Bài tập 6: Hệ mật dựa trên đường cong Elliptic

Bài 1: Thực hiện tính toán sau

1. $(13,7)+(6,3)$
2. $(13,7)+(13,7)$

trên nhóm điểm trên đường cong $y^2 = x^3 + 2x + 2 \mod 17$.

Bài 2: Hãy kiểm tra định lý Hasse cho đường cong $y^2 = x^3 + 2x + 2 \mod 17$.

Bài 3: Xét đường cong Elliptic trên $\mathbb{Z}_7$:

$$E : y^2 = x^3 + 3x + 2.$$

1. Liệt kê các điểm của đường cong này.
2. Cấp của nhóm là gì? (*Gợi ý:* Đừng quên điểm $\mathcal{O}$)
3. Xét phần tử $P = (0,3)$, xác định cấp của P. Liệu P có phải phần tử sinh không?

Bài 4: Xét đường cong Elliptic trên $\mathbb{Z}_{29}$ và điểm cơ sở $P = (8,10)$:

$$E : y^2 = x^3 + 4x + 20 \mod 29.$$

Hãy tính điểm $k \cdot P$ đưới đây dùng thuật toán bình phương liên tiếp. Đưa ra kết quả trung gian ở mỗi bước.

1. $k = 9$
2. $k = 20$

Bài 5: Xét đường cong của **Bài 4**. Cấp của đường cong là $\#E = 37$. Hơn nữa, biết thêm điểm $Q = 15 \cdot P = (14,23)$ trên đường cong. Hãy xác định kết quả của phép nhân dưới đây dùng ít phép toán nhóm nhất có thể, tức là bạn nên sử dụng điểm Q một cách thông minh. Hãy xác định cách bạn đơn giản hoá tính toán ở mỗi bước.

Gợi ý: Ngoài việc dùng điểm Q, hãy dùng sự kiện rằng ta dễ tính điểm $-P$.

1. $16 \cdot P$
2. $38 \cdot P$
3. $53 \cdot P$
4. $14 \cdot P + 4 \cdot Q$
5. $23 \cdot P + 11 \cdot Q$

Bài 6: Nhiệm vụ của bạn là tính khoá phiên trong giao thức DHKE dựa trên đường cong Elliptic. Khoá bí mật của bạn là $a = 6$. Bạn nhận được khoá công khai của Bob $B = (5, 9)$. Đường cong Elliptic bạn sử dụng là

$$y^2 = x^3 + x + 6 \mod 11.$$

Thực hành với Sagemath

Đường cong Elliptic

$$E : y^2 = x^3 + 4x + 20 \mod 29.$$

định nghĩa trên Sagemath như sau:

```
sage: E = EllipticCurve(GF(29), [4,20])
sage: E
Elliptic Curve defined by y^2 = x^3 + 4*x + 20 over Finite Field of size 29
sage: P = E(8,10)
sage: P
(8 : 10 : 1)
```

Thực hiện cộng điểm và nhân một điểm với hằng số trên Sagemath:

```
sage: Q = 5*P
sage: Q
(20 : 3 : 1)
sage: P + Q
(10 : 25 : 1)
```

Để liệt kê các điểm $\{k \cdot P \mid k = 1..10\}$ ta thực hiện lệnh

```
sage: for k in [1..10]:
....:     print (k*P)
....:
(8 : 10 : 1)
(0 : 22 : 1)
(16 : 2 : 1)
(6 : 17 : 1)
(20 : 3 : 1)
(10 : 25 : 1)
(2 : 6 : 1)
(13 : 6 : 1)
(4 : 10 : 1)
(17 : 19 : 1)
```

Để vẽ các điểm trên đường cong Elliptic E, ta thực hiện lệnh:

```
sage: plot (E)
```

ta được kết quả

Bài tập với Sagemath

Bài 1: Xét đường cong `brainpoolP256r1`. Đường cong định nghĩa bởi phương trình $y^2 = x^3 + ax + b$ trên trường 256 bit $K = GF(p)$. Điểm cơ sở $g = (x_g, y_g)$ có cấp n là một số nguyên tố 256 bit.

```
p = A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
a = 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
b = 26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
g = (xg,yg)
xg= 8BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262
yg= 547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
n = A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
h =1
```

1. Hãy dùng `is_prime()` và `E.order()` của Sagemath để kiểm tra tính nguyên tố của p, n và cấp của đường cong E.
2. Giả sử rằng Alice và Bob chọn các khoá bí mật:

```
a=81DB1EE100150FF2EA338D708271BE38300CB54241D79950F77B063039804F1D
b=55E40BC41E37E3E2AD25C3C6654511FFA8474A91A0032087593852D3E7D76BD3
```

Hãy tính A, B, aB, bA.

Chú ý: Các số hexa trong Sagemath có thể định nghĩa dùng tiền tố `0x`.