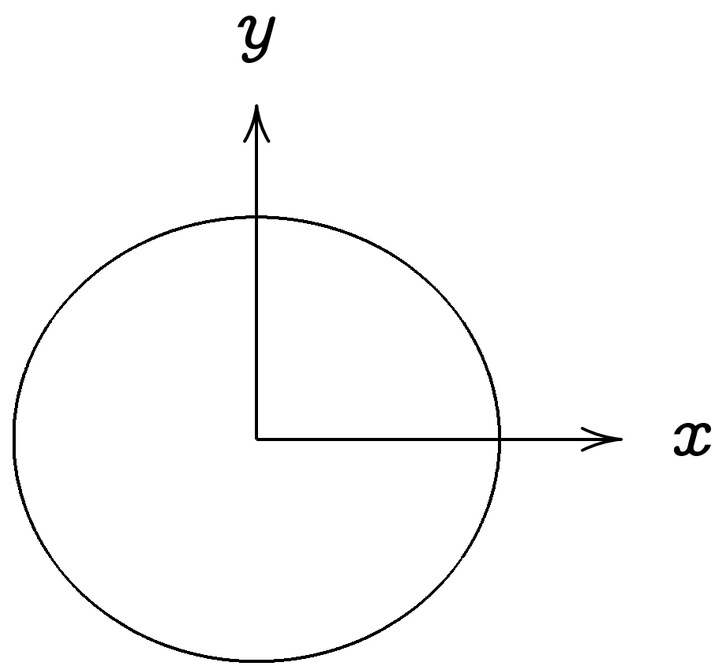
Introduction to elliptic curves

D. J. Bernstein
University of Illinois at Chicago

The clock



This is the curve $x^2 + y^2 = 1$.

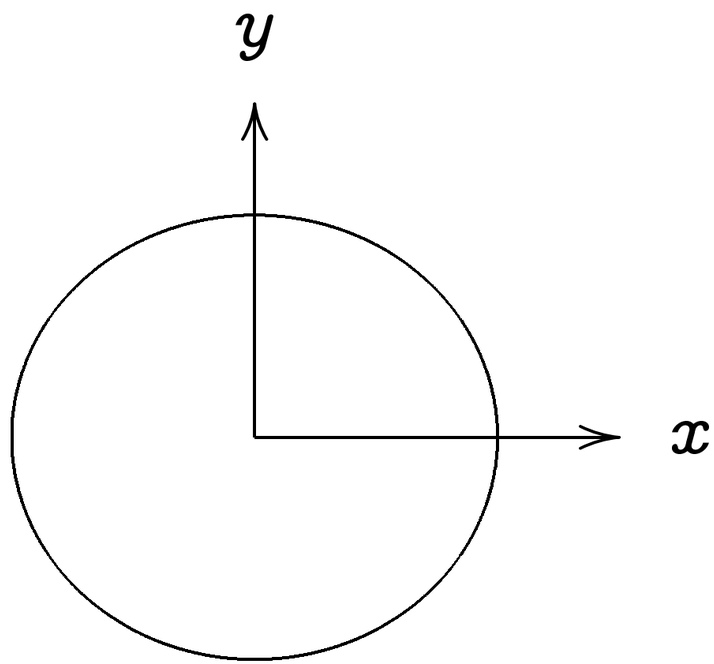
Warning:
This is *not* an elliptic curve.
"Elliptic curve" $\neq$ "ellipse."

uction to elliptic curves

Bernstein

sity of Illinois at Chicago

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

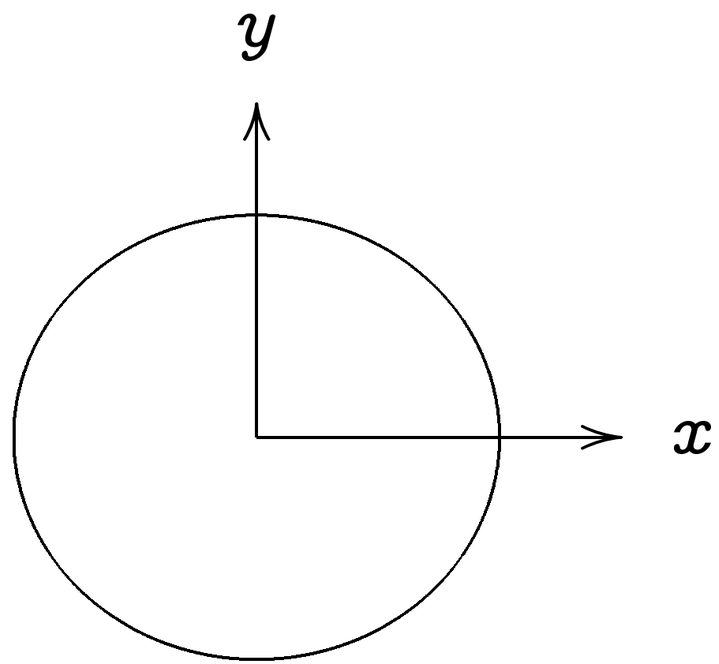
Examp

$(0, 1)$ =

lliptic curves

ois at Chicago

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

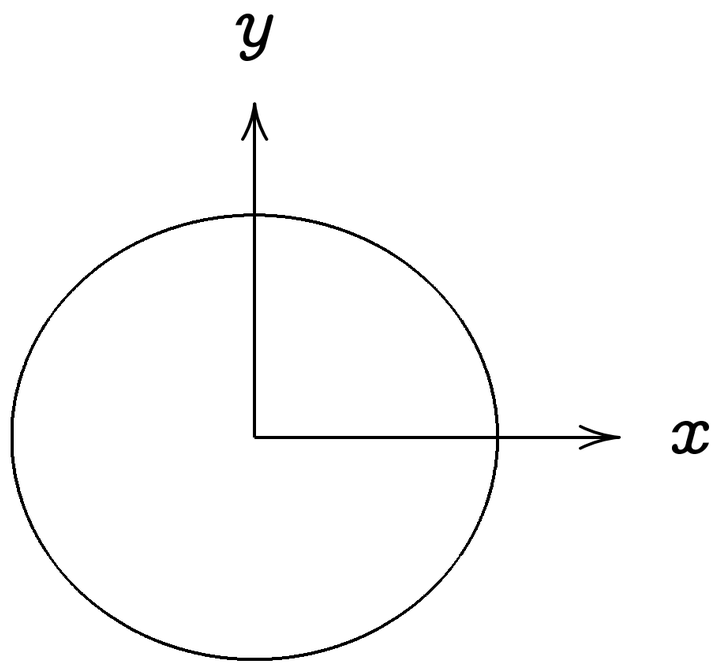
Examples of poin

$(0, 1)$ = "12:00".

ves

cago

The clock



This is the curve $x^2 + y^2 = 1$.

