OLD DOMINION UNIVERSITY
CS 463

# Homework 8

Madelene McFarlane

10/27/2023

#01096496

Question 1. Consider the curve $y^2 \equiv x^3 + 5x + 11 \bmod 17$.

(i) Confirm that it is an elliptic curve.

(ii) Determine points on the curve over real numbers with $x = 0, 1, 2,$ and $3$.

CS 463 Madeleine McFarlane

HW8

■ : answer

$y^2 \equiv x^3 + 5x\ 11 \bmod 17$ (with $5 = a$, $11 = b$, $17 = p$)

(i) $4 \cdot a^3 + 27 \cdot b^2 \bmod p \neq 0$

$(4(5)^3 + 27 \cdot (11)^2) \bmod 17$

$4 \cdot 125 + 27 \cdot 121 \bmod 17$

$500 + 3{,}267 \bmod 17$

$3{,}767 \bmod 17$

$\boxed{10}$

$\boxed{10 \neq 0}$

yes, it is an elliptic curve

(ii) 0, 1, 2, 3 $\quad x^3 + 5x\ 11 \bmod 17 = y^2$

$0 = 0^3 + 5(0) + 11 \bmod 17$

$11 \bmod 17$

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

$3.317$

$\boxed{(0, 3.317)}$ or $\boxed{(0, \sqrt{11})}$

$1 = 1^3 + 5(1) + 11 \bmod 17$

$1 + 5 + 11 \bmod 17$

$17 \bmod 17$

$0$

$\boxed{(1, 0)}$

$2 = 2^3 + 5(2) + 11 \bmod 17$

$8 + 10 + 11 \bmod 17$

$29 \bmod 17$

$\sqrt{12} = \sqrt{y^2}$

$\boxed{(2, 3.464)}$ or $\boxed{(2, \sqrt{12})}$

$3 = 3^3 + 5(3) + 11 \bmod 17$

$27 + 15 + 11 \bmod 17$

$53 \bmod 17$

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

$\boxed{(3, 1.414)}$ or $\boxed{(3, \sqrt{2})}$

(iii) Determine all the points on the curve over integer numbers (Hint: Take x=0, 1,2, ...,15,16; compute $y^2$. Find y. If you find that $y^2$ is not a perfect square, then keep on trying other mod 17 equivalents of $y^2$. For example, if $y^2 = 2$, then try other equivalents of 2 such as 19, 36, 53, ... In this case, we can stop at 36 since it is a perfect square. Sometimes you may not get any perfect square. This means there is no integer point. For example, if $y^2 = 7$, the other mod 17 equivalents are 24, 41, 58, 75, 92, 109, 126, 143, 160, 177, 194, 211, 228, 245, 262, 279. None of them are perfect squares. So we have no integer point. Also, you will get a + value and a – value since it is a square root. For the – value, since it is mod 17, add 17 to make it positive. For example, if $y^2 = 25$, y = +5, -5. So we take it as y= +5, +12. The final answers are (x,y) points on the elliptic curve.

CS 463 Madelene McFarlane

HW8

(iii)

■ : answer

| x | $y^2 = x^3 + 5x + 11 \bmod 17$ P-val until 256 | Y (int val) | (x, y) |
|---|---|---|---|
| 0 | 11 = 28, 45, 62, 79, 96, 113, 130, 147, 164, 181, ... 249 | | |
| 1 | 17 = $\boxed{0}$, 17, 34, 51, 68, ..., 221, 238, 255 | 0 | (1, 0) |
| 2 | 29 = 12, 29, 46, 63, 80, 97, 114, 131, 148, 165, ...., 250 | | |
| 3 | 53 = 2, 19, $\boxed{36}$, 53, 70, 87, 104, $\boxed{121}$, 138, 155, ..., 240 | 6, 11 | (3, 6) (3, 11) |
| 4 | 95 = 10, 27, 44, 61, 78, 95, 112, 129, 146, 163, 180, 197, ..., 248 | | |
| 5 | 161 = 8, $\boxed{25}$, 42, 59, 76, 93, 110, 127, $\boxed{144}$, 161, 178, 195, ..., 246 | 5, 12 | (5, 5) (5, 12) |
| 6 | 257 = 2, 19, $\boxed{36}$, 53, 70, 87, 104, $\boxed{121}$, 138, 155, 172, 189, ..., 240 | 6, 11 | (6, 6) (6, 11) |
| 7 | 389 = 15, 32, $\boxed{49}$, 66, 83, 100, 117, 134, 151, 168, 185, 202, ..., 253 | 7 | (7, 7) |
| 8 | 563 = 2, 19, $\boxed{36}$, 53, 70, 87, 104, $\boxed{121}$, 138, 155, 172, 189, ..., 240 | 6, 11 | (8, 6) (8, 11) |
| 9 | 785 = 3, 20, 37, 54, 71, 88, 105, 122, 139, 156, 173, 190, ..., 241 | | |
| 10 | 1061 = 7, 24, 41, 58, 75, 92, 109, 126, 143, 160, 177, ..., 245 | | |
| 11 | 1,397 = 3, 20, 37, 54, 71, 88, 105, 122, 139, 156, 173, 190, ..., 241 | | |
| 12 | 1,799 = 14, 31, 48, 65, 82, 99, 116, 133, 150, 167, 184, ..., 252 | | |

