**Отзыв**
**официального оппонента**
**на диссертацию Копьева Дмитрия Викторовича**
**«Квадратичные вычеты и невычеты и их приложения»,**
**представленную на соискание ученой степени кандидата**
**физико-математических наук по специальности 01.01.06 —**
**Математическая логика, алгебра и теория чисел**

В диссертационной работе Д. В. Копьева изучаются задачи о распределении квадратичных вычетов и невычетов в совместно распределенных последовательностях по различным модулям, распределение значений очень коротких двумерных сумм Гаусса, а также рассмотрены приложения квадратичных вычетов к анализу одного криптографического протокола. Этим задачам посвящены фундаментальные работы И. М. Виноградова, Ю. В. Линника, А. А. Карацубы, Г. И. Архипова, В. Н. Чубарикова, Г. Полиа, Г. Дэвенпорта, П. Эрдеша, Д. Берджесса и других.

Диссертационная работа Д. В. Копьева состоит из введения, трёх глав и списка литературы. Во введении приведён литературный обзор по исследуемым проблемам, обосновывается актуальность темы и излагается краткое содержание диссертации.

В первой главе, состоящей из пяти параграфов, изучена задача о совместном распределении значений символов Якоби по различным попарно взаимно простым модулям $m_1, m_2, \dots, m_n$, а именно задача о количестве значений $x \le X$, удовлетворяющих соотношениям

$$\left(\frac{x+a_1}{m_1}\right) = \varepsilon_1, \quad \dots, \quad \left(\frac{x+a_n}{m_n}\right) = \varepsilon_n, \tag{1}$$

где $\varepsilon_1, \dots, \varepsilon_n$ принимают значения $\pm 1$, суть которого заключается в следующем:

- *если* $Q = m_1 m_2 \dots m_n$, $m_1, m_2, \dots, m_n$ — *безкубические числа,* $V(x)$ — *количества* $x \le X$, *удовлетворяющих соотношениям (1),* $0 < \varepsilon < 0,0625$, $Q^{\frac{1}{4}+\omega} < X \le Q$, $\omega = \frac{3\sqrt{\varepsilon}}{2-4\sqrt{\varepsilon}}$, *то*

$$V(x) = \frac{X}{2^n} + W(X), \qquad W(X) \ll XQ^{-\frac{\varepsilon}{4}};$$

- *если* $Q = m_1 m_2 \dots m_n$, $m_1, m_2, \dots, m_n$ — *произвольные числа,* $V(x)$ — *количества* $x \le X$, *удовлетворяющих соотношениям (1),* $0 < \varepsilon < 0,15625$,

$Q^{\frac{3}{8}+\omega} < X \leq Q$, $\omega = 4\varepsilon$, *то*

$$V(x) = \frac{X}{2^n} + W(X), \qquad W(X) \ll XQ^{-\frac{3\varepsilon}{8}};$$

- *если* $Q = m_1 m_2 \dots m_n$, $m_1, m_2, \dots, m_n$ — *безкубические числа,* $F(x)$ — *количества бесквадратных* $x \leq X$, *удовлетворяющих соотношениям (1),* $0 < \varepsilon < 0,0533$, $Q^{\frac{1}{4}+\omega+2\varepsilon} < X \leq Q$, $\omega = \frac{3\sqrt{\varepsilon}}{2-4\sqrt{\varepsilon}}$, *то*

$$F(x) = \frac{6}{\pi^2} \cdot \frac{X}{2^n} + W(X), \qquad W(X) \ll XQ^{-\frac{\varepsilon}{4}};$$

- *если* $Q = m_1 m_2 \dots m_n$, $m_1, m_2, \dots, m_n$ — *произвольные числа,* $F(x)$ — *количества бесквадратных* $x \leq X$, *удовлетворяющих соотношениям (1),* $0 < \varepsilon < \frac{5}{48}$, $Q^{\frac{3}{8}+\rho} < X \leq Q$, $\rho = 6\varepsilon$, *то*

$$F(x) = \frac{6}{\pi^2} \cdot \frac{X}{2^n} + W(X), \qquad W(X) \ll XQ^{-\frac{3\varepsilon}{8}};$$

Первый и второй результаты являются обобщением соответствующего результата Э.К.Жимбо для символов Лежандра на случай символа Якоби и многомерным аналогом теорем Д.Берджесса об асимптотической равенстве квадратичных вычетов и невычетов на промежутке длины превосходящей $Q^{\frac{1}{4}+\varepsilon}$.

