Assignment 7

Konstantinos Filippou
ics23044

Exercise 1

For the elliptic curve parameters:

$$a = 5, \quad b = 1,$$

defined over $\mathbb{Z}_{97}$, verify that the curve is non-singular.

Solution

The curve is non-singular if:

$$4a^3 + 27b^2 \not\equiv 0 \pmod{97}.$$

Compute:

$$4a^3 = 4 \cdot 5^3 = 4 \cdot 125 = 500,$$
$$27b^2 = 27 \cdot 1 = 27.$$

$$4a^3 + 27b^2 = 500 + 27 = 527.$$

Reduce modulo 97:

$$527 - 5 \cdot 97 = 527 - 485 = 42.$$

Since:

$$42 \not\equiv 0 \pmod{97},$$

the curve satisfies the non-singularity condition.

Exercise 2

Let $P_1 = (3, 25)$ and $P_2 = (6, 21)$ on the curve over $\mathbb{Z}_{97}$.

Case 1: $P_1 \neq P_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{21 - 25}{6 - 3} = \frac{-4}{3}.$$

Find the inverse of 3 modulo 97:

$$97 = 3 \cdot 32 + 1,$$

$$1 = 97 - 3 \cdot 32.$$

Thus:

$$3^{-1} \equiv -32 \equiv 65 \pmod{97}.$$

$$\lambda = -4 \cdot 65 = -260.$$

Reduce modulo 97:

$$260 - 2 \cdot 97 = 260 - 194 = 66,$$

$$-260 \equiv 97 - 66 = 31.$$

$$\lambda = 31.$$

Compute:

$$x_3 = \lambda^2 - x_1 - x_2 = 31^2 - 3 - 6 = 961 - 9 = 952.$$

$$952 - 9 \cdot 97 = 952 - 873 = 79.$$

$$x_3 = 79.$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 31(3 - 79) - 25 = 31(-76) - 25 = -2381.$$

$$2381 - 24 \cdot 97 = 2381 - 2328 = 53.$$

Thus:

$$-2381 \equiv 97 - 53 = 44.$$

$$\boxed{P_3 = (79, 44)}.$$

Case 2: $P_1 = P_2 = (10, 9)$

Use the doubling formula:

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

$$\lambda = \frac{3 \cdot 10^2 + 5}{2 \cdot 9} = \frac{305}{18}.$$

$$305 \equiv 14 \pmod{97}.$$

Find inverse of 18 modulo 97 using EEA:

$$97 = 18 \cdot 5 + 7$$

$$18 = 7 \cdot 2 + 4$$

$$7 = 4 \cdot 1 + 3$$

$$4 = 3 \cdot 1 + 1$$

Back substitution yields:

$$1 = 27 \cdot 18 - 5 \cdot 97.$$

Thus:

