МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра геометрии

Группы точек на гладких кривых

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Мамедова Бахруза Эльсевана оглы

Научный руководитель
доцент, к.ф.-м.н. ____________________ В.Е. Новиков
подпись, дата

Зав. кафедрой
к.ф.-м.н., доцент ____________________ С.В. Галаев
подпись, дата

Саратов 2023

Введение. В центре внимания современной абстрактной математики и сфер ее приложения находятся различные алгебраические структуры, среди которых не последнее место занимают группы. В данной работе речь пойдет не только об образовании группы на множестве точек гладких кривых, но и о понятии гладких кривых на плоскости. Отдельно будет рассмотрена эллиптическая кривая, как вид алгебраической кривой.

Долгое время теория эллиптических кривых не имела никаких приложений, пока Нил Коблиц и Виктори Миллер не предложили использовать эллиптические кривые для построения криптосистем с открытым ключом, использую построения алгоритмов факторизации больших числел. Причиной всего этого является то, что эллиптические кривые над конечными полями доставляют неистощимый источник абелевых групп, которые удобны для вычисления и обладают богатой структурой.

Данная бакалаврская работа разделена на три раздела.

Первый раздел посвящен понятии кривой на плоскости. Рассматриваются основные понятия кривой общего типа, такие как определение касательного вектора, кривизна кривой и сопровождающий базис Френе. Также рассматриваются алгебраические кривые и, в частности, эллиптические кривые.

Во втором разделе рассматривается геометрическое построение группы точек на окружности и на эллиптической кривой над вещественными числами. Также рассматривается и реализовывается интерполяция кубическим сплайном для построения гладкой кривой.

Третий раздел основан на рассмотрении эллиптической кривой над разлиными конечными полями. Дано определение эллиптической кривой над произвольным полем F. Также в работе находятся формулы сложения двух точек и обратной точки на эллиптической кривой. Рассматривается схема разделения секрета, используя интерполяционный многочлен Лагранжа.

Содержание. В начале работы рассматривались основные понятия гладкой кривой, такие как: понятие простой кривой, касательного вектора, кривизна кривой и остальные основные характеристики гладкой кривой. Дальше в работе были рассмотренны алгебраические кривые и эллиптические кривые.

Определение 1.4.1. *Алгебраической кривой порядка n над полем F называется множество точек* (x, y), *где* $x, y \in F$, *удовлетворяющих уравне-*

нию $F(X,Y)=0$*, где* $F(X,Y)$ *многочлен степени* n *с коэффициентами из* F.

Под степенью одночлена понимается сумма степеней входящих в него переменных, а под степенью многочлена - максимальная степень составляющих его одночленов.

Определение 1.4.2. *Точка* (x_1, y_1) *кривой* $F(X,Y) = 0$ *называется неособой, если в ней не равны нулю обе частные производные многочлена* $F(X,Y)$.

Дадим определение гладкой кривой

Определение 1.4.3. *Кривая называется неособой, или гладкой, если все ее точки неособые. В любой такой точке* (x,y) *к ней можно провести касательную.*

Неособая кривая третьего порядка над полем F *и называется эллиптической кривой над тем же полем, если на ней есть хотя бы одна точка.* В случае произвольного поля всякую эллиптическую кривую можно преобразовать к виду:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in F, \tag{1.6}$$

также называемому формой Вейерштрасса.

Далее для произвольного поля используем следующее определение.

Эллиптической кривой над полем F называется гладкая кривая, задаваемая уравнением вида (1.6). Будем обозначать $E(F)$ множество точек $(x,y) \in F^2$, удовлетворяющих этому уравнению (1.6), и содержащее, кроме того, *бесконечно удаленную точку*, обозначаемую Θ.

Самым важным свойством нашего множества точек $E(f)$ эллиптической кривой является то, что они образуют абелеву группу. Для этого на множестве $E(F)$, состоящем из точек эллиптической кривой (1.8) и еще одного элемента - бесконечно удаленой точки кривой Θ, можно определить операцию сложения. А наша бесконечно удаленная точка будет играть роль нейтрального элемента.

