NMMB430 - DÚ 4

Jan Oupický

1

Let M be a Montgomery curve given by $f(x,y) = By^2 - (x^3 + Ax^2 + x)$ where $A, B \in K, B \neq 0$. The partial derivatives of f are:

$$\frac{\partial f}{\partial x}(x,y) = -3x^2 - 2Ax - 1$$
$$\frac{\partial f}{\partial y}(x,y) = 2By$$

Since $B \neq 0$ we see that a singular point $(\alpha_1, \alpha_2) \in M$ has to satisfy $\alpha_2 = 0$. Therefore candidates for a singular point on M are only points $(\alpha_1, 0) \in M$. There are at most 3 such points of M since α_1 has to satisfy $f(\alpha_1, 0) = \alpha_1^3 + A\alpha_1^2 + \alpha_1 = \alpha_1(\alpha_1^2 + A\alpha_1 + 1) = 0$. Clearly $(0,0)$ is a point of M but it is not singular since $\frac{\partial f}{\partial x}(0,0) \neq 0$.

The other 2 points are $(\xi_1, 0), (\xi_2, 0)$ where $\xi_{1,2}$ are the roots of $x^2 + Ax + 1$ i.e.

$$\xi_1 = \frac{-A + \sqrt{A^2 - 4}}{2}, \xi_2 = \frac{-A - \sqrt{A^2 - 4}}{2}$$

For these points to be singular they also have satisfy $\frac{\partial f}{\partial x}(\xi_{1,2}, 0) = 0$ i.e. $\xi_{1,2}$ have to also be roots $\xi'_{1,2}$ of $-3x^2 - 2Ax - 1$ which are:

$$\xi'_1 = \frac{-A + \sqrt{A^2 - 3}}{3}, \xi'_2 = \frac{-A - \sqrt{A^2 - 3}}{3}$$

Now we want to know what A has to be for $\xi_1 = \xi'_1$ or $\xi_1 = \xi'_2$ and same for ξ_2.

$\xi_1 = \xi'_1$:

$$\frac{-A + \sqrt{A^2 - 4}}{2} = \frac{-A + \sqrt{A^2 - 3}}{3} \iff -A + 3\sqrt{A^2 - 4} = 2\sqrt{A^2 - 3} \implies$$
$$A^2 - 4 = A\sqrt{A^2 - 4} \implies A^2 = 4 \iff A = \pm 2$$

We have shown that if $\xi_1 = \xi'_1$ then $A = 2$ or $A = -2$. In this case only $A = -2$ works. For the case $\xi_1 = \xi'_2$ A has to be equal to 2. Cases $\xi_2 = \xi'_{1,2}$ give the same conditions. Since we are considering only $A = \pm 2$ we see that in these cases $\xi_1 = \xi_2$.

We have shown that M is singular iff $A = \pm 2$. In both cases the affine singular point is $(\frac{-A}{2}, 0)$.

The projective curve $\hat{M}$ is given by $F(X,Y,Z) = BY^2Z - X^3 - AX^2Z - XZ^2$. The only projective point with $Z = 0$ is $(0 : 1 : 0)$. Using the partial derivatives:

$$\frac{\partial F}{\partial X}(X,Y,Z) = -3X^2 - 2AXZ - Z^2$$
$$\frac{\partial F}{\partial Y}(X,Y,Z) = 2BYZ$$
$$\frac{\partial F}{\partial Z}(X,Y,Z) = BY^2 - AX^2 - 2XZ$$

Since $\frac{\partial F}{\partial Z}(0,1,0) = B \neq 0$ we see that $\hat{M}$ is smooth at $(0:1:0)$ i.e. M is smooth at the point at infinity.

We have shown that if M is singular the only singularity is at $(\frac{-A}{2}, 0)$.

2

Since $\alpha = (\alpha_1, \alpha_2) \neq (0,0)$ we can assume that $\alpha_1 \neq 0$ because if $\alpha_1 = 0$ and $\alpha \in M$ then $\alpha_2 = 0$. Using the formula $\alpha \tilde{\oplus} \beta, \alpha \neq \beta$ for Montgomery curve in a case when $\beta = (0,0)$ we have:

$$(\gamma_1, \gamma_2) = \alpha \tilde{\oplus} (0,0)$$
$$\tilde{\lambda} = \frac{-\alpha_2}{-\alpha_1} = \frac{\alpha_2}{\alpha_1} \implies$$
$$\gamma_1 = -\alpha_1 + B\left(\frac{\alpha_2}{\alpha_1}\right)^2 - A = \frac{-\alpha_1^3 + B\alpha_2^2 - A\alpha_1^2}{\alpha_1^2}$$
$$\text{Substituting } B\alpha_2^2 = \alpha_1^3 + A\alpha_1^2 + \alpha_1:$$
$$\gamma_1 = \frac{\alpha_1}{\alpha_1^2} = \frac{1}{\alpha_1}$$
$$\gamma_2 = \frac{\alpha_2}{\alpha_1}\left(\alpha_1 - \frac{1}{\alpha_1}\right) - \alpha_2 = \frac{-\alpha_2}{\alpha_1^2} \implies$$
$$(\alpha_1, \alpha_2) \tilde{\oplus} (0,0) = \left(\frac{1}{\alpha_1}, \frac{\alpha_2}{\alpha_1^2}\right)$$

3

Using $M.6$ we can find curves which are surely $\mathbb{Z}_5$-equivalent to a Montgomery curve. Those are:

$$y^2 = x^3 + x$$
$$y^2 = x^3 + 4x$$

The first curve is a Montgomery curve with $A = 0, B = 1$. For the second curve we have equivalences $y^2 = x^3 + 4x \iff (2^2y)^2 = (2x)^3 + 2^2(2x) \iff 2y^2 = x^3 + x$ i.e. Montgomery curve with $A = 0, B = 2$.

For the rest we will also use $M.5$. Here is a list of the polynomials and their roots in $\mathbb{Z}_5$ and if the roots satisfy the condition in $M.5$ we write the corresponding Montgomery curve:

$$\begin{aligned}
&x^3+1, \{4\}, f'(4) = 3 \notin (\mathbb{Z}_5^*)^2 \\
&x^3+2, \emptyset \\
&x^3+x+1, \emptyset \\
&x^3+x+2, \{4\}, f'(4) = 4 \in (\mathbb{Z}_5^*)^2 \approx 2y^2 = x^3+x^2+x \\
&x^3+2x, \{0\}, f'(0) = 2 \notin (\mathbb{Z}_5^*)^2 \\
&x^3+2x+1, \emptyset \\
&x^3+3x, \{0\}, f'(0) = 3 \notin (\mathbb{Z}_5^*)^2 \\
&x^3+3x+2, \emptyset \\
&x^3+4x+1, \{3\}, f'(3) = 1 \in (\mathbb{Z}_5^*)^2 \approx y^2 = x^3+4x^2+x \\
&x^3+4x+2, \emptyset
\end{aligned}$$

In total we have 4 curves which are $\mathbb{Z}_5$-equivalent to Montgomery curves $y^2 = x^3 + x, y^2 = x^3 + 4x, y^2 = x^3 + x + 2, y^2 = x^3 + 4x + 1$.

4

$102_{10} = 1100110_2 \implies$

$$\begin{gathered}
n_1 = 1_2 = 1 \\
n_2 = 11_2 = 3 \\
n_3 = 110_2 = 6 \\
n_4 = 1100_2 = 12 \\
n_5 = 11001_2 = 25 \\
n_6 = 110011_2 = 51 \\
n_7 = 102
\end{gathered}$$