# Symmetries of Singular Elliptic Curve Solutions in Finite Fields

Isaac Gibbons

## Overview

If you are reading this then it might be useful to go to my "outputs" folder and locate the files named "$GF(5^2)$" and "$GF(5^3)$". These are what I am referencing when I talk about the symmetries at the end of the proofs. "$GF(5^2)$" is a case of proposition 1, "$GF(5^3)$" is a case of proposition 2, and both showcase proposition 3. In terms of the tables the columns represent the element $y$ and the rows represent the element $x$ of the point $(x, y)$. This means we are ignoring the first row and column as we are only looking to elements that belong to the multiplicative cyclic group in our fields.
With that said, we look to transformations such as

$$(g^r, g^t) \mapsto \left(g^{r+\lambda_1},\ g^{t+\lambda_2}\right)$$

in the set $\mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*$, and show that the number of singular elliptic curves that pass through these points remains invariant under the said transformations. This insight was discovered by computationally creating tables to represent the space of all coordinates in $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, and filling the cells with the number of singular curves that a given coordinate satisfied. I do not claim these proofs to be novel in anyway; they are simply results that I stumbled upon while playing around with my code. I am writing them up as formally as I can to show that interplay between experimenting and rigorously proving, that can often be lost in academic courses.

## Setup

Let $\mathbb{F}_{p^n}$ be a finite field with $p > 3$. One can generate the tables for $p \leq 3$ but the singularity condition is somewhat simplified making it, in my opinion, less interesting structurally. Let $g$ be a generator of the multiplicative group $\mathbb{F}_{p^n}^*$, that is, $g$ is a root of some primitive polynomial of degree $n$ over $\mathbb{F}_{p^n}$.
We consider the family of elliptic curves in Weierstrass form:

$$E_{a,b}: \quad y^2 = x^3 + ax + b \tag{1}$$

and focus on the singular curves, defined by the vanishing of the discriminant:

$$\Delta = 4a^3 + 27b^2 = 0. \tag{2}$$

We are interested in fixing a point $(x, y)$ and finding all pairs $(a, b)$ such that the elliptic curve defined by (1) is singular and contains the fixed point $(x, y)$.
To proceed, we fix $a$ and rearrange (1) to express $b$ in terms of $x, y$, and $a$:

$$b = y^2 - x^3 - ax.$$

We then substitute this expression for $b$ into the discriminant condition for singularity, yielding:

$$\Delta = 4a^3 + 27(y^2 - x^3 - xa)^2 = 0. \tag{3}$$

Equation (3) is cubic in $a$, and for each fixed $(x, y)$, the solutions correspond to the values of $a$ (and thus $b$) that define a singular elliptic curve passing through the point.
Now, we apply a change of variable by setting $a = x^2A$. This transformation preserves the number of solutions, but introduces structural symmetry in $x$, which will be helpful in the proofs that follow. The motivation for this substitution will become clear when we explore how symmetries in $x$ occur in the structure of $\Delta$ and how they help reveal invariance under certain transformations of $(x, y)$. Using the substitution in (3) we get:

$$\Delta = 4x^6A^3 + 27(y^2 - x^3 - x^3A)^2 = 0. \tag{4}$$

This equation, (4), will allow all our transformations to resolve smoothly for our needs.

# Results

## Proposition 1

Let $(g^r, g^t) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*$, $p > 3$ be a point that lies on exactly $k$ singular elliptic curves, $k \in \{0, 1, 2, 3\}$. In the cases where:

- $p \cong 1 \mod 3, \quad \forall n \in \mathbb{N},$
- $p \cong 2 \mod 3, \quad \forall \text{ even } n \in \mathbb{N}.$

The point

$$\left(g^{r+\frac{p^n-1}{3}},\ g^{t+\frac{p^n-1}{2}}\right),$$

also lies on $k$ singular curves (not necessarily the same curves). This shift makes sense as, with our above restrictions on $p$, we have $p^n - 1 \cong 0 \mod 2, 3$, and thus $p^n - 1$ must be divisible by both 2 and 3.

