Международный конкурс исследовательских работ школьников

«Research start»

**Проектно - исследовательская работа**

**на тему: «Геометрия конгруэнтных чисел – эллиптические кривые»**

Выполнил:

ученик 10 «А» класса МОУ «СОШ № 48»

Ленинского района г. Саратова

Курдутов Илья Романович

Научный руководитель:

Винокурова Светлана Александровна

2023 - 2024

**Содержание**

|  |  |
| --- | --- |
| Введение……………………………………………………………………….. | 3 |
| 1. Кубические кривые…………………..………………………..…………. | 5 |
| 1. Конгруэнтные числа…...………………………………….……………….. | 10 |
| 1. Конгруэнтные числа и эллиптические кривые..….……………………..... | 13 |
| 1. Методы поиска конгруэнтных чисел………………………...……….….. | 14 |
| Заключение……………………………………………………………………. | 16 |
| Библиографический список…………………………………………………... | 17 |

**Введение**

***Обоснование выбора темы.*** Одним из основополагающих понятий математики является число. Даже простейшие числовые множества: натуральные, рациональные числа, обладают замечательными свойствами. Например, натуральные числа можно разделять на четные и нечетные, выстраивать последовательности Фибоначчи, выделять простые и составные и многое другое. У «более богатого» множества рациональных чисел значительно больше закономерностей. Одним из замечательных свойств, имеющих практическое применение, является свойство равенства площади прямоугольного треугольника с рациональными сторонами целому числу. Такие числа называются конгруэнтными. Изучению конгруэнтных чисел, а также их неожиданной связи с эллиптическими кривыми, то есть кривыми, задаваемых уравнениями третьей степени, посвящена данная работа.

***Цель исследования*** - познакомиться с понятием конгруэнтного числа и с задачами, относящимся к конгруэнтным числам.

***Задачи исследования:***

* развить навыки самостоятельной исследовательской работы посредством изучения конгруэнтных чисел и эллиптических кривых;
* установить связь конгруэнтных чисел с эллиптическими кривыми;
* доказать, что число один не является конгруэнтным;
* рассмотреть критерий Таннелла.

Задача о конгруэнтных числах, упоминавшаяся еще в арабских математических текстах X века, состоит в следующем: для каких рациональных чисел s найдется прямоугольный треугольник с рациональными сторонами и площадью s? Долгое время ученые не могли вычислить конгруэнтные числа, которые больше 1000. В 2009 году математики из США, Европы, Австралии и Южной Америки составили полный список конгруэнтных чисел, лежащих в диапазоне от нуля до одного триллиона. Полученная учеными последовательность оказалась настолько велика, что если этот ряд цифр записать от руки в строчку, то он протянется до Луны и обратно. Древний математический вопрос удалось решить благодаря возможностям современной техники. Для того чтобы обеспечить точность результатов, учёные одновременно проводили вычисления на двух мощных компьютерах, используя разные алгоритмы. Объём оперативной памяти в обоих случаях составлял 128 Гб. Этого оказалось недостаточно для оперирования получавшимися в процессе числами, и специалистам пришлось активно использовать дисковую подсистему. В результате учёные составили список из 3 148 379 694 конгруэнтных чисел, наибольшее из которых не превышает триллиона. По некоторым оценкам, в промежутке от триллиона до квадриллиона должно содержаться ещё около 800 миллиардов конгруэнтных чисел. Но в ближайшее время проверить это не получится из-за технических ограничений. Удивительным образом проблема о нахождении конгруэнтных чисел оказывается связанной с самой современной математикой - ее решение может быть получено по модулю так называемой гипотезы Берча и Свиннертона-Дайра, входящей в список «Проблем тысячелетия» института Клэя, и за решение которой предлагается миллион долларов.

**1. Кубические кривые**

Рассмотрим следующие задачи:

А. Найти все пары натуральных чисел m и n, такие что сумма первых m

натуральных чисел равна сумме квадратов первых n натуральных чисел:

1 + 2 + 3 + · · · + m = 12 + 22 + 32 + · · · + n2.

