Конкурс научных проектов школьников

в рамках краевой научно-практической конференции «Эврика»

Малой академии наук Кубани

**ИССЛЕДОВАНИЕ СВОЙСТВ ПРОСТЫХ ЧИСЕЛ.**

**НЕРЕШЁННЫЕ ГИПОТЕЗЫ. ИНТЕРЕСНЫЕ ЗАДАЧИ**

секция «Математика»

Авторы:

**Усольцев Олег Андреевич**

**Кавицян Лаврентий Михайлович**

10 -А класс МОУ СОШ №35

п. Новомихайловский

Туапсинского района

Научный руководитель:

**Колмакова Валентина Ивановна**

учитель математики

МОУ СОШ №35

п. Новомихайловский

п. Новомихайловский, 2011 год.

**Оглавление**

1. Аннотация стр. 3
2. Введение стр. 4
3. Выведение простых чисел стр. 4
4. Распределение простых чисел стр. 7
5. Числа Мерсена стр. 8
6. Гипотеза Римана стр. 8
7. Обобщенная гипотеза Римана стр. 9
8. Скатерть Улама стр. 9
9. Гипотеза Гольдбаха стр. 9
10. Известные выводы и теоремы из теории простых чисел стр. 11
11. Некоторые загадки и задачи простых чисел стр. 12
12. Заключение стр. 14
13. Использованная литература стр. 15
14. Приложения стр. 16

**Аннотация**

Работа содержит краткий обзор статей о простых числах, их распределение в числовом ряду, расширенную таблицу простых чисел, получающихся просеиванием (до 100);расширенную таблицу получения простых чисел по способу Мирослава Соукупа (до600); приведены примеры простых чисел, полученных нами самостоятельно; доказательства теорем, решённые составленные нами и задачи на простые числа, составленную нами гипотезу.

Целью работы является более глубокое изучение закономерностей, связанных с простыми числами, и в дальнейшем мы хотим попробовать составить программу расчёта простых чисел, а может, и найти формулу простого числа, которая не изобретена до сих пор, более глубоко изучить вопрос распределения простых чисел, чтобы принять участие в международном конкурсе научно-технических работ школьников «Старт в науку».

**Введение**

Как много сложного скрыто среди простого, как много несовершенного среди самого продвинутого и как много открыто нового, не зная изначального…

Мы можем производить операции с гигантскими цифрами, но можем ли мы сказать то же и о простых? Мы пользуемся сетью интернет, загружая туда все больше и больше конфиденциальной информации о себе, но так ли он безопасен, как кажется?

Безусловно, речь идет о простых числах. Они, известные еще с древности, несут с собой множество загадок, не решенных человечеством, в том числе гипотеза Римана, не доказанная и не опровергнутая в течении тысячелетий (ей посвящена большая часть нашей работы), гипотеза Гольдбаха, проблема вычисления и определения простого числа, нахождение простых чисел среди больших и так далее…

Безопасность интернет обеспечивается кодами на основе простых чисел, но за основу взято предположение, что эти числа не являются последовательностью, а из этого следует, что при доказательстве гипотезы Римана появляется гипотетическая перспектива на взлом интернет в целом. Над проблемой простых чисел работали многие умы человечества, но решить ее не удалось.

Но что же такое - простое число? Это натуральное число, имеющее ровно два различных натуральных делителя: единицу и самого себя. Но, не смотря на простоту, они хранят загадок не меньше, чем квантовая физика и генная инженерия!

**Выведение простых чисел.**

Наиболее простым и знаменитым методом нахождения простых чисел является Решето Эратосфена.Принцип действия:

В созданном числовом массиве (например от 2 до 100), берем первый элемент – 2, затем исключаем все числа делящиеся на него, далее следующее число – 3, исключаем все числа делящиеся на 3, и так далее, за исключением вычеркнутых чисел, все оставшиеся и есть простые (смотрите приложение 1).

Так же известно Решето Аткина. Принцип действия:

1. Все числа, равные (по модулю 60[[1]](#footnote-2)) 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, или 58, делятся на два и заведомо не простые. Все числа, равные (по модулю 60) 3, 9, 15, 21, 27, 33, 39, 45, 51, или 57, делятся на три и тоже не являются простыми. Все числа, равные (по модулю 60) 5, 25, 35, или 55, делятся на пять и также не простые. Все эти остатки (по модулю 60) игнорируются.

2) Все числа, равные (по модулю 60) 1, 13, 17, 29, 37, 41, 49 или 53, имеют остаток от деления на 4 равный 1. Эти числа являются простыми тогда и только тогда, когда количество решений уравнения 4x² + y² = n нечётно и само число не кратно никакому квадрату простого числа.

3) Числа, равные (по модулю 60) 7, 19, 31, или 43, имеют остаток от деления на 6 равный 1. Эти числа являются простыми тогда и только тогда, когда количество решений уравнения 3x² + y² = n нечётно и само число не кратно никакому квадрату простого.

4) Числа, равные (по модулю 60) 11, 23, 47, или 59, имеют остаток от деления на 12 равный 11. Эти числа являются простыми тогда и только тогда, когда количество решений уравнения 3x² − y² = n нечётно и само число не кратно никакому квадрату простого.

Ни одно из рассматриваемых чисел не делится на 2, 3, или 5, соответственно, они не могут делиться и на их квадраты. Поэтому проверка, что число не кратно квадрату простого числа, не включает 2², 3², и 5².

Нам пришла мысль, что проблема в решении гипотезы Римана и гипотезы Гольдбаха (смотри далее) могла возникнуть из-за неправильного взгляда на числа и мы составили таблицу для составных чисел 1-100 (смотри приложение 3).

Однако, в 1954 год Инженер-связист Мирослав Соукуп (Прага) придумал новый способ получения простых чисел и составил таблицу по следующему принципу.

Известно, например, что если нечётное число N при делении на 6 даёт в остатке 2, 3 или 4,то оно составное. Значит простые числа (кроме 2 и 3) надо искать среди тех, которые имеют вид 6n±1, где n – любое число.

**Докажем эту теорему.**

Пусть р – простое число>3, которое при делении на 6 даёт в частном q, а в остатке r, r<6. Тогда р=6q+r

Число р будет простым только в том случае, если r=1 или r=5. Так как если r=2,3,4, то:

р=6q+2=2(3q+1) – составное

р=6q+3=3(2q+1) – составное

р=6q+4=2(3q+2) – составное(смотрите приложение 2).

