Elliptic Curve Review - Formulas Adding

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

Curve is called $E_p(a,b)$

$4a^3 + 27b^2 \not\equiv 0 \pmod p$

$P = (x_P, y_P) \quad Q = (x_Q, y_Q) \quad R = P + Q$

1. $P + O = P$
2. $P + (-P) = O$, if $P = (x_P, y_P)$ Then $-P = (x_P, -y_P)$ under mod $-y_P \equiv p - y_P$.
3. If $P \neq Q$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

4. If $P = Q$, $\lambda = \dfrac{3x_P^2 + a}{2y_P} \bmod p$

Division is Multiply by mod Inverse!

$P_{23}(1,1) \qquad P = (3,10) \quad Q = (9,7)$

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = -3(6^{-1} \bmod 23)$$

$$= (-1)(3) \times (2^{-1} \bmod 23)(3^{-1} \bmod 23)$$

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

$$= (-1)12 = -12 \equiv 11 \pmod{23}$$

$$x_R = (11^2 - 3 - 9) = 121 - 12 = 109 \equiv \boxed{17 \bmod 23}$$

$$y_R = (11(3-17) - 10) = 11(-14) - 10$$
$$\equiv 11(9) - 10$$
$$\equiv 89 \equiv \boxed{20 \bmod 23}$$

On $P_{23}(1,1)$ $\quad (3,10) + (9,7) = (17,20)$

$P + P = R \qquad P = (3,10) \qquad E_{23}(1,1)$

$$\lambda = \frac{3x_p^2 + a}{2y_p} = \frac{3 \cdot 3^2 + 1}{2 \times 10} = \frac{28}{20} = \frac{7}{5}$$

$$= 7(5^{-1} \bmod 23)$$
$$= 7(-9)$$
$$\equiv -63 \equiv 6 \pmod{23}$$

$23 = 4 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$

$3 - 2 = 1$
$3 - (5 - 3) = 1$
$2 \times 3 - 5 = 1$
$2(23 - 4 \times 5) - 5 = 1$
$2 \times 23 - 9 \times 5 = 1$

$$x_R = (\lambda^2 - x_p - x_p) = 6^2 - 3 - 3$$
$$= 30 \equiv 7 \pmod{23}$$

$$y_R = (\lambda(x_p - x_R) - y_p) = 6(3-7) - 10$$
$$= 6(-4) - 10$$
$$= -34$$
$$\equiv \boxed{12 \bmod (23)}$$

$$\boxed{2 \times (3,10) = (7,12)}$$

$E_{31}(2,3) \quad y^2 = x^3 + 2x + 3 \mod 31$

$$4a^3 + 27b^2 = 4 \cdot 2^3 + 27 \cdot 3^2$$
$$= 32 + 243$$
$$= 275$$
$$- 248$$
$$27 \checkmark$$

$P = (7,9) \qquad Q = (19,24)$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{24-9}{19-7} = \frac{15}{12} = \frac{5}{4} = 5(4^{-1} \mod 31)$$
$$\equiv 5 \times 8 \equiv 40 \equiv \boxed{9 \mod 31}$$

$$x_R = (\lambda^2 - x_P - x_Q) = (9^2 - 7 - 19)$$
$$= 81 - 26 = 55 \equiv \boxed{24 \mod 31}$$

$$y_R = (\lambda(x_P - x_R) - y_P) = 9(7-24) - 9$$
$$= 9(7-24-1)$$
$$= 9(-18)$$
$$\equiv 9(13) \equiv 117$$
$$-93$$
$$24$$

On $E_{31}(2,3) \quad (7,9) + (19,24) = (24,24)$

$Q = (19, 24)$ $\quad Q + Q$

$$\lambda = \frac{3x_Q^2 + a}{2y_Q} = \frac{3 \cdot 19^2 + 2}{48}$$

$$= \frac{3 \cdot (-12)^2 + 2}{17} = \frac{434}{17} \equiv 0 \times 17^{-1} \equiv 0$$

$$x_R = (\lambda^2 - 2x_Q) = 0^2 - 2 \cdot 19 \quad 24$$

$$= -38 \equiv \text{[illegible]} \bmod 31$$

$$y_R = 0(19 - \text{[illegible]}) - 24 \equiv -24 \equiv 7 \bmod 31$$

On $E_{31}(2,3)$ $\quad 2x(19,24) = (24,7)$

Can make elliptic curves with polynomials under GF_{2^k}.

Points (x,y) where x and y are polynomials

$(1010, 1110) + (\ldots)$

$x^3+x \quad x^3+x^2+x$

$= (\quad)$