Б. При каких n сумма квадратов первых n натуральных чисел является

квадратом некоторого натурального числа?

В. Какие натуральные числа являются одновременно произведением двух

последовательных натуральных чисел и произведением трех последовательных натуральных чисел?

Все эти задачи объединяет то, что они сводятся к изучению решений в целых или рациональных числах кубических уравнений с двумя переменными [1].

Уравнение от двух переменных задает некоторую кривую на плоскости. Так как наши кривые задаются уравнениями третьей степени, они являются примерами кривых третьего порядка или кубических кривых.

Назовем кубической кривой (кубикой) на плоскости алгебраическую кривую C, заданную многочленом , где наибольшее значение i + j равно 3.

Для исследования кубических кривых удобно использовать проективные замены координат, то есть замены вида:

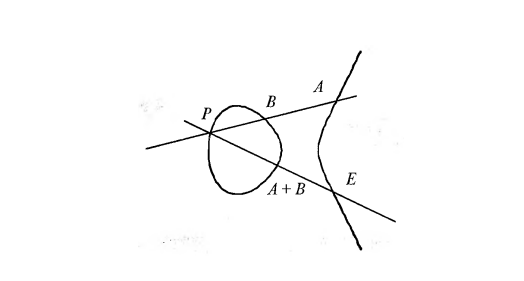
x′ = , y′ = , γ1 + γ2 + γ3 ≠ 0.

При этом введем обозначения: X = α1x + α2y + α3, Y = β1x + β2y + β3,

Z = γ1 + γ2 + γ3.

В дальнейшем кубические кривые, уравнения которых получены путем проективных замен координат, будем называть проективными кубиками. На любой кубике существует естественный закон сложения [2].

Зафиксируем произвольную точку E кривой. Для сложения точек A и B проведем прямую AB, она пересечет кривую C в некоторой точке P. Точку пересечения прямой PE с кубикой будем называть суммой точек A и B в соответствии с рисунком 1.



*Рисунок 1 - Сложение точек на кубике*

Обычно в качестве точки E выбирают бесконечно удаленную точку O. Существование такой точки следует из того, что, положив в проективном уравнении кубической кривой Z = 0, получим непустое множество решений для координат X, Y, которое соответствует точкам пересечения кубики с бесконечно удаленной прямой (в противном случае бесконечно удаленной можно назвать прямую X = 0 или Y = 0).

В определении сложения использовано следующее свойство кубики: если прямая пересекает кубическую кривую C в двух точках, то она пересекает ее еще ровно в одной точке. Действительно, из уравнения прямой ax + by + c = 0 можно выразить x через y и подставить результат в уравнение кубики. Получим уравнение от одной переменной. Если рассматривать проективную кривую, то степень уравнения после подстановки равна 3.

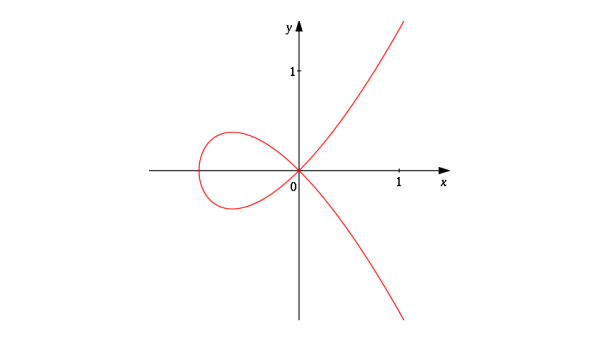
Рассмотрим примеры пересечения кубики с прямой.

**Пример 1.** Пересечения кубики с прямой.

Рассмотрим кубическую кривую, переходя к проективной форме этой кривой.

1. Покажем, что кривая y2 = x3 + Ax + B пересекает бесконечно удаленную прямую Z = 0 в одной точке, причем кратность пересечения равна 3. Подставляя в уравнение кривой Y2Z = X3 +AXZ2 +BZ3 значение Z = 0, получаем X3 = 0. Последнее уравнение имеет тройной корень X = 0. По определению проективной кривой Y ≠ 0, так как точка (0, 0, 0) не лежит на проективной плоскости, поэтому координаты точки пересечения кривой с бесконечно удаленной прямой можно записать как (0, 1, 0). Поскольку эта точка лежит на бесконечно удаленной прямой, она является бесконечно удаленной.

