

## Наименьший квадратичный невычет и гипотез Виноградова

Абдунабиев Джамшид

Магистратура Термезского государственного университета

70540101 - Математика (Алгебра и теория чисел) специализация II курс 223 - студент магистратуры

+998919769616

jamshidabdunabiyev5@gmail.com

### ABSTRACT

Гипотезы Виноградова — фундаментальные проблемы теории чисел, которые интриговали математиков на протяжении десятилетий. Одним из ключевых аспектов этих гипотез является концепция наименьшего квадратичного невычета, которая играет решающую роль в понимании распределения простых чисел и поведения арифметических функций. Эта статья исследует значение наименьшего квадратичного невычета в контексте гипотез Виноградова, проливая свет на его значение для изучения простых чисел и более глубокие связи между теорией чисел и алгебраическими структурами. Углубляясь в сложности этих гипотез и их связь с наименьшим квадратичным невычетом, данный реферат призван предоставить всесторонний обзор текущего состояния исследований в этой увлекательной области математики.

### ARTICLE INFO

**Received:** 24<sup>th</sup> December 2023

**Revised:** 20<sup>th</sup> January 2024

**Accepted:** 26<sup>th</sup> February 2024

### KEYWORDS:

наименьший квадратичный невычет, гипотезы Виноградова, теория чисел, простые числа, арифметические функции, квадратичные вычеты, квадратичные невычеты.

Гипотезы Виноградова, с другой стороны, являются предположениями о распределении простых чисел в арифметических прогрессиях. Эти темы имеют глубокие связи с различными областями математики и вызывают обширные исследования и исследования. В этой статье представлен обзор концепции наименьшего квадратичного невычета, обсуждаются гипотезы Виноградова и исследуется их значение в области теории чисел.<sup>1</sup>

Концепция наименьшего квадратичного невычета и гипотезы Виноградова — увлекательные темы теории чисел, интригующие математиков на протяжении десятилетий. Наименьший квадратичный невычет относится к наименьшему положительному целому числу, которое не является квадратичным вычетом по модулю данного простого числа. Квадратичные вычеты — это числа, которые имеют квадратные корни по модулю простого числа, а невычеты — нет. Изучение наименьших квадратичных невычетов дает представление о распределении квадратичных остатков и невычетов, а также об их свойствах и отношениях с простыми числами. Гипотезы Виноградова, названные в честь русского математика Ивана Матвеевича Виноградова, представляют собой набор гипотез, связанных с распределением простых чисел. Эти гипотезы предполагают определенные

<sup>1</sup> Виноградов И. М. (1947). Метод тригонометрических сумм в теории чисел. Издательство Интерсайенс.

закономерности и связи между простыми числами и их распределением в арифметических прогрессиях. Гипотезы Виноградова имеют глубокие последствия для теории простых чисел и вдохновили на обширные исследования в области теории чисел.

Связь между наименьшим квадратичным невычетом и гипотезами Виноградова заключается в их общей направленности на распределение и свойства чисел по отношению к простым числам. Изучая наименьший квадратичный невычет и его связь с квадратичными остатками и невычетами, математики могут получить представление о распределении простых чисел и потенциально обнаружить новые закономерности или связи, которые прольют свет на гипотезы Виноградова. Исследование наименьшего квадратичного невычета и гипотез Виноградова открывает богатую и сложную среду для математических исследований с потенциалом углубить наше понимание теории чисел и распределения простых чисел.<sup>2</sup>

Для каждого простого числа  $p$  пусть  $n(p)$  обозначает наименьший квадратичный невычет по модулю  $p$ . Виноградов предположил, что  $n(p) = O(p^\epsilon)$  для любого фиксированного  $\epsilon > 0$ . Эта гипотеза следует из обобщенной гипотезы Римана и, как известно, верна почти для всех простых чисел  $p$ , но в целом остается открытой. Гипотезы Виноградова являются одними из наиболее известных и важных гипотез в области теории чисел. Они были предложены русским математиком Иваном Виноградовым в 1937 году и до сих пор остаются нерешенными.

