NMMB430 - DÚ 5

Jan Oupický

1

Using E.7 we get that we have to set $a = \frac{A-2}{B}, d = \frac{A+2}{B}$ which we can always do since $B \neq 0$ and $A \neq \pm 2$ and therefore $a \neq d$ and $a, d \in K^*$. Here are the Montgomery curves from the previous exercise and their birationally equivalent Edwards counterparts. We are working with $K = \mathbb{Z}_5$:

$$M : 2y^2 = x^3 + x^2 + x \implies (A, B) = (1, 2) \implies$$
$$(a, d) = \left(-\frac{1}{2}, \frac{3}{2}\right) = (2, 4) \implies E : 2x^2 + y^2 = 1 + 4x^2y^2$$

$$M : y^2 = x^3 + 4x^2 + x \implies (A, B) = (4, 1) \implies$$
$$(a, d) = (2, 1) \implies E : 2x^2 + y^2 = 1 + x^2y^2$$

$$M : y^2 = x^3 + x \implies (A, B) = (0, 1) \implies$$
$$(a, d) = (3, 2) \implies E : 3x^2 + y^2 = 1 + 2x^2y^2$$
since $3 = 2^3 = 2 \cdot 2^2$ in $\mathbb{Z}_5$ we get E is $\mathbb{Z}_5$-equivalent to E':
$$E' : 2x^2 + y^2 = 1 + 3x^2y^2$$

$$M : 2y^2 = x^3 + x \implies (A, B) = (0, 2) \implies$$
$$(a, d) = (4, 1) \implies E : 4x^2 + y^2 = 1 + x^2y^2$$
which is $\mathbb{Z}_5$-equivalent to E':
$$E' : x^2 + y^2 = 1 + 4x^2y^2$$

2

First assume $d > 0$. Since $a < 0$ we can easily see that $y^2 = 1 + dx^2y^2 - ax^2 \geq 1 \implies$ all points (α, β) on the curve must have $|\beta| \geq 1$. Also we can express the equation as $y^2 = \frac{1-ax^2}{1-dx^2} \implies y = \pm\sqrt{\frac{1-ax^2}{1-dx^2}}$. Real points therefore must satisfy $\frac{1-a\alpha^2}{1-d\alpha^2} \geq 0$. The numerator is always positive. Therefore we have to only look at the denominator. We have condition $1 - d\alpha^2 > 0$ and this happens only if $|\alpha| < \sqrt{\frac{1}{d}}$. From this we can conclude that the curve is bounded by lines $x = \pm\sqrt{\frac{1}{d}}$. It is symmetrical with respect to the lines $x = 0$ and $y = 0$. It has therefore 2 parts. If we look at the part where $\beta \geq 1$ it has a U-shape form bounded by the lines mentioned. The part $\beta \leq -1$ looks similar since it is symmetrical. Changing the a parameter affects the "narrowness"of the U-shape. Changing the parameter d changes the bounds of the U-shape.

Now assuming $d < 0$. We still have $y = \pm\sqrt{\frac{1-ax^2}{1-dx^2}}$ which is defined everywhere since both the denominator and numerator is positive. It is symmetrical with respect to the lines $x = 0$ and $y = 0$. We have to differentiate between cases when $a < d$ and $a > d$.

First assuming $a < d$ we get that $\frac{1-ax^2}{1-dx^2} \geq 1 \implies |\beta| \geq 1$. But we also have an upper bound since $\lim_{x\to\infty} \sqrt{\frac{1-ax^2}{1-dx^2}} = \sqrt{\frac{a}{d}}$. Considering only the part $\beta \geq 1$ the curve has a V-shape upper bounded by the line $y = \sqrt{\frac{a}{d}}$. Similarly the part $\beta \leq -1$ is lower bounded by the line $y = -\sqrt{\frac{a}{d}}$

The case $a > d$ means that $\frac{1-ax^2}{1-dx^2} \leq 1 \implies |\beta| \leq 1$ and the limit is the same but $\sqrt{\frac{a}{d}} < 1$ therefore it is a lower bound. Considering the case for $\beta > \sqrt{\frac{a}{d}}$ we get that the shape is a flipped V with an upper bound $y = 1$ and the mentioned lower bound $y = \sqrt{\frac{a}{d}}$ and symetrically for the case $\beta < -\sqrt{\frac{a}{d}}$.