Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра геометрии

Группа точек эллиптической кривой.

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления ***02.03.01 – Математика и компьютерные науки***

механико-математического факультета

АТКИНА КИРИЛЛА СТАНИСЛАВОВИЧА

Научный руководитель
Доцент, к.ф.-м.н _____ Новиков В.Е.
подпись, дата

Зав. кафедрой
доктор физ.-мат. наук, профессор _____ Розен В.В.
подпись, дата

Саратов 2018

Введение.

В центре внимания современной абстрактной математики и сфер ее приложения находятся различные алгебраические структуры, среди которых не последнее место занимают группы. Группы, по существу, являются одним из основных типов алгебраических структур. Теория групп нашла свое применение в областях, связанных с изучением объектов самого разного происхождения с точки зрения общих свойств их структуры. Группы возникают во всех областях математики, и методы теории групп оказывают сильное влияние на многие разделы алгебры. Построение групп возможно и на геометрических объектах, в частности и на множестве точек кривых.

В данной работе речь пойдет об образовании группы на множестве точек эллиптической кривой. Эллиптические кривые — это кривые, выведенные, благодаря труду Ньютона И. (1642-1727 гг.) по классификации кривых третьего порядка. Их исследование, в конечном счете, привело к появлению формул сложения точек на эллиптической кривой.

Цель данной работы рассмотреть возможность образования группы на множестве точек эллиптической кривой и ее приложения в сфере защиты информации.

Задачи:

1. Дать определение эллиптической кривой
2. Рассмотреть операцию сложения точек на эллиптической кривой
3. Показать, что точки эллиптической кривой образуют группу
4. Рассмотреть применение группы точек эллиптической кривой в сфере защиты информации
5. Построить алгоритм ЭЦП с применением группы точек эллиптической кривой

Во введении обозначена причина заинтересованности данной тематикой, упомянуто историческое развитие данного вопроса, определены цели и задачи.

В первой части работы «Кривые 3-его порядка» даются определения алгебраической кривой, кривой третьего порядка, приведена классификация кривых третьего порядка, определенная Ньютоном, а так же рассмотрена 5-ая группа в этой классификации, из которой и выводятся эллиптические кривые.

Во второй части работы «Эллиптические кривые» кривые рассматриваются над произвольным полем F. Дано определение эллиптической кривой над произвольным полем F. Дана классификация эллиптических кривых относительно характеристики конечных полей, над которыми они заданы. Также приведены требования предъявляемые к эллиптическим кривым и графики некоторых эллиптических кривых.

В третьей части «Группа точек эллиптической кривой над полем $\mathbb{R}$» задана операция сложения точек эллиптической кривой, образующая на точках кривой группу, ее геометрическое представление и выведены арифметические формулы для данной операции. А также дано представление о точке в бесконечности.

Четвертая часть «Эллиптические кривые над конечным полем», рассматриваются выведенные в предыдущей части арифметические формулы операции сложения точек в понятиях характеристики конечных полей. Определена операция скалярного умножения точки эллиптической кривой на число k, понятие порядка точки кривой и порядка кривой, а также определена проблема поиска порядка кривой.

Пятая часть «Алгоритмы на эллиптических кривых» состоит из двух разделов, в которых излагаются методы приложения группы точек эллиптической кривой в области сфере защиты информации — криптографии. Дано представление о требованиях предъявляемых к эллиптическим кривым при построении криптосистем, определены параметры кривой для представления в компьютере. Приведены в виде псевдокода алгоритмы сложения точек над полем характеристики большого простого числа, характеристики три и характеристики два для случая несуперсингулярных кривых, а также выведены арифмитические формулы для операций в соответствующих алгоритмах. Приведен алгоритм построения ЭЦП при помощи группы точек эллиптической кривой.

В шестой части «Реализация ЭЦП с помощью эллиптических кривых» дается информация о параметрах кривой использованной при построении ЭЦП.

В заключении перечисляется ключевые моменты проделанной работы.

Также к разбору основной темы прилагается часть работы, посвященная введению определений, необходимых для понимания разбираемого материала, связанного с алгеброй и, в особенности, с рассматриваемой в работе областью приложения группы точек эллиптической кривой — криптографии.