Средняя часть этой таблицы роли не играет: она лишь делит таблицу на две части: верхнюю и нижнюю части. Число 6n – 1 простое, если в нижней части таблицы нет числа n. Например: n=7.Тогда 6·7 – 1=41-простое. Число 6n+1 простое, если в верхней части таблицы нет числа n. Например: n=21. Тогда 6·21+1=127-простое.

А вот ещё один способ получения простых чисел.

Возьмём 1 и любое количество n первых простых чисел. Все эти числа произвольным образом распределим на 2 группы. Перемножим числа каждой группы; образуется два произведения. Если сумма или разность этих произведений даст число N, меньшее чем квадрат (n+1)-ого простого числа, то N – простое число.

Возьмём, например, 1 и четыре первых простых числа, то есть 1,2,3,5,7. Пятое простое число 11. Заметим, что 112=121. Значит, указанным способом мы можем образовать простые числа, меньшие 121.

Распределим числа на две группы: *2,3,5,7* и *1*. Образуем число: *2·3·5·7-1=209* .Так как *209>121*, то поручиться за то, что оно простое, мы не можем. Действительно, в таблице простых чисел его нет

Распределим взятые числа по-другому:*1,3,5,7* и *2.* Образуем два числа: *N1=1·3·5·7-2=103 N2=1·3·5·7+2=107.*

Каждое из них меньше 121, следовательно, они простые.

Если к первой группе отнесём числа *1,5,7,* а ко второй *2* и *3*, то сможем образовать ещё два простых числа:

*1·5·7-2·3=29* и *1·5·7+2·3=41*

Ещё несколько возможных комбинаций:

*1·3·7-5·2=11 1·3·7+5·2=31*

*1·2·3·5-7=23 1·2·3·5+7=3·7*

Очевидно также, что можно повысить степень любого сомножителя первой или второй группы и сумма или разность будет по-прежнему давать простое число, если только оно не превышает квадрат(n+1)-ого простого числа.

*1·3·5·7-23=89; 1·3·5·7+23=113*

*1·5·7-2·32=17; 1·5·7·+2·32=53*

*1·3·52-22·7=47; 1·3·52+22·7=103.*

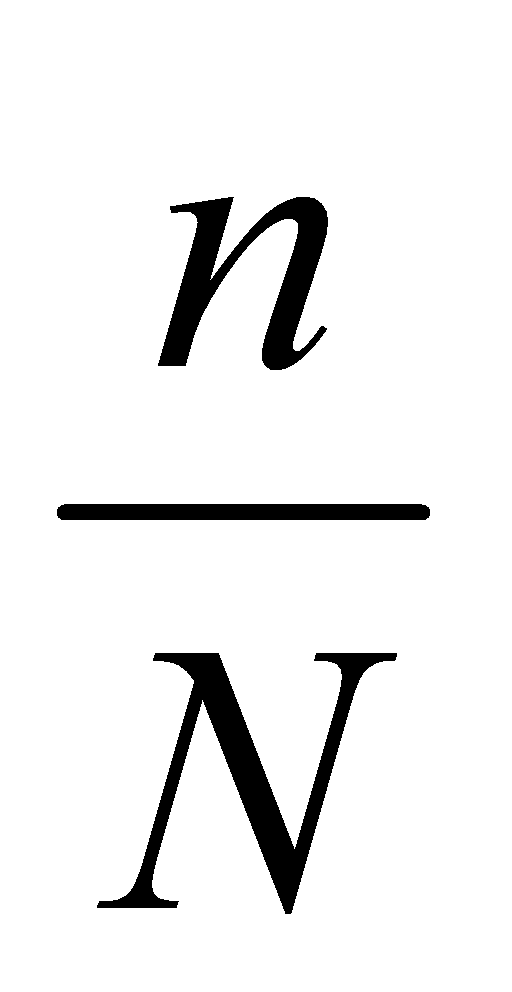
Бесконечность множества простых чисел

Простых чисел бесконечно много. Самое старое известное доказательство этого факта было дано Евклидом в «Началах» (книга IX, утверждение 20). Его доказательство может быть кратко воспроизведено так:

Представим, что количество простых чисел конечно. Перемножим их и прибавим единицу. Полученное число не делится ни на одно из конечного набора простых чисел, потому что остаток от деления на любое из них даёт единицу. Значит, число должно делиться на некоторое простое число, не включённое в этот набор.

