The Menezes, Okamoto, and Vanstone (MOV) algorithm is one of the few known subexponential algorithms for tackling the discrete logarithm on an elliptic curve \( E/F_q \). It applies when the full \( n \)-torsion subgroup \( E[n] \subset E(F_q) \) is defined over a small extension field \( F_{q^r} \). The primary application of this method is to supersingular elliptic curves.

The MOV algorithm makes use of the Weil pairing to map an elliptic curve discrete logarithm problem into a finite field discrete logarithm problem. In this exercise we use Magma to investigate the properties of the Weil pairing and its application to discrete logarithms.

1. Let \( e_n(R, S) \) be the Weil pairing of points \( R \) and \( S \). In Magma this is constructed as \( \text{WeilPairing}(R, S, n) \). For points \( R \) and \( S \) in the subgroup \( \langle P, Q \rangle \) verify the properties
   a. \( e_n(R, R) = 1; \)
   b. \( e_n(R, S) = e_n(S, R)^{-1}; \) and
   c. \( e_n(xR, yS) = e_n(R, S)^{xy} \) for all \( x, y \in \mathbb{Z}; \)

2. The MOV reduction algorithm makes use of property (3) to reduce a discrete logarithm problem \( \log_P(xP) \) on an elliptic curve to the discrete logarithm problem \( \log_\alpha(\beta) \) where \( \alpha = e_n(P, Q) \) and \( \beta = e_n(xP, Q) \). Using your points \( P \) and \( Q \), verify the equivalence of these two discrete logarithms for several values of \( x \).

3. Use the constructor \( \text{SupersingularEllipticCurve} \) to create larger examples and compare the performance of the elliptic curve and finite field discrete logarithms.

4. Let \( E/F_p \), where \( p = 1000081 \) be the supersingular elliptic curve
   \[ y^2 = x^3 + 394763x + 255869, \]
   and let \( P = (416961 : 144117 : 1) \). Show that \( P \) has prime order 500041, and find a point \( Q \in E(F_{p^2}) \) such that \( E[500041] = \langle P, Q \rangle \).

5. The multiplication-by-\( n \) maps \( [n] \) on an elliptic curve \( E : y^2 = x^3 + ax + b \) induces a well-defined rational map on the \( x \)-coordinates. In order to allow for roots of the denominator polynomial, we express \( E \) in projective coordinates and write
   \[ E : Y^2Z = X^3 + aXZ^2 + bZ^3. \]
Then we express the maps \([n]\) on the \(XZ\)-projective line:

\[
[n](X : Z) = \begin{cases} 
  (\Phi_n(X, Z) : \Psi_n(X, Z)^2 Z) & \text{n odd} \\
  (\Phi_n(X, Z) : \Psi_n(X, Z)^2 F_2(X, Z) Z) & \text{n even}
\end{cases}
\]

with initializations

\[
\Psi_0 = 0 \quad \Psi_1 = 1 \quad \Psi_2 = 1 \\
\Psi_3 = 3X^4 + 6aX^2Z^2 + 12bXZ^3 - a^2Z^4 \\
\Psi_4 = 2X^6 + 10aX^4Z^2 + 40bX^3Z^3 - 10a^2X^2Z^4 - 8abXZ^5 - (2a^3 - 16b^2)Z^6
\]

\(F_2 = 4X^3 + 4aXZ^2 + 4bZ^3\) and subsequent recursions

\[
\Psi_{4m+1} = \frac{F_2^2}{2}\Psi_{2m+2}\Psi_{2m}^3 - \Psi_{2m-1}\Psi_{2m+1}^3 \\
\Psi_{4m+3} = \Psi_{2m+3}\Psi_{2m+1}^3 - \frac{F_2^2}{2}\Psi_{2m}\Psi_{2m+2}^3 \\
\Psi_{2m} = \Psi_m(\Psi_{m+2}\Psi_{m-1} - \Psi_{m-2}\Psi_{m+1}^3).
\]

The recursions for \(\Phi_n(X, Z)\) are given by \(\Phi_0 = 1\) and

\[
\Phi_n = \begin{cases} 
  XF_2\Psi_n^2 - \Psi_{n+1}\Psi_{n-1} & \text{n even} \\
  X\Psi_n^2 - F_2\Psi_{n+1}\Psi_{n-1} & \text{n even}
\end{cases}
\]

for all \(n \geq 1\).