## Proof

We substitute the coordinates of the transformation into (4). This gives:

$$4(g^{r+\frac{p^n-1}{3}})^6A^3 + 27((g^{t+\frac{p^n-1}{2}})^2 - (g^{r+\frac{p^n-1}{3}})^3 - (g^{r+\frac{p^n-1}{3}})^3A)^2 = 0.$$

$$4g^{6r+2(p^n-1)}A^3 + 27(g^{2t+2(p^n-1)} - g^{3r+p^n-1} - g^{3r+p^n-1}A)^2 = 0.$$

Given that $g^{p^n-1} = 1$ in $\mathbb{F}_{p^n}$, we get that:

$$4g^{6r}A^3 + 27(g^{2t} - g^{3r} - g^{3r}A)^2 = 0.$$

$$4(g^r)^6A^3 + 27((g^t)^2 - (g^r)^3 - (g^r)^3A)^2 = 0.$$

Note this is just what we would get if we substituted $(g^r, g^t)$ into (4) and so both points must have the same number of solutions. In these cases of $p$ and $n$ we have split the whole grid of $\mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*$ into 6 identical windows (from the perspective we are taking). It may be useulf to look at "$GF(5^2)$".

□

**Proposition 2**

Let $(g^r, g^t) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*, \quad p > 3, \quad p \cong 2 \mod 3, \quad n \in \mathbb{N}$ odd, be a point that lies on exactly $k$ singular elliptic curves, $k \in \{0, 1, 2, 3\}$. The point

$$\left(g^{r+\frac{p^n+1}{3}},\ g^{t+1}\right),$$

also lies on $k$ singular curves (not necessarily the same curves). This shift makes sense as, with our above restrictions on $p$ and $n$, we have $p^n + 1 \cong 0 \mod 3$, and thus $p^n + 1$ must be divisible by 3.

**Proof**

We substitute the coordinates of the transformation into (4). This gives:

$$4(g^{r+\frac{p^n+1}{3}})^6 A^3 + 27((g^{t+1})^2 - (g^{r+\frac{p^n+1}{3}})^3 - (g^{r+\frac{p^n+1}{3}})^3 A)^2 = 0.$$

$$4g^{6r+2(p^n+1)} A^3 + 27(g^{2t+2} - g^{3r+p^n+1} - g^{3r+p^n+1} A)^2 = 0.$$

Given that $g^{p^n-1} = 1$ in $\mathbb{F}_{p^n}^*$, we get that:

$$4g^{6r+4} A^3 + 27(g^{2t+2} - g^{3r+2} - g^{3r+2} A)^2 = 0.$$

$$4g^4 (g^r)^6 A^3 + 27g^4((g^t)^2 - (g^r)^3 - (g^r)^3 A)^2 = 0.$$

$$4(g^r)^6 A^3 + 27((g^t)^2 - (g^r)^3 - (g^r)^3 A)^2 = 0.$$

Note, again this is just what we would get if we substituted $(g^r, g^t)$ into (4) and so both points must have the same number of solutions. In the case of $p \cong 2 \mod 3$ we get columns hold all the same values, in the same order, with a row rotation of $p^n + 1$. It may be useful to look at "$GF(5^3)$". □

**Proposition 3**

Finally $\forall p > 3, \forall n \in \mathbb{N}$ . Let $(g^r, g^t) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*$, be a point that lies on exactly $k$ singular elliptic curves, $k \in 0, 1, 2, 3$. The point

$$\left(g^{r+2},\ g^{t+3}\right).$$

also lies on $k$ singular curves (not necessarily the same curves).

**Proof**

We substitute the coordinates of the transformation into (4). This gives:

$$4(g^{r+2})^6 A^3 + 27((g^{t+3})^2 - (g^{r+2})^3 - (g^{r+2})^3 A)^2 = 0.$$

$$4g^{6r+12} A^3 + 27(g^{2t+6} - g^{3r+6} - g^{3r+6} A)^2 = 0.$$

$$4g^{12} (g^r)^6 A^3 + 27g^{12}((g^t)^2 - (g^r)^3 - (g^r)^3 A)^2 = 0.$$

$$4(g^r)^6 A^3 + 27((g^t)^2 - (g^r)^3 - (g^r)^3 A)^2 = 0.$$

Note, again this is just what we would get if we substituted $(g^r, g^t)$ into (4) and so both points must have the same number of solutions. Therefore for all $p > 3$ we get this shift of 3 to the right, 2 down. It may be useful to look at both "$GF(5^2)$" and "$GF(5^3)$". □