Let \( E \) be an elliptic curve of the form

\[
E : y^2 = x^3 + ax + b.
\]

1. The multiplication-by-\( n \) maps \([n]\) on an elliptic curve \( E \) with equation as above is defined by simple recursive formulas for the coordinates. The maps \([n] : E \to E\) take the form

\[
P = (x, y) \mapsto nP = \left( \frac{\phi_n(x)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right),
\]

For polynomials \( \phi_n(x) \), \( \psi_n(x, y) \), and \( \omega_n(x, y) \). This means that the \( n \)-th multiple of a point on \( E \) is given by the evaluation of the polynomial expressions for the image coordinates at the point coordinates.

The polynomials \( \psi_n(x, y) \) are of crucial importance since they are zero precisely on the points of \( E[n] = \ker([n]) \). They can be defined by the recursions:

\[
\begin{align*}
\psi_0 &= 0, \quad \psi_1 = 1, \quad \psi_2 = 2y \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\psi_4 &= \psi_2 \cdot (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - (2a^3 - 16b^2)) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^2 - \psi_m\psi_{m+1}^3 \quad (m \geq 2), \\
\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/\psi_2 \quad (m > 2).
\end{align*}
\]

Moreover the polynomials \( \phi_n \) are determined by \( \phi_0 = 1 \) and

\[
\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}
\]

for all \( n \geq 1 \).

a. Use the relation \( y^2 = x^3 + ax + b \) to show that \( \psi_n(x, y)^2 \) can be expressed as a polynomial in \( x \).

b. Show that this multiplication by 2 determines the addition law in the case \( P_1 = P_2 \) not covered by the addition formula, and compute \( 2P_1 \). How can the group law be extended to the case \( x_1 = x_2 \) but \( y_1 \neq y_2 \)?

c. Let \( E \) be the elliptic curve \( y^2 = x^3 + x + 3 \) over \( \mathbb{F}_{61} \), having 55 elements. Use the above recursion to construct the polynomial \( \psi_5(x) \). Find two roots \( x_1 \) and \( x_2 \) of this polynomial and verify that they determine 5-torsion points \((x_1, \pm y_1)\) and \((x_2, \pm y_2)\).

\textit{Solution}
a. Using $\psi_2(x, y)^2 = 4(x^3 + ax + b)$, one verifies that for odd $n$, the polynomial $\psi_n(x, y)$ is a polynomial only in $x$, and for even $n$ that $\psi_n(x, y)/\psi_2(x, y)$ is a polynomial in $x$. Applying the relation for $\psi_2(x, y)^2$ again gives the result.

b. When $P_1 = P_2$ the addition law becomes multiplication by two; the only other case not covered by the previous rule is when $-P_1 = P_2$, which is the other case with $x_1 = x_2$, but in this case, the result is the identity $O$.

The duplication formula can be determined from the formulas for $n = 2$.

\[(x, y) \mapsto (x_2, y_2) = \frac{\phi_2(x)}{\psi_2^2}, \frac{\omega_2(x)}{\psi_3^3}\]

First we take $\psi_2(x, y) = 2y$, noting that $\psi_2^2 = 4(x^3 + ax + b)$, and compute

$\phi_2(x) = 4x(x^3 + ax + b) - (3x^4 + 6ax^2 + 12bx - a^2)$
$= x^4 - 2ax^2 - 8bx + a^2$,

then solve the equation $y_2^2 = x_2^3 + ax_2 + b$ for $\omega_2(x)$:

$w_2(x) = x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2$.

c. This elliptic curve, and the “division polynomial” $\psi_5(x)$ can be created in Magma with the lines:

```magma
> E := EllipticCurve([ GF(61) | 1, 3 ]); > psi := DivisionPolynomial(E,5); The roots of this polynomial are then found by factoring $\psi_5(x)$:
> P<x> := Parent(psi); // define printing > Factorization(psi);
```

\[
\begin{align*}
<x + 23, 1>,
<x + 29, 1>,
<x^5 + 25*x^4 + 20*x^3 + 23*x^2 + 44*x + 54, 1>,
<x^5 + 45*x^4 + 26*x^3 + 19*x^2 + 20*x + 8, 1>
\end{align*}
\]

We can then verify that the roots $x = 32$ and $x = 38$ are the $x$-coordinates of 5-torsion points:

```magma
> x1 := FiniteField(61)!32; > x2 := FiniteField(61)!38; > _, y1 := IsSquare(x1^3+x1+3); > _, y2 := IsSquare(x2^3+x2+3); > P1 := E![x1,y1]; > P2 := E![x2,y2]; > P1; (32 : 31 : 1) > 5*P1; (0 : 1 : 0)
```
In this exercise we investigate the conditions under which an elliptic curve can have
3.

Let \( E / \mathbb{F}_q \) be an elliptic curve and \( P \in E(\mathbb{F}_q) \) be a point of prime order \( n \). The
\( n \)-torsion group \( E[n] \) is defined to be
\[
E[n] = \{ Q \in E(\mathbb{F}_q) : nQ = O \}.
\]
Assume the structure theorem for the \( n \)-torsion group \( E[n] \), which states that if \( (n, p) = 1 \) then
\[
E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},
\]
and if \( n = p \) then \( E[n] \cong \mathbb{Z}/n\mathbb{Z} \) or \( E[n] \cong \{ O \} \).

a. Show that there exists a finite extension \( \mathbb{F}_{q^r} \), and a point \( Q \in E(\mathbb{F}_{q^r}) \) such that
\( E[n] = \langle P, Q \rangle \).

b. For the elliptic curve \( E / \mathbb{F}_{61} \) of the previous exercise with 5-torsion point \( P = (x_1, y_1) \in E(\mathbb{F}_{61}) \), find an extension \( \mathbb{F}_{61^2} \) and a point \( Q \in E(\mathbb{F}_{61^2}) \) generating the 5-torsion subgroup.