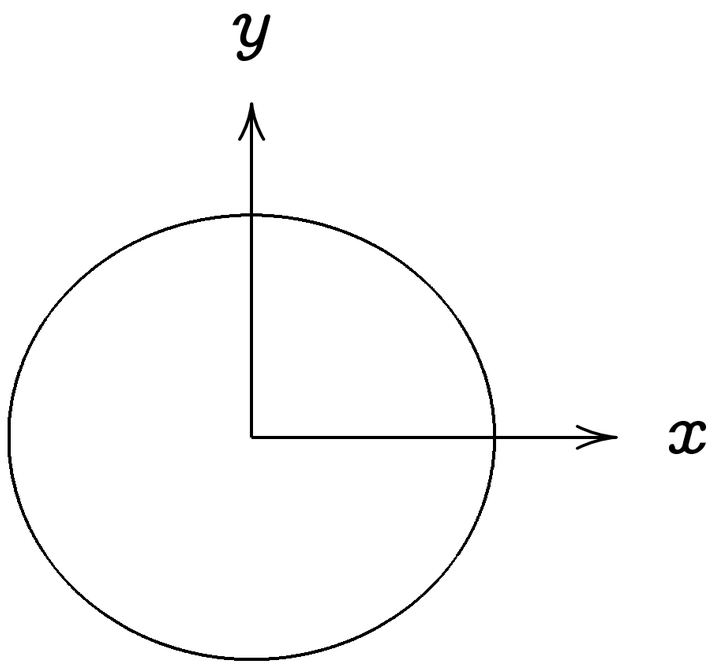
Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this
$(0, 1) =$ "12:00".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

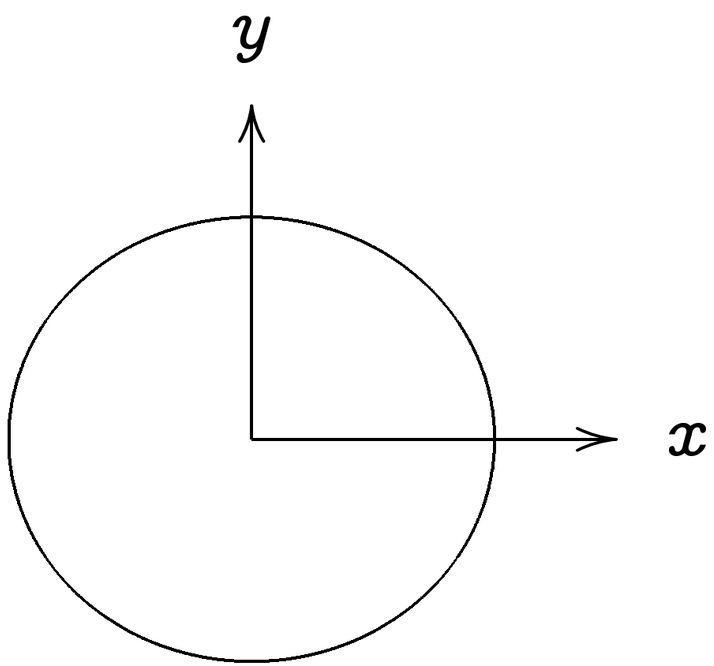
This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

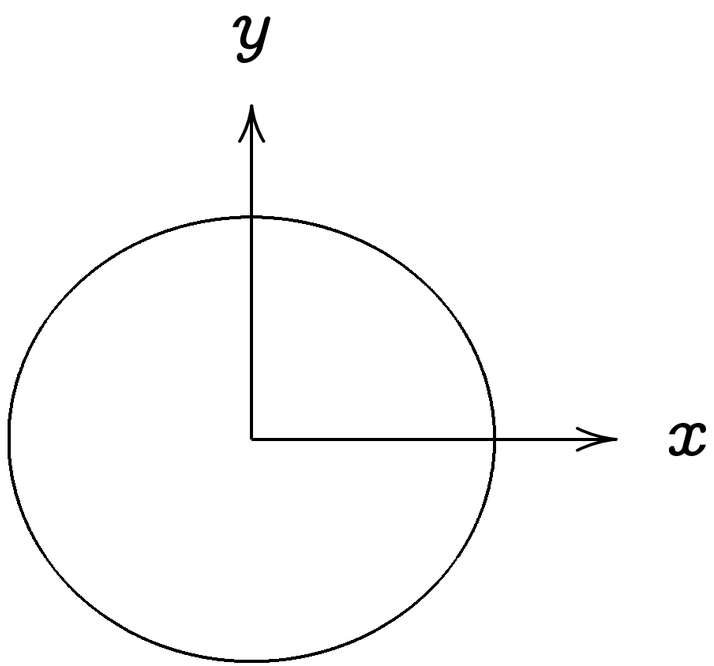
"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

