Jenin Ali Hw #9

Hi! Work and notes can be found on the next pages! :)

$\Delta = 10$

I) i) $\Delta \neq 0$ ✓

curve is non singular $\Rightarrow$ it is an elliptical curve

ii) $(0, \sqrt{11})$, $(1, \sqrt{17})$, $(2, \sqrt{29})$

iii)

x	$y^2 = x^3 + 5x + 11 \mod 17$	y	(x, y)
0	/	/	/
1	0	0	(1,0)
2	/	/	/
3	2	6, 11	(3,6), (3,11)
4	/	/	/
5	8	5, 12	(5,5), (5,12)
6	2	6, 11	(6,6), (6,11)
7	15	7, 10	(7,7), (7,10)
8	2	6, 11	(8,6), (8,11)
9	/	/	/
10	/	/	/
11	/	/	/
12	/	/	/
13	4	2, 15	(13,2), (13,5)
14	/	/	/
15	1	1, 16	(15,1), (15,16)
16	9	3, 14	(16,3), (16,4)

iv.) $2P = (3, 11)$

v.) $P + Q = (6, 6)$

vi.) $10 \leq N \leq 26$

1) i) $y^2 \equiv x^3 + 5x + 11 \bmod 17$

Standard form of an elliptic curve

$y^2 \equiv x^3 + ax + b \bmod p$

$a = 5$

$b = 11$

$p = 17$

Discriminant to ensure non-sing curve:

$a = 5$
$b = 11$

$\Delta = -16(4a^3 + 27b^2)$

$\Delta = 4(5^3) + 27(11^2) = 4(125) + 27(121) = 500 + 3267 = 3767$

$\Rightarrow$ $3767 \bmod 17 = 3767 - 17 \cdot 221 = 10 \neq 0$

$\Delta \neq 0$, curve non singular, elliptical curve!

$x = 0, 1, 2, 3$

ii) $y^2 = 0^3 + 5(0) + 11 = 11$

$\sqrt{y^2} = \sqrt{11}$

$y = \pm\sqrt{11}$ $\Rightarrow$

$\boxed{(0, \sqrt{11}), (0, -\sqrt{11})}$

$y^2 = 1^3 + 5(1) + 11 = 17$

$\sqrt{y^2} = \sqrt{17}$

$y = \pm\sqrt{17}$

$\boxed{(1, \sqrt{17}), (1, -\sqrt{17})}$

$y^2 = 2^3 + 5(2) + 11 = 29 \Rightarrow y = \pm\sqrt{29} \Rightarrow$

$\Rightarrow \boxed{(2, \sqrt{29}), (2, -\sqrt{29})}$

~~$y^2 = 3^3 + 5(3) + 11 = 27 + 15 + 11$~~ $= 53 \Rightarrow y = \pm\sqrt{53} \Rightarrow$

$\Rightarrow \boxed{(3, -\sqrt{53})\ (3, \sqrt{53})}$

$\boxed{(0, \sqrt{11}), (1, \sqrt{17}), (2, \sqrt{29})}$

iii) $y^2 \equiv x^3 + 5x + 11 \bmod 17$ $\rightsquigarrow y^2$ quadratic residue?
ouc whether integer square root mod 17

$x = 0$

$y^2 = 0^3 + 5(0) + 11 = \underbrace{11}\bmod 17$
$\hookrightarrow 11^{(17-1)/2} \bmod 17 \Rightarrow 11^8 \bmod 17 = 16$
$\neq$ (not 1)
x

No integer $y \Rightarrow$ ignore $x = 0$

$x = 1$

$y^2 = 1^3 + 5(1) + 11 = 17 \equiv 0 \bmod 17 \Rightarrow y = 0 \Rightarrow (1, 0)$ ✓ P+

$x = 2$

$y^2 = 2^3 + 5(2) + 11 = 29 \equiv \underbrace{12}\bmod 17$
$\hookrightarrow 12^8 \bmod 17 = 16$ (not 1) quadratic residue

No integer $y \Rightarrow$ ignore $x = 2$

$x = 3$

$y^2 = 3^3 + 5(3) + 11 = 27 + 15 + 11 = 53 \equiv 2 \bmod 17$
quadratic residue
$\hookrightarrow 2^8 \bmod 17 = 1$ ✓
$\hookrightarrow y = 6$ since $6^2 \equiv 2 \bmod 17$
negative root:
$-6 \equiv 11 \bmod 17 \Rightarrow$
pr
$(3, 6), (3, 11)$

$y^2 \equiv n \bmod p$ Euler!