0) $0^3 + 5(0) + 11 \bmod 17$

11 mod 17

$11 \rightarrow$ 1 val

initial val

$17 \cdot 1 + 11 = 28$
$17 \cdot 2 + 11 = 45$
$17 \cdot 3 + 11 = 62$
$17 \cdot 4 + 11 = 79$
$17 \cdot 5 + 11 = 96$
$17 \cdot 6 + 11 = 113$
$17 \cdot 7 + 11 = 130$
$17 \cdot 8 + 11 = 147$
$17 \cdot 9 + 11 = 164$
$17 \cdot 10 + 11 = 181$
$17 \cdot 11 + 11 = 198$
$17 \cdot 12 + 11 = 215$
$17 \cdot 13 + 11 = 232$
$17 \cdot 14 + 11 = 249$

1) $1^3 + 5(1) + 11 \bmod 17 \rightarrow \underline{17} \bmod 17 \rightarrow \underline{0}$

$17 \cdot 1 + 0 = 17$
$17 \cdot 2 + 0 = 34$
$17 \cdot 3 + 0 = 51$
$17 \cdot 4 + 0 = 68$
$17 \cdot 13 + 0 = 221$
$17 \cdot 14 + 0 = 238$
$17 \cdot 15 + 0 = 255$

2) $2^3 + 5(2) + 11 \bmod 17 \rightarrow \underline{29} \bmod 17 \rightarrow 12$

$17 \cdot 1 + 12 = 29$
$17 \cdot 2 + 12 = 46$
$17 \cdot 11 + 12 = 199$
$17 \cdot 12 + 12 = 216$
$17 \cdot 13 + 12 = 233$
$17 \cdot 14 + 12 = 250$

3) $3^3 + 5(3) + 11 \bmod 17 \rightarrow 53 \bmod 17 \rightarrow \underline{2}$

$17 \cdot 1 + 2 = 19$
$17 \cdot 2 + 2 = \boxed{36}$
$17 \cdot 3 + 2 = 53$
$17 \cdot 4 + 2 = 70$
$17 \cdot 7 + 2 = \boxed{121}$
$17 \cdot 13 + 2 = 223$
$17 \cdot 14 + 2 = 240$

4) $4^3 + 5(4) + 11 \bmod 17 \rightarrow \underline{95} \bmod 17 \rightarrow \underline{10}$

$17 \cdot 1 + 10 = 27$
$17 \cdot 2 + 10 = 44$
$17 \cdot 10 + 10 = 180$
$17 \cdot 14 + 10 = 248$

5) $5^3 + 5(5) + 11 \bmod 17 \rightarrow \underline{161} \bmod 17 \rightarrow \underline{8}$

$17 \cdot 1 + 8 = 25$
$17 \cdot 2 + 8 = 42$
$17 \cdot 10 + 8 = 178$
$17 \cdot 14 + 8 = 246$

6) $6^3 + 5(6) + 11 \bmod 17 \rightarrow \underline{257} \bmod 17 \rightarrow \underline{2}$

$17 \cdot 1 + 2 = 19$
$17 \cdot 2 + 2 = \boxed{36}$
$17 \cdot 13 + 2 = 223$
$17 \cdot 14 + 2 = 240$

