Verifying the computations given on page 6 of the article by Craig Costello.
Since the j-invariant of supersingular elliptic curves lies in $F_{p^2}$ it is sufficient to work with quadratic extension of $F_p$.
The prime $p = 431$ is chosen such that $x^2 + 1$ is irreducible since $431 = 3 \pmod{4}$ hence $F_{p^2} = F_p[x]/(x^2 + 1)$.
Next we pick those supersingular elliptic curves which have $(p + 1)^2 = 432^2$ $F_{p^2}$-rational points so that trace of frobenius is $-2p$ and $E(F_{p^2}) = E[p + 1]$.

see Costello p. 8 and 11; Feo-Jao-Plut section 4.1.

```
[2]: K.<a> = GF(431^2, name="a", modulus=x^2+1); K
[2]: Finite Field in a of size 431^2
[3]: E = EllipticCurve(K, [0,208*a+161,0,1,0]); E
[3]: Elliptic Curve defined by y^2 = x^3 + (208*a+161)*x^2 + x over Finite Field in a of size 431^2
[4]: E.cardinality() # Schoof 1985
[4]: 186624
[5]: 186624 == 432^2
[5]: True
[6]: E.abelian_group() # Rück 1987
[6]: Additive abelian group isomorphic to Z/432 + Z/432 embedded in Abelian group of points on Elliptic Curve defined by y^2 = x^3 + (208*a+161)*x^2 + x over Finite Field in a of size 431^2
[7]: E.j_invariant()
[7]: 364*a + 304
[8]: P = E(350*a+68,0); P
[8]: (350*a + 68 : 0 : 1)
[10]: P.order()
[10]: 2
[11]: phi = EllipticCurveIsogeny(E,P); phi # Vélu 1971; not Montgomery form
```
Isogeny of degree 2 from Elliptic Curve defined by \( y^2 = x^3 + (208a+161)x^2 + x \) over Finite Field in \( a \) of size 431\(^2\) to Elliptic Curve defined by \( y^2 = x^3 + (208a+161)x^2 + (343a+209)x + (363a+398) \) over Finite Field in \( a \) of size 431\(^2\)

\[
\text{phi.is_separable()}
\]

True

\[
\text{phi.rational_maps()}
\]

\[
((x^2 + (81a - 68)x + (190a - 214))/(x + (81a - 68)), \\
(x^2y + (162a - 136)x*y + y)/(x^2 + (162a - 136)x + (190a - 213)))
\]

\[
E2 = \text{EllipticCurve}(K, [0,208a+161,0,343a+209,363a+398]); E2
\]

Elliptic Curve defined by \( y^2 = x^3 + (208a+161)x^2 + (343a+209)x + (363a+398) \) over Finite Field in \( a \) of size 431\(^2\)

\[
P2 = \text{phi}(P); P2
\]

(0 : 1 : 0)

\[
P2.order()
\]

1

\[
E2.cardinality()
\]

186624

\[
E2.abelian_group()
\]

Additive abelian group isomorphic to \( \mathbb{Z}/432 + \mathbb{Z}/432 \) embedded in Abelian group of points on Elliptic Curve defined by \( y^2 = x^3 + (208a+161)x^2 + (343a+209)x + (363a+398) \) over Finite Field in \( a \) of size 431\(^2\)

\[
E2.j_invariant()
\]

344*a + 190