**Распределение простых чисел**

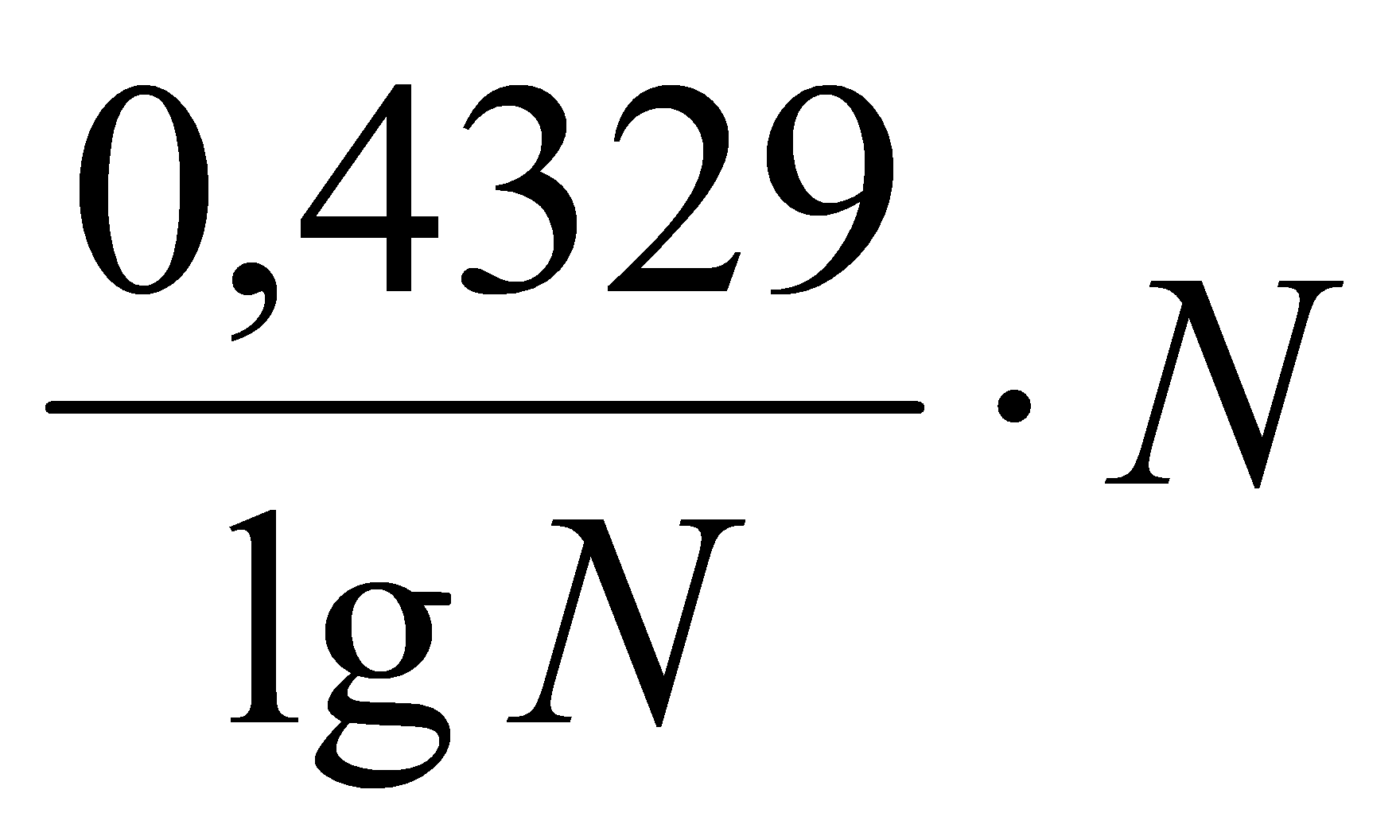
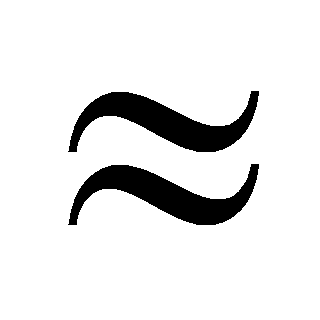
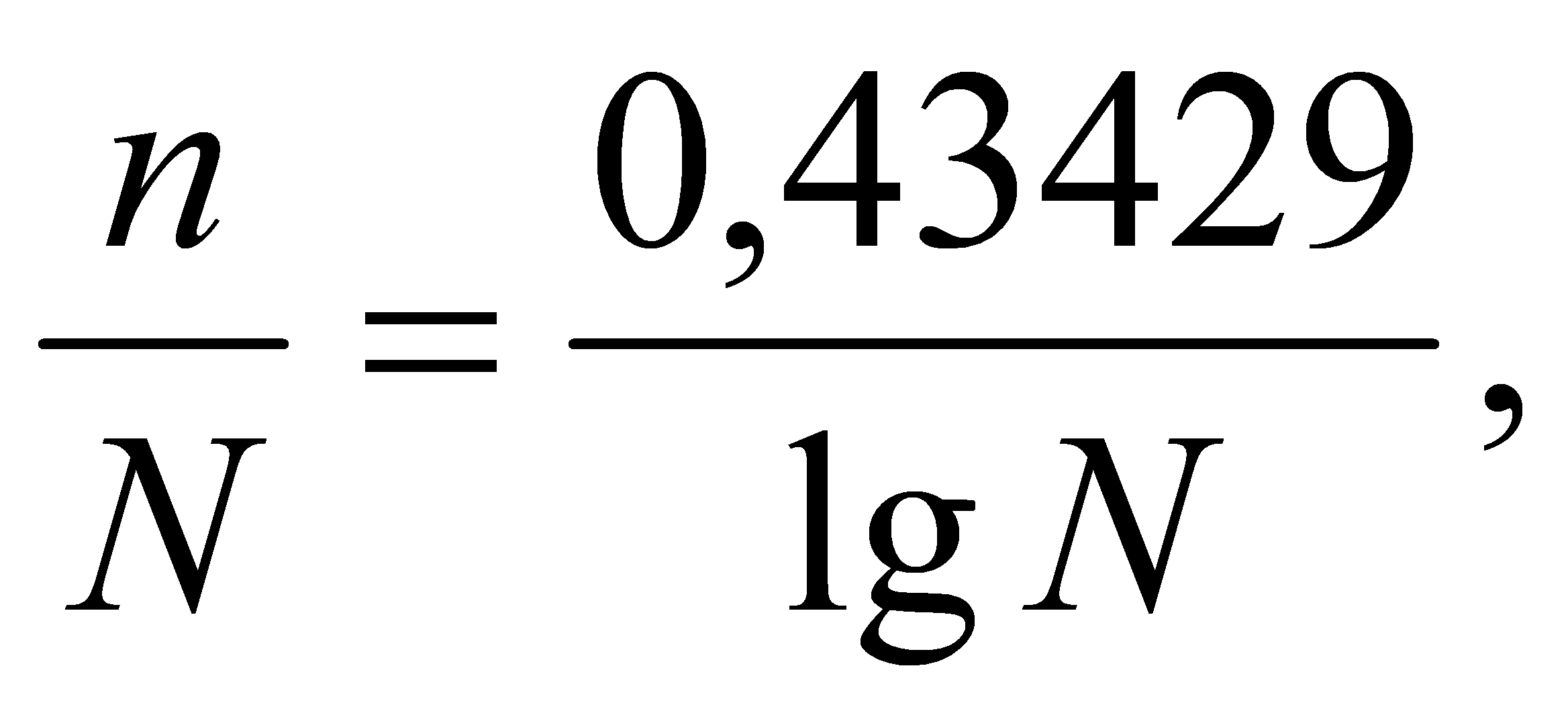
Изучая таблицу простых чисел, можно подметить, что простые числа не одинаково густо распределены в натуральном ряду чисел: в первом десятке их четыре, от 20 до 30 –два, от 850 до 860 – три, от 3990 до 4000 – нет ни одного, от 4000 – 4010 – три. Таким образом, распределение простых чисел среди натурального ряда отличается чрезвычайной неправильностью. Но эта неправильность исчезает, если судить по густоте распределения, где n – число простых чисел натурального ряда



