УДК

ТЕОРЕМА ЛАГРАНЖА О СУММЕ ЧЕТЫРЁХ КВАДРАТОВ

Трубач К.И., студент гр.251002, Крутько А.А., студент гр.251004

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Баркова Е.А. – канд. физ.-мат. наук, доцент

Аннотация. Эта статья исследует взаимосвязь между теоремой Лагранжа о разложении натуральных чисел в сумму четырёх квадратов и бинарной проблемой Гольдбаха. Результаты показывают, что количество и размер делителей существенно влияют на количество неуникальных разложений Лагранжа. Открытия подтверждаются формулой Якоби о сумме квадратов четырёх чисел. Работа имеет перспективы в комбинаторике, криптографии и представляет интерес с художественной точки зрения.

Ключевые слова. Разложение Лагранжа, теорема Эйлера-Ферма, проблема Гольдбаха, криптография, комбинаторика, алгоритмы, математические свойства, простые множители, числовая теория, анализ данных, связь математических концепций.

В третьем веке нашей эры древнегреческий учёный Диофант описал теорему [1], которая позднее была доказана Жозефом Луи Лагранжем и была названа в его честь. Суть теоремы заключается в следующем: всякое натуральное число можно представить в виде суммы четырёх квадратов целых чисел. Она приобрела множество вариаций в теории чисел, таких как проблема Варинга, теорема Лежандра о трёх квадратах, теорема Ферма о многоугольных числах, теорема Якоби о сумме четырёх квадратов и так далее. В данной работе внимание было направлено на решение следующих вопросов: сколько уникальных разложений имеет данное натуральное N? От чего зависит количество разложений для данного натурального N?

Поставленные вопросы требуют решения ряда дополнительных вычислительных задач. Чтобы обнаружить и объяснить закономерности в распределении количества разложений в зависимости от натурального N, необходимо обнаружить все разложения для каждого N и сосчитать их.

Наивный подход заключается в решении задачи методом “грубой силы”. Это включает в себя поочерёдную генерацию всех возможных комбинаций натуральных чисел a, b, c, d и последующую проверку, равняется ли сумма их квадратов N. В случае нахождения такой комбинации программа дополнительно проверяет, уникален ли данный набор a, b, c, d, и если, так, то он входит в итоговое число разложений для данного N. Однако такой подход приводит к вычислительной сложности O(N^3), что является плохим показателем. В 1986 году Майкл О. Рабин и Джеффри Шаллит [2] предложили рандомизированные алгоритмы полиномиального времени для вычисления разложения для заданного целого числа n за ожидаемое время работы O(log(n)^2). В дальнейшем время было улучшено Полом Поллаком и Энрике Тревиньо в 2018 году [3]. Используя известные оптимизации, мы собрали набор данных, представленных на рисунке 1.

