Краевой конкурс учебно-исследовательских и проектных работ учащихся
«Прикладные вопросы математики»

Прикладные вопросы математики

Приложение теории чисел в современной криптографии

Желнин Максим Сергеевич,
МОУ «Лицей №1» г. Перми, 11 кл.
Грайфер Лазарь Борисович,
к. ф.-м. н., доцент ПНИПУ

Наука арифметика зародилась в глубокой древности, и является старейшей отраслью математики. Научным обобщением арифметики является теория чисел. Интерес к теории чисел был высок во все времена, а результатами теории чисел и арифметики, полученными древними учеными, активно пользуются и в сегодняшнее время. В середине XX века и XXI веке существенно изменилась роль теории чисел. Если в предыдущие три века она была красивейшим разделом математики, привлекавшим внимание лучших математиков своего времени, таких как Ферма, Эйлер, Лагранж, Гаусс, Риман, Гильберт, то с появлением компьютеров теория чисел нашла многочисленные приложения при обработке, передаче и защите информации, представимой в числовом виде. Поэтому в школьный курс математики вошли некоторые разделы теории чисел, ранее не изучавшихся, например: алгоритм Евклида и решение уравнений в целых числах. Задачи теории чисел из школьного курса входили в олимпиады и вступительные экзамены лучших ВУЗов страны, а сегодня представлены в ЕГЭ в виде задачи С6.

Следует отметить, что особое место задач С6 – теоретический материал для их решения. Он преподается достаточно рано (в 6 – 7-ом классах), а некоторые разделы не входят в обязательную программу и изучаются только в профильных классах (с 7 по 9). Поэтому для успешного решения задач С6, следует повторить школьный материал по теории чисел. Исходя из этого, первая часть учебно-исследовательской работы посвящена классификации задач С6 по темам и сравнительному анализу методов их решения.

Целью данной учебно-исследовательской работы является изучение применения теории чисел в реальной жизни, а именно в математической криптографии. Криптография – это наука занимающаяся разработкой методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

Итак, целями учебно-исследовательской работы являются:

- Способы применение теории чисел, изучаемой в школе, в криптографии
- Способы применение алгебраической геометрии в решении криптографических задач

Для того чтобы реализовать эти цели, необходимо решить следующие задачи:

- Применить теорию чисел, проходимую в школе, для решения задач С6 ЕГЭ.
- Рассмотреть шифр с открытым ключом.
- Рассмотреть решение целочисленных задач с помощью алгебраической геометрии.
- Рассмотреть шифры с открытым ключом, построенные на эллиптических кривых.

Решая задачи С6 и делая их классификацию, я знакомился с различными пособиями и интернет-изданиями и узнал, что разработчики задач ЕГЭ, в частности, известные московские математики И.В. Ященко, И.Н. Сергеев и другие в жизни занимаются математической криптографией, применяя новые результаты алгебраической геометрии, теории сложности вычислений и других разделов математики для защиты информации. С многими из этих результатов я познакомился по материалам конференции “ Современная математика”, ежегодно проводимой для учащихся школ и студентов младших курсов в городе Дубна в июле, начиная с 2001 года, и опубликованных в сборниках и серии «Математическое просвещение». Я решил изучить применение теории чисел и алгебраической геометрии в криптографии и проверить понимание, решая прикладные задачи шифрования этими методами. Для подготовки базы к решению таких задач мы включаем во вторую часть работы краткую сводку основных математических сведений (глоссарий), используемых в дальнейшем при решении нескольких практических задач криптографии.

1. Шифры с открытым ключом, система RSA.

Глоссарий.

Шифр с открытым ключом[8] – эта функция fx обладающая следующими свойствами:

1. существует достаточно быстрый алгоритм вычисления значений fx;
2. существует достаточно быстрый алгоритм вычисления значений обратной функции f-1x;
3. функция f(x) обладает некоторым «секретом», знание которого позволяет быстро вычислять значения f-1x; в противном случае вычисление f-1x становится трудно разрешимой задачей, требующей для своего решения столь много времени, что по его прошествии зашифрованная информация перестает представлять интерес для лиц, использующих отображение f в качестве шифра.

Назовем *шифровальным ключом* функцию E, преобразующую сообщение M в шифрограмму C, а *дешифровальным ключом* функцию D, преобразующую шифрограмму C в исходное сообщение M.

Алгоритм Ферма разложения на множители[3].

Берем нечетное натуральное число n, если бы n было четным, то 2 было бы его делителем. Ключевая идея алгоритма состоит в том, чтобы попробовать представить n в виде n=x2-y2, где x, y – неотрицательные целые числа. Если такие числа найдены, то n=x2-y2=x-y(x+y). Значит, x-y и x+y являются делителями числа n.

Расширенный алгоритм Евклида[3].

Пусть a и b – натуральные числа, а d – их наибольший общий делитель. Тогда с помощью расширенного алгоритма Евклида можно найти d, и два целых числа α,β таких, что α*a+β*b=d. Поиск этих чисел сводится к решению линейного диофантового уравнения.

Функция Эйлера[3].

Функция Эйлера φ(n) определяется как количество положительных целых чисел, меньших n, и взаимно простых с n. Из функции Эйлера видно, что если число p простое, то все числа 1, 2, … (p-1) вазимно просты с ним, поэтому φp=p. Также функция Эйлера мультипликативна – это значит, что φab=φa*φ(b).

1.1. Система шифрования RSA.

Для реализации системы RSA, которая предназначена для одного пользователя, необходимо выбрать два различных простых числа p и q и вычислить их произведение n = p×q. Простые p и q хранятся в тайне, в то время как число n становиться частью открытого ключа. Число n называется модулем системы RSA.

Сообщение – всякое число, которое обладает одновременно двумя свойствами:

1) Оно меньше модуля системы.
2) Оно взаимно просто с ним.