Первая гипотеза Виноградова, известная как Теорема о трех простых числах, утверждает, что для любого большого числа  $N$  существуют три простых числа  $p$ ,  $p+2$  и  $p+2N$ , где  $p$  - это наименьшее простое число, большее  $N$ . Эта гипотеза имеет важные последствия в области криптографии и доказательства сложности некоторых алгоритмов. Вторая гипотеза Виноградова утверждает, что для любого натурального числа  $a$  и любого большого числа  $N$  существует простое число  $p$ , такое что  $p \equiv a \pmod{N}$ . Это означает, что простые числа равномерно распределены в арифметических прогрессиях. Эта гипотеза имеет важные последствия в области криптографии, а также в решении некоторых диофантовых уравнений. Исследование гипотез Виноградова имеет глубокие связи с другими областями математики, такими как алгебраическая и аналитическая теория чисел. Оно также имеет практическое значение в криптографии и вычислительных методах.<sup>3</sup>

Хотя ни одна из гипотез Виноградова не была полностью доказана, существует множество работ и исследований, направленных на их подтверждение или опровержение. Недавние прорывы и открытия в этой области привели к новым методам и техникам, которые могут быть использованы для дальнейшего исследования. В заключение, гипотезы Виноградова представляют собой важные и интересные проблемы в области теории чисел. Их исследование имеет значительное значение для различных областей математики и может привести к новым открытиям и применениям.

Исследование гипотез Виноградова имеет глубокие связи с другими областями математики, такими как алгебраическая и аналитическая теория чисел. Взаимодействие этих областей позволяет разрабатывать новые методы и подходы к решению этих гипотез. Алгебраическая теория чисел изучает свойства целых чисел и их алгебраических связей. Она помогает анализировать структуру простых чисел и их распределение в различных арифметических прогрессиях. Эти знания могут быть применены для изучения гипотез Виноградова.<sup>4</sup>

Аналитическая теория чисел, с другой стороны, использует методы математического анализа для изучения численных свойств последовательностей чисел. Она позволяет анализировать распределение

---

<sup>2</sup> Монтгомери, Х.Л., и Воган, Р.К. (2007). Мультипликативная теория чисел I: Классическая теория (Том 97). Издательство Кембриджского университета.

<sup>3</sup> Харди Г. Х. и Райт Э. М. (2008). Введение в теорию чисел. Издательство Оксфордского университета.

<sup>4</sup> Ирландия К. и Розен М. (2013). Классическое введение в современную теорию чисел (2-е изд.). Спрингер.

простых чисел и исследовать их поведение в контексте гипотез Виноградова. Кроме того, исследование гипотез Виноградова имеет практическое значение в криптографии и вычислительных методах. Понимание распределения простых чисел и свойств арифметических прогрессий может быть использовано для разработки безопасных криптографических алгоритмов. Это также может помочь в оптимизации вычислительных методов, основанных на арифметике больших чисел.

В целом, исследование гипотез Виноградова имеет глубокие связи с другими областями математики и имеет практическое значение в криптографии и вычислительных методах. Это является важным направлением исследований, которое может привести к новым открытиям и применениям в будущем.<sup>5</sup>

#### Литературы:

1. Виноградов И. М. (1947). Метод тригонометрических сумм в теории чисел. Издательство Интерсайенс.
2. Монтгомери, Х.Л., и Воган, Р.К. (2007). Мультипликативная теория чисел I: Классическая теория (Том 97). Издательство Кембриджского университета.
3. Харди Г. Х. и Райт Э. М. (2008). Введение в теорию чисел. Издательство Оксфордского университета.
4. Ирландия К. и Розен М. (2013). Классическое введение в современную теорию чисел (2-е изд.). Спрингер.
5. Натансон, М.Б. (2015). Элементарные методы теории чисел. Спрингер.

---

<sup>5</sup> Натансон, М.Б. (2015). Элементарные методы теории чисел. Спрингер.