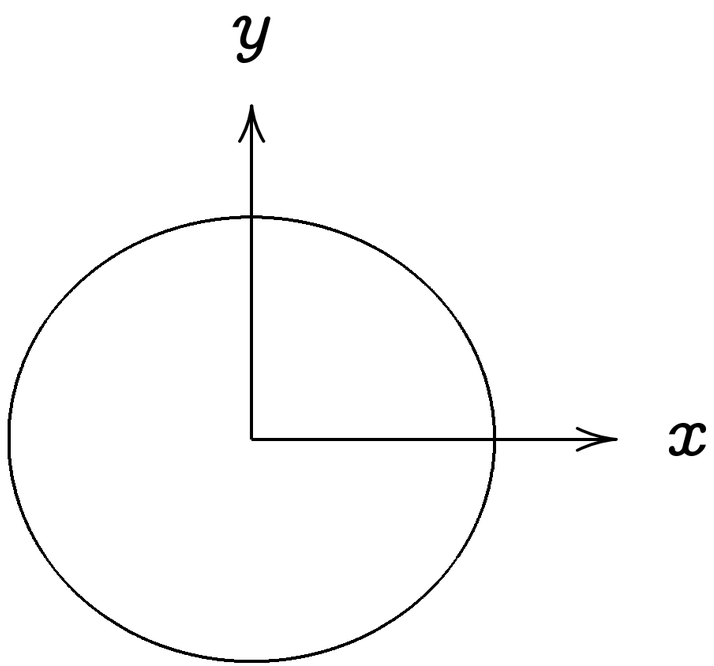
"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

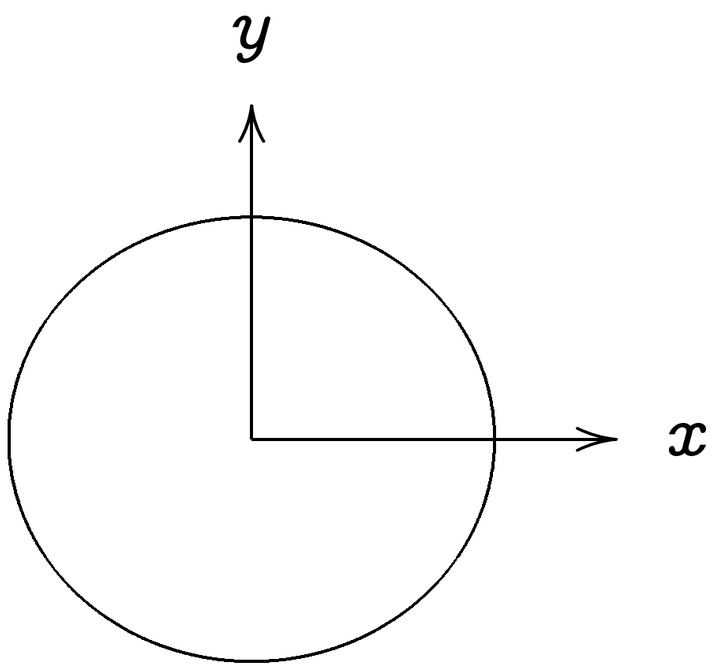
$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$

$(-1, 0) =$

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

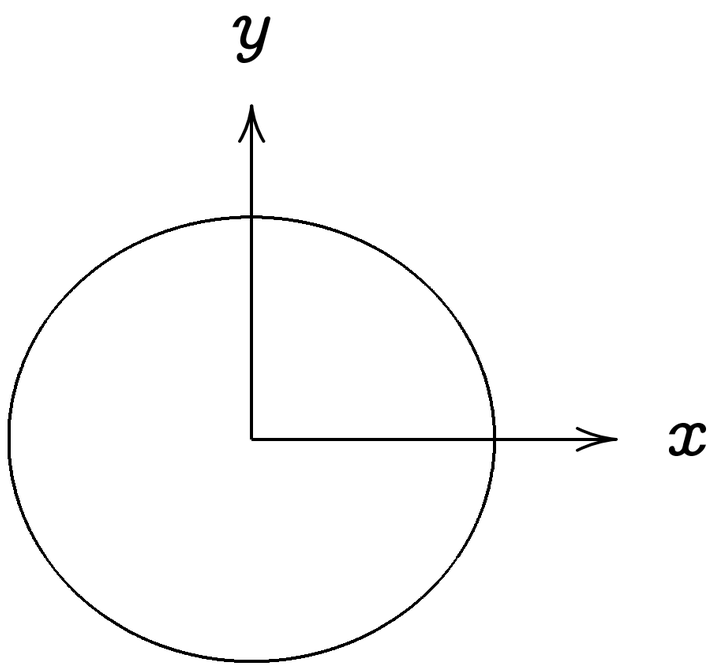
$(0, 1)$ = "12:00".

$(0, -1)$ = "6:00".

$(1, 0)$ = "3:00".

$(-1, 0)$ = "9:00".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

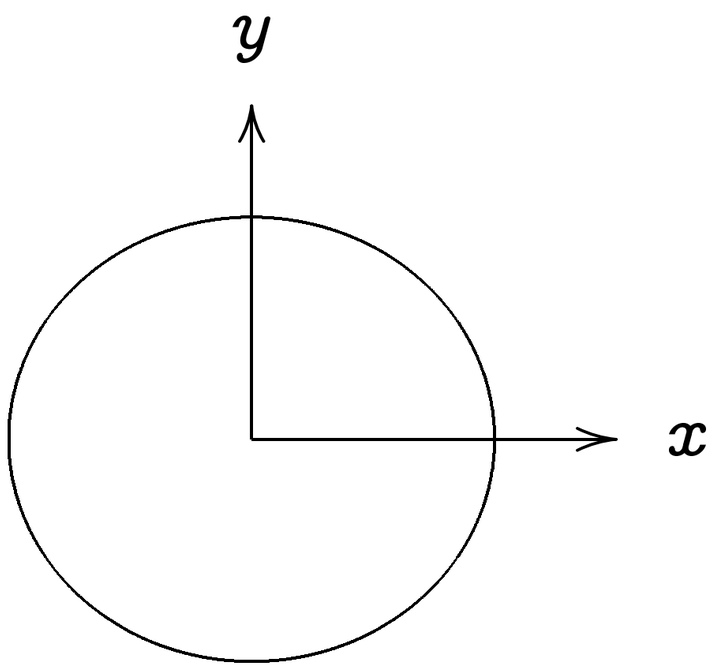
$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