$y^2 = x^3 + 5x + 11 \bmod 17$

~~x=0~~ => ignore, calculated previously

→ $x=1$ => calculated previously $y=0$ => (1, 0)

~~x=2~~ => ignore, calculated previously

→ $x=3 \Rightarrow y^2 = 3^3 + 15 + 11 = 27 + 15 + 11 = 53 \equiv 2 \bmod 17$

quadratic residue

$2^8 \bmod 17 = 1 \Rightarrow$ ✓

square root

$y = 6$ $\quad 6^2 \equiv 2 \bmod 17$ ✓

$-6 \equiv 11 \bmod 17$ ✓

(3, 6), (3, 11)

$x=4$ => ignore, calculated previously

→ $x=5 \Rightarrow 125 + 25 + 11 = 161 \equiv 8 \bmod 17$

(5, 5), (5, 12)

quadratic residue $8^8 \bmod 17 \equiv 1$ ✓ $\Rightarrow$ $y=5$ $\quad 5^2 \equiv 8 \bmod 17$ ✓

$-5 \equiv 12 \bmod 17$

→ $x=6 \Rightarrow 257 \equiv 2 \bmod 17 \Rightarrow$ quadratic residue? => yes => $y = 6$

$-6 \equiv 11 \bmod 17$ ✓ => (6, 6), (6, 11)

→ $x = 7 \Rightarrow 389 \equiv 5 \bmod 17 \Rightarrow$ quad residue? => yes => $7^2 \equiv 15$

(7, 7), (7, 10) $\quad 15^8 \bmod 17 = 1$ ✓ $\quad -7 \equiv 10$

→ $x=8 \Rightarrow 563 \equiv 2 \bmod 17 \Rightarrow 6^2 \equiv 2 \bmod 17$

$-6 \equiv 11 \bmod 17$ => (8, 6), (8, 11)

~~x=9~~ => $785 \equiv 3 \bmod 17$ => quadratic residue? => $3^8 \bmod 17 \equiv 16$

not 1!

$x=10 \Rightarrow \cancel{7^8 \bmod 17 \not\equiv 16}$ not 1

$x=11 \Rightarrow \cancel{x=9, 3 \text{ no quad residue}}$

Q residue

$x=12 \Rightarrow \cancel{1799 \equiv 6 \bmod 17 \Rightarrow 6^8 \bmod 17 \not\equiv 16}$ not 1

Q reside

$\rightarrow x=13 \Rightarrow \cancel{2273} \equiv 4 \bmod 17 \Rightarrow 4^8 \bmod 17 \equiv 1$ ✓ $\Rightarrow 2^2 \equiv 4 \bmod 17$

$(13,2), (13,5)$ ✓ $-2 \equiv 15 \bmod 17$

$x=14 \Rightarrow \cancel{2825 \equiv 14 \bmod 17 \Rightarrow 14^8 \bmod 17 \not\equiv 16}$

$\rightarrow x=15 \Rightarrow \cancel{3461} \equiv 1 \bmod 17 \Rightarrow 1^8 \equiv 1 \bmod 17 \Rightarrow 1^2 \equiv 1 \bmod 17$

$(15,1)$, $(15,16)$ $-1 \equiv 16 \bmod 17$

$\Rightarrow x=16 \Rightarrow \cancel{4187} \equiv 9 \bmod 17 \Rightarrow$ ✓ $y=3 \Rightarrow 3^2 \equiv 9 \bmod 17$

