11

6.6

a

Make an addition table for $E_5 : Y^2 \equiv X^3 + X + 2 \pmod 5$

✓ **Answer** ⌄

Only $0, 1, 4$ are possible quadratic residues $\mod 5$

When $X = 0, Y^2 = 2 \pmod 5$, which has no solutions for Y
When $X = 1, Y^2 = 4 \pmod 5 \implies \{2, 3\} \in Y$
When $X = 2, Y^2 = 2 \pmod 5$, which has no solutions for Y
When $X = 3, Y^2 = 2 \pmod 5$, which has no solutions for Y
When $X = 4, Y^2 = 0 \pmod 5 \implies \{0\} \in Y$

This gives us solution points of $\{\mathcal{O}, (1,2), (1,3), (4,0)\}$

$+$	$\mathcal{O}$	$(1,2)$	$(1,3)$	$(4,0)$
$\mathcal{O}$	$\mathcal{O}$	$(1,2)$	$(1,3)$	$(4,0)$
$(1,2)$	$(1,2)$	$(4,0)$	$\mathcal{O}$	$(1,3)$
$(1,3)$	$(1,3)$	$\mathcal{O}$	$(4,0)$	$(1,2)$
$(4,0)$	$(4,0)$	$(1,3)$	$(1,2)$	$\mathcal{O}$

6.7

Let E be the elliptic curve $y^2 = x^3 + x + 1$

Compute the number of points in the group $E(\mathbb{F}_p)$
and the trace of Frobenius $t_p = p + 1 - \#E(\mathbb{F}_p)$
and verify that $|t_p|$ is smaller than $2\sqrt{p}$

for each of the following primes:

a

$p = 3$

✓ **Answer**

Only $0, 1$ are possible quadratic residues $\mod 3$

When $X = 0, Y^2 = 1 \pmod 3 \implies \{1, 2\} \in Y$
When $X = 1, Y^2 = 0 \pmod 3 \implies \{0\} \in Y$
When $X = 2, Y^2 = 2 \pmod 3$, which has no solutions for Y

This gives us solution points of $\{\mathscr{O}, (0, 1), (0, 2), (1, 0)\}$

$\#E(\mathbb{F}_3) = 4$
$t_3 = 0$
$0 < 2\sqrt{3}$

b

$p = 5$

✓ **Answer**
Only $0, 1, 4$ are possible quadratic residues $\mod 5$

When $X = 0, Y^2 = 1 \pmod 5 \implies \{1, 4\} \in Y$
When $X = 1, Y^2 = 3 \pmod 5$, which has no solutions for Y
When $X = 2, Y^2 = 1 \pmod 5 \implies \{1, 4\} \in Y$
When $X = 3, Y^2 = 1 \pmod 5 \implies \{1, 4\} \in Y$
When $X = 4, Y^2 = 4 \pmod 5 \implies \{2, 3\} \in Y$

This gives us solution points of $\{\mathscr{O}, (0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)\}$

$\#E(\mathbb{F}_5) = 9$
$t_5 = -3$
$3 < 2\sqrt{5}$

c

$p = 7$

✓ **Answer**
Only $0, 1, 2, 4$ are possible quadratic residues $\mod 7$

When $X = 0, Y^2 = 1 \pmod 7 \implies \{1, 6\} \in Y$
When $X = 1, Y^2 = 3 \pmod 7$, which has no solutions for Y
When $X = 2, Y^2 = 4 \pmod 7 \implies \{2, 5\} \in Y$
When $X = 3, Y^2 = 3 \pmod 7$, which has no solutions for Y
When $X = 4, Y^2 = 6 \pmod 7$, which has no solutions for Y
When $X = 5, Y^2 = 5 \pmod 7$, which has no solutions for Y
When $X = 46, Y^2 = 6 \pmod 7$, which has no solutions for Y

This gives us solution points of $\{\mathscr{O}, (0,1), (0,6), (2,2), (2,5)\}$

$\#E(\mathbb{F}_7) = 5$
$t_7 = 3$
$3 < 2\sqrt{7}$

d

$p = 11$

✓ **Answer**

Only $0, 1, 3, 4, 5, 9$ are possible quadratic residues $\mod 11$

When $X = 0, Y^2 = 1 \pmod 1)1 \implies \{1, 10\} \in Y$
When $X = 1, Y^2 = 3 \pmod 1)1$, which has no solutions for Y
When $X = 2, Y^2 = 0 \pmod 1)1 \implies \{0\} \in Y$
When $X = 3, Y^2 = 9 \pmod 1)1 \implies \{3, 8\} \in Y$
When $X = 4, Y^2 = 3 \pmod 1)1$, which has no solutions for Y
When $X = 5, Y^2 = 10 \pmod 1)1$, which has no solutions for Y
When $X = 6, Y^2 = 6 \pmod 3)$, which has no solutions for Y
When $X = 7, Y^2 = 6 \pmod 1)0$, which has no solutions for Y
When $X = 8, Y^2 = 6 \pmod 4) \implies \{2, 9\} \in Y$
When $X = 9, Y^2 = 3 \pmod 4)$, which has no solutions for Y
When $X = 10, Y^2 = 3 \pmod 1)0$, which has no solutions for Y

This gives us solution points of $\{\mathscr{O}, (0,1), (0,10), (2,0), (3,3), (3,8), (8,2), (8,9)\}$

$\#E(\mathbb{F}_7) = 8$
$t_7 = 4$
$8 < 2\sqrt{11}$