Бакалаврская работа состоит из введения, 6 частей, заключения, списка использованных источников и трех приложений. Общий объем работы — 50 страниц, из них 27 страниц — основная часть, насчитывающая 9 рисунков и список использованных источников из 10 наименований.

1 Основное содержание работы.

В первой части даются вводные понятия из учения о кривых необходимые для определения эллиптических кривых.

Определение 1.1. *Кривой третьего порядка называется множество точек* (x, y)*, удовлетворяющих уравнению вида:*

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 + 3ex^2 + 6fxy + 3gy^2 + hx + iy + k = 0 \qquad (1.1)$$

Кривая третьего порядка также называется кубическим многочленом.

Рассмотрим способ классификации кривых на группы в зависимости от количества и характера бесконечных ветвей, полученное Ньютоном.

Пусть $y = \alpha x + \beta$ — уравнение асимптоты кривой. Для нахождения параметров α и β необходимо подставить в уравнение кривой правую часть уравнения асимптоты — выражение $\alpha x + \beta$ на место y. В полученном таким образом уравнении необходимо взять коэффициенты двух членов со старшими степенями x и приравнять их нулю. При этом получится система с неизвестными α и β, из которой выводятся равенства определяющие их.

Для кривой 1.1 угловой коэффициент α определится равенством:

$$a + 3b\alpha + 3c\alpha^2 + d\alpha^3 = 0 \qquad (1.2)$$

А второй параметр асимптоты — ее начальная ордината β — определится равенством:

$$(b + 2c\alpha + d\alpha^2)\beta = -(e + 2f\alpha + g\alpha^2) \qquad (1.3)$$

где α имеет соответствующее значение из 1.2

Количество бесконечных ветвей кривой 1.1 зависит от числа действительных корней уравнения 1.2, в то время как характер ветвей определяется равенством 1.3. Заметим, что очевидно, что параметр β не определяется уравнением 1.3, если одновременно выполняются условия:

$$b + 2c\alpha + d\alpha^2 = 0 \qquad (1.4)$$

$$e + 2f\alpha + g\alpha^2 \neq 0 \qquad (1.5)$$

или

$$b + 2c\alpha + d\alpha^2 = 0 \qquad (1.6)$$

$$e + 2f\alpha + g\alpha^2 = 0 \tag{1.7}$$

На основе получаемых вариаций сочетаний количества корней α и условий существования/несуществования β Ньютон подразделил все кривые третьего порядка на 7 групп, каждая из которых имеет характерные формы кривых. Рассмотрим 5-ую группу.

Кривые этой группы называются расходящимися параболами, а общее уравнение кривой в этом случае сводится к виду:

$$y^2 = ax^3 + bx^2 + cx + d$$

Основные формы кривых этой группы определяются видом корней вспомогательного уравнения:

$$ax^3 + bx^2 + cx + d = 0 \tag{1.8}$$

В зависимости от решения вспомогательного уравнения, различают следующие случаи:

1. если уравнение 1.8 имеет один действительный корень, то кривая состоит из одной бесконечной ветви параболического типа

2. если корни уравнения 1.8 действительны и различны, то кривая состоит из параболической ветви и овала Рис. 1

3. если все корни уравнения 1.8 действительны и среди них два больших корня равны между собой, то кривая состоит из параболической ветви, имеющей узловую точку Рис. 3

4. если все корни 1.8 действительны и среди них два меньших корня равны между собой, то кривая состоит из параболической ветви, имеющей изолированную точку

5. если все корни уравнения 1.8 равны между собой, то кривая представляет собой параболическую ветвь, имеющую точку возврата

Во второй части задается определение эллиптической кривой над полями различных характеристик.

Все данные в предыдущей части определения, касающиеся кривой третьего порядка справедливы и аналогичны для произвольного поля F.

Определение 1.2. *Пусть F — поле характеристики отличной от 2, 3 и $x^3 + ax + b$ — кубический многочлен без кратных корней, где $a, b \in F$. Эллиптическая кривая над F — это множество точек (x, y), где $x, y \in F$, удовлетворяющих уравнению:*

$$y^2 = x^3 + ax + b \tag{1.9}$$

вместе с единственным элементом, обозначаемым O называемым точка в бесконечности. Уравнение вида 1.9 называется уравнением Вейерштрасса.

