МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Розрахунково-графічна робота

з дисципліни «Безпека ПД»

Варіант №5

«Виконання операцій з точками еліптичних кривих

над полем GF(q)»

Виконав студент:

групи ПІ-421Б

Іванюк Н. О.

Перевірив викладач:

Радішевський М. Ф.

Київ 2022

**Вихідні дані:**

У полі Галуа GF(11) для рівняння еліптичної кривій E11 (2,1)

y2 = x3 + 2\*x + 1 (mod 11)

знайдено 15 точок, що задовольняють цьому рівнянню

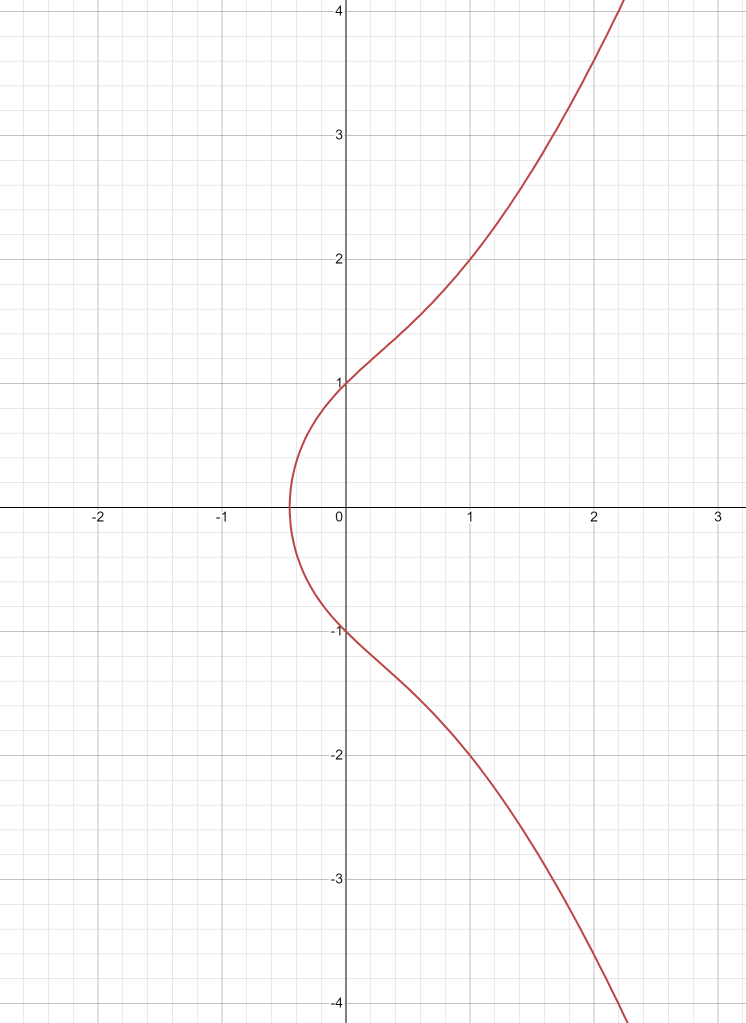
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ім’я точки | I | J | K | L | M | N |  | O |
| Координати | (0,10) | (1,9) | (3,10) | (5,9) | (6,8) | (8,10) |  | (10,8) |
|  |  |  |  |  |  |  |  |  |
| Ім’я точки | A | B | C | D | E | F | G | H |
| Координати | (0,1) | (1,2) | (3,1) | (5,2) | (6,3) | (8,1) | (9,0) | (10,3) |

|  |  |  |  |
| --- | --- | --- | --- |
| № | Точка 1 | Точка 2 | Прізвище студента |
| 5 | A | F | Іванюк Назар |

**Виконання:**

***1.Побудувати графік еліптичної кривій в полі дійсних чисел***

З рівняння еліптичної кривої y2 = x3 + 2\*x + 1 слідує, що крива існує тільки для x, для яких x3 + 2\*x + 1 > 0. Також крива симетрична відносно осі абсцис x.



***2.Побудувати розміщення точок в полі Галуа GF(11)***

***3. Переконатися, що точки 1 та 2 дійсно задовольняють еліптичної***

***кривій E11 (2,1).***

Точка 1 A(0,1)

y2= x3 + 2\*x + 1 (mod 11)= 03+2\*0+1(mod 11)= 1 (mod 11)=1

1>0, точкаа A належить еліптичній кривій E11

Точка 2 F(8,1)

y2= x3 + 2\*x + 1 (mod 11)=83+2\*8+1(mod 11)=529(mod 11)=1

1>0, точкаа F належить еліптичній кривій E11

***4.Знайти суму: точка 1+ точка 2 (згідно варіанту)***

Точка 1 A(0,1), точка 2 F(8,1). Розраховуємо за формулою:

*X3* = *s*2 – *x1* – *x2* (mod p),

*Y3* = − *y1* + *s*(*x1* – *x3*) (mod p)

*Де S* = (*y1* – *y2*)/(*x1* – *x2*) (mod p) - нахил січної.