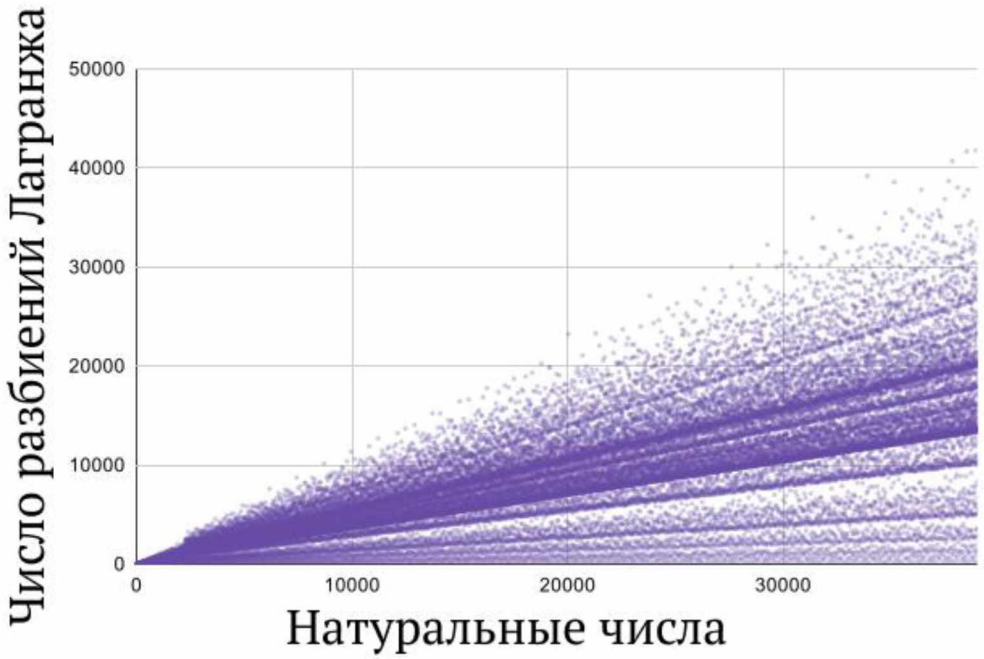

Рисунок 1 – Диаграмма зависимости количества разложений Лагранжа от натурального N

Обратим внимание, что плотность покрытия диаграммы неоднородна. Заметны также более четкие, чем прочие, линии, как лучи выходящие из начала координат. На данном этапе становится понятным тот факт, что представленная зависимость получается нелинейным способом, а путем сложения (вычитания) каких-то функций (условий), которые и задают наблюдаемые «лучи», совмещенные на одном изображении.

Хорошей отправной точкой для исследования стала бинарная проблема Гольдбаха, которая была исследована нами год назад [4]. Тогда нами был открыт ряд свойств, что объясняли поведение точек на диаграмме, а, поскольку диаграммы первичных данных для обоих математических вопросов оказались похожи, оставалось только обосновать присутствующую связь.

Бинарная проблема Гольдбаха предполагает, что каждое чётное натуральное число может быть представлено в виде суммы двух простых (18 = 5+13 и т.д.). При этом некоторые простые числа, а именно: вида p=4n+1 – согласно теореме Ферма-Эйлера могут быть представлены в виде суммы двух квадратов. Например, при n = 1 и n = 3 можно получить уже упомянутые числа 5 и 13, которые раскладываются на 1^2+2^2 и 2^2+3^2.

То есть, по своей сути, числа из проблемы Гольдбаха могут раскрываться в разложения теоремы Лагранжа с двумя ограничениями: во-первых, это раскрытие применимо только для чётных N, и, во-вторых, приблизительно лишь каждое второе простое число имеет упомянутое представление (эти данные были получены эмпирически с помощью вспомогательной программы: из 7 271 035 первых простых чисел 3 635 171 могут быть представлены как p=4n+1, что в отношении равняется 2.000190637524342).

Хотя обнаруженная связь не слишком сильна, она всё же присутствует, поэтому мы приступили к проверке свойств, присущих распределению разложений Гольдбаха. Согласно нашей прошлогодней работе, количество разложений Гольдбаха зависело преимущественно от следующих показателей: количество уникальных простых множителей для данного N и общее количество простых множителей для данного N. Теперь необходимо было проверить их истинность для исследования теоремы Лагранжа о четырёх квадратах.

Для примера возьмём число 8. Известно, что оно обладает следующим набором простых множителей: 2, 2, 2. Теперь, пользуясь свойствами коммутативности, дистрибутивности и ассоциативности, можно показать следующее:

$$8 = 2 * 2 * 2 = 2 * 2 * (2 + 0 + 0 + 0) \quad (1)$$

$$8 = 2 * 2 * 2 = 2 * 2 * (1 + 1 + 0 + 0)$$

$$8 = 2 * 2 * 2 = (2 * 2 + 2 * 2 + 0 + 0) \quad (2)$$

(3)

Таким образом, разложение одной двойки привело к одному разложению Лагранжа. При этом неважно, брали бы мы третью двойку, вторую или первую – результат оставался бы тем же – единственный вариант представления. Как следствие, вывод: повторение простых множителей не будет значительно изменять количество доступных разложений.

