Frobenius and the endomorphism ring of \( j = 1728 \).

KATHERINE E. STANGE

Abstract. We give the endomorphism ring of the supersingular elliptic curve over \( \mathbb{F}_p \) with \( j = 1728 \), and show that although the endomorphism ring is invariant under isomorphism of the curve, the placement of Frobenius in that endomorphism ring is not.

I always have to look up the endomorphism ring of \( j = 1728 \) for the purposes of supersingular isogeny based cryptography, and the literature gave seemingly contradictory answers to this, until I did the computation contained in this note. The computation shows that on isomorphic models of \( j = 1728 \), Frobenius can actually be identified with non-isomorphic elements of the endomorphism ring. This behaviour is a result of the extra automorphisms of the curve, in this case manifest as the existence of a quartic twist.

Let \( p \equiv 3 \pmod{4} \) so that \( j = 1728 \) is a supersingular \( j \)-invariant over \( \mathbb{F}_p \). I know of at least two places the basis for the associated endomorphism is given:

1. Eisenträger, Hallgren, Lauter, Morrison, and Petit [1, Section 5.1] use the model \( E_1 : y^2 = x^3 + x \) and give the endomorphism ring as
   \[
   \text{End}(E_1) = \mathbb{Z} + i\mathbb{Z} + \frac{1 + k}{2}\mathbb{Z} + \frac{i + j}{2}\mathbb{Z}
   \]
   where \( i \) is the endomorphism \( \left[ i \right] : (x, y) \mapsto (-x, iy) \) and \( j \) is the Frobenius endomorphism \( \pi_p : (x, y) \mapsto (x^p, y^p) \).

2. McMurdy [2, Section 3.1] use the model \( E_2 : y^2 = x^3 - x \) and give the endomorphism ring as
   \[
   \text{End}(E_2) = \mathbb{Z} + i\mathbb{Z} + \frac{1 + j}{2}\mathbb{Z} + \frac{i + k}{2}\mathbb{Z}
   \]
   where \( i \) is the endomorphism \( \left[ i \right] : (x, y) \mapsto (-x, iy) \) and \( j \) is the Frobenius endomorphism \( \pi_p : (x, y) \mapsto (x^p, y^p) \).

The puzzling observation here is that in the first case, \( \frac{1 + \pi_p}{2} \notin \text{End}(E_1) \), while in the second case, \( \frac{1 + \pi_p}{2} \in \text{End}(E_2) \). In other words, although \( \text{End}(E_1) \cong \text{End}(E_2) \) by swapping \( j \) and \( k \), the element which acts as Frobenius is not preserved under the isomorphism (it remains \( j \)).

The answer to the puzzle is that the two models are quartic twists of one another. The isomorphism is

\[
\phi : E_1 \to E_2, (x, y) \mapsto (ix, e^{\frac{\pi}{p}}y)
\]
whose dual is

\[
\hat{\phi} : E_2 \to E_1, (x, y) \mapsto (-ix, e^{-\frac{\pi}{p}}y).
\]

One verifies that composing these, one obtains the identity.

One can make the identification

\[
\phi \text{End}(E_1)\hat{\phi} = \text{End}(E_2).
\]

In particular, \( \phi[i]\hat{\phi} = [i] \) because

\[
\phi[i]\hat{\phi}(x, y) = \phi[i](-ix, e^{\frac{-\pi}{p}}y) = \phi(ix, e^{\frac{\pi}{p}}y) = (-x, iy).
\]

But, \( \phi\pi_p\hat{\phi} = [i]\pi_p \) because

\[
\phi\pi_p\hat{\phi}(x, y) = \phi\pi_p(-ix, e^{\frac{-\pi}{p}}y) = \phi((-i)^px^p, e^{p-1}\frac{\pi}{p}y^p) = (-i^{p+1}x^p, e^{(p-1)\frac{\pi}{p}}y^p) = (-x^p, iy^p) = [i]\pi_p(x, y).
\]

Date: October 6, 2021, Draft #1.
In concordance with this observation, note that $E_1$ has only two 2-torsion points defined over $\mathbb{F}_p$, with the other two over $\mathbb{F}_{p^2}$, so the action of Frobenius on the 2-torsion can be given (with an appropriate choice of basis) by the matrix
\[
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}.
\]
However, on $E_2$, all 2-torsion is over the base field, meaning the matrix of Frobenius is the identity. Thus $1 + \pi_p$ has the matrix representations
\[
\begin{pmatrix}
1 & 1 \\
1 & 1
\end{pmatrix} : \begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}
\]
on $E_1[2]$ and $E_2[2]$ respectively. Therefore, $1 + \pi_p$ is not divisible by 2 in $\text{End}(E_1)$ but it is divisible by 2 in $\text{End}(E_2)$.

References


Department of Mathematics, University of Colorado, Campus Box 395, Boulder, Colorado 80309-0395

Email address: kstange@math.colorado.edu