Пусть в нашем случае E - эллиптическая кривая над вещественными числами, и пусть P и Q - две точки на . Определим точки -P и P+Q по следующим правилам.

1. Если P - точка в бесконечности, то $P = -P = \Theta$ и $P + Q = Q$, т.е. Θ - нулевой элемент по сложению группы точек. В следующих пунктах будем считать, 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. $-(x, y) = (x, -y)$. Из (2.2) сразу следует, что $(x, -y)$ - также точка на E.

3. Если P и Q имеют различные x-координаты, то прямая $l = \overrightarrow{PQ}$ имеет с еще в точности одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P, и мы тогда полагаем $R =$, или касательной в Q, и мы тогда полагаем $R = Q$). Определяем теперь $P+Q$ как точку $-R$, т.е. как отражение от оси 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 $P + Q = \Theta$ (точке в бесконечности; это является следствием правила 1).

5. Остается возможность $P = Q$. Тогда считаем, что l - касательная к кривой в точке P. Пусть R - единственная другая точка пересечения l с E. Полагаем $P + Q = -R$.

Пример 2.1 Рассмотрим эллиптическую кривую $y^2 = x^3 - x$ в плоскости xy и вышеуказанный случай сложения точек P и Q. Чтобы найти $P+Q$ проводим прямую PQ и в роли точик $P+Q$ берем точку, которая симметричная относительно оси x, определяемой пересечением прямой PQ и кривой.