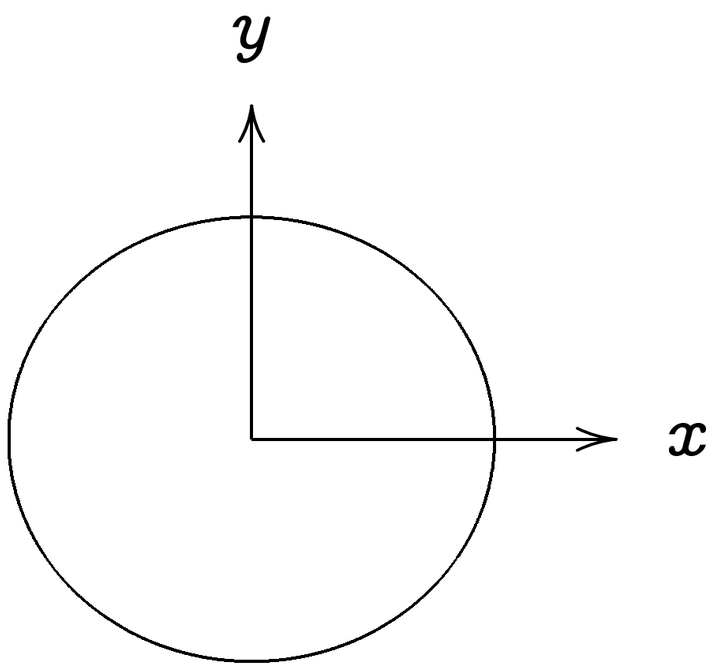
$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

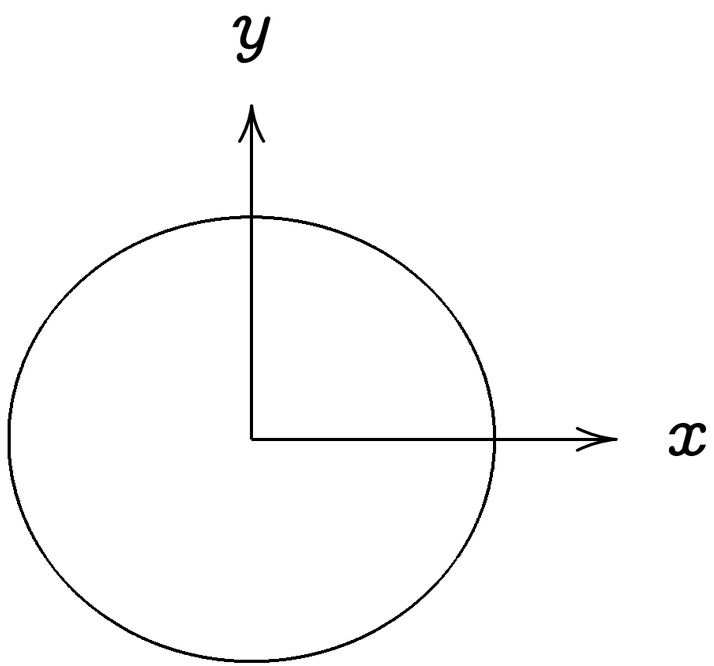
$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$

$(-1/2, -\sqrt{3/4}) =$

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

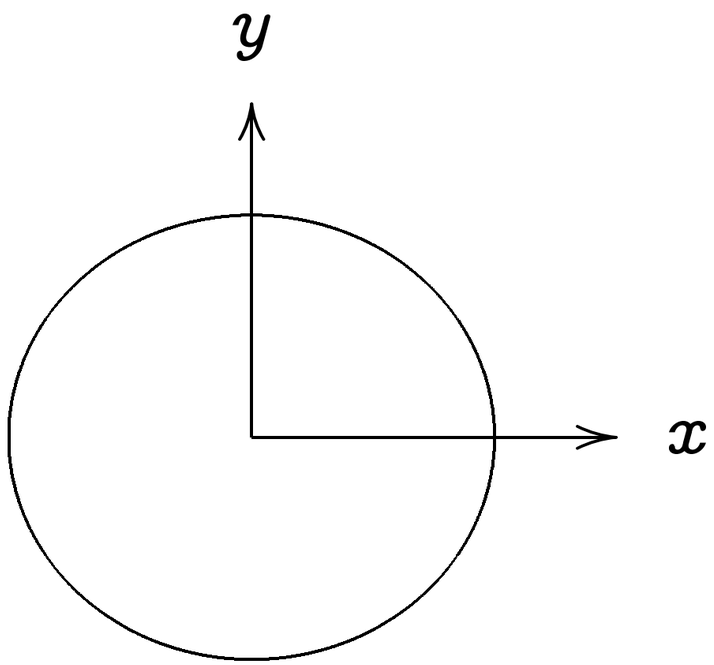
$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

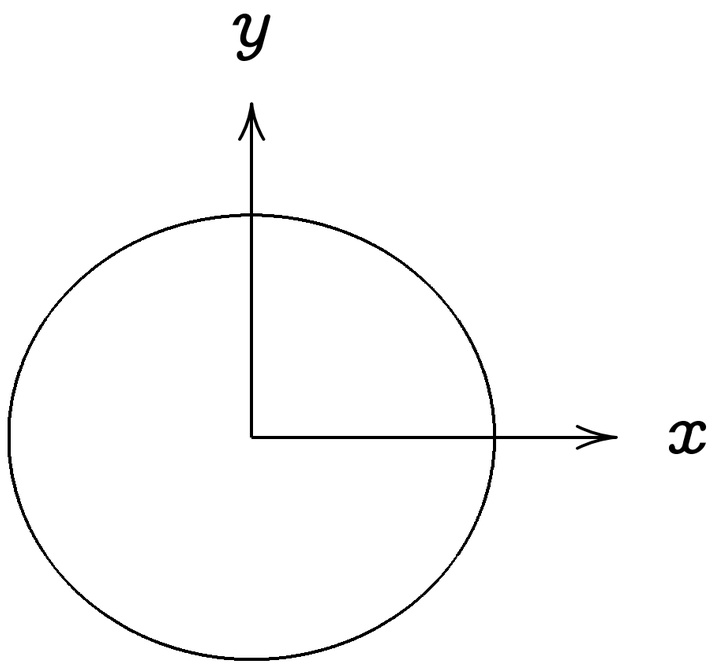
$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

$(\sqrt{1/2}, \sqrt{1/2}) =$ "1:30".