Вторая глава «Уязвимость криптографического протокола "Ментальный покер"» посвящена исследованию арифметических уязвимостей этого протокола. Показано каким образом нужно выбирать кодирующие числа, чтобы исключить возможность раскрытия закрытой информации.

Третья глава состоит из трех параграфов и посвящена вычислению точного значения полной суммы Гаусса с квадратичной формой в показателе степени, у которой коэффициенты взаимно просты со знаменателем и её приложении к распределению коротких усредненых сумм Гаусса: *пусть* $p$ — *простое,* $(a,p) = 1$, *числа* $x$ *и* $h$ – *целые в пределах* $0 \leq x < p$ *и* $0 < h < p$, *а* $\chi$ — *комплексный характер по модулю* $p$.

$$S_h(x) = \sum_{n=x+1}^{x+h} \sum_{m=x+1}^{x+h} \chi(n+m) e\left(\frac{a(n+m)}{p}\right),$$

*где* $p$ — *простое,* $(a,p) = 1$, *числа* $x$ *и* $h$ — *целые в пределах* $0 \leq x < p$ *и* $0 < h < p$, *а* $\chi$ — *комплексный характер по модулю* $p$. *Тогда при* $p \to +\infty$,

*поскольку* $h(p) \to +\infty$ *и* $\frac{\log h}{\log p} \to 0$ *величина*

$$\xi = \xi(h,p) = \left| \frac{S_h(x)}{h^{\frac{3}{2}}} \right|^2$$

*асимптотически имеет экспоненциальное распределение с параметром* $\lambda = \frac{3}{2}$.

В диссертации Д. В. Копьева получены следующие результаты:

1. Получены законы распределения символов Якоби в последовательностях по системе различных попарно взаимно простых модулей по непрерывному промежутку и по последовательности бесквадратных чисел. Получена оценка суммы Гаусса специального вида.

2. Арифметическим методом обнаружены уязвимости одного криптографического протокола.

3. Вычислено точное значение многомерной суммы Гаусса. Найден закон распределения очень коротких усредненных сумм Гаусса.

Полученные результаты обоснованы строгими математическими доказательствами, их достоверность не вызывает сомнения. В целом результаты представляют научный интерес в аналитической теории чисел.

Работа написана грамотно и ясно. Основные результаты, излагаемые в диссертации, опубликованы. Автореферат правильно отражает содержание диссертации. Имеющиеся в диссертации отдельные опечатки (например: стр. 33 ссылка на несуществующую теорему 2, должна быть указана теорема 1.2; в теореме 1.6 описка в условии $Q^{\frac{1}{4}+\omega} < X < Q$, в показателе вместо $\frac{1}{4}+\omega$ должно быть $\frac{3}{8}+\omega$) редакционного и стилистического характера не вносят особых трудностей при ее чтении.

Все это говорит о том, что представленная диссертация Дмитрия Викторовича Копьева *«Квадратичные вычеты и невычеты и их приложения»,* соответствует всем требованиям пунктов 9, 10, 11, 12 и 14 «Положения о порядке присуждения ученых степеней», предъявляемым ВАК РФ к кандидатским диссертациям, а ее автор, Копьев Дмитрий Викторович, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 01.01.06 — Математическая логика, алгебра и теория чисел

**Официальный оппонент, доктор физико-математических наук, член корреспондент АН Республики Таджикистан, профессор** **З. Х. Рахмонов**

10.04.2014 г.