Лабораторная работа

Выполнил: Кощавцев Даниил, 4ПМ

1) Инициалы КДВ. Смотрим номера букв: К=12, Д=5, В=3, значит, число p=1253.

Ближайшее простое: p=1259.

2) Найдём одно решение уравнения y^2=x^3+ax+b(mod 1259) (для каждого x перебираем все y от 0 до p-1=1258, пока не получим верное равенство). Перебором находим точку P = (4, 256)

3) Представим 151 в виде последовательности удвоений. Сначала представим 151 в двоичном виде. 27 = 128 < 151, 28 = 256 > 151 Запишем степени двойки:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| K | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2k | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |

Последовательно отнимаем максимальную степень двойки, не превосходящую текущее число: 151-128=23, 23-16=7, 7-4=3, 3-2=1

Таким образом, 151 = 128 + 16 + 4 + 2 + 1 = 27 + 24 + 21 + 1, значит,

151𝑃 = 128𝑃 + 16𝑃 + 4𝑃 + 2𝑃 + 𝑃

2k𝑃 находится с помощью последовательного удвоения точки.

Найдём 2𝑃 = 𝑃 + 𝑃 = 2 ∙ (4, 256). Используем формулы удвоения точки (по модулю p=1259):

𝑘 = (3𝑥12 + 𝑎) ∙ (2𝑦1)-1 = (3 ∙ 42 + 1) ∙ (2 ∙ 256) -1

def gcdex(a, b):  
 if b == 0:  
 return a, 1, 0  
 else:  
 d, x, y = gcdex(b, a % b)  
 return d, y, x - y \* (a // b)  
  
print(gcdex(2\*256,1259)) возвращает (1, 150, -61)

Следовательно, (2\*256)-1 = 150

Поэтому k = 49 \* 150 = 7350 = 1055 (mod 1259)

𝑥 = 𝑘2 − 2𝑥1 = 10552 − 2 ∙ 4 = 1113017= 841 (mod 1259),

𝑦 = 𝑘\*(𝑥1 − 𝑥) – 𝑦1 = 1055 ∙ (4 − 841) − 256 = -883291 = 527 (mod 1259)

То есть, 2𝑃 = (841, 527).

И так далее:

n = 10  
x1 = 4  
y1 = 256

a = 1  
default = 1259  
  
for i in range (n):  
 k = (3 \* x1\*x1 + a) \* gcdex(2\*y1,default)[1]%default  
 x = (k\*k - 2\*x1)%default  
 y = (k\*(x1-x)-y1)%default  
 print(f'{2\*\*(i+1)}P = ({x} ,{y})')  
 x1 = x  
 y1 = y

Вывод программы: 2P = (61, 41)

4P = (483, 235)

8P = (612, 322)

16P = (972, 677)

32P = (182, 262)

64P = (477, 739)

128P = (1194, 919)

256P = (779, 269)

512P = (1219, 13)

1024P = (320, 626)

151𝑃 = 128𝑃 + 16𝑃 + 4𝑃 + 2𝑃 + P

3𝑃 = 2𝑃 + 𝑃 = (841, 527) + (4, 256) = (1159, 435)

(Небольшая автоматизация):

def obr(a, b):  
#Находит а^(-1) mod b, то есть такое с, что ac=1(mod b)  
 g=gcdex(a, b)  
 if g[0] == 1:  
 return g[1]%b  
 else:  
 return 0

first = [841, 527] // Первое слагаемое (в случае 2P+P – это 2P)  
sec = [4, 256] // Второе слагаемое (аналогично, P)  
k = ((sec [1]-first[1]) \* obr((sec[0]-first[0]), default)) % default  
x = (k\*k - (first [0] + sec [0]))%default  
y=(k\*(first [0]-x)-first [1])%default  
  
print(x, y) // Вывод в случае 2P+P = (.

1159, 435)

7P = 4P + 3P = (361, 926)

23P = 16P + 7P = (624, 366)

151P = 128P + 23P = (85, 327)

4) Найдём порядок кривой с помощью перебора print(porjadok(1,0,1259)): 1260.

def porjadok(a,b,p):

#находит перебором количество всех точек: все конечные точки кривой y^2=x^3+ax+b в поле GF(p) + одна бесконечная

s=1 #всегда есть одна точка -бесконечная, Е=О

for x in range(p): #перебераем х от 0 до <p, то есть до p-1

y2=(pow(x,3)+a\*x+b)%p

for y in range(0,p):

if (pow(y,2)%p)==y2:

s+=1

return(s)

print(porjadok(a,b,p))

def porjadoktime(a,b,p):

t1 = datetime.datetime.now() #запоминаем время начала работы

s=porjadok(a,b,p)

t2 = datetime.datetime.now()

time = t2 - t1

print("Порядок кривой y^2=x^3+",a," x + ",b," (mod ",p,") равен ",s,". Время выполнения ", time," сек")

Вывод: Порядок кривой y^2=x^3+ 1 x + 0 (mod 1259 ) равен 1260 . Время выполнения 0:00:00.486956 сек

5) В пункте 4 было найдено |G|= 1260. Разложим это число на множители: 1260 = 2^2 ∙ 3^2 ∙ 5 ∙ 7, значит, порядок любого элемента может быть только 2k1 \* 3k2 \* 5k3 \* 7k4 , где 0 ≤ 𝑘1 ≤ 2, 0 ≤ 𝑘2 ≤ 2, 0 ≤ 𝑘3 ≤ 1, 0 ≤ 𝑘4 ≤ 1, то есть |𝑃| ∈ {1,2,3,4,5,6,7,8,9,10,12,14,15,16,18,20,21,24,25,27,28,30,32,35,36,40,42,45,48,49,50,56,60,64,70,72,75,... ,1260}

1260 P = E. Простые делители 1260 равны 2, 3, 5, 7. |𝐺|/2 = 630, |𝐺|/3 = 420, |𝐺|/5 = 252, |𝐺|/7 = 180 значит, достаточно проверить 180𝑃, 252P, 420𝑃, 630P.

180P = 128P + 32P + 16P + 4P = (463, 213) != E

Проверяем 252P = 128P + 64P + 32P + 16P + 8P + 4P = (365, 538) != E

Проверяем 420P = 256P + 128P + 32P + 4P = (64, 767) != E

Проверяем 630P = 512P + 64P + 32P + 16P + 4P + 2P = (477, 520) != E

Проверяем 315P = 5 \* 63

Проверим 5P = (38, 237) != E, 63P = (365, 721) != E

Ответ. 1) p=1259, 2) P = (4, 256), 3) 151𝑃 = (2744, 1511); 4) |𝐺| = 1260; 5) |𝑃| = 315.