Для того чтобы понять алгоритм шифрования RSA, напомним кое-какие сведения из теории чисел.

Далее мы приводим алгоритмы шифрования и дешифрования по методу RSA. Мы приводим свою версию данных алгоритмов, но для их составления мы пользовались книгой [3].

Алгоритм шифрования.

Возьмем сообщение M.

1) Берем два простых числа p и q, которые отправитель сообщения держит в тайне. Вычисляем n = p*q. Заметим, что разность p – q, должна быть тоже очень велика, иначе p и q можно будет найти с помощью алгоритма Ферма разложения на множители.
2) Выбираем произвольное положительное число ***e*** **(**открытый показатель), которое взаимно просто с числом φn(функция Эйлера от n). Само же число φn легко найти, воспользовавшись мультипликативностью функции Эйлера и зная, что n = p*q. Поэтому φn=p-1(n-1). Отметим, что пара чисел (n, e) называется открытым, или кодирующим, ключом криптосистемы RSA.
3) Шифруем сообщение M, т.е. применяем шифровальный ключ. *C = E(M) =* вычет Me по модулю n.

После выполнения всех шагов мы получили зашифрованное сообщение C.

Алгоритм дешифрования.

Берем зашифрованное сообщение C.

1. Для дешифровки сообщения нам нужно знать закрытый показатель – число d (закрытый показатель) и модуль системы – число n, которое публикуется в открытой печати. Пара чисел (n,d) называется секретным или декодирующим ключом системы RSA.
   Для того чтобы вычислить d, нужно знать e и φ(n).
   Вычисление закрытого показателя d.
   Пусть m=φn=p-1q-1. По условию НОД(e,m) = 1.
   По расширенному алгоритму Евклида 1 можно представить в виде

линейной комбинации чисел *m* и *e*: x*e+y*m=1 x,y-целые числа. Далее по алгоритму для нахождения частного целого решение линейного диофантового уравнения находим x и y. Затем вычисляем d = φn+ x.

2. Получаем исходное сообщение M, дешифрую сообщение C, т.е. применяем дешифровальный ключ.
   M=DC=DEM=вычет Cd по модулю n

1.2. Реализация метода RSA.

Попробуем зашифровать какое-нибудь сообщение, пользуясь алгоритмами шифрования и дешифрования по методу RSA.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К
10	11	12	13	14	15	16	17	18	19	20

Л	М	Н	О	П	Р	С	Т	У	Ф	Х
21	22	23	24	25	26	27	28	29	30	31

Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
32	33	34	35	36	37	38	39	40	41

Пусть нам дано сообщение: ФИЗМАТ. Заменим каждую букву сообщения числом, выбрав его из таблицы. Численное представления нашего сообщения «ФИЗМАТ» выглядит так: 301817221028.

Следуя алгоритмам, зашифруем и расшифруем наше сообщение.

1. Выберем два числа p и q. Например: p = 71 q = 107. Тогда n = p*q = 71*107 = 7597
2. Вычислим φn=p-1q-1=70*106=7420. Выберем открытый показатель – число e, которое взаимно просто с φn. Например e=4947.
3. Так численное представление данного сообщения больше выбранного модуля системы разделим его на блоки, каждый из которых кодируется по отдельности: 3018 – 1722 – 1028.
4. Применяем шифровальный ключ для каждого блока.
   E3018=30184947mod 7597=4715
   E1722=17644947mod 7597=1764
   E1028=10284947mod 7597=1033

Численное представление данного сообщения после шифрования выглядит так: 471517641033.

Попробуем декодировать блоки зашифрованного сообщения, следуя алгоритму.

1) Вычислим закрытый показатель d, предполагая, что нам известны числа φn и e. Пусть φn=m. Тогда НОД(e,

m) = 1 по условию о взаимной простоте чисел φn и e

Следуя обобщенному алгоритму, Евклида представим числа *m* и *n* в виде линейной комбинации: x*e+y*m=1 x,y-целые числа. x*4947+y*7420=1 x,y-целые числа.

Для решения этого уравнения воспользуемся общим алгоритмом для нахождения частного целого решение диофантового уравнения. x*4947+y*7420=1 x,y-целые числа. a=4947, b=7420=>b=p0*a+ r0; p0=1, r0=2473 a=p1*r0+r1;p1=2, r1=1=> 1=r1=a-p1*r0=a-p1b-p0*a=a-2b-1*a= =3a-2b=>x=3, y= -2.Найдя *x ,* находим d = φn+ x=7420+3=7423

2) Применяем дешифровальный ключ для каждого блока: D4715=47157423mod 7597=3018 D1764=17647423mod 7597=1722 D1033=10337423mod 7597=1028

В итоге мы получаем исходное число: 301817221028. Заменяя каждое из чисел на букву в соответствии с таблицей, получаем исходное сообщение: «ФИЗМАТ».

Из данного примера видно, что сведения из теории чисел, изучаемых в школе, а именно алгоритм решения диофантового уравнения, алгоритм Евклида и алгоритм Ферма, широко применяется для шифрования сообщений с помощью системы RSA.

В заключение этого параграфа расскажем о том, что стойкость шифров с открытым ключом, а в частности системы RSA, от взломов определяет наука, называемая теория сложности вычислений. Краткое знакомство с теорией сложности вычислений ограничивается классами P и NP и знаменитой гипотезой P≠NP.

Классом P называют множество задач, для которых существуют «быстрые» алгоритмы решения (время работы которых полиномиально зависит от размера входных данных).

Классом NP называют множество задач распознавания, решение которых при наличии некоторых дополнительных сведений (так называемого сертификата решения) можно «быстро» (за время, не превосходящее полинома от размера данных) проверить.

В конечном счете, проблема P = NP состоит в следующем: если положительный ответ на какой-то вопрос можно быстро проверить (за полиномиальное время), то правда ли, что ответ на этот вопрос можно быстро найти (за полиномиальное время и используя полиномиальную память)?