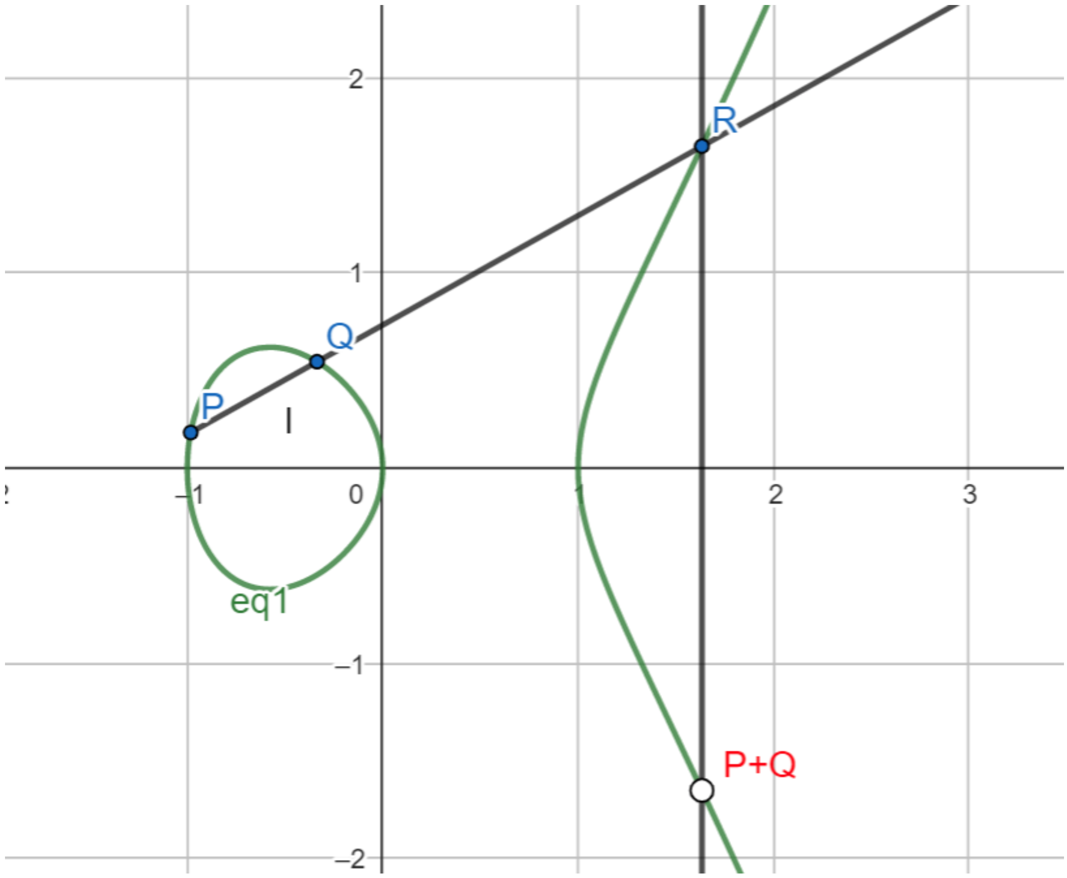

Рисунок 2.5 – Сложения точке на эллиптической кривой

Теперь выведем формулу для нашей точки $P+Q$.

Пусть $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ обозначают координаты соответственно $P, Q, P+Q$. Мы хотим выразить x_3, y_3 через x_1, y_1, x_2, y_2.

Будем рассматривать наш случай по 3 пункту в нашем плане, т.е есть уравнение прямой $y = \alpha x + \beta$, проходящей через P и Q (в этой ситуации она не вертикальна). Тогда $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ и $\beta = y_1 - \alpha x_1$. Наша точки $(x, \alpha x + \beta)$ лежат одновремено и на прямой, и на эллиптической окружности тогда и только тогда, когда $(\alpha x + \beta)^2 = x^3 + \alpha x + b$. Осталось решить это уравнение и получить координаты (x_3, y_3) через x_1 и x_2. Расспишем поподробнее наше уравнение

$$x^3 - (\alpha x + \beta)^2 + ax + b = x^3 - \alpha^2 x^2 + x(a - 2\alpha\beta) + b - \beta^2 = 0$$

С другой стороны, мы знаем, что наше кубическое уравнение имеет 3 решения - x_1, x_2, x_3. То есть мы можем расписать наше уравнение в более подходящий к нам вид:

$$x^3-(\alpha x+\beta)^2+ax+b = (x-x_1)(x-x_2)(x-x_3) = (x^2-x_1x-x_2x+x_1x_2)(x-x_3) =$$

$$= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_2x_3)x - x_1x_2x_3$$

При x^2 мы имееи 2 коэффициента:

$$-\alpha^2 = -x_1 - x_2 - x_3 \Rightarrow x_3 = \alpha^2 - x_1 - x_2$$

.

Таким образом, получаем выражение для x_3 и, следовательно, для y_3. Рассматриваем нашу точку $P+Q = (x_3, -y_3) = (x_3, -(\alpha x_3+\beta))$ и записываем через x_1, y_1, x_2, y_2:

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$$

$$y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3)$$

Если рассмотреть случай $P + P$, то проходящая через них прямая становится касательной к кривой.

Поскольку Q стремится к P, прямая, проходящая через P и Q становится касательной к кривой. В свете этого мы можем сказать, что $P + P = -R$, где R — это точка пересечения между кривой и касательной к кривой в точке P.

Кроме сложения, мы можем определить и другую операцию: скалярное умножение, то есть

$$nP = P + P + \ldots + P,$$

где n — натуральное число.

Очевидно, что потребуется n сложений для вычисления. Если n состоит из k десятичных разрядов, то алгоритм будет иметь сложность $O(2^k)$, что не очень хорошо. Но существуют и более быстрые алгоритмы.

Один из них — алгоритм удвоения-сложения.

Теперь мы ограничим эллиптические кривые конечными полями, а не вещественными числами, и посмотрим, что из этого получится.

Множество точек эллиптической кривой можно рассмотреть в виде:

$$\Big\{(x,y)\in GF(p)^2 \quad | \quad y^2 \equiv x^3+ax+b \pmod p,$$
$$4a^3+27b^2 \not\equiv \Theta \pmod p\Big\} \ \cup \ \{\Theta\}$$

где Θ — по-прежнему точка в бесконечности, а a и b — два целых числа в $GF(p)$.

То, что раньше было непрерывной кривой, теперь стало множеством отдельных точек на плоскости xy.