Отсюда обратное: когда у числа есть несколько различных уникальных множителей (например, 30 = 2 * 3 * 5), каждый из этих множителей может быть представлен некоторым различным набором разбиений и, разбивая каждое число по отдельности, мы получим множество вариаций, некоторые из которых дадут искомые a, b, c, d для теоремы Лагранжа. Отсюда вывод: чем больше уникальных простых множителей есть у числа, тем больше разложений оно будет иметь.

При этом нельзя забывать о том, что в теории чисел и комбинаторике существует такое понятие, как разбиение числа. По своей сути это значение, которое как раз и показывает, сколькими способами путём сложения можно представить данное число (например, число 3 мы можем представить как 1+1+1, как 2+1 и как 3). Нахождение такого значения – это задача нетривиальная, однако для данного исследования имеет ценность тот факт, насколько быстро растёт количество разбиений с возрастанием числа. Например, для 10 их 42. Для 20 – 627. То есть, принимая во внимание два предыдущих вывода (которые, кстати, подтверждают связь с нашими открытиями в сфере проблемы Гольдбаха), можно сделать ещё один вывод: чем больше простой множитель, тем больше у данного числа будет разложений Лагранжа.

Подобным образом на первом этапе анализа был выведен ряд гипотез. Во-первых, наименьшим числом разложений будет обладать то N, которое содержит минимальное количество уникальных простых множителей, каждый из которых также минимален. Во-вторых, числа с большими простыми множителями (или большим количеством уникальных) будут давать больше разложений. В-третьих, простые числа с возрастанием будут давать всё больше, чем их соседи, разложений, поскольку имеют только один, но, на определённых промежутках, большой простой множитель – самого себя. Очень

наглядным примером для второй и третьей гипотез служит выдержка из собранных нами данных, представленная в таблице 1.

Таблица 1 – Выдержка из данных, подтверждающая гипотезы

Число N	Количество разложений Лагранжа	Факторизация числа N	Кол-во уникальных множителей	Общее кол-во множителей
30028	8112	2*2*7507	2	3
30029	16524	30029	1	1
30030	18720	2*3*5*7*11*13	6	6
30031	10632	59*509	2	2
30032	5316	2*2*2*2*1877	2	5

Отсюда как раз видно, что минимум получило число 30032 с большим числом двоек. На втором месте аналогичное по характеристикам число 30028, но оно обладает большим простым множителем (7507 > 1877). За счёт двух одновременно уникальных и достаточно больших простых множителей число 30031 стало на третье место по количеству разложений Лагранжа. Далее идёт 30029, обладающее огромным простым множителем. И, наконец, наивысшую позицию заняло 30030, поскольку оно имеет целых 6 уникальных простых множителей.

Следовательно, ниже всего на диаграмме разместятся числа, содержащие множество двоек (поскольку у них почти нет комбинаторных разложений). Чуть выше будут располагаться простые числа, причём их последовательность должна собираться в довольно плотную кривую. Ещё выше будут располагаться числа с двумя, тремя, четырьмя и т.д. крупными простыми множителями. Стоит отметить, что на данном этапе мы не ожидаем получить число 2*2*2*2*3 выше линии простых, поскольку, хотя у него два простых множителя, они на самом деле очень маленькие. Иными словами, до тех пор, пока у подобных ему чисел не будет крупного простого множителя, количество его разложений не поднимется выше линии простых.

После этого мы совершили ряд действий над исходным набором данных и, следуя гипотезам, разделили их на категории. Была построена диаграмма, представленная на рисунке 2.