Гипотеза P≠NP является необходимым условием для существования стойких шифров. Однако, этой гипотезы недостаточно для существования стойких шифров, а именно, требуется предположение о существовании односторонних функций. Неформальное определение говорит о том, что односторонняя функция – это эффективно вычисляемая функция, для задачи инвертирования которой, не существует эффективных алгоритмов.

Данные предположения до сих пор не доказаны, но многолетний опыт использования шифров с открытым ключом показывает, что шифры с открытым

ключом на современных вычислительных системах не удастся разбить за время, при котором зашифрованное сообщение не потеряет свою актуальность.

2. Теория чисел и алгебраическая геометрия.

Из работы М. А. Цфасмана и В.В. Острика, я узнал, что многие естественные вопросы из теории чисел красиво решаются геометрическими методами, точнее говоря, методами алгебраической геометрии — области математики, изучающей кривые, поверхности, задаваемые полиномиальными уравнениями. Мы используем эти методы для получения шифров с открытым ключом, построенных на целочисленных точках этих кривых, но сначала рассмотрим решения некоторых задач.

2.1 Рациональные кривые.

Рассмотрим задачу на нахождение целых решений уравнения с помощью рациональных кривых. Приемы решения задач на рациональных кривых и на эллиптических кривых во многом похожи, но рациональные кривые по своей структуре проще, чем эллиптические.

Условие задачи.

Решить уравнение в целых числах:

X2+2Y2=3Z2

Решение.

Легко заметим, если Z=0, то X=0, Y=0. Это первое решение уравнения.

Найдем остальные решения данного уравнения.

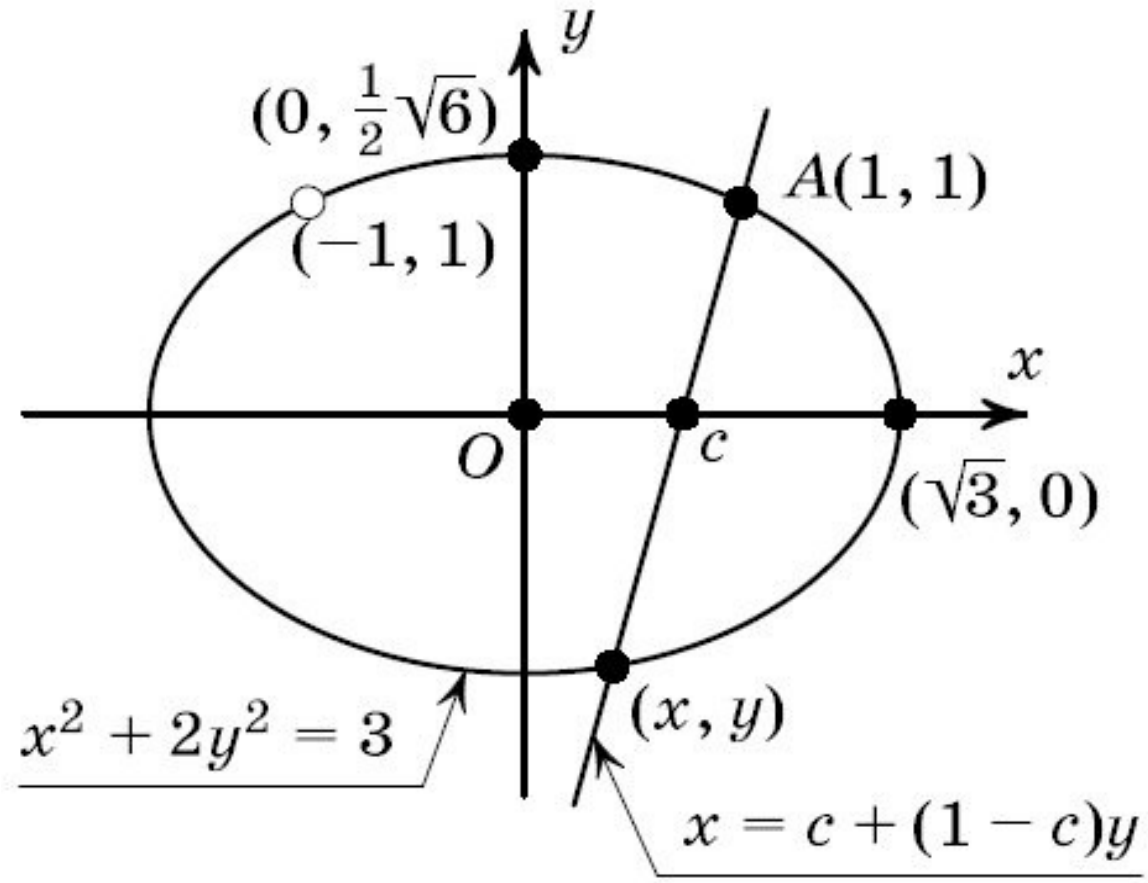
X2+2Y2=3Z2 | :Z2≠0;

XZ2+2*YZ2=3

Замена: XZ=x; yZ=y, где x,y- рациональные числа.

x2+2y2=3(×) - это уравнение эллипса с центром в точке O(0;0) и полуосями: x=3 и y=6/2

Решим уравнение × методом секущих. Найдем рациональную точку на эллипсе. Например, точка A(1,1).



Точку с координатами (-1,1) выкалываем, т.к. она с точкой вместе с точкой *A* лежит на горизонтальной прямой.

Выберем параметр, с помощью которого можно будет найти все решения уравнения. Этот параметр – точка с координатами (c,0).

Запишем уравнение прямой, проходящей через точки A1,1, c,0.

Эта прямая будет пересекать эллипс в точке x,y, координаты которой будут решением уравнения (X).

Уравнение прямой: y=kx+m. В нашем случае x=ky+m.

