Muhammad Izham Bin Norhamadi
B032020039 3BITZ

Tutorial 6b: ECC over finite field $F[2^m]$

An elliptic curve E over $F[2^m]$ is given by

$$y^2 + xy = x^3 + ax^2 + b \text{ modulo } M(t).$$

Let us take $x_1 = 2$, $y_1 = 139$

$a = 3$, compute b

We will always compute in a ring modulo $M=299_{10}$.

Step 1: Double point

Step 2: Add point

Table 5.2b An inverse a^{-1} of $a = xy$ in hexa modulo irreducible polynomial $299_{10} = M(t) = t^8+t^5+t^3+t+1$ written in hexadecimals.

a^{-1}		y															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
x	**0**	00	01	95	E6	DF	BB	73	A4	FA	85	C8	55	AC	CE	52	69
	1	7D	27	D7	F8	64	59	BF	A3	56	50	67	9A	29	33	A1	98
	2	AB	91	86	E8	FE	E1	7C	11	32	1C	B9	30	CA	76	C4	3D
	3	2B	B8	28	1D	A6	B1	4D	3F	81	61	8C	5A	C5	2F	4C	37
	4	C0	F4	DD	44	43	DC	74	FC	7F	8F	E5	C6	3E	36	9D	DA
	5	19	57	0E	68	C9	0B	18	51	65	15	3B	8D	62	97	8B	6F
	6	80	39	5C	96	14	58	9B	1A	53	0F	CD	D9	B3	9E	8A	5F
	7	D5	F2	A5	06	46	FD	2D	CB	F7	E2	82	ED	26	10	8E	48
	8	60	38	7A	EC	FB	09	22	E9	B4	C2	6E	5E	3A	5B	7E	49
	9	AA	21	D2	B7	E7	02	63	5D	1F	A0	1B	66	DB	4E	6D	B2
	A	99	1E	BE	17	07	72	34	B0	F1	EF	90	20	0C	CF	BD	D1
	B	A7	35	9F	6C	88	C3	D3	93	31	2A	DE	05	D0	AE	A2	16
	C	40	F5	89	B5	2E	3C	4B	E4	0A	54	2C	77	D8	6A	0D	AD
	D	BC	AF	92	B6	F3	70	F9	12	CC	6B	4F	9C	45	42	BA	04
	E	FF	25	79	F6	C7	4A	03	94	23	87	EB	EA	83	7B	F0	A9
	F	EE	A8	71	D4	41	C1	E3	78	13	D6	08	84	47	75	24	E0

Step 0: Choose a base point $P_1(x_1, y_1)$.

Let us take $x_1 = 2 = t = 10_2$,

$y_1 = 139_{10} = 8B_{16} = 10001011_2$.

Take $P_1(x_1, y_1) = (02, 8B)$

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

Step 1: Assign parameters a and b.

Given $a = 3 = t + 1 = 11_2$. From an elliptic curve $y^2 + xy = x^3 + ax^2 + b$,

$P_1(x_1, y_1) = (02, 8B)$

We need to compute $b = y^2 + xy - (x^3 + ax^2)$

$y_1^{\,2}$ =10001011·10001011

```
 10001011
     10001011
       10001011
        10001011
 100000001000111
 100101011
    101010000111
    100101011
      1111011111
      100101011
       110001001
       100101011
        10100010  = A2₁₆
```

$x_1 y_1$ = 10·10001011
=100010110= 116₁₆.

We move to the RHS, we need to compute x^3,

$x^2 =$ 10·10 $= t^2 = 100$
100 = 04₁₆.

$x^3 = x \cdot x^2 = t \cdot t^2 = t^3 = 1000.$
10·100
= 1000₂ = 08₁₆.

Let us move on to ax^2 = 11·100
= 100
  100
= 1100 = 0C₁₆.

Finally, we can compute b, from $y^2 + xy = x^3 + ax^2 + b$,

$b = y^2 + xy - (x^3 + ax^2)$
= 10100010+100010110-(1000+1100)

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

```
= 100010110
   10100010
       1000
       1100
-----------
  110110000
  100101011
-----------
   10011011  = 9B16
```

Let us move to Double Point operation on $P_1(x_1, y_1) = (02, 8B)$

Step 2: Double Point

From a basic Point, compute $P_2(x_2, y_2) = 2 \otimes P_1(x_1, y_1)$
From an irreducible polynomial $299_{10} = 12B_{16} = 256 + 32 + 8 + 2 + 1 = M(t) = t^8 + t^5 + t^3 + t + 1$.