Если F — поле характеристики 2, то эллиптическая кривая над F — это множество точек, удовлетворяющих уравнению либо вида (суперсингулярные кривые):

$$y^2 + cy = x^3 + ax + b \tag{1.10a}$$

либо вида (несуперсингулярные кривые):

$$y^2 + xy = x^3 + ax^2 + b \tag{1.10b}$$

(здесь кубические многочлены в правых частях могут иметь кратные корни), вместе с точкой в бесконечности O

Если же F — поле характеристики 3, то:

$$y^2 = x^3 + ax^2 + bx + c \tag{1.11}$$

(здесь кубический многочлен справа не имеет кратных корней), вместе с точкой в бесконечности O

Определение эллиптической кривой также требует, чтобы кривая не имела особых точек (каспов, точек многократного пересечения, изолированных точек и т.п.).

Замечание 1.1. *1. Имеется общая форма уравнения эллиптической кривой, применимая при любом поле:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.12}$$

в случае когда $F \neq 2$, ее можно привести к виду $y^2 = x^3+ax^2+bx+c$ ($y^2 = x^3 + bx + c$, если $F > 3$). В случае, когда поле F имеет характеристику 2, это уравнение преобразуется либо к виду 1.10a, либо к виду 1.10b

2. *Если $F(x, y) = y^2-x^3-ax-b$ (или $F(x, y) = y^2+cy+x^3+ax+b, F(x, y) = y^2 + xy + x^3 + ax + b, F(x, y) = y^2 - x^3 - ax^2 - bx - c$), то точка (x, y)*

этой кривой называется неособой (или гладкой) точкой, если, по крайней мере, одна из частных производных $\dfrac{\partial F}{\partial y}$, $\dfrac{\partial F}{\partial x}$ *в этой точке не равна нулю.*

В случае, когда характеристика поля не равна 2 или 3 алгебраически отсутствие неособых точек выражается через соблюдение условия неравенства нулю дискриминанта, т.е. $4a^3 + 27b^2 \neq 0$.

Определение 1.3. *Кривая называется неособой (или гладкой), если все ее точки неособые. Т. е. в любой из точек* (x, y) *к ней можно провести касательную, т. е. прямую, определяемую уравнением*

$$(X - x)\frac{\partial F}{\partial X}\bigg|_{(X,Y)=(x,y)} + (Y - y)\frac{\partial F}{\partial Y}\bigg|_{(X,Y)=(x,y)} = 0$$

Ниже представлены различные варианты графиков эллиптических кривых.

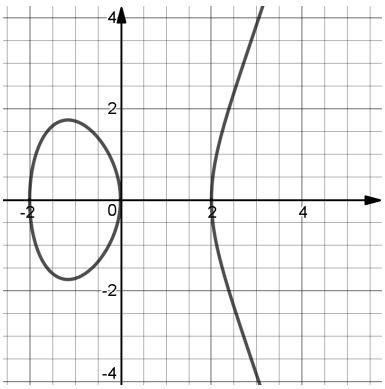

Рис. 1. $y^2 = x^3 - 4x$

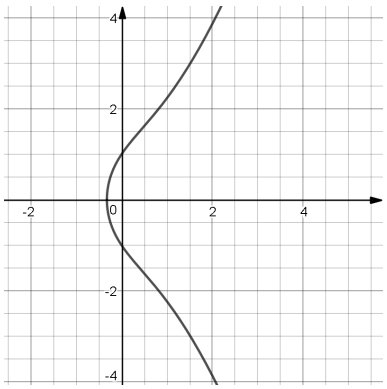

Рис. 2. $y^2 = x^3 + 2x + 1$

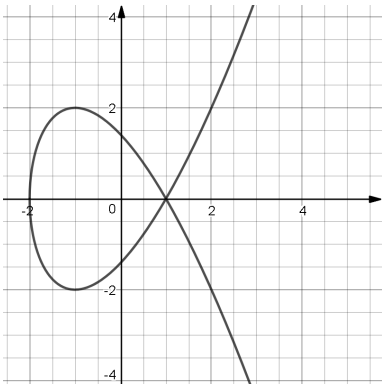

Рис. 3. $y^2 = x^3 - 3x + 2$

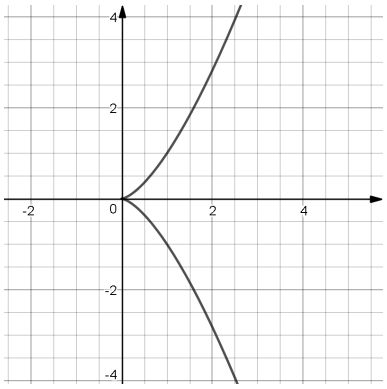

Рис. 4. $y^2 = x^3$

В третьей части задается операция сложения точек эллиптической кривой, образующая на их множестве группу и выводятся арифметические формулы для данной операции.