Получаем систему:

c=m+0*k1=k*1+m<=> c=mk=1-c=> x=1-c*y+c

Уравнение нашего эллипса - x2+2y2=3, уравнение прямой -

x=1-c*y+c. Эта прямая будет пересекать эллипс в точке x,y, следовательно, получаем уравнение:

*(1-c*y+c)2+2*y2=3*

y2*(1-c)2+2c*y*1-c+c2+2y2=3

y2*1-c2+2+2c*y*1-c+c2-3=0

Получили квадратное уравнение, у которого известен один корень – y1=1, т.к. прямая и эллипс проходят через точку A(1,1).

Второй корень уравнения найдем по теореме Виета.

y1+y2=-2c*1-c1-c2+2(1)y1*y2=c2-31-c2+2(2)

Рассмотрим уравнение (1):

*y1+y2=-2c*1-c1-c2+2,y1=1=>*

*y2=-2c*1-c1-c2+2-1=2c2-2c-c2+2c-3c2-2c+3=c2-3c2-2c+3*

Подставим y2 в уравнение прямой и получим решения для x
x=1-c*y+c=1-c*c2-3c2-2c+3+c=-c2+6c-3c2-2c+3
В итоге получаем решение уравнение (X):
x=-c2+6c-3c2-2c+3, y=c2-3c2-2c+3, где x,y,c-рациональные числа. (Также решением будет и точка (-1,1), через которую проходит горизонтальная прямая).

Представим параметр *c* в виде несократимой дроби:
c=mn, где m,n-целые числа. Тогда решение уравнения (X) принимает вид:
x=-mn2+6mn-3mn2-2mn+3=-m2+6mn-3n2m2-2mn+3n2
y=mn2-3mn2-2mn+3=m2-3n2m2-2mn+3n2
x,y-рациональные числа; m,n-целые числа.

Вернемся к замене:
x=XZx=-m2+6mn-3n2m2-2mn+3n2y=YZy=m2-3n2m2-2mn+3n2
Откуда получаем:
X=-m2+6mn-3n2*rY=(m2-3n2)*rZ=(m2-2mn+3n2)*r
где m,n-целые числа, а r-рациональное число, такое, что X,Y,Z – целые.

Ответ: X=-m2+6mn-3n2*r, Y=(m2-3n2)*r,
Z=(m2-2mn+3n2)*r, m,n-целые числа, а r-рациональное число, такое, что X,Y,Z – целые

2.2. Эллиптические кривые.

После того, как мы разобрали метод решения целочисленных задач на рациональных кривых, можно переходить к решению задач на эллиптических кривых.

Глоссарий.

Кривые третьего порядка могут иметь точку возврата или точку самопересечения, это точки являются примерами *особых точек*. Точка (x0,y0) на кривой Fx,y=0 называется *неособой,* если через нее проходит, хотя бы одна прямая x=x0+at , y=y0+at, такая что t=0 – корень уравнения Fx0+at , y0+at=0 кратности 1, а не больше. В противном случае точка (x0,y0) называется *особой*. [9]

Кривые, имеющие, хотя бы одну особую точку, называются *особыми*. Кривые, не имеющие особых точек, называются *неособыми* или *гладкими*.[6]

Неособые кривые третьего порядка, заданные уравнением с рациональными коэффициентами, называются *эллиптическими кривыми.*[6]

Теорема Ньютона[6].

Для любой неособой кубической кривой существует проективная замена координат, приводящая её в форму Вейерштрасса. Более того, если коэффициенты уравнения исходной кривой рациональны и на кривой имеется хотя бы одна рациональная точка, то можно найти проективную замену с рациональными αi,βi,γi (i=1,2,3), преобразующую исходную кривую в кривую в форме Вейерштрасса с рациональными *a* и *b.*

Кривой в форме Вейерштрасса, называется кубическая кривая на

плоскости *(x, y),* задаваемая уравнением вида: $y^2 = x^3 + ax + b$. [6]

Кривая в форме Вейерштрасса является особой тогда и только тогда, когда $4a^3 + 27b^2 = 0$. Число $\Delta = 4a^3 + 27b^2$ называется *дискриминантом кубической кривой*, а также дискриминантом кубического многочлена $x^3 + ax + b$. Если дискриминант $\Delta = 4a^3 + 27b^2$ уравнения $y^2 = x^3 + ax + b$ равен нулю, то эта кривая рациональна, если же дискриминант отличен от нуля, то кривая не является рациональной. Так же стоит отметить, что дискриминант кубического многочлена обращается в ноль тогда и только тогда, когда многочлен имеет кратный корень.[6]

Рассмотрим задачу, для решения которой можно воспользоваться свойствами эллиптических кривых.

Условие задачи.

Найти все пары натуральных чисел m и n, такие, что сумма первых m натуральных чисел равна сумме квадратов первых n натуральных чисел:
$1 + 2 + 3 + ... + m = 1^2 + 2^2 + 3^2 + ... + n^2$.

Решение.

Рассмотрим последовательность: $1 + 2 + 3 + ... + m$

$1 + 2 + 3 + ... + m$ – арифметическая прогрессия, такая что a1=1, d=1

Сумма арифметической прогрессии равна: Sa=a1+ am2*m, где m-номер нужного члена. Следовательно, сумма $1 + 2 + 3 + ... + m$ равна:

S=m(1+m)2.

Рассмотрим последовательность: $1^2 + 2^2 + 3^2 + ... + n^2$

Замечаем, что сумма членов находится по формуле:

S=nn+1(2n+1)6

Докажем наше предположение методом математической индукции.