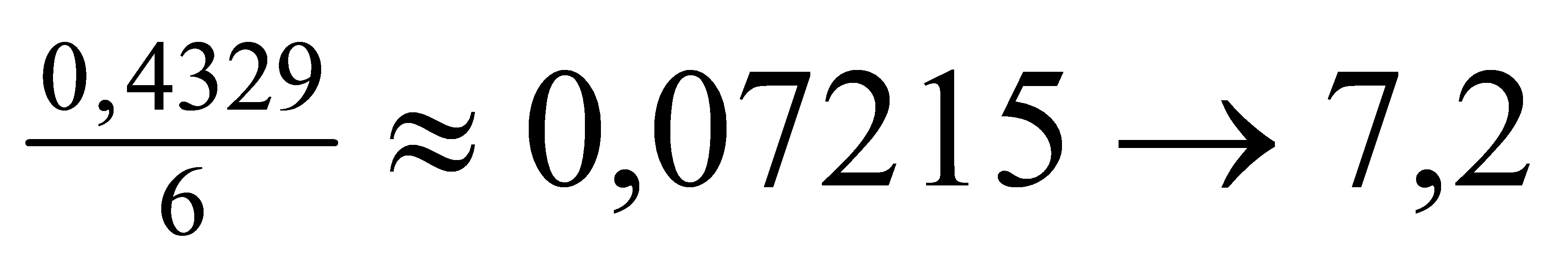
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N | 10 | 102 | 103 | 104 | 105 | 106 |
| n | 4 | 25 | 168 | 1229 | 9592 | 78498 |
|  | 0,4 | 0,25 | 0,168 | 0,1229 | 0,095 | 0,078 |
| % | 40 | 25 | 16,8 | 12,3 | 9,5 | 7,8 |

Эта таблица показывает, что плотность распределения простых чисел постепенно уменьшается, если рассматривать возрастающие числовые промежутки натурального ряда. Начались попытки создания такой формулы, которая позволяла бы рассчитать n по данному N. Эти попытки не увенчались успехом – точной формулы создать не удалось. Созданием приближённой формулы с минимальной ошибкой занимались такие крупнейшие математики как Лежандр(1752–1833), Эйлер(1707–1783), Гаусс(1777–1855), Дирихле(1805 –1859), Бертран(1822–1900), Чебышев(1821–1894).

Закон распределения простых чисел, открытый Чебышевым, выражается формулойточность которой возрастает с возрастанием N. В связи с решением этой задачи Чебышев доказал гипотезу, выдвинутую Бертраном: «Между любым натуральным числом и его удвоением всегда находится хотя бы одно простое число». Эту гипотезу я проверил для небольших чисел. Возьмём N=106 и найдём n. n.



n=%



Давным-давно было замечено, что простые числа иногда отстают друг от друга на *2*: таковы числа *3* и*5;22271* и *22273*; *17* и *19*.Эти числа называются близнецами. Иногда они образуют целые скопления. Например: *101, 103, 107, 109, 113*. Из этого наблюдения возникла гипотеза, что скоплений простых чисел бесконечное множество, но её не доказали по сей день.

Наблюдения над простыми числами показывают, что между квадратами простых чисел всегда имеются близнецы.

*4<5<7<9; 25<29<31<36*

*9<11<13<25; 36<41<43<49*

И так далее. Это порождает гипотезу, что между квадратами двух простых чисел всегда найдутся близнецы. Она, разумеется не доказана, ибо из неё следовало бы, что простых чисел-близнецов бесконечное множество.

**Числа Мерсена**

Простые числа вида 2p-1 (p-простое) называют числами Мерсенна (по имени французского монаха и математика Марена Мерсенна (1588-1648)). Наибольшие из известных пока простых чисел являются числами Мерсенна. Многие выдающиеся математики занимались в свое время поиском и доказательством простоты чисел Мерсенна, так Эйлер доказал, что число 231-1 - простое. В 1952 году самое большое простое число содержало 157 цифр, в 1985 году - 65050. Таких чисел найдено всего 40 (ноябрь 2004г.). Используя метод распределенных вычислений в августе 2002г. было вычислено 39 простое число Мерсенна: 213466917-1, имеющее в десятичной записи 4053946 цифр. В декабре 2004г. этот результат был улучшен и следующее, 40-ое число Мерсенна 220996011 - 1 , имело уже 6320430 цифр.На данный момент самым больши́м известным простым числом является число Мерсенна[*M*43112609 = 243112609 − 1](http://ru.wikipedia.org/wiki/43112609), найденное в августе [2008 года](http://ru.wikipedia.org/wiki/2008_%D0%B3%D0%BE%D0%B4) в рамках проекта [распределённых вычислений](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F)[GIMPS](http://ru.wikipedia.org/wiki/GIMPS). Длина *M*43112609 составляет 12978189 десятичных цифр. Интерес к таким числам вызван, во-первых, возможностью привлечения разработанного аналитического аппарата теории чисел и, во-вторых, прогрессом в вычислительной технике. Если мы зададимся вопросом, какое же наибольшее простое число известно человечеству - то ответом будет какое-то простое число Мерсенна

**Гипотеза Римана**

Сама гипотеза о распределении нулей [дзета-функции Римана](http://ru.wikipedia.org/wiki/%D0%94%D0%B7%D0%B5%D1%82%D0%B0-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%A0%D0%B8%D0%BC%D0%B0%D0%BD%D0%B0) была сформулирована [БернхардомHYPERLINK "http://ru.wikipedia.org/wiki/%D0%A0%D0%B8%D0%BC%D0%B0%D0%BD,\_%D0%91%D0%B5%D1%80%D0%BD%D1%85%D0%B0%D1%80%D0%B4" Риманом](http://ru.wikipedia.org/wiki/%D0%A0%D0%B8%D0%BC%D0%B0%D0%BD,_%D0%91%D0%B5%D1%80%D0%BD%D1%85%D0%B0%D1%80%D0%B4) в [1859 году](http://ru.wikipedia.org/wiki/1859_%D0%B3%D0%BE%D0%B4).

Функция ζ(s) определена для всех комплексных*, и имеет нули в отрицательных чётных . Из функционального* уравнения , и явного выражения при следует, что все остальные нули, называемые «нетривиальными», расположены в полосе симметрично относительно так называемой «критической линии» . Гипотеза Римана утверждает, что:

Все нетривиальные нули дзета-функции имеют действительную часть, равную .

