Доказательство бинарной проблемы Гольдбаха для чисел высокого порядка

Бредихин Арсентий Игоревич – магистрант Югорского государственного университета.

Аннотация: В данной статье описывается доказательство бинарной проблемы Гольдбаха для двух произвольных промежутков натуральных четных чисел высокого порядка ($\sim 10^{18}$) методом полного перебора. Здесь обосновывается выбор данных промежутков, описывается алгоритм определения простоты числа и его последующая модификация с целью повышения его быстродействия. Также представлены результаты перебора чисел из данных 2 промежутков данным алгоритмом и полученные практические результаты.

Ключевые слова: Теория чисел, простые числа, четные числа, бинарная проблема Гольдбаха, алгоритмы, перебор, программа.

Введение

В 1742 г. Гольдбах в письме к Эйлеру поставил проблему доказать, что *каждое нечетное число может быть представлено в виде суммы трех простых чисел (начиная с 7)*. Эйлер в ответном письме высказал гипотезу, что имеет место гораздо более сильное утверждение, которое гласит, что *каждое четное число, начиная с 4, может быть представлено в виде суммы двух простых чисел*. Эти проблемы получили название проблемы Гольдбаха-Эйлера [1, с. 360]. Последняя из этих проблем носит название бинарной гипотезы Гольдбаха.

Бинарная проблема Гольдбаха относится к проблемам аддитивной теории простых чисел, т.е. теории простых чисел, рассматривающей их в качестве слагаемых [1, с. 360]. За 276 лет ее существования данная проблема так и не была решена для всех четных чисел. Однако до сих пор предпринимаются попытки ее доказательства, но не для всех четных чисел, а для некоторых конечных промежутков четных чисел. Краткая история доказательств бинарной проблемы Гольдбаха представлена в таблице 1.

Таблица 1. История доказательств бинарной проблемы Гольдбаха [2].

Верхняя граница	**Авторы доказательства**
10^4 (10 тыс.)	Desboves 1885
10^5 (100 тыс.)	Pipping 1938
10^8 (100 млн.)	Stein and Stein 1965ab
$2*10^{10}$ (20 млрд.)	

Granville et al. 1989

$4*10^{11}$ (400 млрд.)

Sinisalo 1993

10^{14} (100 трлн.)

Deshouillers et al. 1998

$4*10^{14}$ (400 трлн.)

Richstein 1999, 2001

$2*10^{16}$ (20 квадрлн.)

Oliveira e Silva (Mar. 24, 2003)

$6*10^{16}$ (60 квадрлн.)

Oliveira e Silva (Oct. 3, 2003)

$2*10^{17}$ (200 квадрлн.)

Oliveira e Silva (Feb. 5, 2005)

$3*10^{17}$ (300 квадрлн.)

Oliveira e Silva (Dec. 30, 2005)

$1,2*10^{18}$ (1,2 квинтлн.)

Oliveira e Silva (Jul. 14, 2008)

$4*10^{18}$ (4 квинтлн.)

Oliveira e Silva (Apr. 2012)

Как видно из таблицы 1, верхняя граница на́чала резко возрастать, начиная с 60-х годов XX века. Основным толчком к этому послужило, как нетрудно догадаться, появление и развитие вычислительной техники.

Также можно увидеть, что по состоянию на апрель 2012 года верхняя граница равна 4 квинтиллионам. Данный факт оказал решающее значение на выбор промежутков четных чисел в данном исследовании.

Выбор промежутков и метода доказательства

Чтобы определить, соответствует ли некоторое четное число бинарной проблеме Гольдбаха, необходимо проверить все (в худшем случае) неповторяющиеся комбинации слагаемых, которые в сумме дают это число, на простоту. Если для данного четного числа найдется хотя бы одна из комбинаций слагаемых, то оно соответствует бинарной проблеме Гольдбаха.

Следовательно, для определения соответствия четного числа бинарной проблеме Гольдбаха необходимо использовать алгоритм определения простоты числа.

