|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | X^3 + x + 1 | X^3 + x + 1 mod 3 | Y | Points |
| 0 | 1 | 1 | 1,2 | (0,1) (0,2) |
| 1 | 3 | 0 | 0 | (1,0) |
| 2 | 11 | 2 | - | - |

The number of points: 3 and one point at infinity

#E(F3) = 4

Fp = |4 – 4| = 0

0 < 2√3 CHECK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | X^3 + x + 1 | X^3 + x + 1 mod 5 | Y | Points |
| 0 | 1 | 1 | 1,4 | (0,1) (0,4) |
| 1 | 3 | 3 | - | - |
| 2 | 11 | 1 | 1,4 | (2,1) (2,4) |
| 3 | 31 | 1 | 1,4 | (3,1) (3,4) |
| 4 | 69 | 4 | 2,3 | (4,2) (4,3) |

The number of points: 8 and one point at infinity

#E(F5) = 9

Fp = |6 – 9| = 3

3 < 2√5 CHECK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | X^3 + x + 1 | X^3 + x + 1 mod 7 | Y | Points |
| 0 | 1 | 1 | 1,6 | (0,1) (0,6) |
| 1 | 3 | 3 | - | - |
| 2 | 11 | 4 | 2,5 | (2,2) (2,5) |
| 3 | 31 | 3 | - | - |
| 4 | 69 | 6 | - | - |
| 5 | 131 | 5 | - | - |
| 6 | 223 | 6 | - | - |

The number of points: 4 and 5 points at infinity

#E(F7) = 9

Fp = |8 – 9| = 1

1 < 2√7 CHECK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | X^3 + x + 1 | X^3 + x + 1 mod 11 | Y | Points |
| 0 | 1 | 1 | 1,10 | (0,1) (0,10) |
| 1 | 3 | 3 | 5,6 | (1,5) (1,6) |
| 2 | 11 | 0 | 0 | (2,0) |
| 3 | 31 | 9 | 3,8 | (3,3) (3,8) |
| 4 | 69 | 3 | 5,6 | (4,5) (4,6) |
| 5 | 131 | 10 | - | - |
| 6 | 223 | 6 | - | - |
| 7 | 351 | 3 | 5,6 | (7,5) (7,6) |
| 8 | 521 | 4 | 2,9 | (8,2) (8,9) |
| 9 | 739 | 2 | - | - |
| 10 | 1011 | 10 | - | - |

The number of points: 13 and 1 points at infinity

#E(F11) = 17

Fp = |12 – 17| = 5

5 < 2√11 CHECK