Let ψ an endomorphism on E, an elliptic curve over a field K.

Let's look at ψ on the n-torsion: ψ_n.

The n-torsion is $E[n] = \{ P \in E : [n]P = \mathcal{O} \}$.

The n-torsion is two-dimensional

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n \qquad (\mathbb{Z}_n \text{ stands for } \mathbb{Z}/n\mathbb{Z})$$

So we have for a basis (P, Q) of $E[n]$:

$$\begin{aligned} \psi_n(P) &= aP + bQ \quad \text{and} \\ \psi_n(Q) &= cP + dQ \end{aligned} \quad \longleftrightarrow \quad M_\psi = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$ a square matrix over $\mathbb{Z}_n$.

Actually $\boxed{\text{the trace of } \psi_n \text{ is } (d+d) \bmod n}$

Why?

- $\psi_n^2 \longleftrightarrow M_\psi^2$, indeed: $M_\psi^2 = \begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix}$

- on the endomorphism side,

$$\psi_n \circ \psi_n(P) = \psi_n(aP+bQ) = \psi_n(aP) + \psi_n(bQ) = a\psi_n(P) + b\psi_n(Q)$$
$$= a(aP+bQ) + b(cP+dQ) = (a^2+bc)P + (ab+bd)Q$$

$$\psi_n \circ \psi_n(Q) = \psi_n(cP+dQ) = \psi_n(cP) + \psi_n(dQ) = c\psi_n(P) + d\psi_n(Q)$$
$$= c(aP+bQ) + d(cP+dQ) = (ac+cd)P + (bc+d^2)Q$$

Hence we see that $\psi_n \circ \psi_n$ is represented by the squared matrix

$$M_\psi^2 = \begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix}$$ in the basis $[P \quad Q]$.

How do we compute the trace? We know that ψ as an endomorphism of E has a quadratic characteristic polynomial $\psi^2 - [\text{trace}] \circ \psi + [\deg \psi] = \mathcal{O}$ (the O map).

- $\deg \psi$ is the degree of ψ, this is the max degree of the numerator and denominator of the x-coordinate: $(x,y) \longmapsto (\psi_x(x), \psi_y(x,y))$ and $\psi_x(x) = \dfrac{\psi_{x,num}(x)}{\psi_{x,den}(x)}$

$$\deg(\psi) = \max(\deg(\psi_{x,num}), \deg(\psi_{x,den})).$$

so we know $\deg(\psi)$. $\longleftrightarrow \begin{bmatrix} \deg(\psi) & 0 \\ 0 & \deg(\psi) \end{bmatrix}$ a diagonal matrix.

- ψ^2 and ψ correspond to M_ψ^2 and M_ψ.

$\psi_n^2 - [\text{trace } \psi_n]\psi_n + [\deg \psi_n] = 0$ on the n-torsion

in terms of matrices: $M_\psi^2 - [\text{trace}]\, M_\psi + [\deg \psi_n] I_2 = 0$.

$$\begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix} - \text{trace}\cdot\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} \deg\psi_n & 0 \\ 0 & \deg\psi_n \end{bmatrix} = 0.$$

(1) $a^2+bc - \text{trace}\cdot a + \deg\psi_n = 0$
(2) $ab+bd - \text{trace}\cdot b + 0 = 0 \iff b(a+d-\text{trace}) = 0$
(3) $ac+cd - \text{trace}\cdot c + 0 = 0 \iff c(a+d-\text{trace}) = 0$
(4) $bc+d^2 - \text{trace}\cdot d + \deg\psi_n = 0.$

- so either $b=c=0$ and then (1) is $a^2 - \text{trace}\cdot a + \deg\psi_n = 0$
  (4) is $d^2 - \text{trace}\cdot d + \deg\psi_n = 0.$

$(1)-(4) \iff a^2 - \cancel{a}d^2 - \text{trace}(a-d) = 0$
$\iff (a-d)(a+d) - \text{trace}(a-d) = 0$
$\iff (a-d)(a+d-\text{trace}) = 0.$ either: $a=d$ (~~and~~ trace $= a+d = 2a$)

and ψ_n is the mult. by a map:

$M_{\psi_n} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and we know that $\deg([a]) = a^2$,

so $\psi^2 - \text{trace}\cdot\psi + \deg\psi \to [a^2] - [\text{trace}]\cdot[a] + [a^2] = 0$
$\to$ trace $= 2a$.

or: trace $= a+d$.

$M_\psi = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$ and trace $= a+d$. and M_ψ is diagonal in this case.

- or, $b \neq 0$, $c \neq 0$, and trace $= a+d$ (for (2), (3)).
  $(1)-(4)$ gives $a^2-d^2 - \text{trace}(a-d) = 0$, $(a-d)(a+d-\text{trace}) = 0$,
  we find again trace $= a+d$.

To wrap up: • either $b=c=0$ and $M_\psi = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$. trace $= a+d$.

• or, $b \neq 0$ and/or $c \neq 0$ and trace $= a+d$.

• special case: $M_\psi = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and M_ψ is the multiplication-by-a-map on $E[n]$, and (P,Q) is orthogonal.

When n is prime, $n \mid \#E(\mathbb{F}_p)$, but $n^2 \nmid \#E(\mathbb{F}_p)$, then we know that $\psi_n(P) = [\lambda]P$ for some λ mod n and $P \in E(\mathbb{F}_p)[n]$ because Q is not defined over $\mathbb{F}_p$, but since ψ_n is defined over $\mathbb{F}_p$, then Q is not involved, and

$M_\psi = \begin{bmatrix} \lambda & 0 \\ * & * \end{bmatrix}$ where $*$ means some (non-zero) integer mod n.