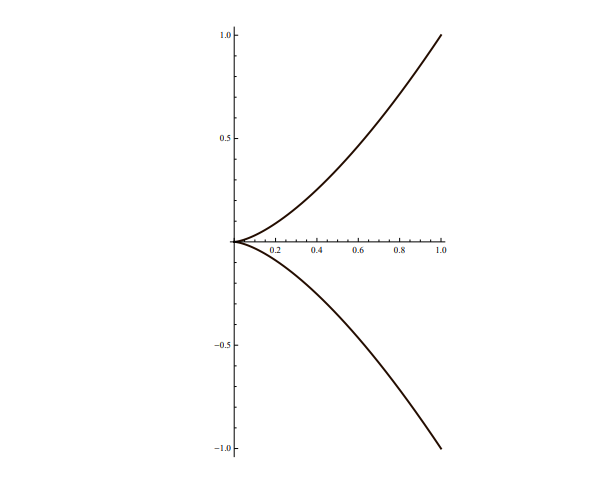
2. Покажем, что кривая y2 = x3+x2, в соответствии с рисунком 2, пересекает произвольную прямую, проходящую через точку (0, 0), в двух или трех точках.



*Рисунок 2 - Кривая y2 = x3 + x2*

Уравнение кривой имеет вид Y2Z = X3 + X2Z. Уравнение прямой, проходящей через точку (0, 0): y = ax. Соответствующее проективное уравнение: Y = aX. Подставляя уравнение прямой в уравнение кубики, получаем X2 (X + Z − a2Z) = 0, то есть имеем двойное (тройное при a = ±1) пересечение в проективной точке (0, 0, 1). Отсюда по правилу сложения точек следует, что P + (0, 0) = (0, 0).

3. Покажем, что кубика y2 = x3, в соответствии с рисунком 3, пересекает произвольную прямую, проходящую через точку (0, 0), в этой точке с кратностью 2 или 3.



*Рисунок 3 - Кривая y2 = x3*

Рассуждая аналогично, получаем для пересечения прямой и кубики уравнение aX2Z = X3. Пересечение двойное (тройное при a = 0). Следовательно, также имеет место равенство P + (0, 0) = (0, 0).

Из рассмотренных примеров видно, что в двух последних случаях точка

(0, 0) ведет себя по-особому, а именно является аналогом понятия «бесконечность» для натуральных чисел [4], [5].

**Пример 2.** Особые точки.

1. Кривая y2 = x3+x2 (см. рисунок 2) содержит особую точку (0, 0), которая называется точкой самопересечения, или узлом.

2. Кривая y2 = x3 (см. рисунок 3) содержит особую точку (0, 0), которая

называется острием, или точкой возврата.

Кубическая кривая на плоскости (x, y) называется кривой в форме Вейерштрасса, если она задается уравнением вида

y2 = x3 + ax + b. (1.1)

Неособой кривой называется кривая, не имеющая особых точек.

Для неособой кривой справедлива следующая теорема.

**Теорема 1.1. Теорема Ньютона.** *Для любой неособой кубической кривой*

*существует проективная замена координат, приводящая ее в форму Вейерштрасса.*

Неособая кривая третьего порядка называется эллиптической кривой. Теорема Ньютона утверждает, что любая эллиптическая кривая при помощи некоторой проективной замены координат приводится к форме Вейерштрасса.

Сложение точек эллиптической кривой полностью совпадает с методом сложения точек на произвольной кубике.

Замечательно, что введенное нами сложение точек на кубической кривой обладает свойствами сложения чисел, а именно:

а) коммутативностью (для любых точек P и Q кубической кривой выполняется тождество P + Q = Q + P);

б) наличием нуля (такой точки 0, что P + 0 = P = 0 + P для любой точки P);

в) наличием для любой точки P противоположной точки (такой точки −P, что P + (−P) = 0 = (−P) + P);

г) ассоциативностью (для любых точек P, Q и R должно выполняться тождество (P + Q) + R = P + (Q + R)).

