EC 1-6, 9

EC-1) $y^2 = x^3 + 17$ $P_1 = (-2, 3)$ $P_2 = (2, -5)$

$a_1 = 0$ $a_3 = 0$ $a_2 = 0$ $a_4 = 0$ $a_6 = 17$

$$\lambda = \frac{y_2 - y_1}{x_2 - x} = \frac{-5-3}{2+2} = -\frac{8}{4} = -2$$

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 = (-2)^2 - (-2) - 2 = 4 + 2 - 2 = 4$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3 = -(-2)(4) - (-1) = 8 + 1 = 9$$

$$\nu = \frac{(3)(2) - (-5)(-2)}{2+2} = \frac{6-10}{4} = -1$$

$(-2, 3) + (2, -5) = (4, 9)$

Line intersection

$m = -2$

$y = mx + b \rightarrow 3 = -2x + b \rightarrow y = -2x - 1$

$y^2 = x^3 + 17$ $y = -2x - 1$

$0 = (x+2)(x-2)(x-4)$

$y = -2(4) - 1 = -9$

$(-2, 3) + (2, -5) + (4, -9) = 0$

$(-2, 3) + (2, -5) = -(4, -9)$

$y^2 = 4^3 + 17 = 81$ $y = -9, 9$

$(-2, 3) + (2, -5) = (4, 9)$

2) $y^2 = x^3 + 17$

$\frac{d}{dx}(y^2) = \frac{d}{dx}(x^3 + 17)$

$(2y)\left(\frac{dy}{dx}\right) = 3x^2$

$\frac{dy}{dx} = \frac{3x^2}{2y}$ $P = (-2, 3)$

$\frac{dy}{dx} = \frac{3(4)}{2(3)} = 2$

$y - 3 = 2(x + 2) = y = 2x + 7$

$y^2 = x^3 + 17$

$(2x+7)^2 = x^3 + 17$

$4x^2 + 28x + 49 = x^3 + 17$

$0 = x^3 - 4x^2 - 28x - 32$

$0 = (x+2)^2 (x-8)$

$x = 8$

$y = (2)(8) + 7 = 23$

$2[-2, 3] + [8, 23] = 0$

$2[-2, 3] = -[8, 23] = [8, -23]$

$y^2 = 8^3 + 17 = \pm 23$

EC-3) $2Q = [8, -23]$

$Q + R = \left[\frac{1}{4}, -\frac{33}{8}\right]$

$3Q = \left[\frac{19}{25}, \frac{522}{125}\right]$

$4Q = \left[\frac{752}{529}, -\frac{54239}{12167}\right]$

$2R = \left[-\frac{64}{25}, \frac{59}{125}\right]$

$Q - R = [4, 9]$

$2Q - R = [-1, -4]$

$3Q - R = [52, 375]$

$4Q - R = [-\frac{206}{81}, \frac{541}{729}]$

$2Q - 2R = [-\frac{8}{9}, \frac{109}{27}]$

$E(-4)$ $y^2 = x^3 - 4$

$\mathbb{F}_2$ $0^2 = 0$, $1^2 = 1$

x	$x^3 - 4$	$y \pm \sqrt{x^3-4}$
0	0	$(0,0)$
1	1	$(1,1)$ and O

$\mathbb{F}_3$ $0^2 = 0$ $1^2 = 1$ $2^2 = 1$

x	$x^3 - 4$	$y \pm \sqrt{x^3-4}$
0	2	–
1	0	$(1,0)$
2	1	$(2,1), (2,2)$, and O

$\mathbb{F}_5$

x	$x^3 - 4$	$y \pm \sqrt{x^3-4}$
0	1	$(0,1)$, $(0,4)$
1	2	–
2	4	$(2,2), (2,3)$
3	3	–
4	1	$(4,0)$ and O

EC-5) $Q = [0,0]$ $P = 7$

$y^2 + y = x^3 - x$

$a_1 = 0$ $a_3 = 1$ $a_2 = 0$ $a_4 = -1$ $a_5 = 0$

e = [0, 0, 1, -1, 0]

e = Mod(1, p) * e

ellpow(e, q, 2) = [1, 0]

ellpow(e, q, 3) = [6, 6]

ellpow(e, q, 4) = [2, 4]

ellpow(e, q, 5) = [2, 2]

ellpow(e, q, 6) = [6, 0]

ellpow(e, q, 7) = [1, 6]

ellpow(e, q, 8) = [0, 6]

ellpow(e, q, 9) = [0, 0]

9Q

EC-6) ec = [0, 0, 0, 0, -4]   g = [2, 2]

p = nextprime(10^{25})

Mod(ag, 2^{16}) = 4542

Message = `tiara is a recursive acronym'

EC-9) $f = t^{16} + t^6 + t^2 + t + 1$

E = [1, 0, 0, 0, 1]

Private = 31415

ellpow(E, public, private) =

$t^{14} + t^{13} + t^{12} + t^{9} + t^{6} + t^{2}$

$= 0111001001000100$

'no dark sarcasm in the classroom'