Note that Magma does not handle elliptic curves over rings such as \(\mathbb{Z}/N\mathbb{Z}\) which are not fields, but using the above formulas you can determine the application of exponentiation in the group law on the \(x\)-coordinates of points over general rings.

In the following exercise, let \(E\) be the elliptic curve \(y^2 = x^3 - x + 1\) with point \(P = (1, 1)\).

a. Compute \([11]P\) over \(\mathbb{Q}\), over \(\mathbb{F}_{101}\) and over \(\mathbb{F}_{103}\). Use these results to find \([11]P\) in \(E(\mathbb{Z}/N\mathbb{Z})\) where \(N = 10403 = 101 \cdot 103\).

b. Use the recursions above to verify the value of the \(x\)-coordinates of \([n]P\) in the group \(E(\mathbb{Q})\) of points over \(\mathbb{Q}\). You may use the function:

```magma
function EllipticExponential(n,a,b,X,Z)
if n mod 2 eq 1 then
  return [ Phi(n,a,b,X,Z), Psi(n,a,b,X,Z)^2 * Z ];
else
  F2 := 4*(X^3 + a*X*Z^2 + b*Z^3);
  return [ Phi(n,a,b,X,Z), Psi(n,a,b,X,Z)^2 * F2 * Z ];
end if;
end function;
```

together with the Magma functions \(\Psi\) and \(\Phi\) below.

c. Compute the \(x\)-coordinates of \([n]P\) in \(E(\mathbb{Z}/N\mathbb{Z})\) for \(n\) a product of high powers of small primes. At what point can you identify the factorization of \(N\)?

Magma code for the functions \(\Psi_n(X,Y)\) and \(\Phi_n(X,Y)\), given any \(a\) and \(b\) in a ring \(R\) are given below, first for \(\Psi_n\):

```magma
function Psi(n,a,b,X,Y)
if n mod 2 eq 1 then
  return [ Phi(n,a,b,X,Y), Psi(n,a,b,X,Y)^2 * Z ];
else
  F2 := 4*(X^3 + a*X*Z^2 + b*Z^3);
  return [ Phi(n,a,b,X,Y), Psi(n,a,b,X,Y)^2 * F2 * Z ];
end if;
```
function Psi(n,a,b,X,Z)
    if n eq 0 then return 0; end if;
    if n le 2 then return 1; end if;
    if n eq 3 then
        return 3*X^4+(6*X*(a*X+2*b*Z)-(a*Z)^2)*Z^2;
    elif n eq 4 then
        return 2*X^6 + 10*a*X^4*Z^2 + 40*b*X^3*Z^3
            - 10*a^2*X^2*Z^4 - 8*a*b*X*Z^5 - (2*a^3+16*b^2)*Z^6;
    end if;
    m := n div 2;
    if n mod 2 eq 0 then
        return Psi(m,a,b,X,Z) * (Psi(m+2,a,b,X,Z) * Psi(m-1,a,b,X,Z)^2
            - Psi(m-2,a,b,X,Z) * Psi(m+1,a,b,X,Z)^2);
    else
        F2 := 4*(X^3+(a*X+b*Z)*Z^2);
        if m mod 2 eq 0 then
            return F2^2 * Psi(m+2,a,b,X,Z) * Psi(m,a,b,X,Z)^3
                - Psi(m-1,a,b,X,Z) * Psi(m+1,a,b,X,Z)^3;
        else
            return Psi(m+2,a,b,X,Z) * Psi(m,a,b,X,Z)^3
                - F2^2 * Psi(m-1,a,b,X,Z) * Psi(m+1,a,b,X,Z)^3;
        end if;
    end if;
end function;

and subsequently for $\Phi_n$:

function Phi(n,a,b,X,Z)
    if n eq 0 then return 0; end if;
    if n eq 1 then return X; end if;
    F2 := 4*(X^3+(a*X+b*Z)*Z^2);
    if n mod 2 eq 0 then
        return X * Psi(n,a,b,X,Z)^2 * F2
            - Psi(n+1,a,b,X,Z) * Psi(n-1,a,b,X,Z);
    else
        return X * Psi(n,a,b,X,Z)^2
            - Psi(n+1,a,b,X,Z) * Psi(n-1,a,b,X,Z) * F2;
    end if;
end function;