**Обобщённая гипотеза Римана**

Она состоит из того же самого утверждения для обобщений дзета-функций, называемых L- функциями Дирихле.

Большинство математиков уверено, что гипотеза верна. Многие утверждения о распределении простых чисел, в том числе о сложности некоторых целочисленных [алгоритмов](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC), доказаны в предположении верности гипотезы Римана. В то время как не существует простой закономерности, описывающей распределение [простых чисел](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) среди натуральных, [Риман](http://ru.wikipedia.org/wiki/%D0%A0%D0%B8%D0%BC%D0%B0%D0%BD,_%D0%91%D0%B5%D1%80%D0%BD%D1%85%D0%B0%D1%80%D0%B4) обнаружил, что число π(*x*) простых чисел, не превосходящих *x*, выражается через распределение нетривиальных нулей дзета-функции.

Стоит отметить, что гипотеза Римана входит в список семи «[проблем тысячелетия](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D1%8B_%D1%82%D1%8B%D1%81%D1%8F%D1%87%D0%B5%D0%BB%D0%B5%D1%82%D0%B8%D1%8F)», за решение каждой из которых [Математический институт HYPERLINK "http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9\_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82\_%D0%9A%D0%BB%D1%8D%D1%8F"Клэя](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82_%D0%9A%D0%BB%D1%8D%D1%8F) (ClayMathematicsInstitute, Кембридж, Массачусетс) выплатит приз в 1 млн. [долларов США](http://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BB%D0%BB%D0%B0%D1%80_%D0%A1%D0%A8%D0%90). Интересно, что опровержение гипотезы Римана не даст права на получение приза.

**Скатерть Улама**

Однажды математику Станиславу М. Уламу пришлось присутствовать на одном длинном и скучном, по его словам, докладе. Чтобы как-то развлечься, он начал писать на клетчатой бумаге числа, поставив в центре 1 и двигаясь по спирали против часовой стрелки. Без всякой задней мысли, он начал обводить простые числа кружками. Вскоре, к его удивлению, кружки с поразительным упорством стали выстраиваться вдоль прямых.

Написав программу, Улам получил рисунок (смотрите приложение 4) из чисел от 1 до 65000, из которого видно, что даже у края картины простые числа продолжают послушно укладываться на прямые. Участкам прямых соответствуют квадратные трёхчлены, порождающие простые числа, например *х2+х+17*, или найденный Эйлером *х2+х+41*, у которого первые *40* решений простые (при подстановке *х= 0,1,2,…,40)*, а из *2398* первых значений простых чисел ровно половина!

Однако этому есть логичное обоснование:

Если мы посмотрим на диагональ от 1, идущую через чифры 9,25,49,81,121 и так далее, то мы увидим, что это квадраты нечетных последовательных цифр, показывающие площадь «пройденных» квадратов спирали.

Возьмём квадраты таким образом, что бы длины сторон были нечетны. Первый квадрат это сама единица, второй заканчивается на 9, третий на 25 и так далее. Так как крайний угол квадрата обязательно задан числом равным его площади, а оно является нечетным, то у каждой вершины подобного квадрата будет стоять нечетное число и так как длина каждого квадрата увеличивается на 2, то идет смещение четности/ нечетности чисел таким образом, что бы по углам были нечетные цифры, иными словами сдвиг нечетности на 1 ячейку. О чем идет речь? Если провести от единицы диагонали во все стороны, то мы увидим, что на них располагаются нечетные числа, а если проведем (опять же от единицы) вертикальную и горизонтальную прямую, то мы увидим чередование четных чисел с нечетными. Таким образом если взять произвольный квадрат площадью 9, в центре которого будет находиться нечетное число, то по вертикальным и горизонтальным сторонам его будут окружать четные числа, а нечетные только по диагонали. Нам известно что простые числа нечетны (кроме 2), а значит находиться они будут только диагонально друг к другу. Это следует из четности и нечетности чисел.

**Гипотеза Гольдбаха**

Проблемой или гипотезой Гольдбаха называется следующая проблема:

Любое нечётное число не меньшее семи можно представить в виде суммы трёх простых чисел.

Например,

7 = 3 + 2 + 2

9 = 3 + 3 + 3

и так далее.

Вариантом проблемы Гольдбаха (её ещё называют тернарной проблемой Гольдбаха) является проблема Эйлера (или бинарная проблема Гольдбаха), которая до сих пор является одной из старейших нерешённых проблем:

Любое чётное число не меньшее четырёх можно представить в виде суммы двух простых чисел.

4 = 2 + 2

6 = 3 + 3

8 = 3 + 5

10 = 3 + 7 = 5 + 5

12 = 5 + 7

14 = 3 + 11 = 7 + 7

16 = 3 + 13 = 5 + 11

18 = 5 + 13 = 7 + 11

20 = 3 + 17 = 7 + 13

и так далее.

Теоретическое решение возможно при доказательстве гипотезы Римана, так как будет ясно распределение простых чисел.

**Известные выводы и теоремы из теории простых чисел.**

**Теорема 1.** Если натуральное число*р* большее 1, не делится ни на одно из простых чисел, квадраты которых не превосходят р, то число р простое.

Прежде чем провести доказательство этой теоремы в общем случае, рассмотрим следующую лемму.

**Лемма.** Всякое натуральное число, большее единицы, имеет хотя бы один простой делитель.

***Доказательство.*** Пусть *а1*- натуральное число, большее единицы. Если *а1* - простое число, то *а1* иесть простой делитель числа *а1*. Если же число *а1* не является простым, то найдётся делитель *а2* числа *а1*, отличный от *1* и *а1*. Таким образом **а1>а2**. Если а2- простое число, то *а2*есть простой делитель *а1*. Если же число *а2* не является простым, то найдётся делитель *а3* числа *а2*, отличный от *1* и *а2*. Таким образом, *а1>а2>а3*, причём *а3* есть отличный от *1* делитель числа *а1*. Если *а3*- простое число, то *а3* и есть простой делитель числа а1.Если же число *а3* не является простым, то найдётся такой делитель *а4* (отличный от *1*), что *a1>a2>a3>a4*. Каждый раз, если делитель не является простым, можно подобрать следующий, ещё меньший делитель числа *а1*.Но так не может продолжаться бесконечно: ведь натуральных чисел, меньших а1, имеется лишь конечное множество. Поэтому в конце концов мы обязательно получим простой делитель числа *а1*.

