах в рецензируемых научных изданиях. Автореферат соответствует содержанию диссертации.

Диссертация является научно-квалификационной работой, содержащей решения задач, имеющих существенное значение для аналитической теории чисел. Она соответствует требованиям пп.9, 10,11,13,14 «Положения о присуждении учёных степеней», предъявляемым к кандидатским диссертациям, а ее автор Д.В. Копьев заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Рецензент - кандидат физико-математических наук, доцент кафедры теории чисел Марис Евгеньевич Чанга.

Отзыв обсуждён и утверждён на заседании кафедры теории чисел математического факультета 7 апреля 2014г., протокол № 9.

И.о. зав. кафедрой теории чисел,
профессор кафедры теории чисел, д.ф.-м.н. В.Г.Чирский

МГУ для заверения документов
ПОДПИСЬ
УДОСТОВЕРЯЮ
Начальник Управления делами Л.А. Шведова