Рассмотрим алгебраическую сумму для точек эллиптических кривых над конечным полем.

Уравнения для выполнения сложений точек в точности такие же, как в предыдущем резделе, за исключением того, что нам нужно добавлять в конце каждого выражения "mod p". Поэтому, если $P=(x_1,y_1)$, $Q=(x_2,y_2)$ и $R=(x_3,y_3)$, то $P+Q=-R$ можно вычислить следующим способом:

$$x_3 = \Big((\frac{y_2-y_1}{x_2-x_1})^2 - x_1 - x_2\Big) \bmod p$$
$$y_3 = \Big(-y_1 + \frac{y_2-y_1}{x_2-x_1}(x_1-x_3)\Big) \bmod p$$

Для вычисления суммы точек использовался язык программирования Python, так как он очень прост в написании наших функций, таких как: проверка на бесконечно удаленную точку, обратная точка и само сложение точек.

Рассмотрим частный случай: $y^2 \equiv x^3 - x + 3 \pmod{127}$, при $P=(16,20)$ и $Q=(41,120)$. Нужно сложить точки P и Q для это кривой. В данном случае мы имеем, что p= 127, a = -1, b = 3. Но есть небольшое отличие прямых на $GF(p)$ от прямых на поле действительных чисел R. Можно сказать, что прямая над $\mathbb{F}_p$ — это множество точек (x,y), удовлетворяющих уравнению $ax+by+c\equiv 0 \pmod p$ (это стандартное уравнение прямой с добавленной частью "(mod p)").

Введём наши первичные данные и обсудим результат. Результат представлен на рисунке 3.1:

```
Введите модуль p: 127
Введите число a: -1
Введите число b: 3
Point(x=86, y=81)
```

Рисунок 3.1 – Сложение точек для кривой $y^2 \equiv x^3 - x + 3 \pmod{127}$

Программа вывела нашу точку $R = P + Q$ с координатами $(86, 81)$. Если рассмотреть множество точек на данной эллиптическо кривой, то можно увидеть наши точки (рисунок 3.2):

