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

This ECC is by far the most efficient elliptic curve cryptosystem and it is part of An ECC standard.

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

*y*2 + *xy* = *x*3 + *ax*2 + *b* modulo *M*(*t*).

Let us take *x*1=2, *y*1=100+*i*, where *i* is the last 2 digits of your matrix number or newly assigned number. Take *a*=3, compute *b*. We will always compute in a ring modulo M=29910.

Step 1: Double point

Step 2: Add point

Note: Refer to an inverse table modulo *M*(*t*).

Table 5.2b An inverse *a*−1 of *a* = *xy* in hexa modulo irreducible polynomial 29910 = *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** |  |
|  | **0** | 0 | 0 | 0 | 1 | 9 | 5 | E | 6 | D | F | B | B | 7 | 3 | A | 4 | F | A | 8 | 5 | C | 8 | 5 | 5 | A | C | C | E | 5 | 2 | 6 | 9 |
|  | **1** | 7 | D | 2 | 7 | D | 7 | F | 8 | 6 | 4 | 5 | 9 | B | F | A | 3 | 5 | 6 | 5 | 0 | 6 | 7 | 9 | A | 2 | 9 | 3 | 3 | A | 1 | 9 | 8 |
|  | **2** | A | B | 9 | 1 | 8 | 6 | E | 8 | F | E | E | 1 | 7 | C | 1 | 1 | 3 | 2 | 1 | C | B | 9 | 3 | 0 | C | A | 7 | 6 | C | 4 | 3 | D |
|  | **3** | 2 | B | B | 8 | 2 | 8 | 1 | D | A | 6 | B | 1 | 4 | D | 3 | F | 8 | 1 | 6 | 1 | 8 | C | 5 | A | C | 5 | 2 | F | 4 | C | 3 | 7 |
|  | **4** | C | 0 | F | 4 | D | D | 4 | 4 | 4 | 3 | D | C | 7 | 4 | F | C | 7 | F | 8 | F | E | 5 | C | 6 | 3 | E | 3 | 6 | 9 | D | D | A |
|  | **5** | 1 | 9 | 5 | 7 | 0 | E | 6 | 8 | C | 9 | 0 | B | 1 | 8 | 5 | 1 | 6 | 5 | 1 | 5 | 3 | B | 8 | D | 6 | 2 | 9 | 7 | 8 | B | 6 | F |
|  | **6** | 8 | 0 | 3 | 9 | 5 | C | 9 | 6 | 1 | 4 | 5 | 8 | 9 | B | 1 | A | 5 | 3 | 0 | F | C | D | D | 9 | B | 3 | 9 | E | 8 | A | 5 | F |
| *x* | **7** | D | 5 | F | 2 | A | 5 | 0 | 6 | 4 | 6 | F | D | 2 | D | C | B | F | 7 | E | 2 | 8 | 2 | E | D | 2 | 6 | 1 | 0 | 8 | E | 4 | 8 |
|  | **8** | 6 | 0 | 3 | 8 | 7 | A | E | C | F | B | 0 | 9 | 2 | 2 | E | 9 | B | 4 | C | 2 | 6 | E | 5 | E | 3 | A | 5 | B | 7 | E | 4 | 9 |
|  | **9** | A | A | 2 | 1 | D | 2 | B | 7 | E | 7 | 0 | 2 | 6 | 3 | 5 | D | 1 | F | A | 0 | 1 | B | 6 | 6 | D | B | 4 | E | 6 | D | B | 2 |
|  | **A** | 9 | 9 | 1 | E | B | E | 1 | 7 | 0 | 7 | 7 | 2 | 3 | 4 | B | 0 | F | 1 | E | F | 9 | 0 | 2 | 0 | 0 | C | C | F | B | D | D | 1 |
|  | **B** | A | 7 | 3 | 5 | 9 | F | 6 | C | 8 | 8 | C | 3 | D | 3 | 9 | 3 | 3 | 1 | 2 | A | D | E | 0 | 5 | D | 0 | A | E | A | 2 | 1 | 6 |
|  | **C** | 4 | 0 | F | 5 | 8 | 9 | B | 5 | 2 | E | 3 | C | 4 | B | E | 4 | 0 | A | 5 | 4 | 2 | C | 7 | 7 | D | 8 | 6 | A | 0 | D | A | D |
|  | **D** | B | C | A | F | 9 | 2 | B | 6 | F | 3 | 7 | 0 | F | 9 | 1 | 2 | C | C | 6 | B | 4 | F | 9 | C | 4 | 5 | 4 | 2 | B | A | 0 | 4 |
|  | **E** | F | F | 2 | 5 | 7 | 9 | F | 6 | C | 7 | 4 | A | 0 | 3 | 9 | 4 | 2 | 3 | 8 | 7 | E | B | E | A | 8 | 3 | 7 | B | F | 0 | A | 9 |
|  | **F** | E | E | A | 8 | 7 | 1 | D | 4 | 4 | 1 | C | 1 | E | 3 | 7 | 8 | 1 | 3 | D | 6 | 0 | 8 | 8 | 4 | 4 | 7 | 7 | 5 | 2 | 4 | E | 0 |

Step 0: Choose a base point P1(*x*1, *y*1).

