**Tutorial 5.1: ECC over prime field P**

**Instruction: Take your *i* = 10 + (ID mod 100 or nearest assigned number).**

Step 0: My sample number is *i*=10+42=52. I am taking P1(*x*1, *y*1) = (50, 26).

Choose a prime number. Let *p*=257.

1. Choose a random sample *a* = −4 and *b* = 7 for the curve

*E*: *y*2 = *x*3 + *ax* + *b*

such that 4*a*3 + 27*b*2 ≠0 (mod p).

1. Choose a base Point P1(*x*1, *y*1) = (*xi*, *yi*). Compute P2(*x*2, *y*2) = 2⊗P1(*x*1, *y*1)

**Double Point**

Let (*x*1, *y*1) be a point on an elliptic curve E(Fp), and (*x*1, *y*1) ≠ (*x*2, –*y*2)

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



Let slope of the tangent line

 ,

then

*x*2 = c2 – 2*x*1 and *y*2 = c (*x*1 – *x*2) – *y*1.

Take 2*y*1= 2⋅26 = 52 (mod 257).

First, we need to compute an inverse of denominator (2*y*1)−1 ≡ (52)−1 = 173 (mod 257) using Extended Euclidean Algorithm in excel.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Extended Euclidean Algorithm | | | | | | |  | |
| b = | | *a* | *q* | +*r* |  | u | v | | w = uvq | |
| 257 | | 52 | 4 | 49 |  | 0 | 1 | | -4 | |
| 52 | | 49 | 1 | 3 |  | 1 | -4 | | 5 | |
| 49 | | 3 | 16 | 1 |  | -4 | 5 | | -84 | |

The answer is 52−1 ≡ −84+ 257 = 173.

Second, we compute the slope of the tangent line

c = = [3(50)2 − 4](173) = 7496⋅173 = 43⋅173 ≡ 243 (mod 257)

Third, we can start compute the

*x*2 = c2 – 2*x*1 = 2432 – 2⋅50 = 196 – 100 = 96 (mod 257)

Fourth, we can compute

*y*2 = c(*x*1 – *x*2) – *y*1 = 243⋅(50 – 96) – 26

= 243⋅( – 46) – 26 = 243⋅( – 46+257) – 26

= 243(211) – 26 = 130 – 26 = 104 (mod 257).

A double point here is P2(*x*2, *y*2) = (96, 104).

1. **Add Point**

To compute P3(*x*3, *y*3) = P1(*x*1, *y*1) ⊕ P2(*x*2, *y*2) = (50, 26) ⊕ (96, 104).

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 line connecting (*x*1, *y*1) and (*x*2, *y*2)

then

*x*3 = *m*2 – (*x*1 + *x*2) and *y*3 = *m*⋅(*x*1 – *x*3) – *y*1.

Let us add 2 points, namely, P1(*x*1, *y*1) + P2(*x*2, *y*2) = (50, 26) ⊕ (96, 104).

First, we compute denominator of the slope of secant line,

*x*2 – *x*1 = 96 – 50 = 46.

Extended Euclidean Algorithm

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| b = | *a* | *q* | +*r* |  | u | v | w = uvq |
| 257 | 46 | 5 | 27 |  | 0 | 1 | -5 |
| 46 | 27 | 1 | 19 |  | 1 | -5 | 6 |
| 27 | 19 | 1 | 8 |  | -5 | 6 | -11 |
| 19 | 8 | 2 | 3 |  | 6 | -11 | 28 |
| 8 | 3 | 2 | 2 |  | -11 | 28 | -67 |
| 3 | 2 | 1 | 1 |  | 28 | -67 | 95 |

Second, we need to compute an inverse of the denominator,

(*x*2 – *x*1)−1 = 46−1 ≡ 95 (mod 257).

Let us compute the numerator = *y*2 – *y*1 = 104 – 26 = 78.