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1)$ = "12:00".

$(0, -1)$ = "6:00".

$(1, 0)$ = "3:00".

$(-1, 0)$ = "9:00".

$(\sqrt{3/4}, 1/2)$ = "2:00".

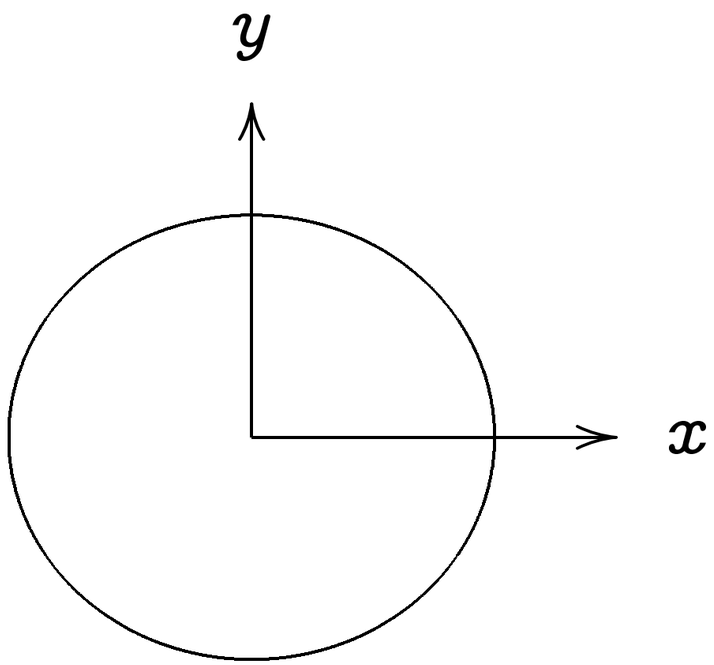
$(1/2, -\sqrt{3/4})$ = "5:00".

$(-1/2, -\sqrt{3/4})$ = "7:00".

$(\sqrt{1/2}, \sqrt{1/2})$ = "1:30".

$(3/5, 4/5)$. $(-3/5, 4/5)$.

The clock



This is the curve $x^2 + y^2 = 1$.

Warning:

This is *not* an elliptic curve.

"Elliptic curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

$(\sqrt{1/2}, \sqrt{1/2}) =$ "1:30".

$(3/5, 4/5)$. $(-3/5, 4/5)$.

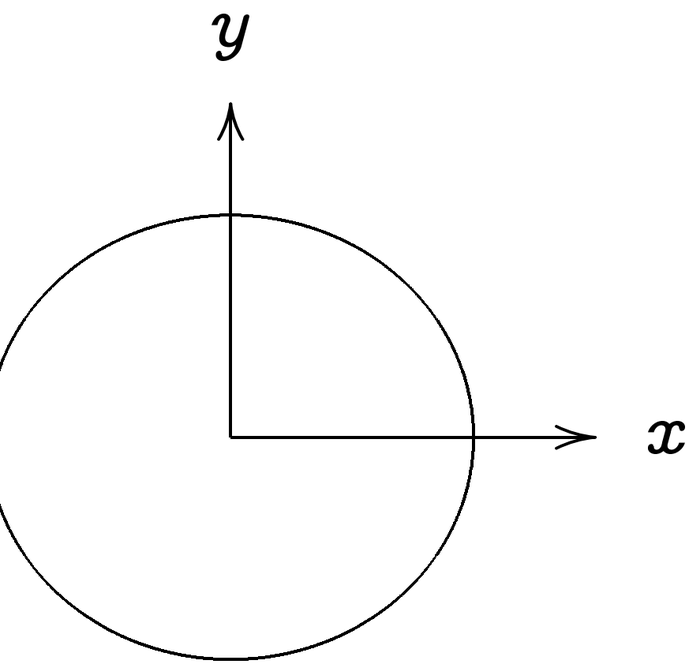
$(3/5, -4/5)$. $(-3/5, -4/5)$.

$(4/5, 3/5)$. $(-4/5, 3/5)$.

$(4/5, -3/5)$. $(-4/5, -3/5)$.

Many more.

ock



the curve $x^2 + y^2 = 1$.

g:

not an elliptic curve.

c curve" $\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

$(\sqrt{1/2}, \sqrt{1/2}) =$ "1:30".

$(3/5, 4/5)$. $(-3/5, 4/5)$.

$(3/5, -4/5)$. $(-3/5, -4/5)$.

$(4/5, 3/5)$. $(-4/5, 3/5)$.

$(4/5, -3/5)$. $(-4/5, -3/5)$.

Many more.

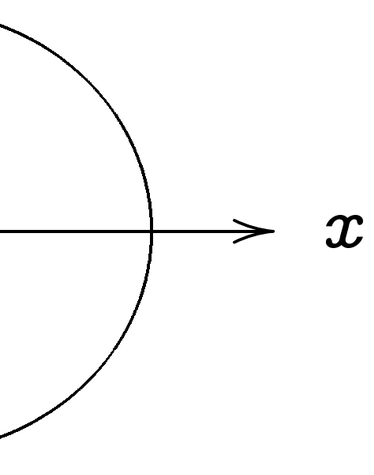
Clock a

Standa

for the

sum of

$(x_1y_2 +$



$x^2 + y^2 = 1.$

liptic curve.

$\neq$ "ellipse."

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

$(\sqrt{1/2}, \sqrt{1/2}) =$ "1:30".

$(3/5, 4/5)$. $(-3/5, 4/5)$.