Let us take *x*1= 2 = *t* = 102, *y*1=10810 = 6C16 = 11011002.

Take P1(*x*1, *y*1) = (02, 6C)

Step 1: Assign parameters *a* and *b*.

Given *a* = 3 = *t* + 1 = 112. From an elliptic curve *y*2 + *xy* = *x*3 + *ax*2 +*b*,

P1(*x*1, *y*1) = (02, 6C)

We need to compute *b* = *y*2 + *xy* – (*x*3 + *ax*2)

*y*12 =1101100⋅1101100

1101100

1101100

1101100

110110000

1010001010000

100101011

11011100000

100101011

1001001100

100101011

11010= 1A16.

*x*1 *y*1 = 10⋅1101100

=11011000= D816.

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

*x*2 = 10⋅10 = *t*2 = 100

100 = 0416.

*x*3 = *x* ⋅ *x*2 = *t* ⋅ *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 )

= 11010+11011000-(1000+1100)

= 11011000

11010

1000

1100

= 11000110 = C616.

Let us move to Double Point operation on P1(*x*1, *y*1) = (02, 6C)

**Step 2: Double Point**

Describe a double point operation given a point on an elliptic curve.

From a basic Point, compute P2(*x*2, *y*2) = 2⊗P1(*x*1, *y*1)

From an irreducible polynomial 29910 =12B16 =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) ≠ (*x*2, –*y*2)

then let (*x*2, *y*2) = 2⊗(*x*1, *y*1) such that



P1(*x*1, *y*1) = (02, 6C)

From *x*12= 100, refer to Table 5.2b in *xy*=04, we get an inverse *x*1−2=DF.

Let us compute

*bx*1−2= 82⋅DF

= 11000110⋅11011111

= 11011111

11011111

11011111

110111110

101101010000010

100101011

1000001000010

100101011

= 1011110010

100101011

10100100=A416.

*x*2 = *x*12+ *bx*1−2= 100+10100100

= 10100100

100

= 10100000=A016.

From *x*1 = 10=216, refer to Table 5.2b in *xy*=02, we get an inverse *x*1−1=9516.

Let us compute

*y*1⋅ *x*1−1= 6C⋅95

= 1101100⋅10010101

= 10010101

10010101

10010101

1001010100

= 11000100011100

100101011

1010001111100

100101011

11011001100

100101011

1001100000

100101011

110110=3616.

Next 1 + *x*1 + *y*1⋅ *x*1−1 = 1+10+110110

= 110110

10

+ 1

110101=3516.

(1 + *x*1 + *y*1⋅ *x*1−1 )⋅ *x*2 =110101⋅10100000

=10100000⋅110101

110101

11010100000

1110000100000

100101011

111010010000

100101011

11111001000

100101011

1101100100

100101011

100110010

100101011

11001=1916.

Then we are ready to compute *y*2 =  *x*12 + (1 + *x*1 + *y*1⋅ *x*1−1 )⋅ *x*2

= 100+11001

= 11001

100

= 11101=1D16.

**Step 3: Add Point**

Compute P3(*x*3, *y*3) = P1(*x*1, *y*1) ⊕ P2(*x*2, *y*2)

Let (*x*1, *y*1) and (*x*2, *y*2) are two points on an elliptic curve E(Fp), and

(*x*1, *y*1) ≠ (*x*2, ± *y*2)

then let (*x*3, *y*3) = (*x*1, *y*1) ⊕ (*x*2, *y*2) such that



Let the slope

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* and *y*3 = *m*⋅(*x*1 – *x*3) – (*x*3 + *y*1)

P3(*x*3, *y*3) = P1(*x*1, *y*1) ⊕ P2(*x*2, *y*2)= (2, 6C)⊕(A0,1D)

Let us start from denominator *x*2 – *x*1 = A0 – 02

= 10100000

10

= 10100020 = A216.

Refer to an inverse table, from (*x*2 – *x*1)−1 = BE. Take *y*2 – *y*1 =1D – 6C=7116.

Now we can compute the slope of secant line,

*m* = (*y*2 – *y*1)⋅(*x*2 – *x*1)−1=71⋅BE

= 1110001⋅10111110

10111110

10111110

10111110

10111110

11001100011110

100101011

1011001111110

100101011

10011001110

100101011

1100010=6216.

*m*2=62⋅62

*=*1100010⋅1100010

=1100010

1100010

11000100

=1010000000100

100101011

11010110100

100101011

1000011000

100101011

1001110=4E16.

*x*3 = *m*2 + *m* – (*x*1 + *x*2) + *a*

= 1001110

1100010

10

10100000

11

10001101=8D16.

*y*3 = *m*⋅(*x*1 – *x*3) – (*x*3 + *y*1)

*x*1 – *x*3=02 – 8D=8F.

*x*3 + *y*1=8D + 6C=E1.

Let us compute *m*⋅(*x*1 – *x*3) = 62⋅8F

= 1100010⋅10001111

10001111

10001111

100011110

11001100111110

100101011

1011001011110

100101011

10011101110

100101011

1000010=4216.

Finally,

*y*3 = *m*⋅(*x*1 – *x*3) – (*x*3 + *y*1)

= 1000010

10001101

1101100

10100011=A316. walla…

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 |
| 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 |