Теперь перейдём к доказательству теоремы. Если число *р* не является простым, то найдётся делитель *а* числа *р*, отличный от *1* и *р*. Таким образом, число *р=ab*. Будем считать для определённости, что*а≤b*. Тогда *а2≤ab*, т.е. *а2≤р*. В силу леммы найдётся простой делитель *q* числа *а*. Ясно, что qявляется и делителем числа *р*. При этом *q≤а*, так что *q2≤р*. Итак, если число *р* не является простым, то найдётся простой делитель *q* числа *р*, квадрат которого не превосходит *р*. Отсюда и вытекает справедливость теоремы.

Одним из первых вопросов, которые могут возникнуть по поводу простых чисел, является вопрос о том, конечно ли их число среди конечного множества чисел натурального ряда или их бесконечное множество.

На этот вопрос ответил Евклид, доказав следующую теорему.

**Теорема 2.** Среди чисел натурального ряда существует бесконечное множество простых чисел.

Справедливость этой теоремы следует из того, что каковы бы ни были различные простые числа:р1, р2, р3,…, рn, можно получить новое простое число, среди них не содержащееся. Таким простым числом будет простой делитель суммы: р1∙р2∙ р3…∙рn+1, который деля всю сумму, не может совпадать ни с одним из простых чисел р1, р2, р3,…,рn,так как при делении указанной суммы на какое-либо из этих простых чисел всегда в остатке получаем 1.Найдя таким образом новое простое число рn+1,составим сумму р1∙р2∙ р3…∙рn+1+1 мы придем к следующему простому числу рn+2, которое является простым делителем суммы р1∙р2∙ р3…·рn+1. И так далее. Таким образом, число простых чисел в натуральном ряду – бесконечно.

**Некоторые загадки и задачи простых чисел**

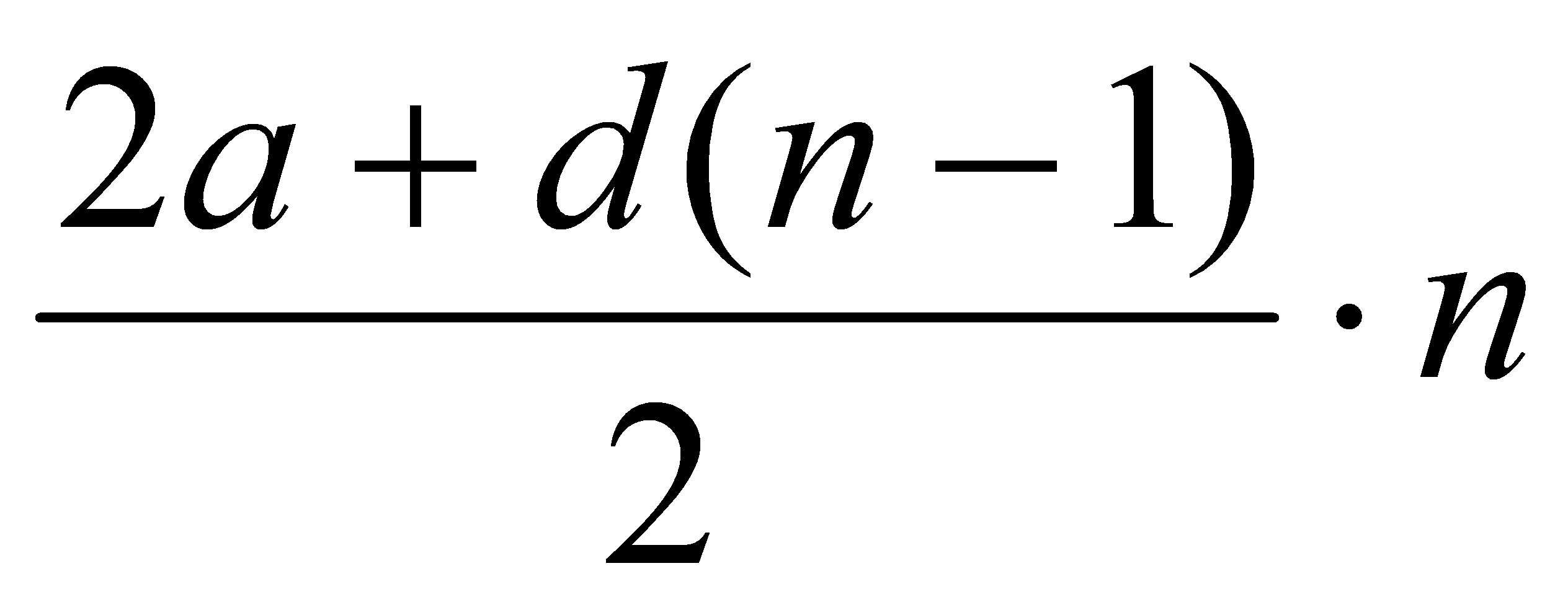
А вот одно интересное геометрическое наблюдение. Нарисуем на координатной плоскости *хОу* параболу *у = х2* и возьмем на ней точки *Аn(-n,n2)* и *Вm(m,m2)*, где *n* и *m* — натуральные числа, причем *n≥2* и *m≥2* (смотрите приложение 5) Проведем через все эти точки прямые. Каждая прямая *lnm*, проходящая через точки *Аn* и *Вm*, пересекает ось параболы *Оу* в точке *(0, mn).*

Немецкий математик Мёбиус (1790 - 1868) заметил, что все возможные прямые *lnm* «перечеркивают» на оси *Oу* все составные числа. Неперечеркнутыми остаются только простые числа и единица. Рисунок наглядно иллюстрирует это (смотрите приложение 4)

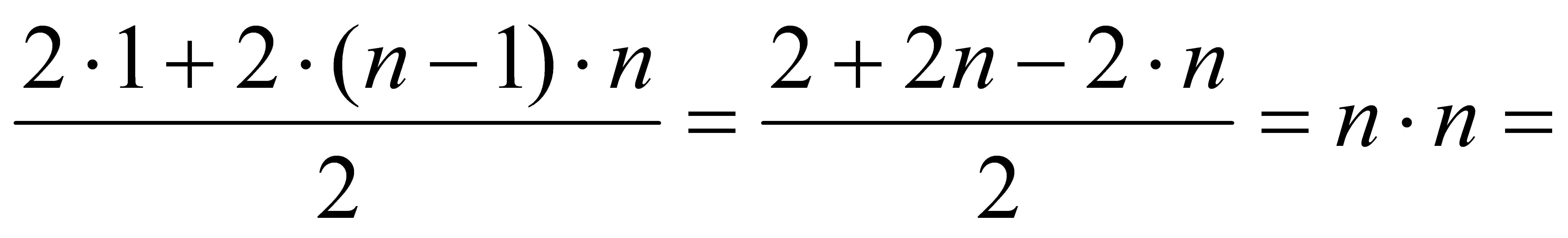
**Задача 1**: Разложить число 667 на простые множители.

Изложим метод Ферма. Пусть n>3 – нечётное натуральное число. Будем прибавлять к нему последовательно нечётные числа 1, 3, 5, 7 и т. д., пока не получим квадрат некоторого числа l: n+1+3+6+7+…+(2k – 1)=l2. Так как 1+3+5+…+(2k – 1)=k2, то n=l2 – k2=(l – k)(l+k) – искомое разложение числа n.

Существует формула: Sn= d=2 а1=1



n2



Теперь для отыскания делителей числа 667 применим метод Ферма:

667+1+3+5=676=262 . Отсюда 667=262-32=(26-3)(26+3)=23·29

Ответ: 667= 23·29

**Задача 2**: Может ли натуральное число иметь ровно 2003 делителя?

Решение. По условию, число n с каноническим разложением n=р1k1р2k2…pmkm имеет (k1+1)(k2+1)…(km+1)=2003 делителя. Так как число 2003 простое, одна скобка равна 2003, остальные равны 1.

Ответ: n=р2002, где р – простое число.

**Задача 3**: С помощью теоремы 1, решим задание: *определить, является ли число 101 простым.*

Что бы это узнать, нам нужно узнать, делится ли 101 на 2, 3, 5, 7, (на 11 проверять не нужно, т.к. 112 больше 101).Поделив 101 на эти числа, мы выяснили, что оно простое.

**Задача 4:** На рисунке (смотрите приложение 6) дана система уравнений, составленную нами, которую нужно решить в простых числах.

Решение:

Из первого уравнения мы находим, что вариантов сложения может быть 3. ***Четное + четное = четное*** (его сразу отбрасываем, так как четное простое число только 1).

***Нечетное + нечетное = четное*** (так как 2 – единственное простое нечетное число и при этом наименьшее из простых).

***Нечетное + четное = нечетное*** (единственный подходящий вариант).

Итак, мы знаем, что или Х или У равны 2. Если мы подставим 2 вместо У, то решение или будет дробным и длинным или вообще невозможным, но если 2 подставить вместо Х, мы получим У = 3. Сложив 2 и 3 мы получим 5 – все числа являются простыми, задача решена.

**Пример применения:** Представьте, что к вам на день рождения пришло 7 гостей (имеется ввиду, что всего семь человекбудут есть угощения) и вам нужно разрезать праздничный торт на 7 частей, при том каждая часть должна быть одинаковой, но сделать это будет не так просто. Так если бы человек было 8 или 6 это сделать было бы гораздо проще.

**Гипотеза**: Нами замечено, что в каждом (исследованном нами) мандарине содержится количество долек равное простому числу. Как бы не было абсурдно это утверждение, опровержения мы пока не нашли.

**Заключение**

Мы не знаем самого простого и элементарного, это заставляет нас использовать все больше ресурсов и знаний. Так организация Клэй объявило награду в 1 миллион долларов тому, кто решит проблему заключенную в гипотезе Римана и такую же сумму тому, кто решит проблему Гольдбаха, а за нахождение простого числа с количеством цифр более 100 000 000 и 1 000 000 000 организация EFF объявила награду в 150 и 250 тысяч долларов соответственно.

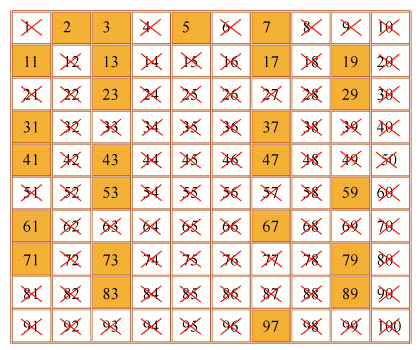
Эта работа позволила мне увидеть мир простых цифр с другой стороны. Несмотря на то, что я понял несовершенство современных познаний, я рад тому, что могу привнести свой вклад в решение этих проблем и задач, и что на уровне современных технологий все же есть над чем задуматься.

**Использованная литература**

* Гальперин Г. [«Просто о простых числах»](http://kvant.mccme.ru/1987/04/prosto_o_prostyh_chislah.htm) // [Квант](http://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82_%28%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB%29). — № 4. — С. 9-14,38.
* Нестеренко Ю. В.[Алгоритмические проблемы теории чисел](http://nature.web.ru/db/msg.html?mid=1157083&uri=node28.html) // [Введение в криптографию](http://nature.web.ru/db/msg.html?mid=1157083&uri=book.html) / Под редакцией В. В. Ященко. — Питер, 2001. — 288 с. — [ISBN 5-318-00443-1](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:BookSources/5318004431)
* Василенко О. Н.[Теоретико-числовые алгоритмы в криптографии](http://www.ict.edu.ru/ft/002416/book.pdf). — М.: [МЦНМО](http://ru.wikipedia.org/wiki/%D0%9C%D0%A6%D0%9D%D0%9C%D0%9E), 2003. — 328 с. — [ISBN 5-94057-103-4](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:BookSources/5940571034)
* Черемушкин А. В.[Лекции по арифметическим алгоритмам в криптографии](http://www.ict.edu.ru/ft/002419/cherem.pdf). — М.: [МЦНМО](http://ru.wikipedia.org/wiki/%D0%9C%D0%A6%D0%9D%D0%9C%D0%9E), 2002. — 104 с. — [ISBN 5-94057-060-7](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:BookSources/5940570607)
* Кноп К.[«В погоне за простотой»](http://web.archive.org/web/20080319163127/http:/www.geocities.com/CapeCanaveral/4344/211.html)
* Кордемский Б. А.[Математическая смекалка](http://ilib.mccme.ru/djvu/klassik/smekalka.htm). — М.: ГИФМЛ, 1958. — 576 с.
* Генри С. Уоррен, мл. Глава 16. Формулы для простых чисел // Алгоритмические трюки для программистов = Hacker'sDelight. — М.: [«Вильямс»](http://ru.wikipedia.org/w/index.php?title=%D0%92%D0%B8%D0%BB%D1%8C%D1%8F%D0%BC%D1%81_%28%D0%B8%D0%B7%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE%29&action=edit&redlink=1), 2007. — 288 с. — [ISBN 0-201-91465-4](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:BookSources/0201914654)
* Ю. Матиясевич [Формулы для простых чисел](http://kvant.mccme.ru/1975/05/formuly_dlya_prostyh_chisel.htm) // [Квант](http://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82_%28%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB%29). — 1975. — № 5. — С. 5-13.
* Н. Карпушина [Палиндромы и «перевёртыши» среди простых чисел](http://www.nkj.ru/archive/articles/17984/) // [Наука и жизнь](http://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%83%D0%BA%D0%B0_%D0%B8_%D0%B6%D0%B8%D0%B7%D0%BD%D1%8C). — 2010. — № 5.
* Д. Цагер [Первые 50 миллионов простых чисел](http://mi.mathnet.ru/umn2506) // Успехи математических наук. — 1984. — Т. 39. — № 6(240). — С. 175–190.
* http://primes.utm.edu/ (англ.) — база данных наибольших известных простых чисел