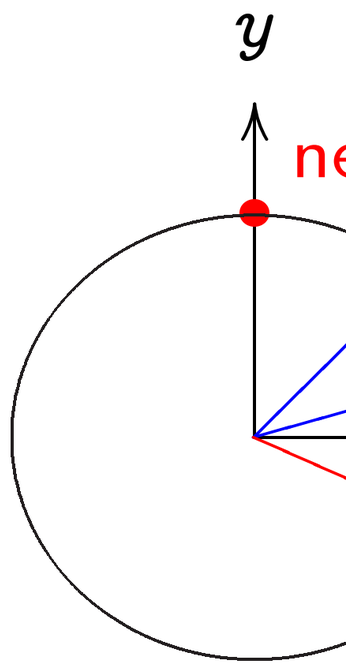
$(3/5, -4/5)$. $(-3/5, -4/5)$.

$(4/5, 3/5)$. $(-4/5, 3/5)$.

$(4/5, -3/5)$. $(-4/5, -3/5)$.

Many more.

Clock addition



Standard additio

for the clock x^2 +

sum of (x_1, y_1) a

$(x_1y_2 + y_1x_2, y_1$

x

$= 1.$

e.

"

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

$(\sqrt{1/2}, \sqrt{1/2}) =$ "1:30".

$(3/5, 4/5)$. $(-3/5, 4/5)$.

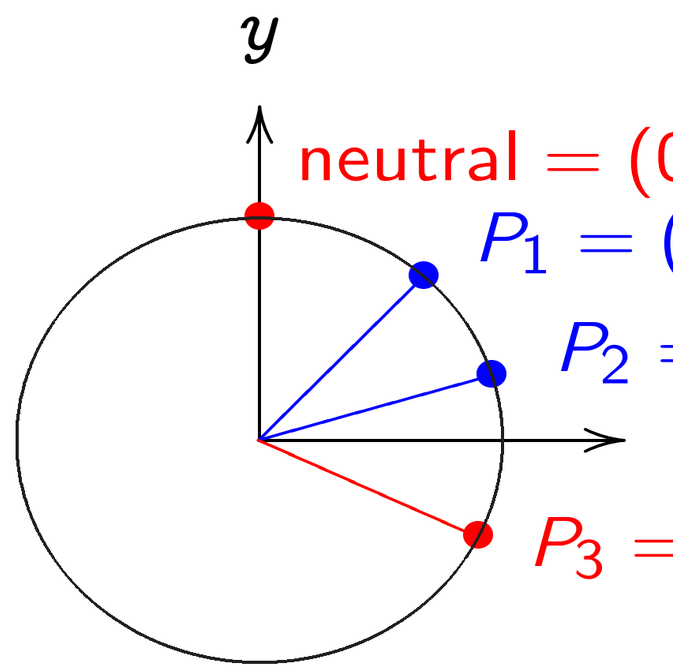
$(3/5, -4/5)$. $(-3/5, -4/5)$.

$(4/5, 3/5)$. $(-4/5, 3/5)$.

$(4/5, -3/5)$. $(-4/5, -3/5)$.

Many more.

Clock addition



Standard addition formula for the clock $x^2 + y^2 = 1$: sum of (x_1, y_1) and $(x_2, y_2$ $(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2$

Examples of points on this curve:

$(0, 1) =$ "12:00".

$(0, -1) =$ "6:00".

$(1, 0) =$ "3:00".

$(-1, 0) =$ "9:00".

$(\sqrt{3/4}, 1/2) =$ "2:00".

$(1/2, -\sqrt{3/4}) =$ "5:00".

$(-1/2, -\sqrt{3/4}) =$ "7:00".

$(\sqrt{1/2}, \sqrt{1/2}) =$ "1:30".

$(3/5, 4/5)$. $(-3/5, 4/5)$.

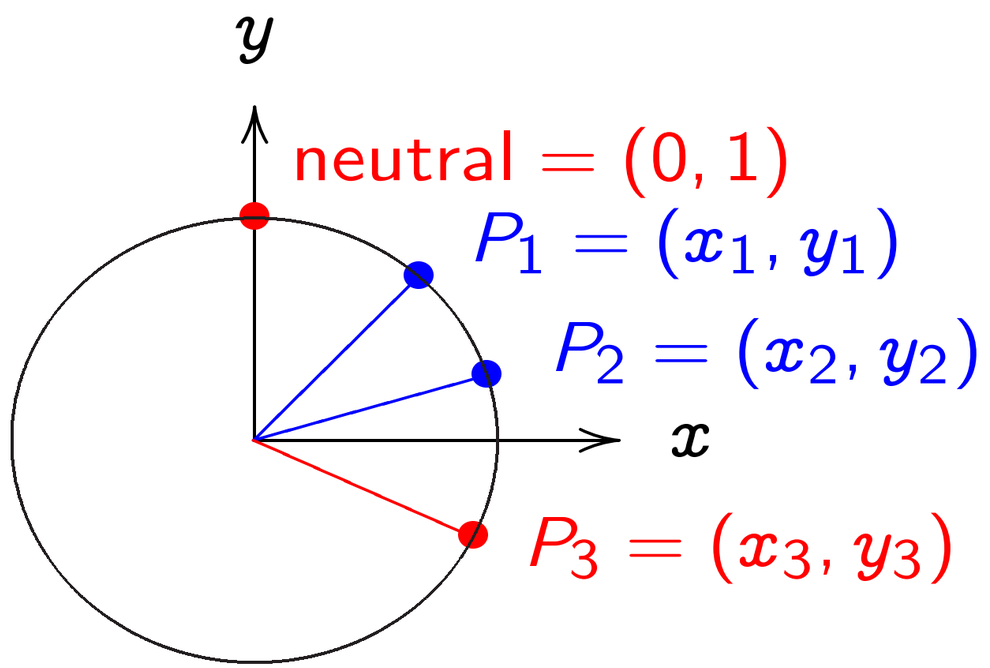
$(3/5, -4/5)$. $(-3/5, -4/5)$.

$(4/5, 3/5)$. $(-4/5, 3/5)$.

