ECC, problem 02.†10

Roman

December 3, 2023

Problem

Let $E/\mathbb{Q}$ be an elliptic curve. Prove that $E[m]$ has m^2 points of order m.

Solution

Proof. As follows from the Mordell-Weil theorem,

$$E[m] \cong Z/mZ \times Z/mZ \tag{1}$$

Employing that fact makes it now obvious that

$$\#E[m] = m^2 \tag{2}$$

□

Another way to see this might be counting the roots of the m-division polynomial $\psi_m(x)$.

For odd m, the division polynomial is of power $(m^2 - 1)/2$ so it has that many roots. Adding points with $-y$ and ∞ gives

$$\#E[m] = \frac{m^2 - 1}{2} * 2 + 1 = m^2 \tag{3}$$

i.e. m^2 points.

For even m, the division polynomial is a product of a polynomial of power $(m^2 - 4)/2$ and $y(x)$ (y is the y-coordinate of the point on the curve). The first factor gives $(m^2 - 4)/2$ roots. Adding to that points symmetric across x-axis, then adding to that 3 points where $y(x) = 0$ and ∞

$$\#E[m] = \frac{m^2 - 4}{2} * 2 + 3 + 1 = m^2 \tag{4}$$

i.e. m^2 points. The gap in this treatment is the repeated roots of the division polynomials. I'm not sure how to deal with that.