4. Given:

$$E/\mathbb{F}_p, E'/\mathbb{F}_p$$

E and E' are $\mathbb{F}_p$-isogenous, $f: E \to E'$

f preserves $\mathbb{F}_p$ rational points

Prove: $|E(\mathbb{F}_p)| = |E'(\mathbb{F}_p)|$

Proof. Let φ_p and φ'_p be the Frobenius maps (automorphisms).

We then have $f \circ \varphi_p = \varphi'_p \circ f$, and also

$$\mathrm{I})\quad f \circ (Id - \varphi_p) = (Id - \varphi'_p) \circ f$$

For an elliptic curve E over $\mathbb{F}_p$ we have:

$$\mathrm{II}\quad |E(\mathbb{F}_p)| = |\ker(Id - \varphi)| = \deg(Id - \varphi)$$

with $Id - \varphi$ being separable.

For isogenies between elliptic curves E, E', E'' and $\alpha: E \to E'$, $\beta: E' \to E''$, we have $\deg(\beta \circ \alpha) = \deg(\beta) \cdot \deg(\alpha)$

So, from I), it must be the case that

$$\deg(Id - \varphi_p) = \deg(Id - \varphi'_p).$$

From II), we can rewrite this as:

$$|E(\mathbb{F}_p)| = |E'(\mathbb{F}_p)| \quad \square$$

⑥ a) Given: $E/\mathbb{F}_p$, $E: y^2 = f(x)$

$f(-x) = -f(x)$ - odd function

$p \equiv 3 \mod 4$

Prove:

$|E(\mathbb{F}_p)| = p+1$

Proof. Since $p \equiv 3 \mod 4$, $\frac{p-1}{2}$ is odd and therefore -1 is not a square mod p, we find that for $\forall n \in \mathbb{F}_p^*$, either n or $-n$ is a square mod p.

We now consider the $\frac{p-1}{2}$ pairs $[x,-x]$, $0 < x \leq \frac{p-1}{2}$.

For each pair, we have one of the three:

I) $f(x) = f(-x) = 0$

II) $\left(\frac{f(x)}{p}\right) = 1$

III $\left(\frac{f(-x)}{p}\right) = 1$

In each of these cases, there are 2 points on $E(\mathbb{F}_p)$ associated with the pair $[x,-x]$:

⑥ a)

I) $(\pm x, 0)$

II) $(x, \pm\sqrt{f(x)})$

III) $(-x, \pm\sqrt{f(-x)})$

So, there are $2 \cdot \frac{p-1}{2} = p-1$ points resulting from these pairs.

Adding the point $(0,0)$ and the point at infinity $\mathcal{O}$, we get $p-1+2 = p+1$ points, so indeed

$$|E(\mathbb{F}_p)| = p+1 \ , \ p \equiv 3 \bmod 4 \ , f(-x) = -f(x)$$

$\square$

⑥ b)

Find: group structure of $E(\mathbb{F}_{107})$ - $p = 107$

$E: y^2 = x^3 - x$, $E(\mathbb{F}_{107}) \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

$a, b \in \mathbb{Z}$

Theorem 12.15: $b = ka$

$\cancel{k \neq 0}$

$k \neq 0$, $a \mid (p-1)$

$f(x) = x^3 - x$ is odd:

$(-x)^3 + x = -x^3 + x$

and $107 \equiv 3 \mod 4$. So, from 6a), we know ~~that~~ the number of elements on the curve: $|E(\mathbb{F}_p)| = p+1$

$$|E(\mathbb{F}_{107})| = 107 + 1 = 108$$

The roots of $x^3 - x = x(x^2-1) = x(x\cancel{^2}+1)(x-1)$ are $-1, 0$ and 1. Together with the point at infinity, there are 4 points, which form a subgroup of $E(\mathbb{Q})$ which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

We know that $p+1$ and $p-1$ do not share a ~~common~~ prime factor (with the exception of 2) and $(\mathbb{Z}/2\mathbb{Z})^2$ is a subgroup.

Since $p-1 \equiv 2 \mod 4 \Rightarrow (\mathbb{Z}/4\mathbb{Z})^2$ is not a subgroup, it must be the case that $E(\mathbb{F}_p) \cong (\mathbb{Z}/2\mathbb{Z}) \times \left(\mathbb{Z}/\frac{|E(\mathbb{F}_p)|}{2}\mathbb{Z}\right)$

In the case of $p = 107$, we therefore have

$$E(\mathbb{F}_{107}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$$

$a = 2$, $b = 54$