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

The point $(0, -1)$ is always on the twisted edwards curve and has order 2.

If $\frac{a}{d} = t^2 \in K$ then we have points (in completed coordinates) $P_{1,2} = ((1 : 0), (\pm t : 1))$. Using the addition formula for completed coordinates we get that both of these points are of order 2 as well. This means that points $\{(0, 1), (0, -1), P_1, P_2\}$ form a subgroup of $E(K)$ which is of order 4 and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

If $d = s^2 \in K$ then we have points (in completed coordinates) $P_{1,2} = ((\pm s : 0), (1 : 0))$. Again using the addition formula we get that both of these points are of order 4 since for example $[2]P_1 = (0, -1)$ and this means $[2]P_1$ is of order 2. Therefore the subgroup generated by P_1 or P_2 is of order 4 and isomorphic to $\mathbb{Z}_4$.

Since we assume K to be a finite field we have that if none of the above hold ($\frac{a}{d}, d$ non square) then $\frac{a}{d} \cdot d = a$ is a square i.e. $a = c^2 \in K$. Then we have $c^2x^2 + y^2 = 1 + dx^2y^2 \iff (cx - 1)(cx + 1) = y^2(dx^2 - 1)$. So $(\pm\frac{1}{c}, 0)$ are points on the curve. Using the addition formula we get that both of these points are of order 4 so as in the 2nd case we can take the subgroup of order 4 generated by one of these points that is isomorphic to $\mathbb{Z}_4$.

3

We will analyze how many points at infinity our curves have. Those are:

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

$E : 2x^2 + y^2 = 1 + 4x^2y^2$: $d = 4$ 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 $((1:2),(1:0)),((1:3),(1:0))$.

$E : 2x^2 + y^2 = 1 + 1x^2y^2$: $d = 1$ 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 $((1:2),(1:0)),((1:3),(1:0)),((1:0),(2:1)),((1:0),(3:1))$.