$$18^{-1} \equiv 27 \pmod{97}.$$

$$\lambda = 14 \cdot 27 = 378 \equiv 87 \pmod{97}.$$

$$x_3 = 87^2 - 10 - 10 = 7569 - 20 = 7549.$$

$$7549 - 77 \cdot 97 = 7549 - 7469 = 80.$$

$$y_3 = 87(10 - 80) - 9 = -6099.$$

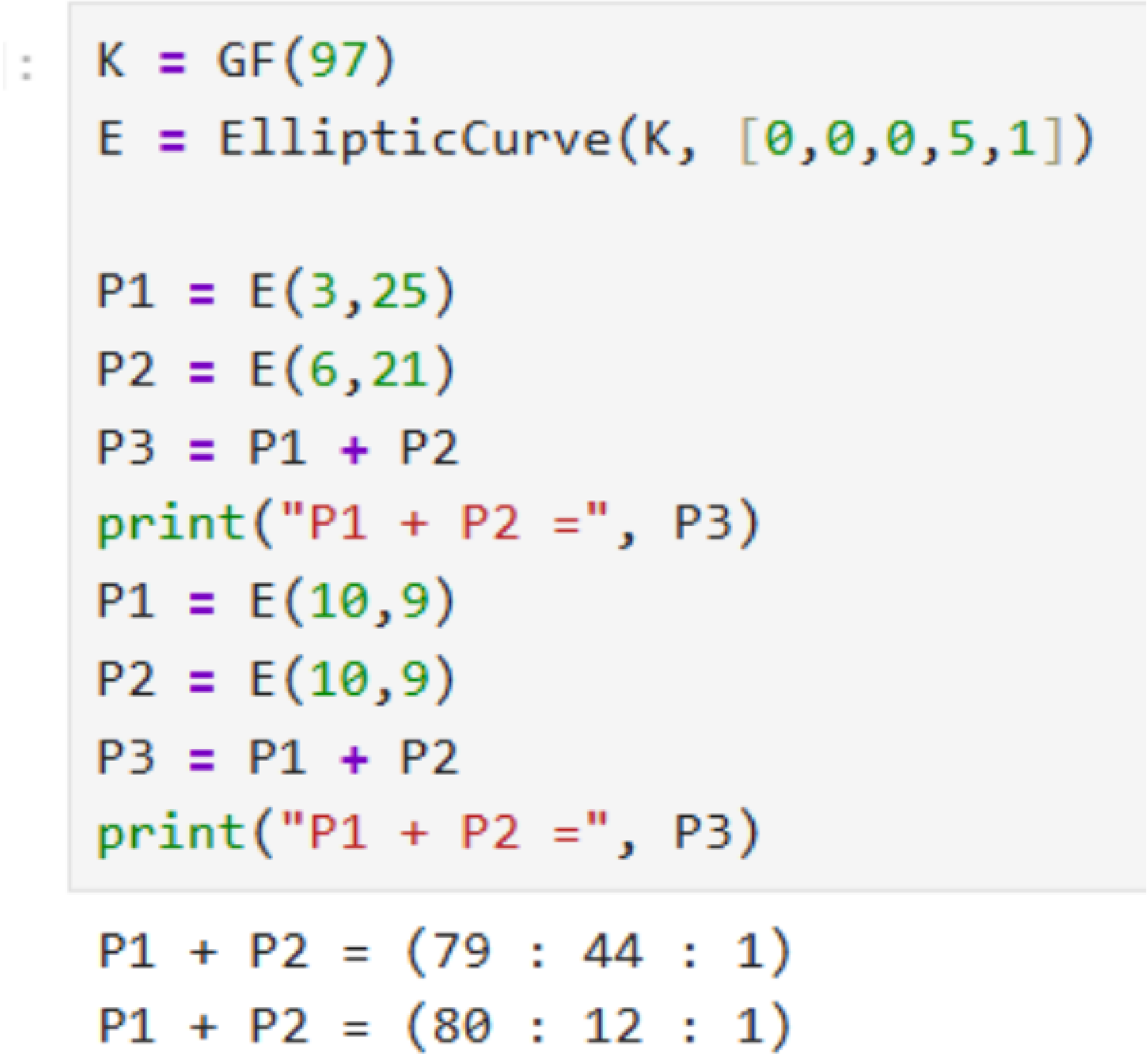
$$6099 - 62 \cdot 97 = 6099 - 6014 = 85.$$

Thus:

$$-6099 \equiv 97 - 85 = 12.$$

$$\boxed{P_3 = (80, 12)}.$$

And we verify using code:



```
K = GF(97)
E = EllipticCurve(K, [0,0,0,5,1])

P1 = E(3,25)
P2 = E(6,21)
P3 = P1 + P2
print("P1 + P2 =", P3)
P1 = E(10,9)
P2 = E(10,9)
P3 = P1 + P2
print("P1 + P2 =", P3)
```

```
P1 + P2 = (79 : 44 : 1)
P1 + P2 = (80 : 12 : 1)
```

Figure 1:

Exercise 3

Let:

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

over $\mathbb{Z}_7$.

The points of E over $\mathbb{Z}_7$ are:

$$\mathcal{O}, (0,3), (0,4), (2,1), (2,6), (4,1), (4,6), (5,1), (5,6).$$

Thus the group order is:

$$|E(\mathbb{Z}_7)| = 9.$$

For $a = (2,4)$, we compute its order:

$$\text{ord}(a) = 3.$$

Since $3 \neq 9$, a is not a generator.
A point with different order is $(5,1)$, which has order 9.

Exercise 4

Scalar multiplication using double-and-add over $\mathbb{Z}_{11}$, starting with:

$$R = \mathcal{O}, \quad P = (5,2).$$

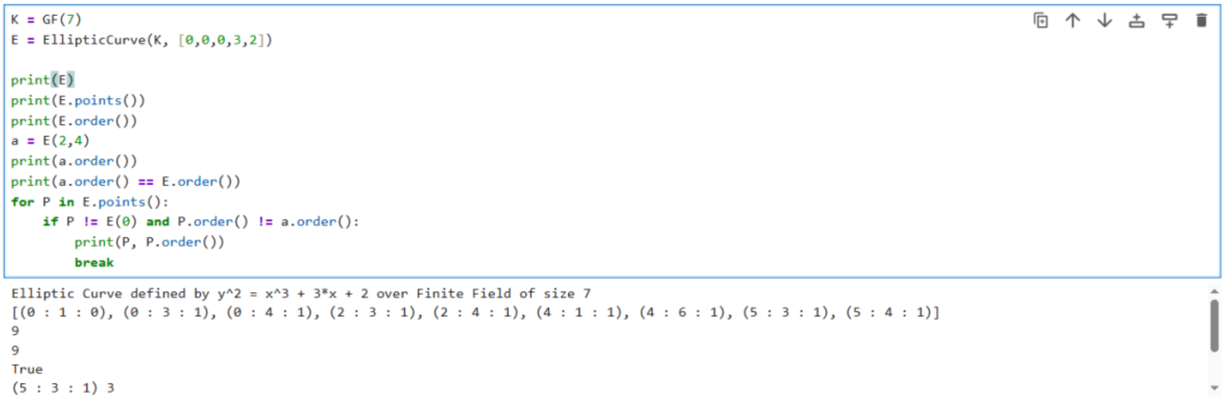
Following the binary expansion process:
After successive doubling and addition steps, we obtain:

$$\boxed{S = (3,6)}.$$

The algorithm performs:

- 3 doublings,
- 1 addition,

for a total of 4 elliptic curve operations.