Принято получающуюся при этом группу рассматривать как аддитивную группу, а операцию называть операцией сложения и обозначать знаком плюс. Уже упомянутая выше точка в бесконечности выполняет здесь роль нейтрального элемента (нуля) этой группы и обозначается O. По определению, полагаем для любой точки $(x, y) \in E(F)$

$$(x, y) + O = O + (x, y) = (x, y), \quad O + O = O.$$

Определение 1.4. *Пусть E — эллиптическая кривая над вещественными числами, и пусть P и Q — две точки на E. Определим точки $-P$ и $P+Q$ по следующим правилам:*

1. *O — нейтральный элемент по сложению т.е. нулевой элемент группы точек. Т. о. если P — точка в бесконечности $O(P = O)$, то $-P = O$ и $P + Q = Q$. В следующих пунктах предполагается, что ни P, ни Q не являются точками в бесконечности.*

2. *Точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, а их y-координаты различаются только знаком, т.е. $-(x, y) = (x, -y)$. Заметим, что из 1.9 очевидно следует, что $(x, -y)$ — также точка на E.*

3. *Если P и Q имеют различные x-координаты, то прямая $l = \overline{PQ}$ имеет с E в точности еще одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P (в случае чего мы полагаем $R = P$), или касательной в Q (в это случае полагаем $R = Q$)). Определяем теперь $P + Q$ как точку $-R$, т.е. как отражение от оси x третьей точки пересечения.*

4. *Если $Q = -P$ (т.е. x-координата Q та же, что и у P, а y-координата отличается лишь знаком), то полагаем $P + Q = O$ (точке в бесконечности; это является следствием пункта 1).*

5. *Остается возможность равенства $P = Q$. Тогда считаем, что l — касательная к кривой в точке P. Пусть R — единственная другая точка пересечения l с E. Полагаем $P + Q = -R$ (в качестве R берем P, если касательная прямая в точке P имеет двойное касание, т.е. если P есть точка перегиба кривой).*

Приведем пример геометрического построения суммы точек эллиптической кривой. На Рис. 5 изображены эллиптическая кривая $y^2 = x^3 - x$ в плоскости $X0Y$ и типичный случай сложения точек P и Q. Чтобы найти $P+Q$, проводим прямую $\overline{PQ}$ и в качестве $P+Q$ берем точку, симметричную относительно оси x третьей точке R, определяемой пересечением прямой $\overline{PQ}$ и кривой.

Возможен также и случай, когда точка $Q = -P$. Построение суммы $P+Q$ для этого случая показано на Рис. 7.

Если бы P совпадала с Q, т.е. если бы нам нужно было найти $2P$, мы использовали бы касательную к кривой в P; тогда точка $2P$ симметрична третьей точке, в которой эта касательная пересекает кривую. Данная ситуация изображена на Рис. 6.

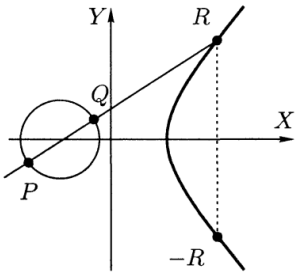

Рис. 5. $P \neq Q$

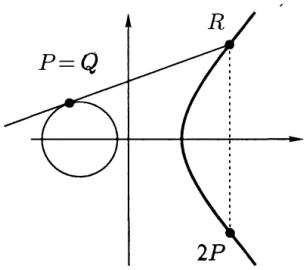

Рис. 6. $P = Q$

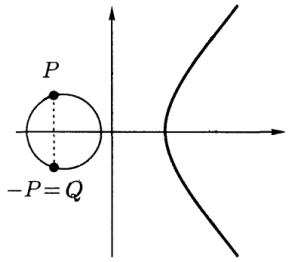

Рис. 7. $Q = -P$

Теперь покажем, почему существует в точности еще одна точка, где прямая l, проходящая через P и Q, пересекает кривую; также введем формулу для координат третьей точки и тем самым для координат $P+Q$