Let (x_1, y_1) be a point on an elliptic curve $E(F2^m)$, and $(x_1, y_1) \neq (x_2, -y_2)$
then let $(x_2, y_2) = 2 \otimes (x_1, y_1)$ such that

$$x_2 = x_1^2 + \frac{b}{x_1^2} \quad \text{and} \quad y_2 = x_1^2 + (1 + x_1 + \frac{y_1}{x_1}) \cdot x_2$$

$P_1(x_1, y_1) = (02, 8B)$

From $x_1^2 = 100$, refer to Table 5.2b in xy=04, we get an inverse x_1^{-2} =DF.
Let us compute

bx_1^{-2} = 9B·DF
= 10011011·11011111

```
= 11011111
     11011111
      11011111
        11011111
         11011111
---------------
  110010111101001
  100101011
---------------
   10111100101001
   100101011
---------------
     101001001001
     100101011
---------------
       1100010001
       100101011
---------------
        101000111
        100101011
---------------
          1101100  =  6C16
```

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

$x_2 = x_1^2 + bx_1^{-2} =$ 100+1101100

```
= 1101100
      100
---------
= 1101000=68₁₆.
```

From $x_1 =$ 10=2_{16}, refer to Table 5.2b in xy=02, we get an inverse x_1^{-1} =95_{16}.

Let us compute

$y_1 \cdot x_1^{-1} =$ 8B·95

= 10001011·10010101

```
= 10010101
      10010101
         10010101
          1001010100
  -------------------
= 10011110001011100
  100101011
      1011101011100
      100101011
         10111101100
         100101011
            101000000
            100101011
               1101011 = 6B₁₆.
```

Next $1 + x_1 + y_1 \cdot x_1^{-1} =$ 1+10+1101011

```
= 1101011
       10
+       1
---------
  1101000 = 68₁₆.
```

$(1 + x_1 + y_1 \cdot x_1^{-1}) \cdot x_2 =$ 1101000·1101000

```
1101000
 1101000
   1101000000
-------------
1010001000000
100101011
  11011110000
  100101011
   1001011100
   100101011
         1010 = 0A₁₆.
```

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

Then we are ready to compute $y_2 = x_1^2 + (1 + x_1 + y_1 \cdot x_1^{-1}) \cdot x_2$

$$
\begin{aligned}
&= 100+1010 \\
&= 1010 \\
&\quad\; \underline{100} \\
&= 1110 = 0E_{16}.
\end{aligned}
$$

Step 3: Add Point

Compute $P_3(x_3, y_3) = P_1(x_1, y_1) \oplus P_2(x_2, y_2)$

Let (x_1, y_1) and (x_2, y_2) are two points on an elliptic curve $E(F_p)$, and $(x_1, y_1) \neq (x_2, \pm y_2)$

then let $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$ such that

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + \frac{y_2 - y_1}{x_2 - x_1} - (x_1 + x_2) + a \quad \text{and} \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - (x_3 + y_1)$$

Let the slope

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$ of the secant line connecting (x_1, y_1) and (x_2, y_2)

then

$$x_3 = m^2 + m - (x_1 + x_2) + a \text{ and } y_3 = m \cdot (x_1 - x_3) - (x_3 + y_1)$$

$P_3(x_3, y_3) = P_1(x_1, y_1) \oplus P_2(x_2, y_2) = (2, 6C) \oplus (A0, 1D)$

Let us start from denominator $x_2 - x_1 = 68 - 02$

$$
\begin{aligned}
&= 1101000 \\
&\quad\; \underline{10} \\
&= 1101010 = 6A_{16}.
\end{aligned}
$$

Refer to an inverse table, from $(x_2 - x_1)^{-1} = 6D$.

Take $y_2 - y_1 = 0E - 8B = 85_{16}$.

Now we can compute the slope of secant line,

$$
\begin{aligned}
m &= (y_2 - y_1) \cdot (x_2 - x_1)^{-1} = 85 \cdot 6D \\
&= 10000101 \cdot 1101101
\end{aligned}
$$

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

= 1101101·10000101

```
10000101
 10000101
   10000101
    10000101
      10000101
______________
11011101011001
100101011
 1001000111001
 100101011
      10001001
      100101011
         111001 = 39₁₆.
```

$m^2 = 39 \cdot 39$

= 111001·111001

```
= 111001
   111001
    111001
       111001
  ___________
  10101000001
  100101011
    111101101
    100101011
     11000110 = C6₁₆
```