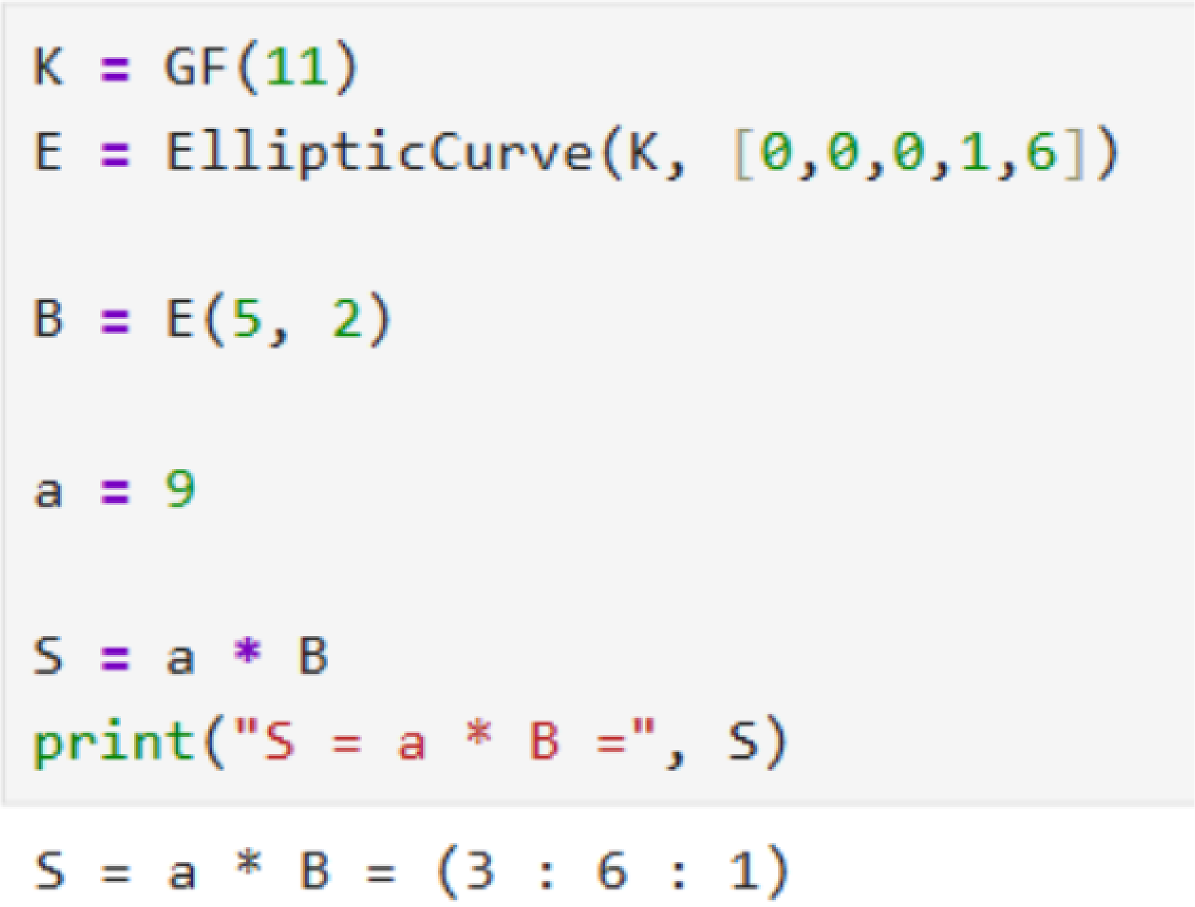


```
K = GF(7)
E = EllipticCurve(K, [0,0,0,3,2])

print(E)
print(E.points())
print(E.order())
a = E(2,4)
print(a.order())
print(a.order() == E.order())
for P in E.points():
    if P != E(0) and P.order() != a.order():
        print(P, P.order())
        break
```

```
Elliptic Curve defined by y^2 = x^3 + 3*x + 2 over Finite Field of size 7
[(0 : 1 : 0), (0 : 3 : 1), (0 : 4 : 1), (2 : 3 : 1), (2 : 4 : 1), (4 : 1 : 1), (4 : 6 : 1), (5 : 3 : 1), (5 : 4 : 1)]
9
9
True
(5 : 3 : 1) 3
```

Figure 2:



```
K = GF(11)
E = EllipticCurve(K, [0,0,0,1,6])

B = E(5, 2)

a = 9

S = a * B
print("S = a * B =", S)
```

```
S = a * B = (3 : 6 : 1)
```

Figure 3: