NMMB430 - DÚ 6

Jan Oupický

1

Twisted Edwards curve in completed coordinates $\mathbb{P}^1 \times \mathbb{P}^1$ is given by the equation $aX_1^2Y_2^2 + Y_1^2X_2^2 = X_2^2Y_2^2 + dX_1^2Y_1^2$ (Xs correspond to the first part of the point and Ys correspond to the second part). Since affine points (α, β) of a Twisted Edwards curve are 1-1 mapped upon points $((\alpha : 1), (\beta : 1))$ the points at infinity must have $X_2 = 0$ or $Y_2 = 0$.

If $X_2 = 0$ then $X_1 \neq 0$ since $(0 : 0) \notin \mathbb{P}^1$. Then the equation is $aX_1^2Y_2^2 = dX_1^2Y_1^2$. Since $X_1 \neq 0$ then it can be simplified into $aY_2^2 = dY_1^2$. $a, d \in K^*$ then $\frac{a}{d} = \left(\frac{Y_1}{Y_2}\right)^2$ Y_2 is also not 0 since that would imply $Y_1 = 0$ as well. Let $\frac{a}{d} = t^2$ then we have points $((1 : 0), (\pm t : 1))$.

Other case $Y_2 = 0$ implies $Y_1 \neq 0$. The equation is $X_2^2 = dX_1^2$. Again $X_1, X_2 \neq 0$ which implies $d = s^2$ and the points are $((1 : \pm s), (1 : 0))$. We have exhausted all possibilities.

Therefore as said in the lecture. The group has 0,2 or 4 points at infinity depending on ad^{-1}, d being squares in K. If both are squares then we have 4 points. If none are then 0 points. If one of them is a square then we have 2.

2

Consider the curve $E : 2x^2 + y^2 = 1 + 3x^2y^2$ over $\mathbb{Z}_5$. The only affine points on the curve are $(0, 1), (0, 4)$. Since $ad^{-1} = 4 = 2^2$ but d is not a square, we have 2 points at infinity. $(0, 1)$ has order 1, $(0, 4) \oplus (0, 4) = (0, 1)$ i.e. $(0, 4)$ has order 2. By using the addition formula in complete coordinates we get that the 2 points at infinity are of order 2 as well. Therefore $|E(\mathbb{Z}_5)| = 4$ and has 3 points of order 2 and 1 point of order 1. This is an example of a twisted edwards curve with no point of order 4 over K.

3

We will analyze how many points at infinity our curves have. We have already analyzed one of then in 2). Remaining ones are:

$E : 2x^2 + y^2 = 1 + 4x^2y^2$: $d = 4$ is a square. $ad^{-1} = 2 \cdot 4 = 3$ is not a square. We have therefore 2 points at infinity in the group $E(\mathbb{Z}_5)$. In completed coordinates they are $((1 : 2), (1 : 0)), ((1 : 3), (1 : 0))$.

$E : 2x^2 + y^2 = 1 + 4x^2y^2$: $d = 1$ is a square. $ad^{-1} = 2 \cdot 1 = 2$ is not a square. We have therefore 2 points at infinity in the group $E(\mathbb{Z}_5)$. In completed coordinates they are $((1 : 1), (1 : 0)), ((1 : 4), (1 : 0))$.

$E : x^2 + y^2 = 1 + 4x^2y^2$: $d = 4$ is a square. $ad^{-1} = 1 \cdot 4 = 4$ is a square. We have therefore 4 points at infinity in the group $E(\mathbb{Z}_5)$. In completed coordinates they are $((1 : 2), (1 : 0)), ((1 : 3), (1 : 0)), ((1 : 0), (2 : 1)), ((1 : 0), (3 : 1))$.