Given:

(4) $E: y^2 = x^3 - x + 2$

Find:

Number of points in $E(\mathbb{F}_q)$ for $q = 3, 5, 9$

I) $q = 3$ q-prime $\Rightarrow$ Using Legendre symbol to check for quadratic residues

$x = 0$ $y^2 = 2$ $\left(\frac{2}{3}\right) = 2^{\frac{3-1}{2}} \bmod 3 = 2 \equiv -1 \bmod 3$ - 0 points

+

$x = 1$ $y^2 = 2$ $\left(\frac{2}{3}\right) = 2^{\frac{3-1}{2}} \bmod 3 = 2 \equiv -1 \bmod 3$ - 0 points

+

$x = 2$ $y^2 = 2$ — || — - 0 points

+

point at infinity - 1 point

1 point

II) $q = 5$ q-prime $\Rightarrow$ Using Legendre symbol to check for quadratic residues

$x = 0$ $y^2 = 2$ $\left(\frac{2}{5}\right) = 2^{\frac{5-1}{2}} \bmod 5 = 4 \equiv -1 \bmod 5$ - 0 points

+

$x = 1$ $y^2 = 2$ — || — - 0 points

+

$x = 2$ $y^2 = 3$ $\left(\frac{3}{5}\right) = 3^{\frac{5-1}{2}} \bmod 5 = 4 \equiv -1 \bmod 5$ - 0 points

+

$x = 3$ $y^2 = 1$ $\left(\frac{1}{5}\right) = 1^{\frac{5-1}{2}} \bmod 5 = 1 \bmod 5$ - 2 points

+

$x = 4$ $y^2 = 2$ $\left(\frac{2}{5}\right) = 2^{\frac{5-1}{2}} \bmod 5 = 4 \equiv -1 \bmod 5$ - 0 points

+

point at infinity - 1 point

3 points

III $q = 9 = 3^2$

We fix an isomorphism $\mathbb{Z}_9 \cong \mathbb{Z}_3[i]$ with $i^2 = -1$

We define $\mathbb{F}_9 = \{a+bi \mid a,b \in F_3,\ i^2 = -1\}$

We have squares in $\mathbb{F}_9$: 0, 1, 2

$$i^2 = (2i)^2$$
$$2i = (i+1)^2 = (2+2i)^2$$
$$i = (2+i)^2 = (1+2i)^2$$

x	0	1	2	i	$2i$	$i+1$	$2+2i$	$2+i$	$1+2i$
x^3	0	1	2	$2i$	i	$2i+1$	$2+i$	$2+2i$	$1+i$
x^3-x+2	2	2	2	$i+2$	$2-i \equiv 2+2i$	$i+2$	$2-i \equiv 2+2i$	$i+2$	$2-i \equiv 2+2i$

No quad. residue, as shown in I)

as noted above, these are quad residues (6 points)

So, the number of points is

6 + point at infinity = 7 points