$x_3 = m^2 + m - (x_1 + x_2) + a$

```
= 11000110
    111001
        10
   1101000
        11
  ________
  10010110 = 96₁₆.
```

$y_3 = m \cdot (x_1 - x_3) - (x_3 + y_1)$

$x_1 - x_3 = 02 - 96 = 94.$

$x_3 + y_1 = 96 + 8B = 1D.$

Let us compute $m \cdot (x_1 - x_3) = 39 \cdot 1D$

= 111001·11101

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

```
= 11101·111001

  111001
   111001
    111001
      111001
  1010000101
  100101011
    11010011 = D3₁₆.
```

Finally,

$y_3 = m\cdot(x_1 - x_3) - (x_3 + y_1)$ = D3 - 1D

```
= 11010011
     11101
  11001110 = CE₁₆.
```

Answer Table for Tutorial 5b

i	x_1	y_1	x_2	y_2	x_3	y_3	i	x_1	y_1	x_2	y_2	x_3	y_3
0	2	100	180	98	59	253	50	2	150	237	242	91	173
1	2	101	254	67	61	196	51	2	151	167	2	89	66
2	2	102	180	214	59	198	52	2	152	255	229	3	62
3	2	103	254	189	61	249	53	2	153	181	193	94	102
4	2	104	166	196	88	133	54	2	154	255	26	3	61
5	2	105	236	123	143	24	55	2	155	181	116	94	56
6	2	106	166	98	88	221	56	2	156	249	181	136	21
7	2	107	236	151	143	151	57	2	157	179	6	102	129
8	2	108	160	29	141	163	58	2	158	249	76	136	157
9	2	109	234	53	182	183	59	2	159	179	181	102	231
10	2	110	160	189	141	46	60	2	160	152	66	167	117
11	2	111	234	223	182	1	61	2	161	210	201	153	224
12	2	112	250	38	156	184	62	2	162	152	218	167	210
13	2	113	176	178	45	8	63	2	163	210	27	153	121
14	2	114	250	220	156	36	64	2	164	158	148	0	23
15	2	115	176	2	45	37	65	2	165	212	136	178	56
16	2	116	252	111	236	66	66	2	166	158	10	0	23
17	2	117	182	108	251	190	67	2	167	212	92	178	138
18	2	118	252	147	236	174	68	2	168	140	244	42	92
19	2	119	182	218	251	69	69	2	169	198	118	195	5
20	2	120	238	194	210	213	70	2	170	140	120	42	118
21	2	121	164	95	96	226	71	2	171	198	176	195	198
22	2	122	238	44	210	7	72	2	172	138	18	162	150
23	2	123	164	251	96	130	73	2	173	192	7	253	213
24	2	124	232	187	42	57	74	2	174	138	152	162	52
25	2	125	162	177	113	174	75	2	175	192	199	253	40
26	2	126	232	83	42	19	76	2	176	208	124	88	16
27	2	127	162	19	113	223	77	2	177	154	213	239	100
28	2	128	163	158	233	136	78	2	178	208	172	88	72
29	2	129	233	145	44	159	79	2	179	154	79	239	139

Muhammad Izham Bin Norhamadi
B032020039 3BITZ

30	2	130	163	61	233	97	80	2	180	214	10	157	108
31	2	131	233	120	44	179	81	2	181	156	52	180	166
32	2	132	165	94	234	4	82	2	182	214	220	157	241
33	2	133	239	198	100	50	83	2	183	156	168	180	18
34	2	134	165	251	234	238	84	2	184	196	97	78	10
35	2	135	239	41	100	86	85	2	185	142	193	7	174
36	2	136	183	175	183	24	86	2	186	196	165	78	68
37	2	137	253	169	3	179	87	2	187	142	79	7	169
38	2	138	183	24	183	175	88	2	188	194	39	103	215
39	2	139	253	84	3	176	89	2	189	136	16	166	184
40	2	140	177	95	178	97	90	2	190	194	229	103	176
41	2	141	251	206	117	229	91	2	191	136	152	166	30
42	2	142	177	238	178	211	92	2	192	47	220	17	232
43	2	143	251	53	117	144	93	2	193	101	141	161	241
44	2	144	235	127	154	205	94	2	194	47	243	17	249
45	2	145	161	82	212	216	95	2	195	101	232	161	80
46	2	146	235	148	154	87	96	2	196	41	239	40	198
47	2	147	161	243	212	12	97	2	197	99	41	21	44
48	2	148	237	31	91	246	98	2	198	41	198	40	238
49	2	149	167	165	89	27	99	2	199	99	74	21	57