$(16,3), (16,4)$ $-3 \equiv 14 \bmod 17$

~~Step 1~~ $P=(x_1,y_1)$

iv) $y^2 \equiv x^3+5x+11 \bmod 17 \Rightarrow P=(3,6) \Rightarrow \lambda = \dfrac{3x^2+a}{2y_1} \bmod p \Rightarrow$

$x_2 = \lambda^2 - 2x_1 \bmod p \Rightarrow y_2 = \lambda(x_1 - x_2) - y_1 \bmod p \Rightarrow$

~~Step 2~~

$\Rightarrow a=5, p=17, x_1=3, y_1=6 \Rightarrow 3x_1^2+a = 3(3^2)+5 = 27+5 = 32$

$\Rightarrow 2y_1 = 12 \Rightarrow \lambda = \dfrac{32}{12} \bmod 17 \Rightarrow 12^{-1} \bmod 17 \Rightarrow 12^{-1} \equiv 10 \bmod 17 \Rightarrow$

$\Rightarrow \lambda = (32 \times 10) \bmod 17 = 14 \Rightarrow \lambda = 14$ ~~Step 3~~ $\Rightarrow x_2 = \lambda^2 - 2x_1 \bmod 17 =$

$\Rightarrow x_2 = 14^2 - 2(3) \bmod 17 = 196 - 6 = 190 \equiv 3 \bmod 17 \Rightarrow x_2 = 3$

Step 4

$y_2 = \lambda(x_1 - x_2) - y_1 \bmod 17 \Rightarrow 14(3-3) - 6 \equiv -6 \bmod 17 \Rightarrow$

$y_2 = 11 \bmod 17$ ✓ $\Rightarrow$ Step 5 $\boxed{2P = (3, 11)}$

v.) $y^2 \equiv x^3 + 5x + 11 \bmod 17 \Rightarrow$ Step 1 slope $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p \Rightarrow (x_3, y_3) \Rightarrow$

$\Rightarrow x_3 = \lambda^2 - x_1 - x_2 \bmod p \Rightarrow y_3 = \lambda(x_1 - x_3) - y_1 \bmod p \Rightarrow$

$p = 17$, $x_1 = 3$, $y_1 = 6$; $x_2 = 7$, $y_2 = 7 \Rightarrow$ Step 2 $y_2 - y_1 = 7 - 6 = 1 \Rightarrow$

$x_2 - x_1 = 7 - 3 = 4 \Rightarrow 4^{-1} \bmod 17 \Rightarrow 4^{-1} \equiv 13 \bmod 17 \Rightarrow$

$\lambda = (1 \times 13) \bmod 17 = 13$ Step 3 $x_3 = \lambda^2 - x_1 - x_2 \bmod 17 \Rightarrow x_3 = 13^2 - 3 - 7$

$\Rightarrow 169 - 3 - 7 = 156 \equiv 6 \bmod 17 \Rightarrow x_3 = 6 \Rightarrow$ Step 4 $y_3 = \lambda(x_1 - x_3) - y_1 \bmod 17$

$\Rightarrow 13(3-6) - 6 \bmod 17 = -45 \equiv 6 \bmod 17 \Rightarrow y_3 = 6 \Rightarrow P + Q = (6, 6)$

vi) $|N - (p+1)| \le 2\sqrt{p} \Rightarrow p + 1 - 2\sqrt{p} \le N \le p + 1 + 2\sqrt{p} \Rightarrow$

$p = 17 \Rightarrow 2\sqrt{17} \Rightarrow$ Step 1 $\sqrt{17} \approx 4.123 \Rightarrow 2\sqrt{17} \approx 8.246 \Rightarrow$

N is integer $\Rightarrow 2\sqrt{17} \approx 8 \Rightarrow$ Compare bounds $17 + 1 - 8 \le N \le 17 + 1 + 8 \Rightarrow$

$10 \le N \le 26$