В данной работе **были** произвольно **выбраны следующие 2 промежутка для доказательства:** [8,736 * 10[illegible]; 8,736 * 10[illegible] + 5 * 10[illegible]] (250001 четное число) и [5 * 10[illegible]; 5 * 10[illegible] + 10[illegible]] (250001 четное число)!

Алгоритм определения простоты числа

В ходе выполнения доказательства был разработан собственный алгоритм определения простоты числа, действие которого основывается на следующей теореме:

Теорема. Натуральное число *m* является простым, если для него не существует целых множителей в промежутке $[2; \sqrt{m}]$.

Доказательство. При доказательстве данной теоремы будем оперировать понятием «**с**

реднее геометрическое
», которое определяется как корень степени
n
из произведения
n
чисел. В данном случае мы рассмотрим натуральное число
m
такое, что
.

Согласно свойству **корня *n*-й степени** для чисел, больших или равных 1, значение корня для таких чисел будет убывать с увеличением степени корня
n
.

Любое число можно представить в виде произведения не менее 2 множителей. Обобщая вышесказанное, получаем, что для числа *m* такого, что $m \geq 1$
, наибольшее значение будет принимать среднее геометрическое 2 чисел, поскольку оно определяется как корень степени 2 числа *m*.

Согласно свойству **среднего геометрического нескольких чисел**, оно всегда больше или равно минимальному числу и всегда меньше или равно максимальному числу. В таком случае как минимум один из множителей числа
m
меньше или равен среднему геометрическому числа
m
. Поэтому
для определения простоты числа
m
достаточно рассмотреть его делимость на натуральные числа со значением не больше
, начиная с 2 (промежуток $[2; \sqrt{m}]$
). Число 1 в промежуток не включаем, поскольку оно по определению не является простым (любое простое число имеет значение не менее 2).

Простое число m, согласно определению, делится только на 1 и само на себя (т.е. m). Эти числа в промежуток $[2; \sqrt{m}]$
 не входят. Следовательно, **теорема доказана**.

Таким образом, реализованный алгоритм определения простоты числа *m* сводится к простому перебору всех целых чисел из промежутка $[\ldots]$ и проверке делимости числа *m* на эти числа. Если на этом промежутке находится хотя бы один делитель числа *m*, то алгоритм завершает свою работу на первом же делителе и число *m* является составным; если же таких делителей нет, то число *m* – простое.

Но данный алгоритм имеет недостаток – невысокая скорость работы для больших чисел (начиная с чисел порядка 10^{12}). А в рамках доказательства необходимо рассмотреть числа порядка 10^{18}.

Лемма. Если число $a \in N$ нацело делится на $m^n : m \in N, n \in N$ и число *m* простое, то число *a* нацело делится на *m*.

Доказательство. Рассмотрим число $a : a \in N, a = q*m^n$; $a \in N$ и $q \in N$. Поскольку число *a* нацело делится на m^n, то $q \in N$; Разделим число *a* на *m*:

$$\frac{a}{m} = \frac{q*m^n}{m} = q*m^{n-1}$$

. (1)

Поскольку $q \in N, m \in N, n \in N$, $(n-1) \in N$; Следовательно $q*m^{n-1} \in N$, **что и требовалось доказать**.

Смысл данной леммы заключается в следующем: если целое число нацело делится на целую положительную степень простого числа, то оно нацело делится и на это простое число. Применяя данный смысл леммы к доказанной ранее теореме о простоте числа *m*, получим, что и перебор всех целых чисел, и перебор только простых чисел из промежутка будут показывать правильные результаты проверки числа *m* на простоту для всех чисел. Но при этом **во втором случае придется перебрать меньшее количество чисел, что сократит время работы алгоритма тем сильнее, чем больше число *m***.

На практике **для обеспечения достаточно высокой скорости выполнения алгоритма определения простоты числа** (путем проверки его делимости только на простые числа) **необходимо использовать массив заранее вычисленных простых чисел**. Причиной является тот факт, что постоянное вычисление простых чисел, используемых в качестве делителей бо́льших простых чисел, значительно снижает скорость выполнения алгоритма, что сводит на нет его достоинства.

