Semih Balki
Yildiz Technical University

semihbalki@sabanciuniv.edu

Assignment 3

BLM 5153 : Fall 2019 : Prof. Koc
Due Sunday, November 17, 2019

Problem - Consider the Weierstrass curve $y^2 = x^3 + 7\text{x} + 4$ in $GF(103)$.
Note that: Point at infinity is represented as ϑ and (0, 0) in the code.

(1) Generate all points and find the group order.

(2) Find a primitive point on the curve.

(3) Show that $P = (5, 24)$ is on the curve.

(4) Find the order of the point P.

(5) Compute $[17]P$.

Solution
(1)

- For discrete square root problem, since p = 103 is small, we can solve such equations using enumeration.
- For x = 0, we get $y^2 = 4 \pmod{103}$ then solutions are (0, 2) and (0, -2) = (0, 101).
- For x = 1, we get $y^2 = 12 \pmod{103}$ then no solution.
- We can discover all squares mod 103 by enumeration
  y^2: y
  0 : [0]
  1 : [1, 102]
  2 : [38, 65]
  3 :
  4 : [2, 101]
  5 :
  6 :
  .
  .
  .

102 :
Note that: you could observe the complete list of the enumeration from: https://github.com/smhblk04/Applied-Cryptography/blob/master/SQUARE

- The table shows that the solution of $y^2 = 4(\text{mod } 103)$ is y = 2, -2. Therefore, we get two points (0, 2) and (0, -2) = (1, 101)

- Proceeding for the other values of x $\in Z^*_{103}$ we find 113 solutions.

  Points of the curve:
  [[0, 2], [0, 101], [2, 51], [2, 52], [3, 19], [3, 84], [5, 24], [5, 79],
  [6, 57], [13, 51], [13, 52], [16, 35], [16, 68], [17, 35], [17, 68],
  [18, 20], [18, 83], [20, 25], [20, 78], [24, 20], [24, 83], [26, 47],
  [26, 56], [27, 10], [27, 93], [28, 25], [28, 78], [29, 44], [29, 59],
  [32, 6], [32, 97], [33, 15], [33, 88], [34, 32], [34, 71], [37, 31],
  [37, 72], [45, 17], [45, 86], [46, 11], [46, 92], [47, 34], [47, 69],
  [48, 1], [48, 102], [49, 24], [49, 79], [52, 22], [52, 81], [54, 16],
  [54, 87], [55, 25], [55, 78], [57, 14], [57, 89], [58, 50], [58, 53],
  [59, 38], [59, 65], [61, 20], [61, 83], [64, 7], [64, 96], [67, 8],
  [67, 95], [68, 12], [68, 91], [69, 23], [69, 80], [70, 35], [70, 68],
  [72, 22], [72, 81], [74, 21], [74, 82], [75, 1], [75, 102], [78, 13],
  [78, 90], [80, 6], [80, 97], [81, 29], [81, 74], [82, 22], [82, 81],
  [83, 1], [83, 102], [84, 4], [84, 99], [86, 15], [86, 88], [87, 15],
  [87, 88], [88, 51], [88, 52], [89, 47], [89, 56], [91, 47], [91, 56],
  [92, 48], [92, 55], [94, 6], [94, 97], [97, 40], [97, 63], [98, 16],
  [98, 87], [99, 18], [99, 85], [100, 33], [100, 70], [0, 0], [6, 46]]

- The elliptic curve group $\varepsilon(7, 4, 103)$ has 113 elements, including point at infinity ϑ.

- The order of the elliptic curve group $\varepsilon(7, 4, 103)$ is 113.

(2)

- According to the Lagrange Theorem, the element orders in $\varepsilon(7, 4, 103)$ can only be the divisors of 1, 113.

- The order of ϑ is 1 since $[1]\vartheta = \vartheta$.

- The order of P = (97, 63) is 113 since:

$$
\begin{aligned}
&[2]P = (97, 63) \oplus (97, 63) = (37, 31) \\
&[3]P = (97, 63) \oplus (37, 31) = (32, 6) \\
&[4]P = (37, 31) \oplus (37, 31) = (2, 52) \\
&. \\
&. \\
&. \\
&[112]P = (37, 72) \oplus (97, 63) = (97, 40) \\
&[113]P = (97, 40) \oplus (97, 63) = (0, 0)
\end{aligned}
$$

- All the points except point at infinity on the $\varepsilon(7, 4, 103)$ elliptic curve are primitive points on the curve.

(3)

- To show a point is on the curve or not, we need to check that left hand side and right hand side of the $\varepsilon(7, 4, 103)$ elliptic curve holds.

$$24^2 = 5^3 + 7.5 + 4 \,(mod 103)$$

$$576 = 125 + 35 + 4 \,(mod 103)$$

$$576 = 164 \,(mod 103)$$

$$61 = 61 \,(mod 103)$$

- Then the point (5, 24) is on the curve.

(4)

- We already know that (5, 24) is a primitive point on the $\varepsilon(7, 4, 103)$ elliptic curve. Therefore, the order of the (5, 24) equals to the order of the $\varepsilon(7, 4, 103)$ curve which is 113.

(5)

- P = (5, 24)

$$[2]P = (5, 24) \oplus (5, 24) = (26, 56)$$
$$[3]P = (26, 56) \oplus (5, 24) = (86, 88)$$
$$[4]P = (26, 56) \oplus (26, 56) = (46, 11)$$
.
.
.
$$[16]P = (69, 80) \oplus (5, 24) = (70, 35)$$
$$[17]P = (70, 35) \oplus (5, 24) = (37, 72)$$