**2. Конгруэнтные числа**

Исторически к некоторому виду эллиптических кривых c рациональными коэффициентами привели исследования Пифагора, Евклида, Диофанта, Ферма при решении задачи о прямоугольном треугольнике с целочисленными длинами сторон («пифагоровы тройки»). Ее развитием стала задача о конгруэнтных числах.

Назовём рациональное число s - конгруэнтным, если существует прямоугольный треугольник площади s с рациональными длинами сторон.

Про некоторые числа известно и доказано, что они конгруэнтны, а про некоторые, что они не конгруэнтные. Например, площадь египетского треугольника (со сторонами 3, 4, 5) равна ∙ 3 ∙ 4 = 6, число 6 - конгруэнтное.

Чуть сложнее показать, что число 5 - конгруэнтное. Для этого нам нужно рассмотреть прямоугольный треугольник со сторонами , , . Его площадь равна 5, тогда число 5-конгруэнтно.

Таким образом, конгруэнтное число – это натуральное число, равное площади прямоугольного треугольника со сторонами, длины которых выражаются рациональными числами.

**Теорема 2.1.** *Если число s - конгруэнтное, то и число sl2 конгруэнтно при любом рациональном l.*

**Доказательство.**

Рассмотрим прямоугольный треугольник с катетами a и b. Площадь этого треугольника равна s = ∙ a ∙ b.

Путем пропорционального увеличения сторон треугольника в *l* раз получим, что катеты равны *al* и *bl*. Тогда площадь получившегося треугольника равна s′ = ∙ a ∙ b ∙ l2, то есть s′ = s ∙ l2.

Одним из первых конгруэнтными числами заинтересовался математик X века ал-Караджи. В его вычислениях не фигурировали треугольники, а расчёты базировались на квадратах чисел.

Для нахождения конгруэнтных чисел ученые работали много лет. В 1225 году великий Фибоначчи установил, что числа 5 и 7 конгруэнтны, и предположил, что число 1, напротив, таковым не является. Только в 1659-м это утверждение было доказано Пьером Ферма.

**Теорема 2.2.** *Число 1 не конгруэнтно.*

**Доказательство.**

Доказывать будем от противного. Допустим, что число 1 конгруэнтно, а значит существует прямоугольный треугольник с целыми длинами сторон a, b, x (где x - гипотенуза), площадь которого равна ∙ a ∙ b = y2, y - целое число

(ясно, что можно выбрать a и b так, чтобы только одно из них было чётным).

Преобразуем выражение

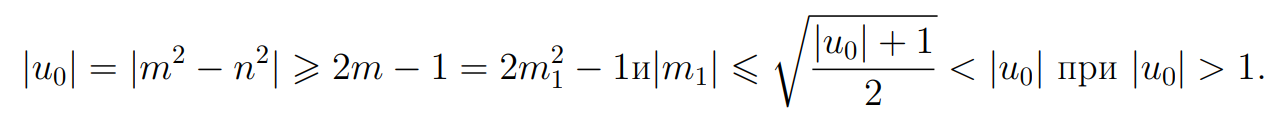
x4 − 16y4 = (x2 − 4y2)(x2 + 4y2) = (x2 −2ab)(x2 + 2ab) = (a2 + b2 − 2ab)(a2 + b2 + 2ab) = (a − b)2(a + b)2

Итак, если 1- конгруэнтное число, то уравнение x4 − (2y)4 = u2 имеет решение в целых положительных числах (число u нечётно). Выберем среди всех ненулевых решений с нечётными u такое решение (x0, y0, u0), для которого |u| минимально.

Числа x0, y0 и u0 попарно взаимно просты: если какие-нибудь два из них имели общий простой делитель p, то и третье число делилось бы на p (причём число u0 делилось бы даже на p2), а для решения (, , значение |u| меньше.