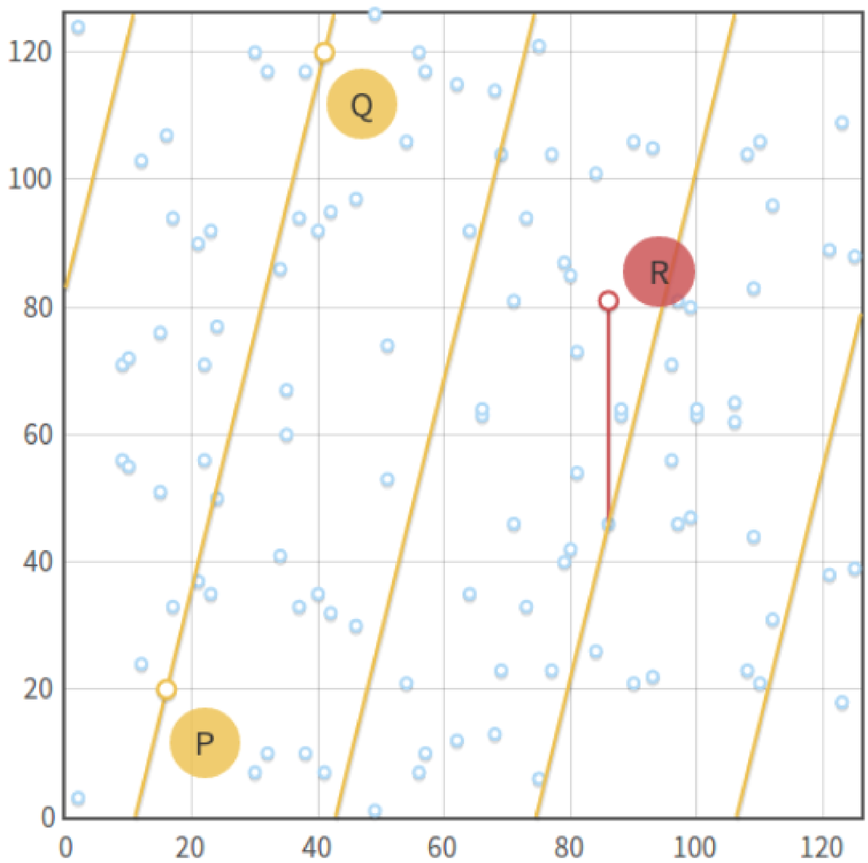

Рисунок 3.2 – Множество точек кривой

Более того, если мы вставим наши данные в формулу (2.1) предыдущего раздела, то сможем точно убедиться в результате: $x_3 = \left(\frac{100-20}{41-16}\right)^2 - 16 - 41 = 16 - 16 - 41 = -41$. Так как $-41 \equiv 86 \pmod{127}$, значит наш ответ точно верный. То же самое делаем с y_3: $y_3 = -20 + 4(16 + 41) = 208$. Так как $208 \equiv 81 \pmod{127}$, тогда у y_3 у нас все сходится.

Теперь обсудим схему интерполяционных полиномов Лагранжа (схема разделения секрета Шамира).

Для интерполяции многочлена степени $(k-1)$ требуется k точек. К примеру, для задания прямой достаточно двух точек, для задания параболы - трех точек, и так далее.

Если мы хотим разделить секрет между n людьми таким образом, чтобы восстановить его могли только k человек $(k \leq n)$, мы «прячем» его в формулу многочлена степени k. Таким образом, восстановить этот многочлен и исходный секрет можно будет только по k точкам.

Всякая схема разделения секрета состоит из двух этапов, этапа деления секрета и этапа восстановления секрета. Секретом будет сообщение M.

Разделение секрета. Доверенный центр T (Трент) выбирает большое простое число p, с условием, что $M < p$. Над простым полем Галуа $GF(p)$ генерируется случайный многочлен степени $k-1$ (исходя из числа долей k, достаточных для восстановления секрета):

$$s(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + M \pmod p, \tag{3.1}$$

где $a_1, \ldots, a_{k-1}$ - случайные коэффиициенты по $\pmod p$. Затем вычисляются доли

$$s(x_i) = a_{k-1}x_i^{k-1} + a_{k-2}x_i^{k-2} + \cdots + a_1 x_i + M \pmod p \tag{3.2}$$

Долями являются $(x_i, s(x_i), p)$, где x_i могут принимать значения $x_i = 1, \ldots, n$ номеров долей, p - общее простое число для восстановления секреты. После этого многочлен (3.1) уничтожается, а доли раздаются участникам протокола. Доли могут раздаваться с учётом статуса получателя.

Восстановление секрета. Для восстановления секрета M достаточно собрать k долей из n. По ним составить подсистему (3.3) системы (3.2):

$$s(x_{i_k}) = a_{k-1}x_{i_k}^{k-1} + a_{k-2}x_{i_k}^{k-2} + \cdots + a_1 x_{i_k} + M \pmod p \tag{3.3}$$

и решить её относительно неизвестных $a_{k-1}, a_{k-2}, \ldots, a_1, M$ и таким образом найти . Для восстановления многочлена (3.1) удобнее воспользоваться формулой интерполяционного многочлена Лагранжа. Так как на доли можно смотреть как на точки этого многочлена, то для точек $(x_{i_1}, s(x_{i_1}), x_{i_2}, s(x_{i_2}), \dots, x_{i_k}, s(x_{i_k}))$ существует единственный многочлен степени не больше $k-1$, который можно вычислить по формуле интерполяционного многочлена Лагранжа.

Заключение. В данной работе были изложены основные понятия и признаки гладкой кривой. Обсудили как эллиптические кривые над вещественными числами можно использовать для определения групп. Также мы вывели геометрический и алгебраический способы вычисления сложения точек и умножение точки на скаляр. Более того, затронули проблему задачи дискретного логарифмирования для эллиптических кривых, используемыми в криптографии. Также была рассмотрена схемы разделения секрета, которая используется в аппаратных криптографических модулях.