7) $7^3 + 5(7) + 11 \bmod 17 \rightarrow \underline{389} \bmod 17 \rightarrow \underline{15}$

$17 \cdot 1 + 15 = 32$
$17 \cdot 2 + 15 = 49$
$17 \cdot 10 + 15 = 185$
$17 \cdot 14 + 15 = 253$

8) $8^3 + 5(8) + 11 \bmod 17 \rightarrow \underline{563} \bmod 17 \rightarrow \underline{2}$

$17 \cdot 1 + 2 = 19$
$17 \cdot 2 + 2 = 36$
$17 \cdot 13 + 2 = 223$
$17 \cdot 14 + 2 = 240$

9) $9^3 + 5(9) + 11 \bmod 17 \rightarrow \underline{785} \bmod 17 \rightarrow \underline{3}$

$17 \cdot 1 + 3 = 20$
$17 \cdot 2 + 3 = 37$
$17 \cdot 13 + 3 = 224$
$17 \cdot 14 + 3 = 241$

10) $10^3 + 5(10) + 11 \bmod 17$

$\underline{1061} \bmod 17 \rightarrow \underline{7}$

$17 \cdot 1 + 7 = 24$
$17 \cdot 2 + 7 = 41$
$17 \cdot 10 + 7 = 177$
$17 \cdot 14 + 7 = 245$

11) $11^3 + 5(11) + 11 \bmod 17$

$\underline{1,397} \bmod 17 \rightarrow \underline{3}$

$17 \cdot 1 + 3 = 20$
$17 \cdot 2 + 3 = 37$
$17 \cdot 13 + 3 = 224$
$17 \cdot 14 + 3 = 241$

12) $12^3 + 5(12) + 11 \bmod 17$

$\underline{1,799} \bmod 17 \rightarrow \underline{14}$

$17 \cdot 1 + 14 = 31$
$17 \cdot 2 + 14 = 48$
$17 \cdot 10 + 14 = 184$
$17 \cdot 14 + 14 = 252$

(iv) For a point P= (3,6), find 2P (or double)

(v) For two of the points P = (3,6) and Q =(7,7), find P+Q

(vi) Find the bound for the number of points on this curve using Hasse's theorem.

CS 463 HW8

Madeleine McFarlane

$x_3 = s^2 - x_1 - x_2 \bmod p$

$y_3 = s(x_1 - x_3) - y_1 \bmod p$

■ = answer

$s = (y_2 - y_1)/(x_2 - x_1) \bmod p$ $\quad P \neq Q$

$s = (3(x_1)^2 + a)/(2(y_1)) \bmod p$ $\quad P = Q$

(iv) (3,6) (3,6) $P = Q$ $\quad s = 14$

$s = (3(3)^2 + 5)/(2(6)) \bmod 17$

$\underset{(\bmod 17)}{32} / \underset{(\bmod 17)}{12} \bmod 17$

$15/12 \bmod 17$

$14 \bmod 17$

$14$

$x_3 = (14)^2 - 3 - 3 \bmod 17$

$190 \bmod 17$

$\boxed{x_3 = 3}$

$y_3 = 14(3-3) - 6 \bmod 17$

$-6 \bmod 17$

$\boxed{y_3 = 11}$

$\boxed{(3,11)}$

(v) (3,6) (7,7) $P \neq Q$

$s = (7-6)/(7-3) = 1/4 \bmod 17$

$17 \cdot 3 = 51 + 1 = 52/4 = 13$

$13 \bmod 17$

$s = 13$

$x_3 = (13)^2 - 3 - 7 \bmod 17$

$159 \bmod 17$

$\boxed{x_3 = 6}$

$\boxed{(6,6)}$

$y_3 = 13(3-6) - 6 \bmod 17$

$-45 \bmod 17$

$+17$

$+17$

$+17$

$\boxed{y_3 = 6}$

(vi)

$m + 1 - 2\sqrt{m} \leq \#E \leq m + 1 + 2\sqrt{m}$

$17 + 1 - 2\sqrt{17} \leq \#E \leq 17 + 1 + 2\sqrt{17}$

$18 - 2\sqrt{17} \leq \#E \leq 18 + 2\sqrt{17}$

$\boxed{9.75 \leq \#E \leq 26.25}$