Шаг 1.

n=1=>12=1=1*1+1(2+1)6=1

n=2=>12+ 22=5=2*2+1(4+1)6=5

n=3=>12+ 22+32=14=3*3+1(6+1)6=14

Шаг 2.

n=k=>12+ 22+ 32+ …+ k2=kk+1(2k+1)6

Шаг 3.

n=k+1=>12+ 22+ 32+ …+ k2+(k+1)2=

=kk+12k+16+k+12=

=kk+12k+1+6k2+12k+66=

=k+1(k2k+1+6k+1)6=k+1(2k2+7k+6)6

Разложим квадратное уравнение, 2k2+7k+6, на множители.

2k2+7k+6=0

D=49-48=1; k1=-2, k2=-1.5

2k2+7k+6=2k+2k+1.5=k+2(2k+3)

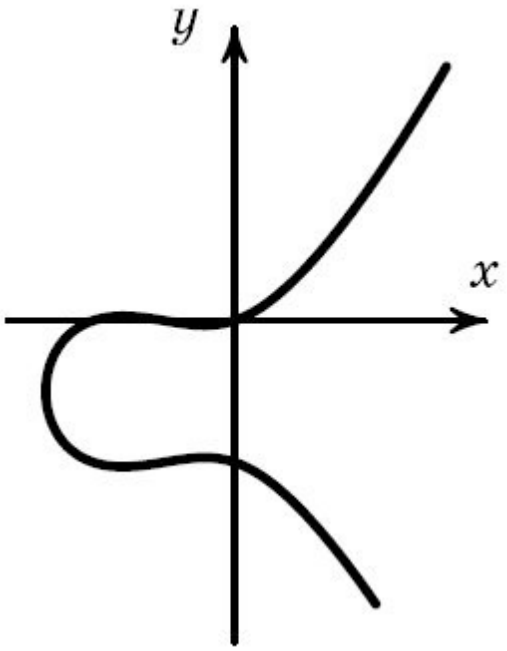
k+1(2k2+7k+6)6=k+1k+1+1(2k+2+1)6

k+1k+1+1(2k+2+1)6=k+1k+1+1(2k+2+1)6

Утверждение доказано.

После преобразований получаем, что наша задача эквивалентна решению в натуральных числах уравнения:

m(1+m)2=nn+1(2n+1)6.
Уравнение от двух переменных задает некоторую кривую на плоскости. Наше уравнение третьей степени, поэтому задает кривую третьего порядка.



$$\frac{y(y+1)}{2} = \frac{x(x+1)(2x+1)}{6}$$

Наша кривая не имеет особых точек, поэтому оно гладкая или эллиптическая.

На нашей кривой очень легко найти точку с целыми координатами, но метод секущих, в данном случае, не позволить решить уравнение, потому что какую бы мы не взяли прямую, она будет пересекать нашу кривую в трех точках. Конечно, все можно решить в случае особых кривых. Проводя секущие, через особую точку и применяя те же рассуждения, что и в случае с кривыми второго порядка, можно решить в рациональных числах уравнение с рациональными коэффициентами, задающее особую кривую. Однако, для метода секущих необходимо, чтобы начальная точка, а в нашем случае – особая точка, имела рациональные координаты.

Такой способ можно использовать для нахождения точек на особой кривой, а на эллиптической кривой, т.е. неособой кривой, для поиска точек используют особые свойства этой кривой, позволяющие с помощью проведения секущих и касательных “размножать” точки.

Для того чтобы воспользоваться свойствами неособой кривой нам нужно упростить ее, используя для этого проективную замену координат, т.е. замену вида:
x'=α1x+α2y+α3γ1x+γ2y+γ3, y'=β1x+β2y+β3γ1x+γ2y+γ3 ,γ12+γ22+γ32≠0
Проективная замена обратима в том случае, когда:

1) Обратная замена (т. е. замена, выражающая x и y через x' и y') тоже является проективной заменой координат
2) Последовательное применение двух обратимых проективных замен

эквивалентно некоторой одной такой замене.

Наша задача сделать такие проективные замены координат, чтоб рассматриваемая нами кривая стала кривой в форме Вейерштрасса. Так как наша кривая является неособой, то по теореме Ньютона мы можем привести ее к форме Вейерштрасса проективной заменой координат.

Производим проективную замену координат:

m=y-918, n=x-36

Проверяем, будет ли она приводить наше уравнение в форму Вейерштрасса.

m(1+m)2=nn+1(2n+1)6

m2+m2=2n3+3n2+n6

Выполняем замену.

y-9182+y-9182=2x-363+3x-362+x-366

y2-18x+81324+18y-1623242=x-36*(2x-362+3x-36+1)6

y2-81648=x-36*(x2-6x+918+9x-2718+1818)6

y2-81648=x-36*x2+3x186

y2-81=x3-9x

y2=x3-9x+81 – данное уравнение соответствует виду

$y^2 = x^3 + ax + b$. Значит, оно является уравнением в форме Вейерштрасса, и значит, что наше замена *m* и *n* верна.

Вычислим дискриминант получившегося уравнения.

$\Delta=4a^3 + 27b^2 = 4*-93+27*812=177147-2916=174231\neq0$=> полученная кривая не является особой, а полученное уравнение не имеет кратного корня.

Для нашей задачи необходимо найти все точки с целыми координатами на эллиптической кривой, но в нашем случае легче найти все точки с рациональными координатами и выбрать среди них точки с целыми координатами. Выше мы уже говорили, что точки на эллиптической кривой можно “размножать” методом секущих и касательных. Докажем это утверждение.

Доказательство. Рассмотрим эллиптическую кривую, заданную уравнением $y^2 = x^3 + ax + b$.