$(4/5, -3/5)$. $(-4/5, -3/5)$.

Many more.

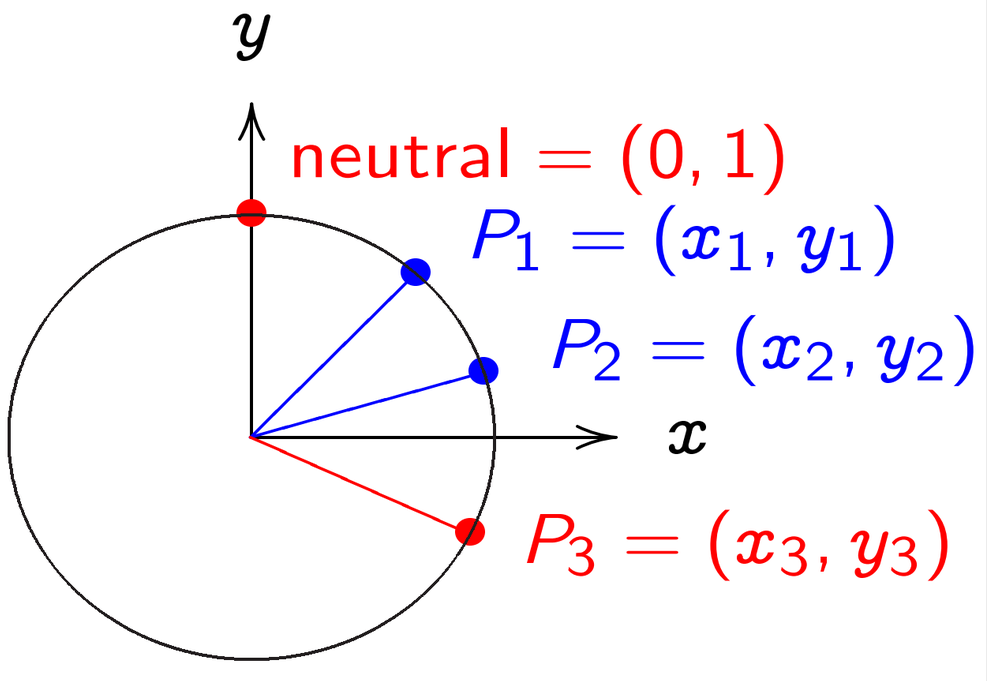
Clock addition



Standard addition formula for the clock $x^2 + y^2 = 1$: sum of (x_1, y_1) and (x_2, y_2) is $(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

les of points on this curve:
= “12:00”.
) = “6:00”.
= “3:00”.
) = “9:00”.
, 1/2) = “2:00”.
$-\sqrt{3/4}) =$ “5:00”.
$-\sqrt{3/4}) =$ “7:00”.
$, \sqrt{1/2}) =$ “1:30”.
/5). $(-3/5, 4/5)$.
-4/5). $(-3/5, -4/5)$.
/5). $(-4/5, 3/5)$.
-3/5). $(-4/5, -3/5)$.
more.

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examp
“2:00”
$= (\sqrt{3}$

nts on this curve:

.

.

.

2:00".

"5:00".

= "7:00".

= "1:30".

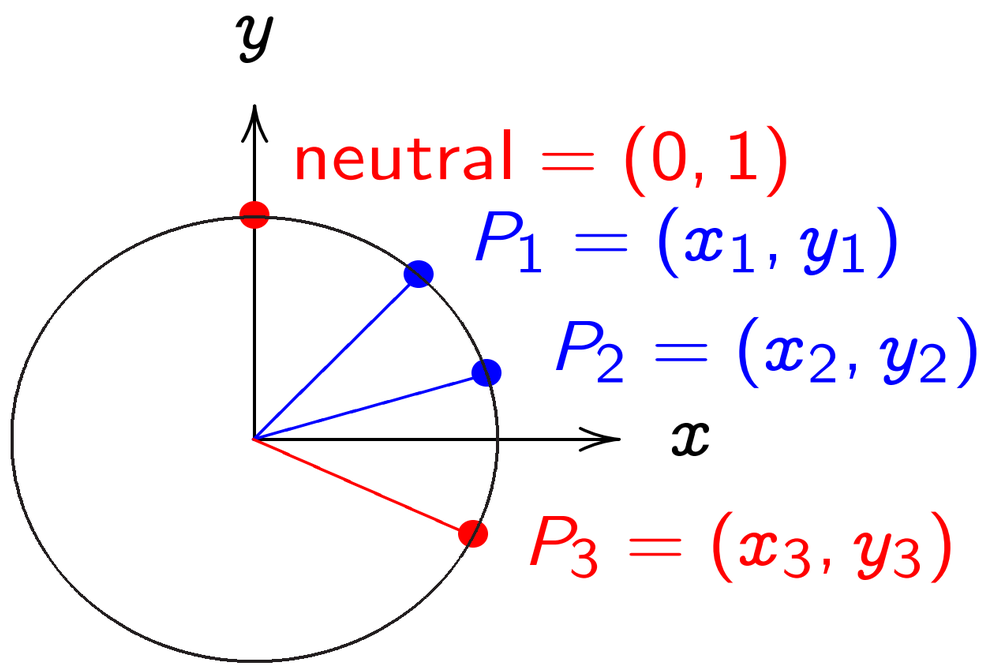
/5, 4/5).

3/5, −4/5).

/5, 3/5).

4/5, −3/5).

