Zelong Li

24569650

Discussion 102

TA: Qi Zhong

CS161 Homework 3

1.

E:

mod 3

|  |  |  |  |
| --- | --- | --- | --- |
| x |  | y | points |
| 0 | 0 | 0 | (0,0) |
| 1 | 2 | - | - |
| 2 | 1 | 1, 2 | (1,1), (1,2) |

Points on curve: (0,0), (2,1), (2,2)

mod 5

|  |  |  |  |
| --- | --- | --- | --- |
| x |  | y | points |
| 0 | 3 | - | - |
| 1 | 3 | - | - |
| 2 | 4 | 2, 3 | (2,2), (2,3) |
| 3 | 2 | - | - |
| 4 | 3 | - | - |

Points on curve: , (2,2), (2,3)

mod 7

|  |  |  |  |
| --- | --- | --- | --- |
| x |  | y | points |
| 0 | 3 | - | - |
| 1 | 1 | 1, 6 | (1,1), (1,6) |
| 2 | 5 | - | - |
| 3 | 0 | 0 | (3,0) |
| 4 | 6 | - | - |
| 5 | 1 | 1, 6 | (5,1), (5,6) |
| 6 | 5 | - | - |

Points on curve: , (1,1), (1,6), (3,0), (5,1), (5,6)

mod 11

|  |  |  |  |
| --- | --- | --- | --- |
| x |  | y | points |
| 0 | 3 | 5, 6 | (0,5), (0,6) |
| 1 | 8 | - | - |
| 2 | 8 | - | - |
| 3 | 9 | 3, 8 | (3,3), (3,8) |
| 4 | 6 | - | - |
| 5 | 5 | 4, 7 | (5,4), (5,7) |
| 6 | 1 | 1, 10 | (6,1), (6,10) |
| 7 | 0 | 0 | (7,0) |
| 8 | 8 | - | - |
| 9 | 9 | 3, 8 | (9,3), (9,8) |
| 10 | 9 | 3, 8 | (10,3), (10,8) |

Points on curve:, (0,5), (0,6), (3,3), (3,8), (5,4), (5,7), (6,1), (6,10), (7,0), (9,3), (9,8), (10,3), (10,8)

mod 13

|  |  |  |  |
| --- | --- | --- | --- |
| x |  | y | points |
| 0 | 3 | 4, 9 | (0,4), (0, 9) |
| 1 | 8 | - | - |
| 2 | 6 | - | - |
| 3 | 3 | 4, 9 | (3,4), (3,9) |
| 4 | 5 | - | - |
| 5 | 5 | - | - |
| 6 | 9 | 3, 10 | (6,3), (6,10) |
| 7 | 10 | 6, 7 | (7,6), (7,7) |
| 8 | 1 | 1, 12 | (8,1), (8,12) |
| 9 | 1 | 1, 12 | (9,1), (9,12) |
| 10 | 3 | 4, 9 | (10,4), (10,9) |
| 11 | 0 | 0 | (11,0) |
| 12 | 11 | - | - |

Points on curve: , (0,4), (0, 9), (3,4), (3,9), (6,3), (6,10), (7,6), (7,7), (8,1), (8,12), (9,1), (9,12), (10,4), (10,9), (11,0)

2.

E: mod p

|  |  |  |  |
| --- | --- | --- | --- |
| p | #E | tp | 2 |
| 3 | 4 | 0 | 3.46 |
| 5 | 3 | 3 | 4.47 |
| 7 | 6 | 2 | 5.29 |
| 11 | 14 | -2 | 6.63 |
| 13 | 16 | -2 | 7.21 |

For all p, .

3.

Addtion table for mod 7

Points on curve: , (1,1), (1,6), (3,0), (5,1), (5,6)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | (1,1) | (1,6) | (3,0) | (5,1) | (5,6) |
|  |  | (1,1) | (1,6) | (3,0) | (5,1) | (5,6) |
| (1,1) | (1,1) | (5,6) |  | (5,1) | (1,6) | (3,0) |
| (1,6) | (1,6) |  | (5,1) | (5,6) | (3,0) | (1,1) |
| (3,0) | (3,0) | (5,1) | (5,6) |  | (1,1) | (1,6) |
| (5,1) | (5,1) | (1,6) | (3,0) | (1,1) | (5,6) |  |
| (5,6) | (5,6) | (3,0) | (1,1) | (1,6) |  | (5,1) |

Computational tools used:

http://www.christelbach.com/ECCalculator.aspx

http://ptrow.com/perl/calculator.old.pl

TI-nspire cas calculator