Предположим мы нашли на ней две точки с рациональными координатами, Pxp,yp и Q(xq,yq). Найдем уравнение прямой PQ:

yp=kxp+myq=kxq+m<=> m=yp-kxpk=yq-yprq-xp

Откуда получаем уравнение:

y=yq-yprq-xpx+ya-yq-yprq-xpxp

y-yprq-xp=x-xp(yq-yp)

Проведем прямую PQ и вычислим координаты третьей точки пересечения прямой с кривой. Эти координаты удовлетворяют системе уравнений:

y2=x3+ax+by-yprq-xp=x-xp(yq-yp)

Выразив *x* через *y* из второго уравнения, подставив получено выражение в первое уравнение, мы приходи к кубическому уравнению по y с рациональными коэффициентами. Два корня этого уравнения нам известны – это ординаты точек P и Q, у которых по условию координаты рациональны. Сумма трех корней также рациональное число, то по теореме Виета, третий корень тоже

рациональное число.
Что и требовалось доказать.

Итак, по двум рациональным точкам, лежащим на эллиптической кривой, можно получить третью точку с рациональными координатами. Еще одна точка с рациональными координатами получается построением точки симметрией относительно оси OX. Эта симметричная точка называется суммой точек P и Q и обозначается P+Q.

Свойства сложения точек такие же, как свойства сложения чисел.

1. Коммутативность (для любых точек P и Q эллиптической кривой выполняется тождество P+Q=Q+P)
2. Наличие нуля (существует такая точка 0, что P+0=0+P=P)
3. На эллиптической кривой для любой точки P находится противоположная точка. (-P+P=0=P+(-P))
4. Ассоциативность (для любых точке R,P,Q эллиптической кривой выполняется тождество R+P+Q=P+(Q+R))

Следует отметить, что для выполнения этих условий на эллиптической кривой введена точка - бесконечность . Считается, что точка ∞ есть точка пересечения всех вертикалей. Тем самым, добавив точку ∞=0, достигается такое свойство, что прямая, проходящая через точку ∞ и любую точку Q, – это вертикальная прямая, проходящая через точку Q. Из этого следует, что любая прямая пересекает эллиптическую кривую в трех точках, а значит, достигается возможность построить любой точке ей противоположную. Введение точки ∞ упростила достаточно громоздкую методику изучения эллиптических кривых.

После введения понятие «сложения точек» остается еще разрешить один вопрос прежде чем приступать к поиску рациональных точек на нашей эллиптической кривой. Этот вопрос заключается в следующем: возможно ли через две рациональные точки найти остальные? На этот вопрос дает ответ теорема Морделла. Согласно этой теореме, что все рациональные точки на эллиптической кривой получаются из конечного числа таких же точек с помощью проведения секущих и касательных. Из этой теоремы также следует, что любая эллиптическая кривая содержит конечное число целых точек.

Зная, что по двум точкам с рациональными координатами можно построить все остальные точки с рациональными координатами, мы можем решить нашу задачу.

Запишем уравнения нашей кривой:

y2=x3-9x+81

В качестве точек P1, P2 из теоремы Морделла можно взять точки с координатами (-3,9) и (0,9).

Теперь нашей задачей осталось найти рациональные точки и выделить среди них точки с целыми координатами.

Все целые точки нашей кривой имеют вид aP1+bP2, где $a,b \leq 13$ и a,b-целые числа

Для решения этой задачи можно использовать аналитический или геометрический метод. На практике, конечно же, используется аналитический метод, потому что его можно реализовать на компьютере. Суть данного метода

заключается в том, что координаты точек, полученных при проведении секущих и касательных можно записать в виде формул, а далее используя сведения, полученные с помощью теоремы Морделла, найти все нужные нам точки. Мы же применим геометрический метод, т.е. будем находить точки методом секущих и касательных.

Применим метод секущих и касательных для нахождения нескольких точек.

Найдем производную *F(x,y).*

y2=x3-9x+81

(y2)'=(x3-9x+81)'

y'=3x2-92y

Уравнение касательной yк=f'x0x-x0+f(x0)

В нашем случае:

yк=3x02-92(x03-9x0+81x-x0+(x03-9x0+81

Возьмем точки P1-3,9, P2 (0,9). Найдем уравнение прямой P1P2

9=0*k+m9=-3k+m< => m=9k=0=> эти точки лежат на одной горизонтальной прямой. Найдем точку пересечения с кривой прямой P1P2 .

y=9y2=x3-9x+81 <=> y=9x=0,±3

x=0, -3-точки с этими абсциссами нам уже известны

=>x=3=>y±(x3-9x+81)=±9

Получили точки P33,-9, -P3(3,9)

Возьмем точку P1-3,9 и найдем точку P1+P1=2P1

y'-3=27-918=1;yк=1*x+3+9=x+12

Получили систему уравнений.

y=x+12y2=x3-9x+81< = > y=x+12x2+24x+144=x3-9x+81

x2+24x+144=x3-9x+81

x3-x2-33x-63=0

x=7-корень (по т.Безу) т.к. 343-49-231-63=0

x3-x2-33x-63x-7=x2+6x+9

x2+6x+9=0;x=3-корень

x=7=>y=±(x3-9x+81)=±343-63-81=±19

Получили точки 2P1(7,-19) , -2P1(7,19).

Возьмем точку P20,9 и найдем точку P2+P2=2P2

y'0=-9/18=-0,5=>yк=-0.5x+9

y=-0.5x+9y2=x3-9x+81<= >y=-0.5x+981-9x+0.25x2=x3-9x+81

81-9x+0.25x2=x3-9x+81

x2x-0.25=0 => x=0,±0,5

x=0,5=>y=±(x3-9x+81)=±0,125-4.5+81 - не является целым числом, а значит, не удовлетворяет условиям задачи. При x=-0,5, y - так же не является целым числом, поэтому это решение не подходит.

Возьмем точки 2P1(7,-19) и P20,9 и найдем точку P4=2P1+P2

Найдем уравнение прямой 2P1P2.