Реализация программы доказательства бинарной гипотезы Гольдбаха

С помощью алгоритма определения простоты числа *m*, принцип которого заключается в переборе всех целых чисел из промежутка и проверке делимости числа *m* на эти числа, был составлен **словарь простых чисел** от 2 до $2{,}5 \cdot 10^5$ (250 тыс.), который позволяет проверять на простоту числа до $(2{,}5 \cdot 10^5)^2 = 6{,}25 \cdot 10^{10}$ (62,5 млрд.).

Но данный словарь простых чисел не устраивает автора статьи – ведь требуется проверить числа до $8{,}736 \cdot 10^{18}$ – $8{,}737 \cdot 10^{18}$. Поэтому с помощью первого словаря простых чисел был составлен **второй словарь простых чисел** от 2 до $3 \cdot 10^9$ (3 млрд.). Он позволяет проверять на простоту числа до $(3 \cdot 10^9)^2 = 9 \cdot 10^{18}$ (9 квинтлн.). Поскольку $9 \cdot 10^{18} > 8{,}737 \cdot 10^{18}$, то данного словаря простых чисел вполне хватает для проверки чисел такого порядка на простоту. Процесс составления словаря простых чисел занял около 6 дней на обычном ПК (персональном компьютере).

Чтобы обеспечить возможность использования словаря простых чисел для определения простоты числа в ходе действия алгоритма, ранее созданный **алгоритм определения простоты числа** ***m*** **был модернизирован**: вместо перебора всех целых чисел из промежутка используется перебор элементов одномерного массива простых чисел из этого же промежутка. Причем элементы массива простых чисел должны быть упорядочены по возрастанию.

Модернизированный алгоритм определения простоты числа требует значительно меньше времени для проверки числа на простоту, чем первоначальный алгоритм определения простоты числа, т.к. в первом случае приходится перебирать только простые числа. **Но он имеет один недостаток – для его работы при проверке достаточно больших чисел необходимо значительное**

количество оперативной памяти ЭВМ , в которой необходимо хранить словарь простых чисел во время его работы. Это действует для чисел порядка и выше.

Затем **модернизированный алгоритм определения простоты числа** и использующая этот алгоритм **программа доказательства бинарной гипотезы Гольдбаха** была реализована на языке программирования Python 3.5, в среде программирования Spyder.

