Practice Assignment 4 Solution

Elliptic Curve Cryptography

Exercise 4–1

Consider the elliptic curve $E : y^2 = x^3 + 4x + 3 \pmod{23}$ and the point $P = (7, 11)$. Compute the point 44P with as few point operations as possible.

Solution:

In order to calculate 44P with as few additions as possible, we can take calculate 44 as the summation of different powers of 2

Thus, we can find $44 = 32 + 8 + 4$, Thus we can calculate $44P$ as $32P + 8P + 4P$

Using the standard rules of point doubling in elliptic curves:

$s = (3X_P^2 + a) * (2Y_P)^{-1}$, where $^{-1}$ indicates the multiplicative inverse
$X_{2P} = s^2 - 2X_P$
$Y_{2P} = s * (X_P - X_{2P}) - Y_P$

we find $2P = (17, 4)$

we repeat the same steps for calculating $4P$, $8P$, $16P$, $32P$, to find:
$4P = (1, 13)$
$8P = (6, 6)$
$16P = (1, 10)$
$32P = (6, 17)$

We then get $40P = 32P + 8P = (0, 0)$

and $44P = 40P + 4P = (1, 13)$

Exercise 4–2

Decide whether the points of the following elliptic curve define a group over Zp where p is a prime? If yes, find its additive group of integers (Zp, +).

E : y2 = x3 + 4x + 1 (mod7)

Solution:

We first need to check the singularity of the EC, we find that $4a^3 + 27b^2 = 3 \bmod 7, \neq 0$, thus this curve is nonsingular and can form a group over Z_7. Substituting x = 0, we get (0, 1) and (0, 6) as 2 points belonging to the elliptic curve, we can use them along with the other points and the point at infinity O to fill the addition table.

	O	(0, 1)	(4, 5)	(4, 2)	(0, 6)
O	O	(0, 1)	(4, 5)	(4, 2)	(0, 6)
(0, 1)	(0, 1)	(4, 5)	(4, 2)	(0, 6)	O
(4, 5)	(4, 5)	(4, 2)	(0, 6)	O	(0, 1)
(4, 2)	(4, 2)	(0, 6)	O	(0, 1)	(4, 5)
(0, 6)	(0, 6)	O	(0, 1)	(4, 5)	(4, 2)

Exercise 4–3

Let $E : y^2 = x^3 + 9x + 17$ be the elliptic curve F_{23}. What is the discrete logarithm k of $Q = (4, 5)$ to the base $P = (16, 5)$?

Solution:

We are looking for k such that $Q = kP$. We compute kP for $k > 1$, until we find Q

K	kP
2	(20, 20)
3	(14, 14)
4	(19, 20)
5	(13, 10)
6	(7, 3)
7	(8, 7)
8	(12, 17)
9	(4, 5)

Thus $k = 9$