ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ОТЧЕТ  
ПО ЛАБОРАТОРНОЙ РАБОТЕ

ПО ДИСЦИПЛИНЕ

«Защита информации»

Руководители \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.А. Харченко

Москва 2023

СПИСОК ИСПОЛНИТЕЛЕЙ

Студ. группы 201-361 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Е. Сильченко

**Ход работы:**

Для генерации и визуализации всех решений уравнения вида:

Зададим переменный a, b и конечное поле p.

Далее генерируем точки, т.е. перебираем все точки поля p и проверяем лежат ли они на кривой. Метод для генерации точек и проверки представлен на рисунке 1 – 2.

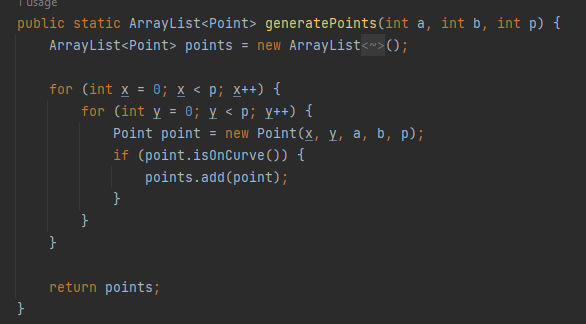


Рисунок 1 – Метод для генерации точек.

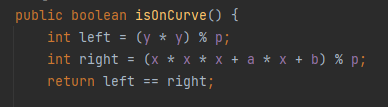
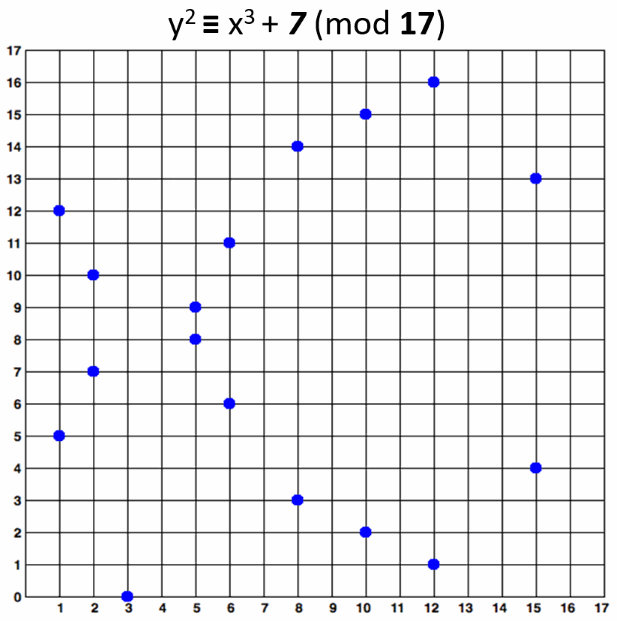


Рисунок 2 – Проверка лежит ли точка на кривой.

В данной программе, переменная a = 0, b = 7, а конечное поле p = 17, следовательно эллиптическая кривая должна выглядеть следующим образом:



На рисунке 3, представлена эллиптическая кривая которая получилась в результате выполнения моей программы.

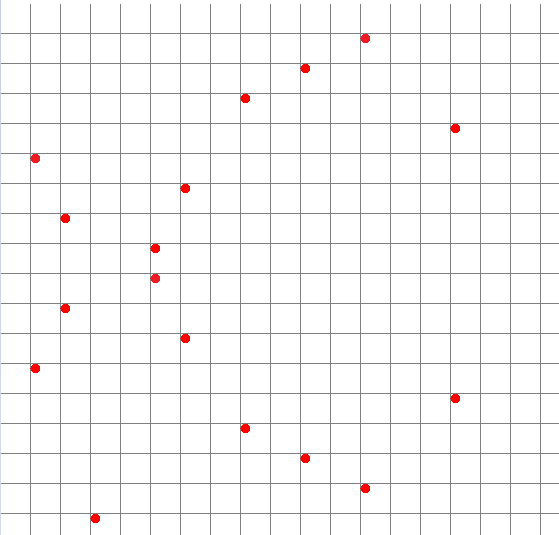


Рисунок 3 – Эллиптическая кривая.

Для сложения точек в данной программе реализован метод summ рисунок 4. В методе рассматриваются два случая: удвоение точки и сложение. Если координаты текущей точки и точки, переданной в качестве аргумента, равны, то это значит, что нужно выполнить удвоение точки, для этого вызывается метод doublePoint(). В противном случае, для сложения двух точек используется формула Лангранжа-Барроуза. Далее вычисляются числитель и знаменатель по формулам: numerator = other.getY() - y и denominator = other.getX() - x соответственно.