Пусть (x_1, y_1), (x_2, y_2) и (x_3, y_3) обозначают координаты соответственно P, Q и $P+Q$. Необходимо выразить x_3 и y_3 через x_1, y_1, x_2, y_2. Предположим, что x-координаты P и Q различны, и пусть $y = \alpha x + \beta$ — это уравнение прямой l, проходящей через P и Q (в этой ситуации она не вертикальна). Тогда $\alpha = \dfrac{y_2 - y_1}{x_2 - x_1}$ и $\beta = y_1 - \alpha x_1$. Точка на l, т.е. точка $(x, \alpha x + \beta)$, лежит на эллиптической кривой тогда и только тогда, когда $(\alpha x + \beta)^2 = x^3 + ax + b$. Таким образом, каждому корню кубического многочлена $x^3 - (\alpha x + \beta)^2 + ax + b$ соответствует точка пересечения. Мы уже знаем, что имеется два корня x_1 и x_2, так как $(x_1, \alpha x_1 + \beta), (x_2, \alpha x_2 + \beta)$ — точки P, Q на кривой. Так как сумма корней нормированного многочлена, по теореме Виета, равна взятому с обратным знаком коэффициенту при второй по старшинству степени многочлена, то в нашем слу-

чае третий корень — это $x_3 = \alpha^2 - x_1 - x_2$. Тем самым получаем выражение для x_3, и, следовательно, $P + Q = (x_3, -(\alpha x_3 + \beta))$ или, в терминах x_1, y_1, x_2, y_2:

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 &= -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) \end{aligned} \tag{1.13}$$

Ситуация, когда $P = Q$ аналогична, только теперь α — производная $\dfrac{dy}{dx}$ в P. Дифференцирование неявной функции, заданной уравнением 1.9, приводит к формуле $\alpha = \dfrac{3x_1^2 + a}{2y_1}$, и мы получаем следующие формулы для координат удвоенной точки P:

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \\ y_3 &= \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1 \end{aligned} \tag{1.14}$$

Принятое выше определение $P + Q$ превращает множество точек на эллиптической кривой в абелеву группу.

В четвертой части кривые рассматриваются над полями конечной характеристики.

В этом разделе будем полагать, что F — конечное поле F_q с $q = p^r$ элементами. Пусть E — эллиптическая кривая, определенная над F_q. Если $p = 2$ или $p = 3$, то E задается уравнением вида 1.10a, 1.10b или 1.11 соответственно. Все математические операции на эллиптических кривых над конечным полем производятся по законам конечного поля над которым построена кривая.

$$P + Q = R \equiv (x_3, y_3)$$

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \pmod p, \\ y_3 &= \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1 \pmod p \end{aligned} \tag{1.15}$$

$$\begin{aligned} \alpha &= \frac{y_2 - y_1}{x_2 - x_1} \pmod p,\ P \neq Q, \\ \alpha &= \frac{3x_1^2 + a}{2y_1} \pmod p,\ P = Q \end{aligned} \tag{1.16}$$

Т. к. для группы точек эллиптических кривых определена операция сложения, то не составит труда определить скалярное умножение числа k на точку P как сумму: $\underbrace{P + P + \cdots + P}_{k}$.

Порядок группы точек эллиптической кривой будем отождествлять с порядком эллиптической кривой.

Определение 1.5. *Порядком n точки P на эллиптической кривой называется такое наименьшее натуральное число, что $nP = O$;*

В пятой части рассматриваются алгоритмы необходимые для построения протоколов на эллиптических кривых, а также параметры которыми задаются кривые и требования предъявляемые при их построении.

Эллиптическая кривая определяется константами a и b из уравнения 1.9. Группа точек выбранной кривой является абелевой циклической группой и задается одной порождающей точкой G. При этом также должно соблюдаться условие, что величина, равная отношению порядка кривой к порядку n точки G, $h = \dfrac{|E|}{n}$ и называемая кофактором, должна быть небольшой $h \leq 4$ (лучше если $h = 1$).