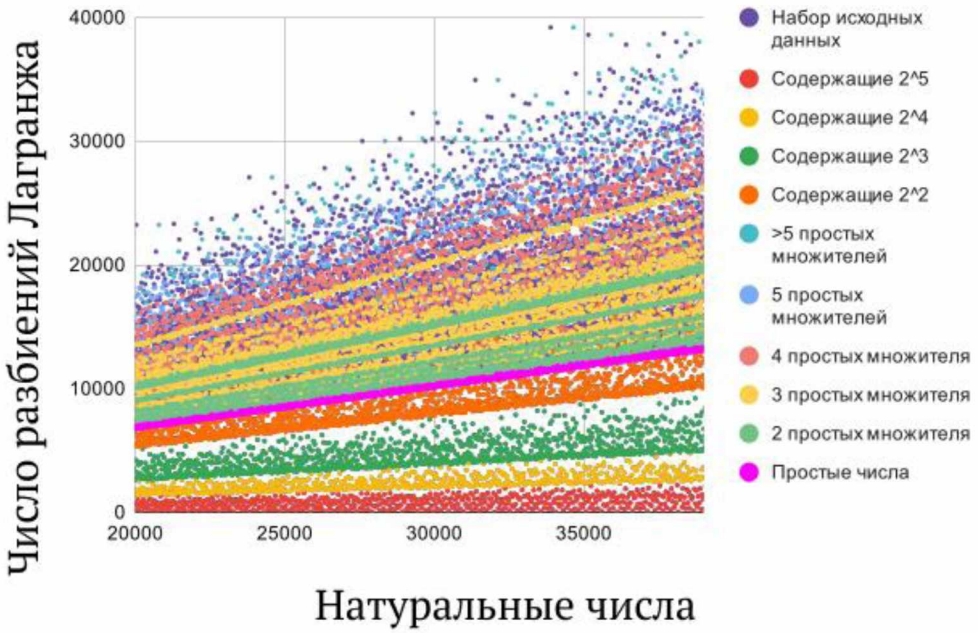

Рисунок 2 – Разбиение первичных данных на категории согласно выведенным гипотезам

График оказался довольно зашумлённым в верхней части, однако отчётливо видно, что у последовательностей выше линии простых есть множество маленьких лучей, порой довольно разрозненных. Однако несомненно, что каждая из описанных гипотез оправдалась. Для наглядности приведём диаграмму, представленную на рисунке 3.

Здесь все N из жёлтой последовательности содержат в своей факторизации такие простые множители, каждый из которых не превышает N/4. Следовательно, в красной последовательности у каждого N есть хотя бы один простой множитель, превышающий N/4. То есть, если у чисел N есть

простой множитель, своим размером входящий в отрезок [N/m; N/n], где n, m – целые положительные числа, такие что 0 <= n < m <= N, то можно утверждать о том, что все эти числа образуют луч.

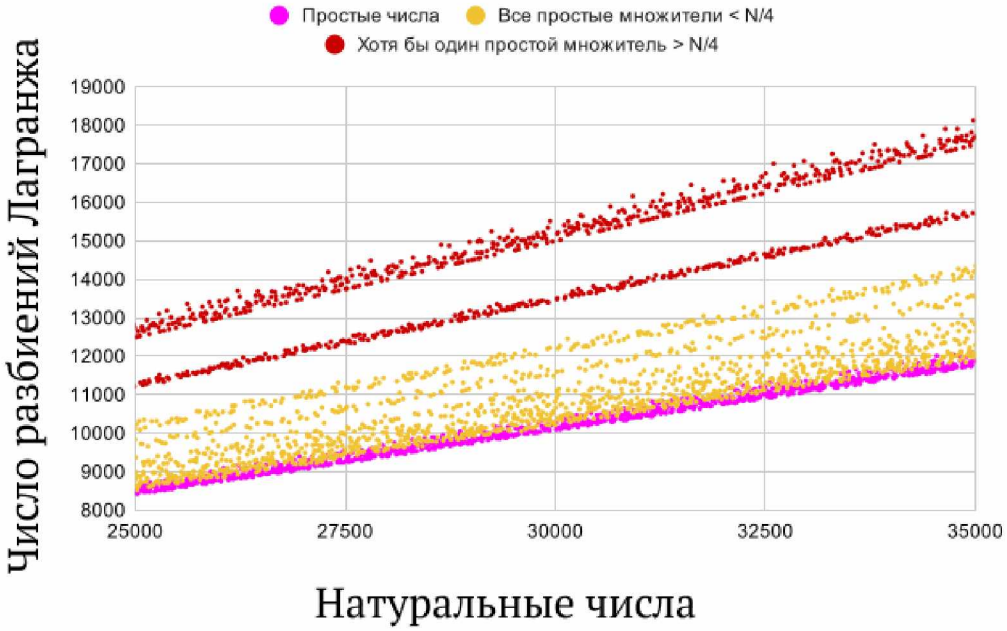

Рисунок 3 – Демонстрация природы возникновения лучей на диаграмме

Также на данном этапе следует напомнить, что в нашей работе мы учитывали, что перестановки одних и тех же a, b, c, d значения не имеют. Однако известна теорема Якоби о сумме квадратов четырёх чисел. От исследуемой нами теоремы она отличалась тем, что Якоби исследовал также вопрос количества разложений с учётом порядка чисел a, b, c, d.

