NMMB430 - DÚ 7

Jan Oupický

1

Denote $E_1 : y^2 = x^3+3x+1, E_2 : y^2 = x^3+3x-1$. Since $-1 \notin (\mathbb{F}_{31}^*)^2$ and $j(E_1) = j(E_2)$ then E_2 is a quadratic twist of E_1. Therefore we have the equality

$$|E_1(\mathbb{F}_{31})| + |E_2(\mathbb{F}_{31})| = 64$$

Also using Hasse theorem we know that $21 \leq |E_1(\mathbb{F}_{31})|, |E_2(\mathbb{F}_{31})| \leq 43$.

Let's calculate the division polynomials for E_1 and factor them in $\mathbb{F}_{31}[x]$:

$$\phi_1 = 1$$
$$\phi_2 = 2y$$
$$\phi_3 = 3x^4 + 18x^2 + 12 + 22 = 3(x+1)(x^3 + 30x^2 + 7x + 28)$$
$$\phi_4 = 4y(x^6 + 15x^4 + 20x^3 + 17x^2 + 19x + 27)$$
$$\phi_5 = 5x^{12} + 8x^9 + 16x^8 + 7x^7 + 30x^6 + 29x^5 + 18x^4 + 22x^3 + 12x^2 + 24x + 12 =$$
$$= 5(x+16)(x+24)(x^5 + 5x^4 + 8x^3 + 27x^2 + 4x + 21)(x^5 + 17x^4 + 7x^3 + 16x^2 + 23x + 13)$$

$E_1[2](\mathbb{F}_{31}) = 1$ since $x^3 + 3x + 1$ is irreducible in $\mathbb{F}_{31}[x]$. $E_1[3](\mathbb{F}_{31}) = 1 + 2$ the point at infinity and 2 points $(30, \pm\beta)$ where $\beta \in \mathbb{F}_{31} : \beta^2 = 30^3 + 3 \cdot 30 + 1$. $E_1[4](\mathbb{F}_{31}) = 1$ is trivial since there are no roots of $\frac{\phi_4}{4y}$ is irreducible $\mathbb{F}_{31}[x]$. ϕ_5 is reducible in $\mathbb{F}_{31}[x]$ but $15^3 + 3 \cdot 30 + 1$ and $7^3 + 3 \cdot 7 + 1$ are not squares in $\mathbb{F}_{31}$ and therefore there are no points with 7 or 15 as their x coordinate. This means that also $E_1[5](\mathbb{F}_{31}) = 1$.

Now we know that since $E_1[3](\mathbb{F}_{31}) \leq E_1(\mathbb{F}_{31})$ that $3 | E_1(\mathbb{F}_{31})$.

So $E_1(\mathbb{F}_{31}) \in \{21, 24, 27, 30, 33, 36, 39, 42\}$.

Let's look at E_2 division polynomials:

$$\phi_1 = 1$$
$$\phi_2 = 2y$$
$$\phi_3 = 3x^4 + 18x^2 + 19 + 22 = 3(x+30)(x^3 + x^2 + 7x + 3)$$
$$\phi_4 = 4y(x^6 + 15x^4 + 11x^3 + 17x^2 + 12x + 27)$$
$$\phi_5 = 5x^{12} + 23x^9 + 16x^8 + 24x^7 + 30x^6 + 2x^5 + 18x^4 + 9x^3 + 12x^2 + 7x + 12 =$$
$$= 5(x+7)(x+15)(x^5 + 14x^4 + 7x^3 + 15x^2 + 23x + 18)(x^5 + 26x^4 + 8x^3 + 4x^2 + 4x + 10)$$

Using the same technique we get that $E_2[2](\mathbb{F}_{31}) = 1, E_2[3](\mathbb{F}_{31}) = 1, E_2[4](\mathbb{F}_{31}) = 1$ and $E_2[5](\mathbb{F}_{31}) = 5$. Therefore $E_2(\mathbb{F}_{31}) \in \{25, 30, 35, 40\}$.

At the start we noticed that $|E_1(\mathbb{F}_{31})| + |E_2(\mathbb{F}_{31})| = 64$. The only solutions are $(E_1(\mathbb{F}_{31}), E_2(\mathbb{F}_{31})) = (24, 40)$ or $(E_1(\mathbb{F}_{31}), E_2(\mathbb{F}_{31})) = (39, 25)$.

If the first case was true then $E_1(\mathbb{F}_{31})$ is isomorphic to one of the following:

$$E_1(\mathbb{F}_{31}) \cong \mathbb{Z}_{24}$$
$$E_1(\mathbb{F}_{31}) \cong \mathbb{Z}_4 \times \mathbb{Z}_6$$
$$E_1(\mathbb{F}_{31}) \cong \mathbb{Z}_3 \times \mathbb{Z}_8$$

In all cases $E_1(\mathbb{F}_{31})$ would have an element of order 4. We have shown that this is not true therefore it must be that $(E_1(\mathbb{F}_{31}), E_2(\mathbb{F}_{31})) = (39, 25)$.