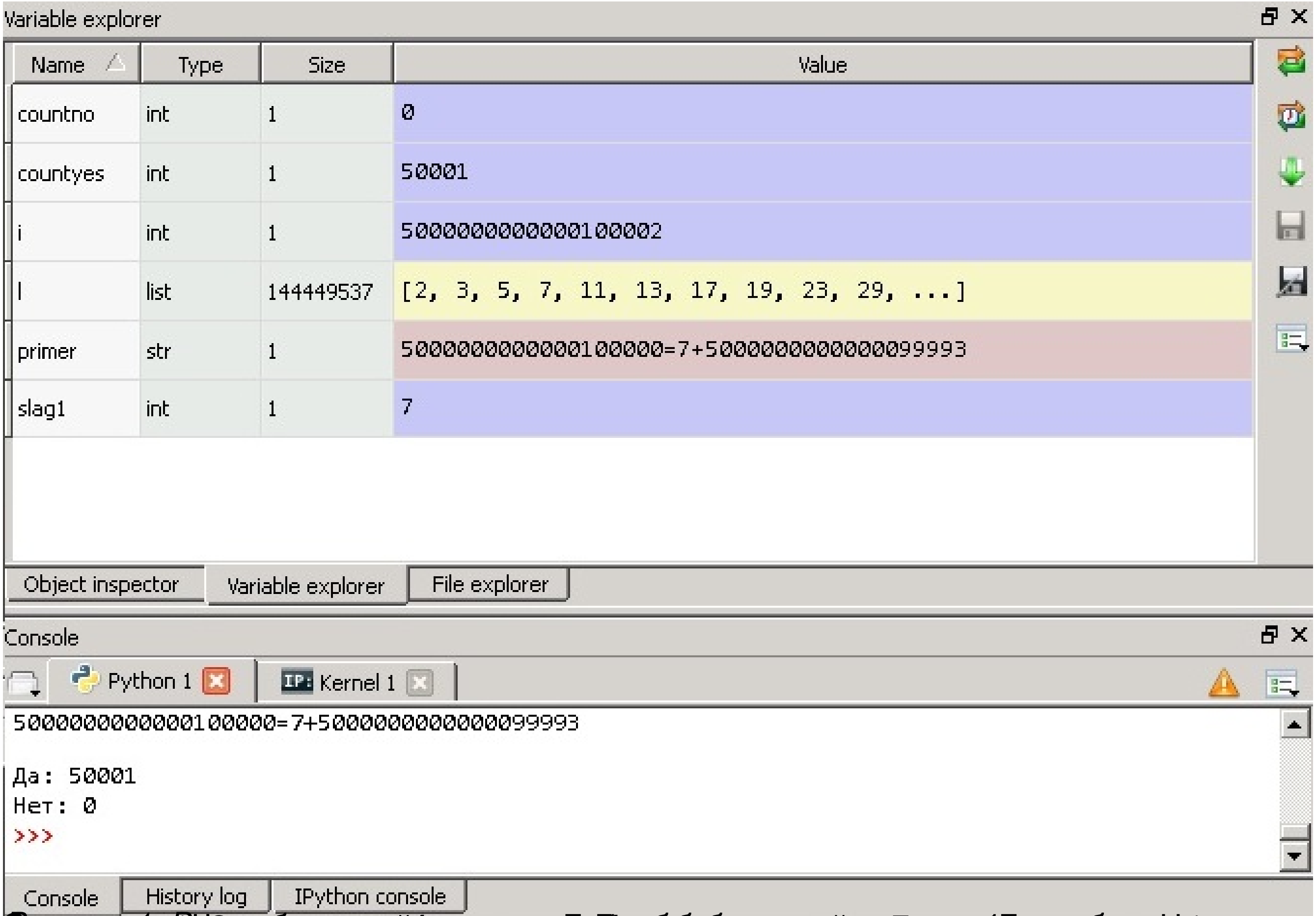
После реализации **программа доказательства бинарной гипотезы Гольдбаха была усовершенствована** – была добавлена возможность сохранения в памяти и дальнейшего использования в программе простых чисел высокого порядка. Эти числа являются одним из слагаемых суммы двух простых чисел, которые в сумме дают четное число, проверяемое на его соответствие бинарной гипотезе Гольдбаха.