Затем вызывается вспомогательная функция multiplicativeInverse(), которая вычисляет обратный элемент denominator в поле p, и вычисляется значение s по формуле: s = numerator \* multiplicativeInverse(denominator, p) % p.

В следующих двух строках вычисляются новые значения координат x и y новой точки, в соответствии с формулами: x3 = (s \* s - x - other.getX()) % p и y3 = (s \* (x - x3) - y) % p.

Наконец, в последних двух строках параметры x3 и y3 изменяются, если они отрицательны, чтобы получить правильные значения.

В результате метод возвращает новую точку, полученную при сложении двух точек на эллиптической кривой результат представлен на рисунке 5. Также в этой программе использован метод multiplicativeInverse для вычисления обратного элемента в поле p метод представлен на рисунке 6. Внутри метода переменная a принимает значение a mod p, чтобы убедиться, что она находится в диапазоне от 0 до p-1. Затем производится цикл от x = 1 до p-1, чтобы найти такое значение x, при котором (a \* x) mod p равно 1. Если такое значение x найдено, функция возвращает его. Если же такого значения не существует, метод возвращает -1.

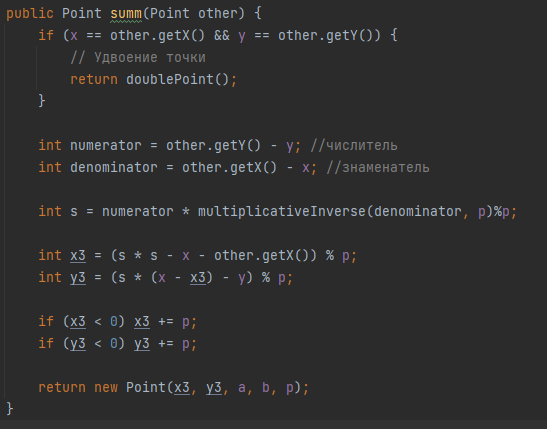


Рисунок 4 - метод summ.

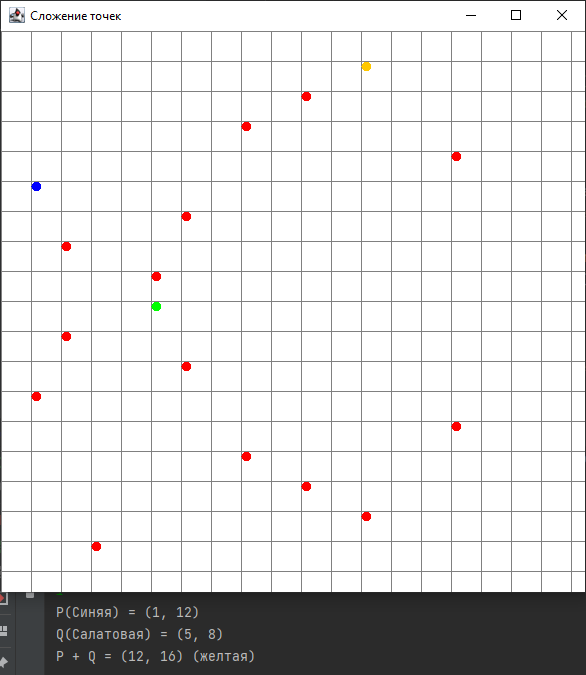


Рисунок 5 – Результат сложения двух точек.

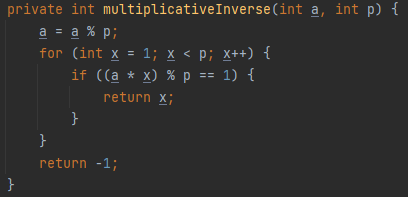


Рисунок 6 - метод multiplicativeInverse.

Результат сложения двух точек в данном примере можно проверить графически рисунок 7.

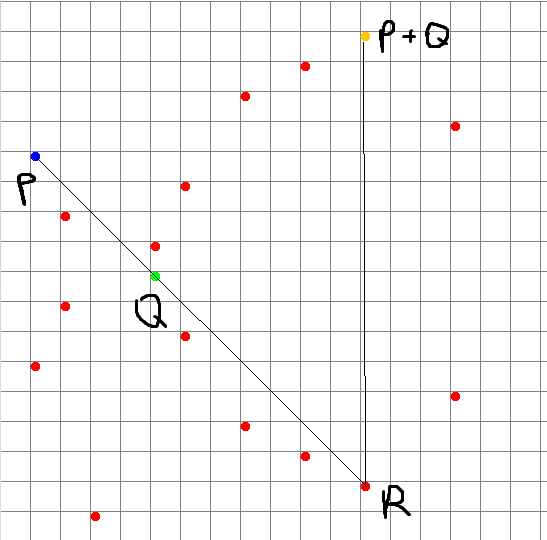


Рисунок 7 – Проверка сложения точек.