Получаем для поля $GF(2^m)$ характеристики 2 набор параметров вида:

$$(m, f, a, b, G, n, h)$$

а для конечного поля F_p, где $p > 3$, набор параметров вида:

$$(p, a, b, G, n, h)$$

Также к эллиптическим кривым предъявляются следующие требования:

1. Кривые рассматриваются или над простыми полями (порядок q которых равен простому числу p), или над полями характеристики 2 ($q = 2^m$).

2. Кривая E задается выбором двух элементов a и $b \in GF(q)$. В случае $p > 2$

имеет вид 1.9; в случае $p = 2$ имеет вид 1.10b. Т. о. стандарт рекомендует только несуперсингулярные кривые.

3. На кривой выбирается точка G с координатами $(x_G, y_G),\ x_G, y_G \in GF(q)$ простого порядка $N > 2^{160},\ N > 4\sqrt{q}$, и как уже было сказано выше, вычисляется кофактор $h = \dfrac{|E(GF(q))|}{N}$.

В этой части работы приведены пошаговые схемы некоторых алгоритмов сложения и удвоения точек, без которых построение криптосистем на эллиптических кривых немыслимо (фактически будет облачена в форму алгоритма информация уже полученная ранее). А так же будет дана схема алгоритма ЭЦП на эллиптических кривых.

Координаты точек $-(x_3, y_3)$ вычисляются по формулам 1.13. В зависимости от вида эллиптической кривой и условия различия или совпадения точек, существует несколько алгоритмов вычисления координат точки R. Далее рассмотрим некоторые из них.

Алгоритм сложения и удвоения для эллиптических кривых над полем большой характеристики:

Вход: Коэффициент a эллиптической кривой, точки $P = (x_1, y_1)$(или $P = O$) и $Q = (x_2, y_2)$(или $Q = O$)

Выход: $R = P + Q$.

1: Вычислить:
2: **если** $P = O$ **то**
3: вернуть $R = Q$,
4: **если** $Q = O$ **то**
5: вернуть $R = P$,
6: **если** $Q = -P$ **то**
7: вернуть $R = O$,
8: **если** $x_1 \neq x_2$ **то**
9: вычислить $\alpha = \dfrac{y_1 + y_2}{x_1 + x_2},\ x_3 = \alpha^2 - x_1 - x_2$.
10: вернуть $P = (x_3, -y_1 + \alpha(x_1 - x_3))$
11: **иначе**
12: принять $x = x_1, y = y_1$,
13: вычислить $\alpha = \dfrac{3x^2 + a}{2y},\ x_3 = \alpha^2 - 2x$,
14: вернуть $(x_3, -y + \alpha(x - x_3))$

Для реализации алгоритма ЭЦП, была выбрана кривая со следующими параметрами.

- $p = 6277101735386680763835789423207666416083908700390324961279$;
- $a = -3$;
- $b = 245515554600894381774029391519745178476910805816119123806 5$;
- $x_G = 602046282375688656758213480587526111916698976636884684818$;
- $y_G = 174050332293622031404857552280219410364023488927386650641$;
- $n = 6277101735386680763835789423176059013767194773182842284081$;
- $h = 1$

где, p— порядок эллиптической кривой, a и b — коэффициенты из уравнения кривой, x_G и y_G — соответствующие координаты образующей точки G, n — порядок точки G, h — величина кофактора.

Код и скриншот с результатами работы программы приведен в приложении к бакалаврской работе.

2 Заключение.

В бакалаврской работе было дано определение кривой третьего порядка, эллиптических кривых, приведена их классификация, введена операция сложения, образующая абелеву группу на точках эллиптической кривой, а также приведено геометрическое описание операции сложения точек и выведены соответствующие арифметические формулы. Рассмотрен механизм построения криптосистем на группе точек эллиптической кривой.

Были рассмотрены алгоритмы сложения точек на нескольких типах кривых в форме псевдокода, применение которого возможно для построения протоколов, использующих в своей основе эллиптические кривые, и приведена схема алгоритма ЭЦП на эллиптической кривой.

Даны общие сведения о требованиях, предъявляемых к кривым криптографических стандартах.

При помощи выбора кривой из стандарта NIST был реализован алгоритм построения и сверки цифровой подписи. Результаты работы данного алгоритма и код программы приведены в приложении к работе.