S = (1 - 1)/(0-8) (mod 11) = (0)/(-8) (mod 11) ) = 0

*X3* = *0*2 – *0* – *8* (mod 11) = 3

*Y3* = − 1 + *0*(*0* – *8*) (mod 11) = -1(mod 11) = 10

Кінцевий результат: A(0,1) + F(8,1)= K(3, 10)

***5.Знайти зворотну точку для точки 2 (згідно варіанту)***

Точка 2 F(8,1)

Зворотні точки H(x1, y1) та –H(x2, y2) знаходяться на вертикальної прямої, тому x2 = x1 та y2= -y1.

Кінцевий результат: F(8,1) = - F(8,1) = N(8,10)

***6. Знайти різницю: точка 1 - точка 2 (згідно варіанту)***

Маємо точки 1: A(0,1)та точку 2: F(8,1).

Віднімання B(0,1)F(8,1) зводиться до додавання зворотної точки:

A(0,1)+ (– F(8,1)).

На попередньому етапі було знайдено точку N:

- F(8,1) = N(8,10)

Тобто, A(0,1)+ (– F(8,1))= A(0,1)+ N(8,10)

X3 = s2 – xC – xX (mod 11);

Y3 = – yX + s(xC – xO) (mod 11);

Де S = (yC – yX) / (xC – xX) (mod 11)

S = (1 - 10)/(0-8) (mod 11) =(2)/(3) (mod 11) = 8

X3 = 9 - 0 - 8(mod 11) = 1

Y3 = -1 + 8(0-1) (mod 11) = -1 + 3(mod 11) =2

Кінцевий результат A(0,1)+ (– F(8,1))= B(1,2)

***7.Знайти суму: точка 2 + точка 2 (згідно варіанту)***

Точка 2 F(8, 1), розраховуємо за формулою:

Х3 ≡ s2 – 2\*x1(mod p)

Y3 ≡ s(x1 – x3) – y1 (mod p)

Де S = (3\*x1\*x1 +a) / (2\*y1) mod p)

S = (3\*8\*8+2)/(2\*1)(mod 11)=7/2(mod 11)=9

X3 = 92-2\*8 (mod 11) = 4-5(mod 11)=10

Y3 = 9(8-10) - 1 (mod 11) = 4-1 (mod 11)= 3

Кінцевий результатF(8, 1) + F(8, 1) = H(10, 3)

***8.Умножити точку №2 на 3 (згідно варіанту)***

3\* F(8, 1) = (L+L)+L

A+A=R – відомо з попереднього завдання

Тепер порахуємо H (10, 3) + F(8, 1):

*X3* = *s*2 – *x1* – *x2* (mod p),

*Y3* = − *y1* + *s*(*x1* – *x3*) (mod p)

*Де S* = (*y1* – *y2*)/(*x1* – *x2*) (mod p)

S = (3 - 1)/(10 – 8) (mod 11) = 1

X3 = 1 - 10 - 8 (mod 11) = 5

Y3 = -3 + (10-5) (mod 11) = 2

Кінцевий результат: 3\* F(8, 1) = F(8, 1) + F(8, 1) + F(8, 1) = D(5, 2)

***9.Умножити точку №2 на 4 (згідно варіанту)***

4\*F = (F+F)+ (F+F)

F+F= B – ми вже знаємо з попереднього завдання.

Тепер порахуємо H (10, 3)+ H (10, 3)

*X3 ≡ s2 – 2\*x1 (mod p)*

*Y3 ≡ s(x1 – x3) – y1 (mod p)*

*Де S = (3\*x1\*x1 +a) / (2\*y1) mod p)*

S =(3\*10\*10+2)/(2\*3) (mod11)=(5)/(6) mod(11) = 10

X3 = 102-2\*10 (mod 11) = 1-9(mod 11)=3

Y3 = 10(10-3) – 3 (mod 11)= 4-3(mod 11)=1

Кінцевий результат: 4\* F(8, 1) = F(8, 1) + F(8, 1) + F(8, 1) + F(8, 1) = C(3,1)

Ще раз перевіримо через формулу

4\*F = (3\*F+F)

F+F+F= D – ми вже знаємо з попереднього завдання.

Тепер порахуємо D (5, 2)+ F (8, 1)

*X3* = *s*2 – *x1* – *x2* (mod p),

*Y3* = − *y1* + *s*(*x1* – *x3*) (mod p)

*Де S* = (*y1* – *y2*)/(*x1* – *x2*) (mod p)

S = (2-1) / (5-8) (mod11) = (1) / (8)(mod 11) = 7

X3 = 72 – 5 – 8 (mod 11) = -8(mod 11) = 3

Y3 = 9 + 7(5-3) (mod 11) = 9+3(mod 11) = 1

Кінцевий результат: 4\* F(8, 1) = F(8, 1) + F(8, 1) + F(8, 1) + F(8, 1) = C(3,1)

**Висновок**: Виконуючи дану розрахунково-графічну роботу, я дослідив виконання операцій з точками еліптичних кривих над полем Галуa GF(q), на прикладі GF(11).

Також, я з’ясував, що однією з переваг використання еліптичних кривих є те, що при однаковій крипто-захищеності можна використовувати менші за величиною числа. Таким чином підвищується швидкодія систем шифрування.

Я переконався, що еліптичні криві є одним з основних об’єктів вивчення в сучасній теорії чисел і криптографії.