Elliptic-curve cryptography III

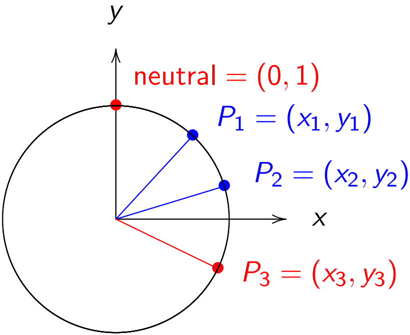
Edwards curves

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

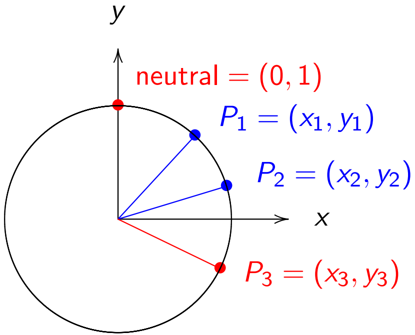
Clock

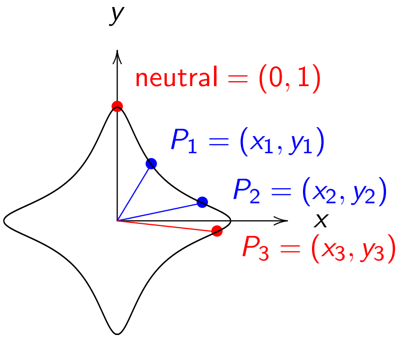


Clock curve:
$x^2 + y^2 = 1.$

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
$= (x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2).$

Clock and Edwards curve (for $d = -30$)





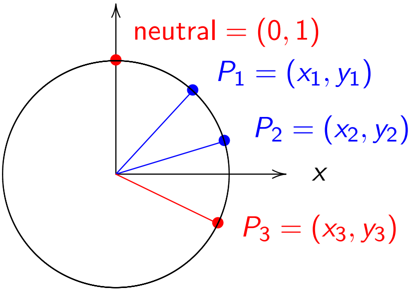
Clock curve:
$x^2 + y^2 = 1$.

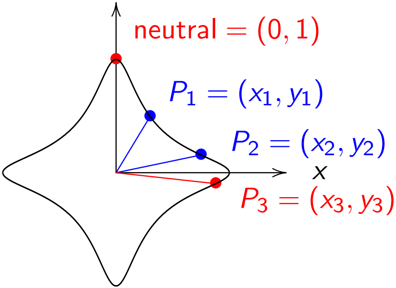
$(x_1, y_1)+(x_2, y_2) = (x_3, y_3)$
$= (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Edwards curve:
$x^2 + y^2 = 1 - 30x^2y^2$.

$(x_1, y_1)+(x_2, y_2) = (x_3, y_3)$
$= ((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

Clock and Edwards curve (for $d = -30$)





Clock curve:
$x^2 + y^2 = 1$.

$(x_1, y_1)+(x_2, y_2) = (x_3, y_3)$
$= (x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.

Edwards curve:
$x^2 + y^2 = 1 - 30x^2y^2$.

$(x_1, y_1)+(x_2, y_2) = (x_3, y_3)$
$= ((x_1 y_2 + y_1 x_2)/(1-30 x_1 x_2 y_1 y_2),$
$(y_1 y_2 - x_1 x_2)/(1+30 x_1 x_2 y_1 y_2))$.

Numerators match. Denominators equal for $x_1 x_2 y_1 y_2 = 0$.

Divisions by 0?

Do we even have a group here?

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 - 30x_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 + 30x_1x_2y_1y_2} \right)$$

- If $x_i = 0$ or $y_i = 0$ then $1 \pm 30x_1x_2y_1y_2 = 1 \neq 0$.

Divisions by 0?

Do we even have a group here?