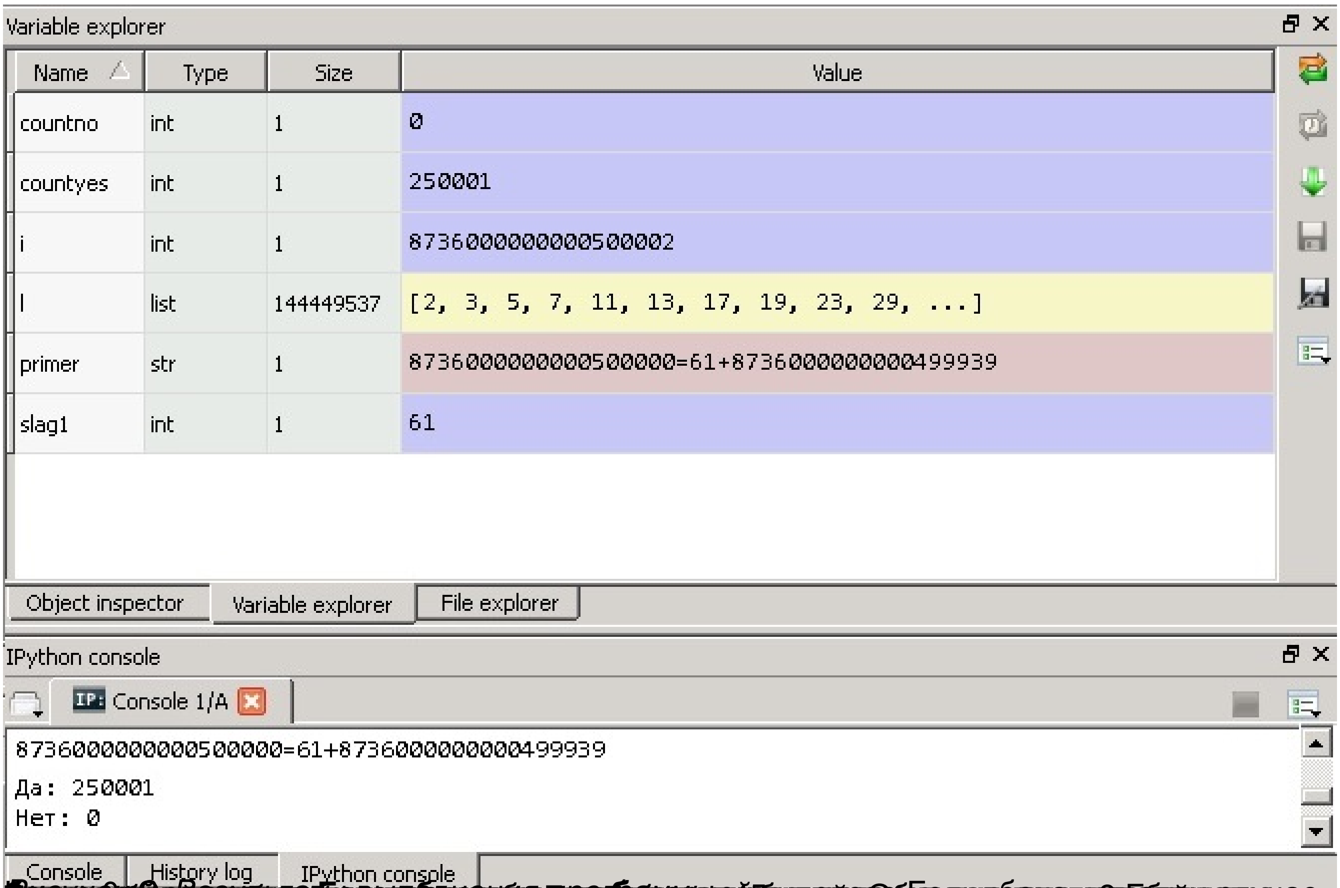
Данное усовершенствование позволило ускорить процесс доказательства бинарной гипотезы Гольдбаха, поскольку все простые числа высокого порядка проверяются на простоту только один раз и после этого помещаются в **словарь проверенных простых чисел**. Впоследствии слагаемое суммы (высокого порядка) двух простых чисел проверяется на простоту алгоритмом определения простоты числа тогда и только тогда, когда его нет в словаре проверенных простых чисел.

Результаты перебора чисел

Реализованная ранее **программа доказательства бинарной гипотезы Гольдбаха** была выполнена на высокопроизводительном сервере. Рассмотрим ее результаты.

Результаты выполнения программы для четных чисел из промежутка [5*10[illegible];5*10[illegible] +10[illegible]]
:


Variable explorer
Name
Type
Size
Value
countno int 1 0
countyes int 1 50001
i int 1 5000000000000100002
l list 144449537 [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...]
primer str 1 5000000000000100000=7+5000000000000099993
slag1 int 1 7
Object inspector
Variable explorer
File explorer
Console
Python 1
Kernel 1
5000000000000100000=7+5000000000000099993
Да: 50001
Нет: 0
>>>
Console
History log
IPython console


Variable explorer
Name
Type
Size
Value
countno int 1 0
countyes int 1 250001
i int 1 8736000000000500002
l list 144449537 [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...]
primer str 1 8736000000000500000=61+8736000000000499939
slag1 int 1 61
Object inspector
Variable explorer
File explorer
IPython console
Console 1/A
8736000000000500000=61+8736000000000499939
Да: 250001
Нет: 0
Console
History log
IPython console