Известно, что в результате своих исследований Якоби пришёл к следующуй формуле, которая позволяет вычислить количество неуникальных разложений Лагранжа для данного n:

$$r_4(n) = \begin{cases} 8\sum\limits_{m|n} m & \text{если n нечётное} \\ 24\sum\limits_{\substack{m|n \\ m \text{ нечёт}}} m & \text{если n чётное} \end{cases} \quad (4)$$

Несмотря на эту формулу, вопрос о том, как определить количество именно уникальных, остаётся открытым в пределах теории комбинаторики. Однако, хоть эта формула и не объясняет, почему именно таким образом происходит влияние делителей, но всё же подтверждает наши теории и закрепляет их право на существование. Во-первых, двойки не имеют практически никакого влияния на высоту точки на диаграмме потому, что для чётных N в формуле они опускаются, а для нечётных (это же правило относится к тройкам и к другим относительно малым простым множителям) – не дают достаточно большую сумму. Во-вторых, простые числа (и все числа, которые обладают большими простыми множителями) находятся так высоко на графике потому, что, как следует из формулы, они дают огромную сумму. Можно сказать, что замечанием о количестве комбинаторных разложений числа мы сумели объяснить такое влияние больших простых множителей на высоту точки на диаграмме.

Нами была проделана огромная работа, в некоторой степени дополняющая предыдущее исследование на тему проблемы Гольдбаха, а также под новым углом раскрывающая вопрос уже, казалось бы, известной и исследованной теоремы Лагранжа о сумме четырёх квадратов. Связь между этими математическими задачами с помощью теоремы Эйлера-Ферма открывает новые пути к оптимальным вычислениям разложений Лагранжа.

Говоря о практических применениях данного исследования, нельзя не упомянуть криптографию. Поскольку формулы для количества уникальных разложений пока не существует, его нахождение – это вычислительно сложная задача, которая, несомненно, может использоваться рядом криптографических алгоритмов.

Список использованных источников:

1. Ireland K., A classical introduction to modern number theory. / Ireland K., Rosen M. I. // Springer Science & Business Media – 1990. – T. 84.

2. Rabin M. O., Randomized algorithms in number theory / Rabin M. O., Shallit J. O. // Communications on Pure and Applied Mathematics. – 1986. – T. 39. – №. S1. – C. S239-S256.

3. Pollack P., Finding the Four Squares in Lagrange's Theorem / Pollack P., Treviño E. // Integers. – 2018. – Т. 18. – №. A15. – С. 7-17.

4. Трубач, К.И. Бинарная проблема Гольдбаха / Трубач К.И., Крутько А.А. // Материалы 59-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению компьютерные системы и сети. – 2023. – 545-5 с.

UDC

LAGRANGE'S FOUR-SQUARE THEOREM

Trubach K.I., Krutsko A.A

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Barkova E.A. – PhD in Physics and Mathematics, Associate Professor

Annotation. This article explores the relationship between Lagrange's theorem on the decomposition of natural numbers into the sum of four squares and the binary Goldbach conjecture. The results indicate that the quantity and size of divisors significantly influence the number of non-unique Lagrange decompositions. Discoveries are supported by Jacobi's formula for the sum of squares of four numbers. The work has prospects in combinatorics, cryptography, and is of interest from an artistic perspective.

Keywords. Lagrange decomposition, Fermat's theorem, Goldbach's conjecture, cryptography, combinatorics, algorithms, mathematical properties, prime factors, number theory, data analysis, interconnection of mathematical concepts.