*9=0*k+m-19=7k+m<=>m=9k=-4=>y=-4x+9*

Найдем точку пересечения прямой 2P1P2 с кривой.

y=-4x+9y2=x3-9x+81<=>y=-4x+981-72x+16x2=x3-9x+81

81-72x+16x2=x3-9x+81
x3-16x2+63x=0<=>xx2-16x+63=0;
x=0, 7, 9
x=0, 7-точки с этими абсциссами нам уже известны => x=9=>y=±(x3-9x+81)=±729-81+81=±27
Откуда получаем: P49,27, -P4(9,-27)

Возьмем точки P49,27, P20,9 и найдем точку P5=P4+P2.
Найдем уравнение прямой P4P2.
9=0*k+m27=9k+m<=>m=9k=2=>y=2x+9
Найдем точку пересечения прямой P4P2 с кривой.
y=2x+9y2=x3-9x+81<=>y=2x+94x2+36x+81=x3-9x+81
4x2+36x+81=x3-9x+81
x3-4x2-45x=0<=>xx2-4x-45=0 => x=0, 9, -5.
x=0, 9-точки с этими абсциссами нам уже известны => x=-5=>y=±(x3-9x+81)=±-125+45+81=±1
Откуда получаем P5-5,-1,-P5-5,1

Зная, что все целые точки нашей кривой имеют вид aP1+bP2, где a,b≤13 и a,b-целые числа, методом секущих и касательных можно найти все точки с рациональными координатами и отобрать из точки с целыми координатами. Однако данный способ очень громоздкий, т.к. количество точек с рациональными координатами велико, поэтому реализовать его для нахождения всех точек очень тяжело. Исходя из этого, мы приводим решение данной задачи, которое получено ее авторами с помощью компьютера.

Вот абсциссы точек, с целыми координатами: -5, -3, 0, 3, 7, 9, 24, 33,3 9, 513, 1099, 5112.

Среди этих абсцисс нужно выбрать такие, которые удовлетворяют условию задачи, т.е. таких при которых
m=y-918 и n=x-36 натуральные числа.

Подставляя значения координат точек в данные уравнения, получаем пары m,n:1,1, 10,5,13,6,645,85.
Ответ: пары натуральных чисел m и n, таких, что сумма первых *m* натуральных чисел равна сумме квадратов первых n натуральных чисел, равны 1,1, 10,5,13,6,645,85.

Решая данную задачу, мы смогли поближе познакомиться с эллиптическими кривыми, что позволить нам понять алгоритм построения шифров с открытым ключом на эллиптических кривых.

В завершение данного параграфа хотелось бы рассказать о том, что кривые третьей степени были обнаружены и проклассифицированы еще Ньютоном. Данные кривые применялись для решения многих проблем, но создавать шифры с их помощью начали совсем недавно. Сейчас эллиптическими кривыми и вообще алгебраической геометрией занимается

множество ученых. В первую очередь это связно с тем, что совсем недавно с помощью эллиптических кривых Эндрю Уайлс смог доказать Великую теорему Ферма, доказать которую не могли более трех веков.

3. Криптосистемы на эллиптических кривых.

В последнее время одна из областей теории чисел и алгебраической геометрии - эллиптические кривые – нашла применение в криптографии.

Глоссарий.

Поле – это множество F с операциями сложения и умножения, которые удовлетворяют обычным правилам: умножение и сложение ассоциативны и коммутативны; существует нейтральный элемент для сложения (0) и для умножения (1); существует обратный элемент для сложения и обратный ненулевой элемент для умножения.

Конечно поле – это конечное множество, которое обладает теми же свойствами, что и поле.

Абелева группа – это группа, у которой для любых элементов $a,b \in G$ (G – множество чисел) выполняется условия: произведение двух ненулевых элементов – не ноль: выполняется ассоциативный и коммутативный законы, существует единичный элемент 1 и любой ненулевой элемент имеет обратный.

Ранее мы уже отмечали, что сумма любых двух точек, принадлежащих эллиптической кривой, обладает всеми свойствами абелевой группы. Также теорема Морделла, о которой было сказано выше, утверждает, что точек с целыми и рациональными координатами на эллиптической кривой конечное количество. Из этих двух замечательных свойств видно, что основная причина широкого применения эллиптических кривых в криптографии состоит в том, что эллиптические кривые над конечными полями предоставляют огромное количество конечных абелевых групп, которые удобны для вычисления и обладают богатой структурой, а возможность размножение точек, принадлежащим эллиптическим кривым, предоставляют возможность составлять некоторое подобие односторонних функций.

Ранее нами был рассмотрен один из шифров с открытым ключом – шифр RSA. На эллиптических кривых также строят криптосистемы с открытым ключом. Рассмотрим один из методов построение таких криптосистем.

3.1 Метод Эль – Гамаля.

Пусть точка P_m - сообщение, которое необходимо зашифровать (например, она означает какую-нибудь букву английского алфавита).

Несекретными данными являются:

1) Конечное поле F_q;
2) Определенная над ним эллиптическая кривая *E;*
3) Точка-“основания” B.

Отправитель и получатель берут случайное целое число *a*, которое держат в секрете. Отправитель и получатель находят и делают общедоступной точку *aB*. Обозначим *kB* точку B, после того как отправитель умножил ее на свое

секретное число, и обозначим *nB* точку B, после того как получатель умножил ее на свое секретное число.

Чтобы послать сообщение P_m, отправитель посылает пару точек: (kB;Pm+ knB).

Чтобы прочитать сообщение, получатель умножает первую точку из полученной пары на свое секретное число *n* и вычитает результат умножения из второй точки: Pm+knB-nkB=Pm

Таким образом, отправитель посылает замаскированное сообщение P_m вместе с "подсказкой" *kB* , при помощи которой можно снять маску *knB*, если знать секретное число *n*.

3.2. Реализация метода Эль-Гамаля.

Возьмем эллиптическую кривую y2=x3-9x+81, определенную над конечным полем, которое состоит из остатков от деления целых чисел на число 149.

y2=x3-9x+81 (mod 149);

Точка B0;9 – точка-"основания". Точка P9;27- сообщение.