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 - 30 x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 + 30 x_1 x_2 y_1 y_2} \right)$$

- If $x_i = 0$ or $y_i = 0$ then $1 \pm 30 x_1 x_2 y_1 y_2 = 1 \neq 0$.
- For (x, y) on $x^2 + y^2 = 1 - 30x^2y^2$, we have $30x^2y^2 < 1$,

Divisions by 0?

Do we even have a group here?

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 - 30 x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 + 30 x_1 x_2 y_1 y_2} \right)$$

- If $x_i = 0$ or $y_i = 0$ then $1 \pm 30 x_1 x_2 y_1 y_2 = 1 \neq 0$.
- For (x, y) on $x^2 + y^2 = 1 - 30x^2y^2$, we have $30x^2y^2 < 1$, thus $\sqrt{30}\,|xy| < 1$.

Divisions by 0?

Do we even have a group here?

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 - 30 x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 + 30 x_1 x_2 y_1 y_2} \right)$$

- If $x_i = 0$ or $y_i = 0$ then $1 \pm 30 x_1 x_2 y_1 y_2 = 1 \neq 0$.
- For (x, y) on $x^2 + y^2 = 1 - 30 x^2 y^2$, we have $30 x^2 y^2 < 1$, thus $\sqrt{30}\,|xy| < 1$.
- $(x_1, y_1), (x_2, y_2)$ are on the curve, thus $\sqrt{30}\,|x_1 y_1| < 1$ and $\sqrt{30}\,|x_2 y_2| < 1$.

Divisions by 0?

Do we even have a group here?

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 - 30 x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 + 30 x_1 x_2 y_1 y_2} \right)$$

- If $x_i = 0$ or $y_i = 0$ then $1 \pm 30 x_1 x_2 y_1 y_2 = 1 \neq 0$.
- For (x, y) on $x^2 + y^2 = 1 - 30x^2y^2$, we have $30x^2y^2 < 1$, thus $\sqrt{30}\,|xy| < 1$.
- $(x_1, y_1), (x_2, y_2)$ are on the curve, thus $\sqrt{30}\,|x_1 y_1| < 1$ and $\sqrt{30}\,|x_2 y_2| < 1$.
  Multiply them to get $30|x_1 y_1 x_2 y_2| < 1$ so

$$1 \pm 30 x_1 x_2 y_1 y_2 > 0.$$

Both numerators are strictly larger than 0.
Same works for any $d < 0$ and not just $d = -30$.

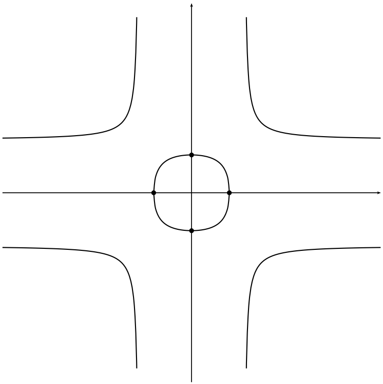
The Edwards addition law

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

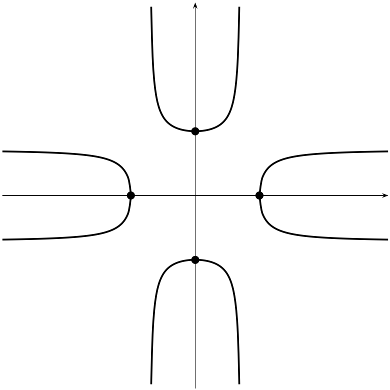
is a group law for the curve $x^2 + y^2 = 1 + dx^2y^2$ for $d < 0$.

- Addition result is on curve. Not shown here, yet, but easy by computer.
- Addition law is associative. Not shown here, yet, but easy by computer.
- $(0, 1)$ is neutral element.
- $(x_1, y_1) + (-x_1, y_1) = (0, 1)$, so $-(x_1, y_1) = (-x_1, y_1)$.
- Addition law is commutative.

Curve shapes for $d > 0$



$0 < d < 1$



$1 < d$

These curve shapes have points at infinity and do not have complete addition laws.