Numericals

ECC →

$$y^2 = x^3 + ax + b$$

elliptic curve = set of pts obtained as a result of solving elliptical funcn. over a predefined space

Scalar multiplication :

$2 * P$ $\quad P \Rightarrow (x, y)$

↳ results in point on the curve

⇓

Key gen + exchange

ECDH + ECDSA

1. Compute all points on curve
2. $-P$ given a point P on EC
3. Addn. over Z_p

TYPE 1 - MATCHING POINTS

Q. $E_{11}(1,6)$ $\rightarrow$ $a=1$, $b=6$

$Z_p = Z_{11}$

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

$$y^2 \bmod 11 = (x^3 + x + 6) \bmod 11$$

Range of points $= 0$ to $p-1$ $= (0, 10)$

$x, y \leftarrow (0, 10) \Rightarrow$ LHS = RHS

x,y	$(x^3 + x + 6) \bmod 11$	$y^2 \bmod 11$	
0	6	0	
1	8	1	
2	5	4	(2,4)
3	3	9	(3,5) (3,6)

4	8	5	(5,2) (5,9)
5	4	3	(7,2) (7,9)
6	8	3	(8,8) (8,3)
7	4	5	(10,2) (10,9)
8	9	9	
9	7	4	
10	4	1	

↳ p will be given

↳ if in $E_p(x,y)$ form $a = x$ $b = y$

↳ subst in curve eqn. $y^2 \bmod p = x^3 + ax + b) \bmod p$

↳ All points $(0, p-1) \Rightarrow$ LHS = RHS

TYPE 2 - COMPUTE '$-p$'

↳ $p(x, y)$

↳ compute $-p$

↳ $(p) = (x, y) \Rightarrow (-p) = (x, -y)$

Q. $y^2 = x^3 + 4x + 20$ $\quad p = 29$

$(x, y) = (4, 8)$

$p \Rightarrow (4, 8)$

$-p \Rightarrow (4, -8) \Rightarrow$ Additive Inv. $(4, 21)$

Q. $E_{23}(1, 1)$ $\quad P(13, 7)$

$p = 23$

$\hookrightarrow y^2 = x^3 + x + 1$

$(P) = (13, 7)$

$(-P) = (13, -7)$

↳ Add. inverse = $(13, 16)$

$= \underline{-P}$

TYPE 3 - ADDITION OVER Z_p

↳ identify curve eqn.

↳ Select points P & Q lie on curve

↳ Calculate slope b/w P & Q

$$P \neq Q \Rightarrow \lambda = \frac{y_q - y_p}{x_q - x_p} \mod p$$

$$P = Q \Rightarrow \lambda = \frac{3x_p^2 + a}{2 * y_p} \mod p$$

Sum ⇒ $R = x_r = \lambda^2 - x_p - x_q \mod p$

$y_r = \lambda * (x_p - x_r) - y_p \mod p$

Q. $P(3,10)$ $Q=(9,7)$ $E_{23}(1,1)$

$P+Q=?$

$y^2 = x^3 + x + 1 \mod 23$

$P \neq Q \Rightarrow \lambda = \frac{y_q - y_p}{x_q - x_p} = \frac{7-10}{9-3} \mod 23$

$= \frac{-1}{2} \mod 23$

$= -(2)^{-1} \mod 23$ $= -12$

$\hookrightarrow$ $2 \times x \mod 23 = 1$

$= -12 \mod 23 \Rightarrow \underline{\underline{11}}$

R=) $x_r = \lambda^2 - x_p - x_q \mod 23$
$= 121 - 3 - 9 \mod 23 = 17$

$y_r = \lambda * (x_p - x_r) - y_p \mod p$

$= (11 * (3 - 17) - 10)\ 23$

$(-154 - 10) \bmod 23$

$= -164 \bmod 23$

$= 20 \bmod 23$

$= 20$

$\therefore R(17, 20)$

Q. $y^2 = x^3 + 2x + 3 \bmod 17$ $\quad P = (5, 11)$

$2P \Rightarrow P + P$

$$\lambda = \frac{3 * x_p^2 + a}{2 * y_p} = \frac{3 * 25 + 2}{2 * 11}$$

$$= \frac{77}{22} \bmod 17$$

$77 \bmod 17 \Rightarrow 9$ $\qquad$ $22 \bmod 17 \Rightarrow 5$

$9 \times 5^{-1} \bmod 17$

$\downarrow$

7

$\Rightarrow 9 \times 7 \bmod 17$

$= 12$

$x_r = \lambda^2 - x_p - x_q \bmod p$

$y_r = \lambda * (x_p - x_r) - y_p \bmod p$

$x_r = 12^2 - 5 - 5 \bmod 17$

$= 15$

$y_r = 12 * (5 - 15) - 11 \bmod 17$

$= -120 - 11 \bmod 17$

$= -131 \bmod 17$

$= 5 \bmod 17 = 5$

$P + Q \Rightarrow P = Q \quad \lambda = \frac{3 * x_p^2 + a}{2 * y_p} \bmod p$

$P \neq Q \quad \lambda = \frac{y_q - y_p}{x_q - x_p} \bmod p$

$$x_r = \lambda^2 - x_p - x_q \mod p$$
$$y_r = \lambda * (x_p - x_r) - y_p \mod p$$