Для удвоения точек реализован метод doublePoint. В методе сначала задаются числитель numerator и знаменатель denominator для выражения s, которое вычисляется по формуле Лангранжа-Барроуза, и используемый для последующего вычисления координат точки.

Далее используется вспомогательная функция multiplicativeInverse, которая вычисляет обратный элемент denominator в поле p. Затем значение s вычисляется по формуле: s = numerator \* multiplicativeInverse(denominator, p) % p.

Используя s, вычисляются новые значения координат x3 и y3 по формулам:

x3 = s \* s - 2 \* x

y3 = s \* (x - x3) - y

Затем, если одно из значений отрицательно, то к этому значению прибавляется p для получения правильного значения.

Наконец, метод возвращает новую точку с вычисленными координатами x3 и y3.

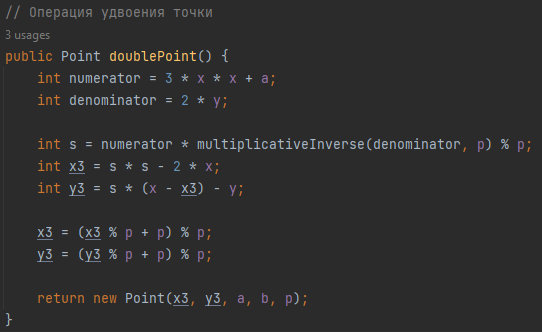


Рисунок 8 – метод doublePoint.

Результат удвоения точки (15, 13) представлен на рисунке 9.

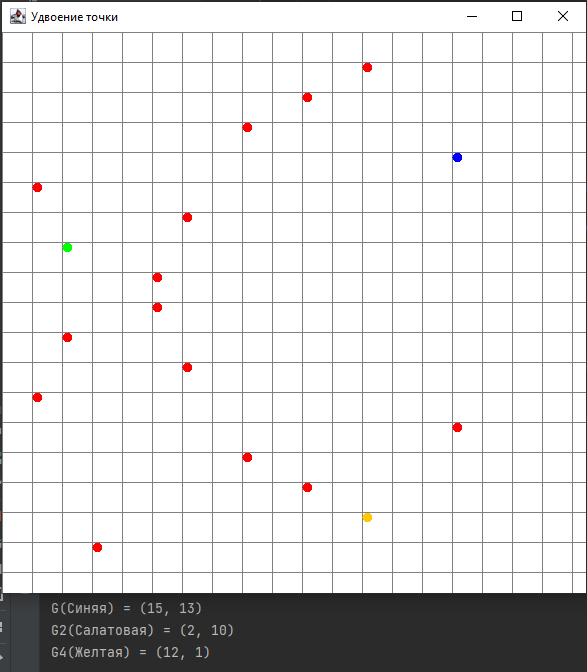


Рисунок 9 – Удвоение точки.

Также для отрисовки осей координат и точек использовался класс Diagram рисунок 10.

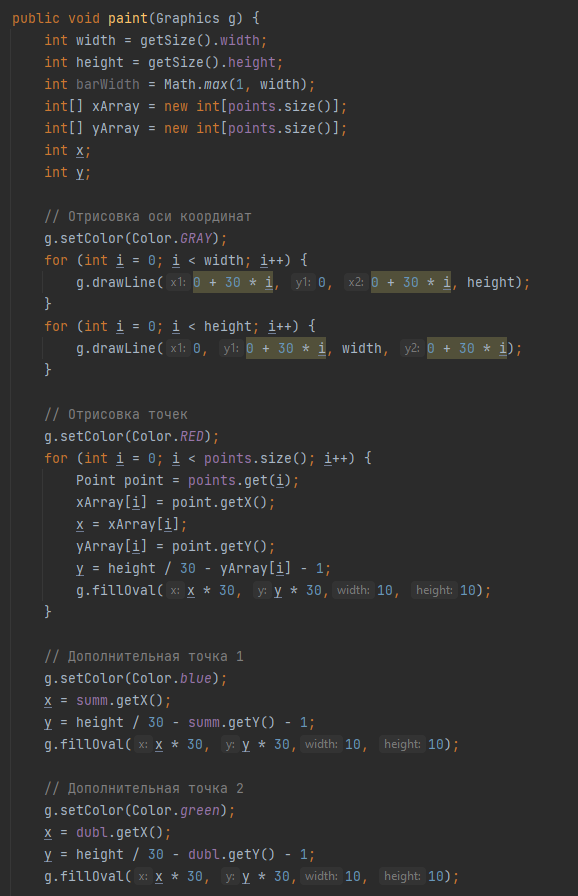


Рисунок 10 – Класс Diagram.