Приложение 1

Решето Эратосфена



Приложение 2

600±20

486±18 540±19

384±16 432±17 480±18

294±14 336±15 378±16 420±17

216±12 252±13 288±14 324±15 360±16

150±10 180±11 210±12 240±13 270±14 300±15

96±8 120±9 144±10 168±11 192±12 216±13 240±14

54±6 72±7 90±8 108±9 126±10 144±11 162±12 180±13

24±4 36±5 48±6 60±7 72±8 84±9 96±10 108±11 120±12

6±2 12±3 18±4 24±5 30±6 36±7 42±8 48±9 54±10 60±11

|  |
| --- |
| 0±1 0±2 0±3 0±4 0±5 0±6 0±7 0±8 0±9 0±10 |

6±0 12±1 18±2 24±3 30±4 36±5 42±6 48±7 54±8 60±9

24±0 36±1 48±2 60±3 72±4 84±5 96±6 108±7 120±8

54±0 72±1 90±2 108±3 126±4 144±5 162±6 180±7

96±0 120±1 144±2 168±3 192±4 216±5 240±6

150±0 180±1 210±2 240±3 270±4 300±5

216±0 252±1 288±2 324±3 360±4

294±0 336±1 378±2 420±3

384±0 432±1 480±2

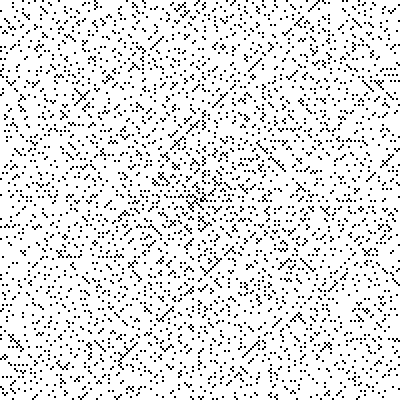
486±0 540±1

600±0

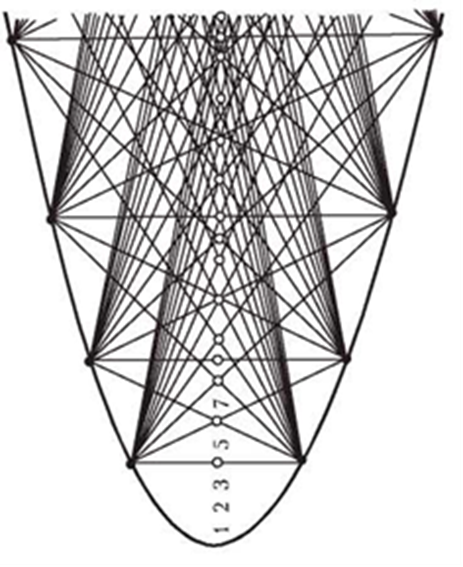
Приложение 3



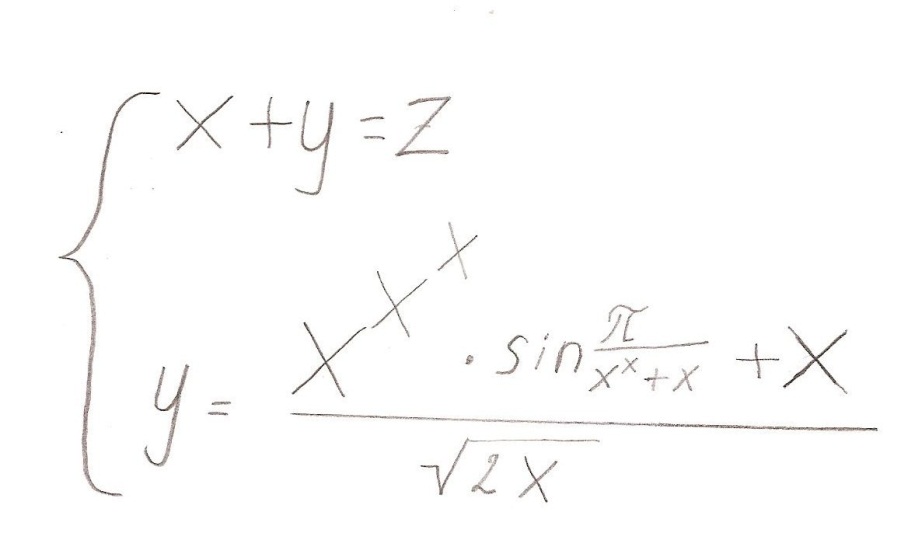
Приложение 4



Приложение 5



Приложение 6



1. Сравнение по модулю натурального числа n — в теории чисел отношение эквивалентности на кольце целых чисел, связанное с делимостью на n. Факторкольцо по этому отношению называется кольцом вычетов. Совокупность соответствующих тождеств и алгоритмов образует модульную (или модулярную) арифметику. [↑](#footnote-ref-2)