Применим формулу X = 2mn; Y = m2 − n2; Z = m2 + n2 к равенству = (2y0)4 + , получаем = m2 + n2, (2y0)2 = 2mn (в нашем случае числа , (2y0)2, u0 попарно взаимно простые и (2y0)2 чётно), где m и n – взаимно простые числа, одно из которых (будем считать, что n) чётно. Из равенства (2y0)2 = 2mn следует, что m = , n = 2. Из равенства = m2 + n2 следует, что x0 = + , n = 2m2n2 = 2, m = − = , где m2 и n2 – также взаимно простые числа, одно из которых чётно, причём из последнего равенства

ясно, что n2 чётно. Получаем: m2 = , n2 = и − = . И так как n3 чётно, (m3, , m1) - решение уравнения x4 − (2y)4 = u2 в целых числах со значением |u| меньшим, чем |u0|:



Случай |u0| = 1 тривиален.

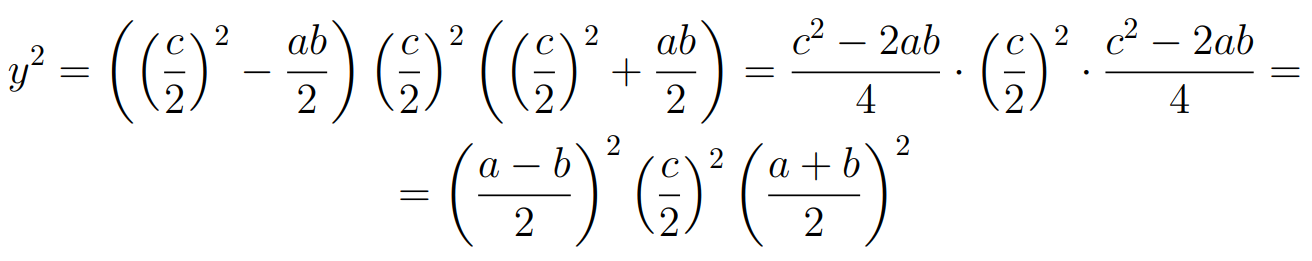
Применённый метод доказательства называется методом бесконечного спуска и помогает решить многие задачи из теории чисел.

**3. Конгруэнтные числа и эллиптические кривые**

Ранг эллиптической кривой - наименьшее число n, такое что любые n+1 рациональных точек этой кривой линейно зависимы, то есть найдутся совпадающие точки.

Замечательно, что задача о конгруэнтных числах эквивалентна вопросу о ранге некоторых эллиптических кривых [3]. Пусть s - конгруэнтное число, т.е. s - площадь прямоугольного треугольника с рациональными катетами a и b и гипотенузой c, c2 = a2 + b2, s = ∙ a ∙ b (считаем s целым числом, свободным от квадратов, то есть не делится на квадраты целых чисел).

Сопоставим числу s эллиптическую кривую Es, заданную уравнением y2 = x3 − s2x = (x − s) ∙ x ∙ (x + s).

Подставим в это уравнение x = ()2:

Таким образом, P = (x, y) = (()2, ) - рациональная точка.

Так же на кривой ES лежат точки P1 = (−s, 0), P2 = (0; 0), P3 = (s; 0).

Эти три точки суть порядка 2, так как касательные к кривой ES в этих точках

вертикальны.

**4. Методы поиска конгруэнтных чисел**

Задача о конгруэнтных числах была известна еще древним грекам, однако ответ на нее удалось сформулировать лишь в XX веке. А именно, в 80-х годах прошлого века был найден удивительный критерий для выяснения вопроса о конгруэнтности произвольного числа.

*Теорема 4.1. Критерий Таннелла.* Нечетное натуральное число n, свободное от квадратов, конгруэнтно тогда и только тогда, когда количество

решений уравнения

n = 2x2 + y2 + 32z2

в целых числах равно половине количества решений в целых числах уравнения

n = 2x2 + y2 + 8z2.