Solution Let \( P = (x_1, y_1) \) and \( Q = (x_2, y_2) \) be elements of \( E[n] \) which generate it
as a group. Then each \( x_i \) and \( y_i \) is an element of \( \mathbb{F}_q \). Recall that every element of
\( \mathbb{F}_q \) is algebraic over \( \mathbb{F}_q \), so lies in a finite degree extension of \( \mathbb{F}_q \), and for each \( r \) there
is a unique subfield \( \mathbb{F}_{q^r} \) of degree \( r \) inside of \( \mathbb{F}_q \). If we take \( r \) equal to the LCM of
each of the extension degrees \( [\mathbb{F}_q(x_i) : \mathbb{F}_q] \), the the subfield of \( \mathbb{F}_q \) of degree \( r \) contains
\( x_1, x_2, y_1, \) and \( y_2, \) hence \( P \) and \( Q \) are in \( E(\mathbb{F}_{q^r}) \). Since the coefficients any linear
combination \( nP + mQ \) is determined by rational functions over \( \mathbb{F}_q \) in evaluated at
the \( x_i \) and \( y_i \), it follows that \( E[n] \subseteq E(\mathbb{F}_{q^r}) \).

3. In this exercise we investigate the conditions under which an elliptic curve can have
a very large \( n \)-torsion subgroup \( E[n] \) contained in the set of points \( E(\mathbb{F}_{p^2}) \).

a. Recall that the Frobenius endomorphism \( \pi \), defined by \( \pi(x, y) = (x^p, y^p) \), is a
homomorphism of \( E(\mathbb{F}_p) \) to itself. For each \( r \) show that
\[
E(\mathbb{F}_{p^r}) = \ker(\pi^r - 1).
\]

b. Make use of the fact that \( |E(\mathbb{F}_{p^2})| \) equals \( p^2 - t + 1 \) where \( \pi^{2r} - t, \pi^r + p^r = 0 \).
If \( |E(\mathbb{F}_{p^2})| = p - t + 1 \), then show that \( |E(\mathbb{F}_{p^2})| = p^2 - (t^2 - 2p) + 1 \).

c. Suppose that \( n \) is a prime greater than \( 4\sqrt{p} \). Show that if \( n \) divides \( |E(\mathbb{F}_p)| \)
and \( n^2 \) divides \( |E(\mathbb{F}_{p^2})| \) then \( t = 0 \).

d. Show that if \( t = 0 \) then \( |E(\mathbb{F}_{p^2})| = (p + 1)^2 \), and prove moreover that
\[
E(\mathbb{F}_{p^2}) = E[p + 1] \cong \mathbb{Z}/(p + 1)\mathbb{Z} \times \mathbb{Z}/(p + 1)\mathbb{Z}.
\]

Hint: Show that \( \pi^2 = p \) and recall that \( \ker(\pi^r - 1) = E(\mathbb{F}_{p^r}) \).
An elliptic curve over a field of characteristic $p$ such that $t \equiv 0 \mod p$ is called \textit{supersingular}. The complement of these curves are \textit{ordinary} elliptic curves.

\textit{Solution}

\begin{enumerate}[a.]
  \item The $r$-th power $\pi^r$ Frobenius endomorphism takes $(x, y)$ to $(x^{p^r}, y^{p^r})$. The fixed points $(x, y)$ are precisely those for which $x$ and $y$ satify
  \[ x^{p^r} - x = y^{p^r} - y = 0, \]
i.e. the elements of $E(\mathbb{F}_{p^r})$. Since $\pi$ is an group endomorphism, to say $\pi^r(x, y) = (x, y)$ is equivalent to the statement that
  \[ (\pi^r - 1)(x, y) = \pi^r(x, y) - (x, y) = O, \]
i.e. $(x, y)$ is in $\ker(\pi^r - 1)$.
  \item It suffices to find the characteristic polynomial of $\pi^2$, which is equal to the characteristic polynomial of the square of the representing matrix, or
    \[ \begin{pmatrix} 0 & 1 \\ -p & t \end{pmatrix}^2 = \begin{pmatrix} -p & t \\ -tp & -p + t^2 \end{pmatrix}. \]
  This gives a characteristic polynomial $X^2 - t_2 X + p^2$, where the trace $t_2$ is $-2p + t^2$.
  \item If $n$ divides $p - t + 1$ and $n^2$ divides $p^2 - (t^2 - 2p) + 1$, then $n$ divides $p + t + 1 = (p^2 - (t^2 - 2p) + 1)/(p - t + 1)$. Therefore $n$ also divides $(p + t + 1) - (p - t + 1) = 2t$. Since $|t| \leq \sqrt{p}$, the lower bound on $n$ implies that that $t = 0$.
  \item If $t = 0$ then $\pi^2 = -p$, hence $\ker(\pi^2 - 1) = \ker(-p - 1) = E[p + 1]$.
\end{enumerate}