Third, the slope of secant line shall be

= 78⋅95 ≡ 214 (mod 257).

Finally, we can compute the add point,

*x*3 = *m*2 – (*x*1 + *x*2) = 2142 – (50 + 96) = 50 – (50 + 96) = −96 +257 ≡ 161 (mod 257).

and

*y*3 = *m*(*x*1 – *x*3) – *y*1 = 214⋅(50 – 161) – 26 = 214⋅(−111) – 26 = 214⋅(−111+257) – 26

= 214⋅(146) – 26 = 147 − 26 ≡ 121 (mod 257)

Final answer is 3⊗(50, 26) = (161, 121). Additional lesson for this tutorial is 3⊗(50, 26) = 3⊗52⊗(1, 2) =156⊗(1, 2) = (156 – 118)⊗(1, 2) = 38⊗(1, 2) = (161, 121).

Table 5: A list of points on a curve E: *y*2 = *x*3−4*x*+7 (mod 257)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *i* | *xi* | *yi* | *i* | *xi* | *yi* | *i* | *xi* | *yi* |
| 1 | 1 | 2 | 21 | 161 | 136 | 41 | 34 | 232 |
| 2 | 239 | 186 | 22 | 193 | 197 | 42 | 57 | 184 |
| 3 | 46 | 28 | 23 | 72 | 211 | 43 | 65 | 47 |
| 4 | 97 | 131 | 24 | 114 | 2 | 44 | 209 | 173 |
| 5 | 18 | 192 | 25 | 142 | 255 | 45 | 96 | 104 |
| 6 | 49 | 36 | 26 | 103 | 154 | 46 | 147 | 128 |
| 7 | 50 | 231 | 27 | 16 | 21 | 47 | 130 | 200 |
| 8 | 28 | 197 | 28 | 44 | 132 | 48 | 172 | 130 |
| 9 | 112 | 53 | 29 | 36 | 197 | 49 | 22 | 95 |
| 10 | 22 | 162 | 30 | 36 | 60 | 50 | 112 | 204 |
| 11 | 172 | 127 | 31 | 44 | 125 | 51 | 28 | 60 |
| 12 | 130 | 57 | 32 | 16 | 236 | 52 | 50 | 26 |
| 13 | 147 | 129 | 33 | 103 | 103 | 53 | 49 | 221 |
| 14 | 96 | 153 | 34 | 142 | 2 | 54 | 18 | 65 |
| 15 | 209 | 84 | 35 | 114 | 255 | 55 | 97 | 126 |
| 16 | 65 | 210 | 36 | 72 | 46 | 56 | 46 | 229 |
| 17 | 57 | 73 | 37 | 193 | 60 | 57 | 239 | 71 |
| 18 | 34 | 25 | 38 | 161 | 121 | 58 | 1 | 255 |
| 19 | 79 | 224 | 39 | 141 | 183 | 59 | -1 | -1 |
| 20 | 141 | 74 | 40 | 79 | 33 | 60 | 1 | 2 |

Step 0: My sample number is *i*=10+42=52. I am taking P1(*x*1, *y*1) = (50, 26).

Step 1: 2⊗P1(*x*1, *y*1) = (96, 104)

P2(*x*2, *y*2) = (96, 104)

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

3⊗(50, 26) = 3⋅52⊗(1, 2) =(3⋅52 mod 59)⊗(1, 2) = 38⊗(1, 2) = (161, 121).

Let us introduce a basic sum. Given a target sum =199.

Let us compute ⊗

|  |  |  |  |
| --- | --- | --- | --- |
| *i* | *ai* | Left | Right |
| 8 | 1 | (1, 2) | (239, 186) |
| 7 | 1 | (46, 28) | (97, 131) |
| 6 | 0 |  |  |
| 5 | 0 |  |  |
| 4 | 0 |  |  |
| 3 | 1 |  |  |
| 2 | 1 |  |  |
| 1 | 1 |  |  |