Четное натуральное число n, свободное от квадратов, конгруэнтно тогда и только тогда, когда количество решений в целых числах уравнения

= 4x2 + y2 + 32z2

равно половине количества решений в целых числах уравнения

= 4x2 + y2 + 8z2.

Заметим, что для заданного n число решений каждого из этих уравнений

находится очень просто, например перебором.

Рассмотрим несколько примеров.

При n = 1 оба соответствующих уравнения имеют по два решения (0, ±1, 0). Следовательно, число 1 не является конгруэнтным.

При n = 2 оба соответствующих уравнения тоже имеют по два решения, значит, и число 2 не является конгруэнтным.

Число n = 34 ведет себя по-другому. Уравнение 17 = 4x2 + y2 + 32z2 имеет четыре решения (±2, ±1, 0), а уравнение 17 = 4x2 + y2 + 8z2 - восемь решений (0, ±3, ±1) и (±2, ±1, 0). В этом случае критерий Таннелла утверждает, что прямоугольный треугольник с площадью 34 существует. И это действительно верно: длины сторон одного из таких треугольников равны , и .

К сожалению, критерий Таннелла не доказан полностью. Сегодня известно лишь то, что если число n конгруэнтно, то выполнены соответствующие утверждения о количествах решений. Обратное утверждение вытекает из некоторой общей гипотезы об эллиптических кривых - гипотезы Бёрча и Свиннертон - Дайера.

В статьях «Notes on elliptic curves. I» и «Notes on elliptic curves. II» Бёрч и Свиннертон-Дайер собрали статистику по рангам пары тысяч эллиптических кривых и предложили титульную гипотезу.

Гипотеза Бёрча - Свиннертон-Дайера связывает ранг эллиптической кривой (в этом она похожа на дзета-функцию Римана - гипотеза Римана, касающаяся свойств дзета-функции, является ещё одной из «задач тысячелетия») с количеством её точек по модулю p для всевозможных простых чисел p.

**Заключение**

Автором рассмотрено понятие конгруэнтного числа и задачи, относящиеся к конгруэнтным числам. Установлена связь конгруэнтных чисел с эллиптическими кривыми. Доказано, что число один не является конгруэнтным. Рассмотрен критерий Таннелла.

Эллиптические кривые находят свое применение в криптографии, например, хорошо известные алгоритмы шифрования Эль-Гамаля, где одним из инструментов являются точки эллиптической кривой. Исходя из этого, можно предположить, что конгруэнтные числа имеют важное значение при получении различных криптосистем.

В своей работе я рассмотрел только начальные сведения и основные факты о конгруэнтных числах. Несмотря на то, что начальное множество рациональных чисел весьма просто, но приложения и методы получения конгруэнтных чисел насыщены большим количеством сложных математических понятий, теорем и выкладок. А кубические кривые сильно отличаются от привычных нам квадратичных кривых, от эллипса, параболы и гиперболы. Данная тема меня очень заинтересовала и сподвигла к ее дальнейшему изучению.

Практическая значимость работы заключается в возможности использования результатов исследования автора на уроках математики, и дальнейших исследований конгруэнтных чисел и эллиптических кривых и в области теории чисел.

**Библиографический список**

1. Зыкин А., Конгруэнтные числа и эллиптические кривые. Летняя школа «Современная математика», г. Дубна, 20-22 июля 2012 г.
2. Коблиц Н. Введение в эллиптические кривые и модулярные формы. Москва, «Мир», 1988
3. Острик В. В., Цфасман М. А. Алгебраическая геометрия и теория чисел: Рациональные и эллиптические кривые. М.: МЦНМО, 2001. - 48 с.
4. Праслов, В. В., Соловьев, Ю. П. Эллиптические кривые и алгебраические уравнения М.: Изд-во "Факториал 1997. – 145 c.
5. Рид М. Алгебраическая геометрия для всех М.: Мир, 1991. – 143 c.
6. <http://www.mathnet.ru/links/55cb2a120c63a684a918f2b0ba682962/mat523.pdf>
7. https://math.wikireading.ru/hS6Zm14yhG