Пусть отправитель выбрал секретное целое число *k=100,* а получатель выбрал секретное целое число *n=250.*

Находить точки *kB* и *nB* вручную очень долгое занятие, поэтому мы воспользуемся формулами, которые очень легко получаются из правил сложения точек на эллиптической кривой, и реализуем их в компьютерной программе, которую можно написать на любом языке программирования. Мы написали свою программу на языке Pascal. Ниже мы приводим формулы, которые реализовали в программе.

Пусть нам даны две точки Px1;y1 и Q(x2;y2). Координаты точки P+Q (x3;y3) находятся по формуле:

x3=y2-y1x2-x12-x1-x2; y3=y2-y1x2-x1x1-x3-y1;

Координаты точки 2P(x3;y3) находятся по формуле:

x3=3x12+a2y12-2x1; y3=3x12+a2y1x1-x3-y1;

где a – коэффициент при x.

В нашем случае следует все операции выполнять по модулю 149.

Находим точку, которую вычисляет отправитель, *kB=100B.* Для того чтобы реализовать формулы, нужно разложить точку *100B* в виде:

*100B=2*2*2*2*2B+2B+B.* Откуда получаем: *100B (66;3).*

Находим точку, которую вычисляет получатель, *nB=250B.* Для этого представляем точку *250B* в виде:

250B=2*2*2*2*2*2B+2B+B+2*2*2*2B+2B+B.

Откуда получаем: *250B (64;68).*

Находим точку *k(nB)=100*(250B).* Так же как и в предыдущие разы раскладываем точку *100*(250B)* в виде:

100*250B=2*2*2*2*2250B+2*250B+B. Откуда получаем точку *100*(250B) (69;13).*

Шифруем наше сообщение, складывая точки P9;27 и *100*(250B) (69;13)* , получаем точку P+knB *(104;20).*

В итоге отправитель посылает пару точек: ((66;3); (104;20)).

Приняв отправленную пару точек, получатель находить точку *n(kB) = 250*(100B),* где *100B* (66;3) . Для этого снова раскладываем точку *250*(100B)* в виде:

250*100B=2*2*2100B+2*100B+100B*2*2*2+2*

*2*2*2100B+2*100B+100B.

Откуда получаем точку *250*(100B) (69;13).*

Следует отметить, что координаты точки *n(kB)* равны координатам точки *k(nB),* что следует из правила коммутативности. Но так как получатель не знал точки *k(nB),* ему пришлось ее находить.

Так как координаты точек *n(kB)* и *k(nB)* равны то, для того чтобы найти сообщение *P.* Нужно вычесть из второй полученной точку *n(kB)*: P+knB-nkB=P.

Координаты точки -nkB (69;136): , координаты остальных точек нам известны.

В итоге получаем P+knB-nkB=P (9;27).

Полученное сообщение расшифровано.

Заключение

В учебно-исследовательской работе мы рассмотрели два вида проблем: учебную – связанную с подготовкой к решению одного из труднейших заданий ЕГЭ, задания С6, и исследовательскую – о возможном применении различных результатов и методов теории чисел и алгебраической геометрии в математической криптографии, от известных 2,5 тыс. лет (алгоритм Евклида для нахождения НОД) до самых современных методов алгебраической геометрии, появившихся в последнем десятилетии XX века (теорема Морделла).

Для взлома шифров, полученных этими методами пока нет алгоритмов, разбивающих их за полиномиальное время, т.е. реально реализуемых на современных ЭВМ. Но уже в конце XX века стало понятно, что есть возможность сделать эти задачи практически решаемыми на новых принципах, связанных с квантовыми вычислениями и квантовыми компьютерами. Я хотел бы продолжить знакомство с криптографией, но уже начать изучать методы квантовой криптографии, которые в последние годы начинают разрабатывать. Создать достаточно мощные и стабильно работающие квантовые компьютеры ученым пока не удалось, но их создание не за горами. Поэтому мне интересно понять, какие задачи будут сложны для решения на этих компьютерах, чтобы они смогли послужить основой для новых квантовых шифров.

Список литературы.

1. Жафяров А. Ж. Математика. ЕГЭ 2010. Экспресс-консультация.– Новосибирск: Сиб. Унив. Изд-во, 2010.
2. Корянов А.Г. Математика ЕГЭ 2010. Задача С6. Интернет-издание. (akoryanov@mail.ru)
3. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. Москва: Постмаркет, 2001.
4. Коблиц Н. Курс теории чисел и криптографии. Москва: Научное изд-во ТВП, 2001.
5. Мордкович А.Г. , Семенов П.В. Алгебра и начала математического анализа. 10 класс. В 2 ч. Ч.1. Учебник (профильный уровень). – М: Мнемозина, 2005.
6. Острик В. В., Цфасман М. А.

Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые

(Серия: «Библиотека „Математическое просвещение"») М.: МЦНМО, 2001.

7. Сергеев И.Н. МАТЕМАТИКА. Задачи с ответами и решениями: Пособие для поступающих в вузы. – М: КДУ, 2004. – 2-е изд., доп.
8. Введение в криптографию / Под общей ред. В.В. Ященко. – СПб.: Питер, 2001.
9. ЕГЭ 2011. Математика. Типовые текстовые задания / под ред. А. Л. Семенова, И.В. Ященко. – М.: Издательство «Экзамен», 2011.
10. ЕГЭ – 2011. Математика: типовые экзаменационные варианты : 30 вариантов / под ред. А. Л. Семенова, И. В. Ященко. – М.: Национальное образование, 2010.
11. ЕГЭ 2011. Математика. Задача С6. Арифметика и алгебра. Пратусевич М.Я. и др / Под ред. А. Л. Семенова и И. В. Ященко. – М.: МЦНМО, 2011.
12. Сайт Википедия. ru.wikipedia.org.