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

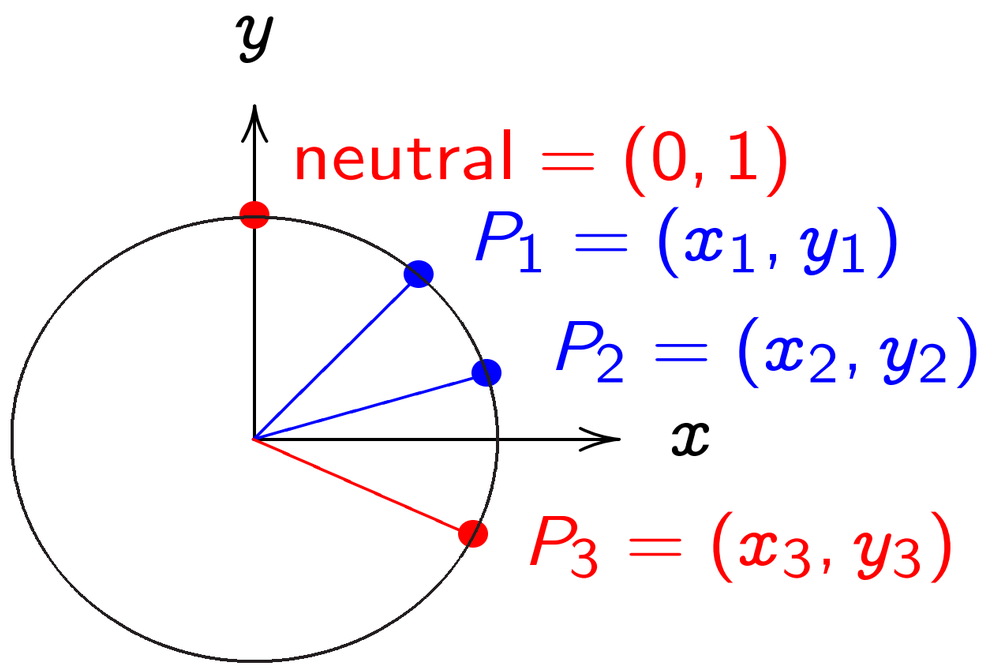
Examples of cloc

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) +$

curve:

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

).

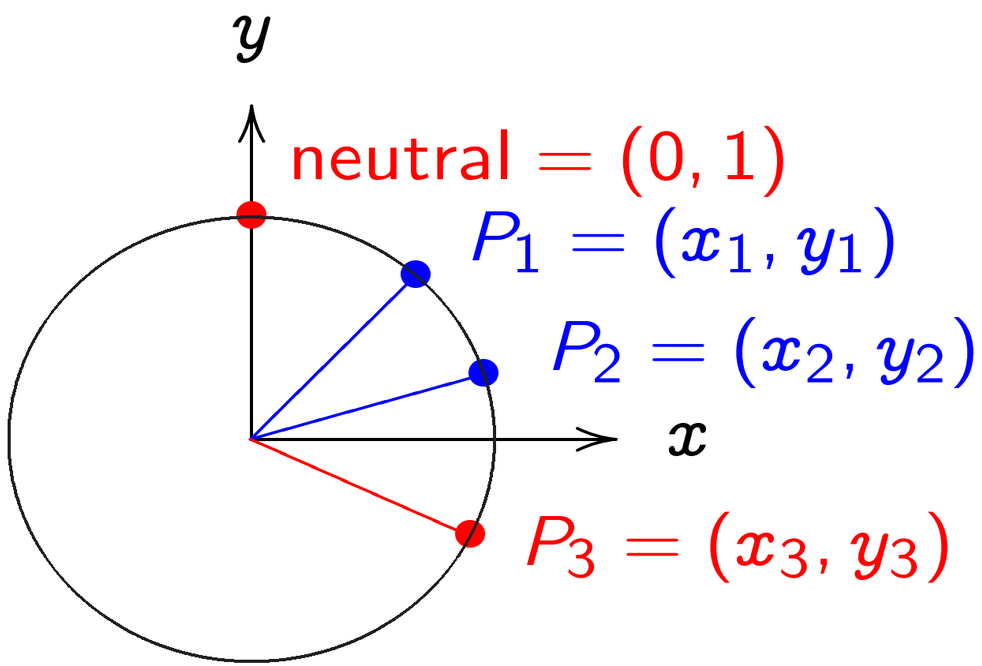
).

Examples of clock addition

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt$

Clock addition



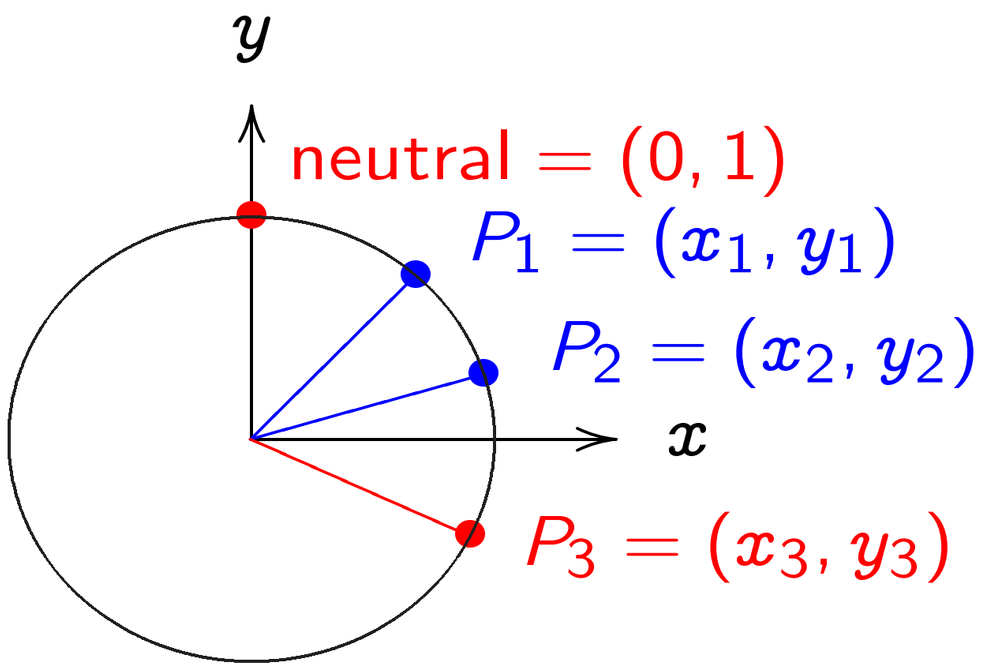
Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

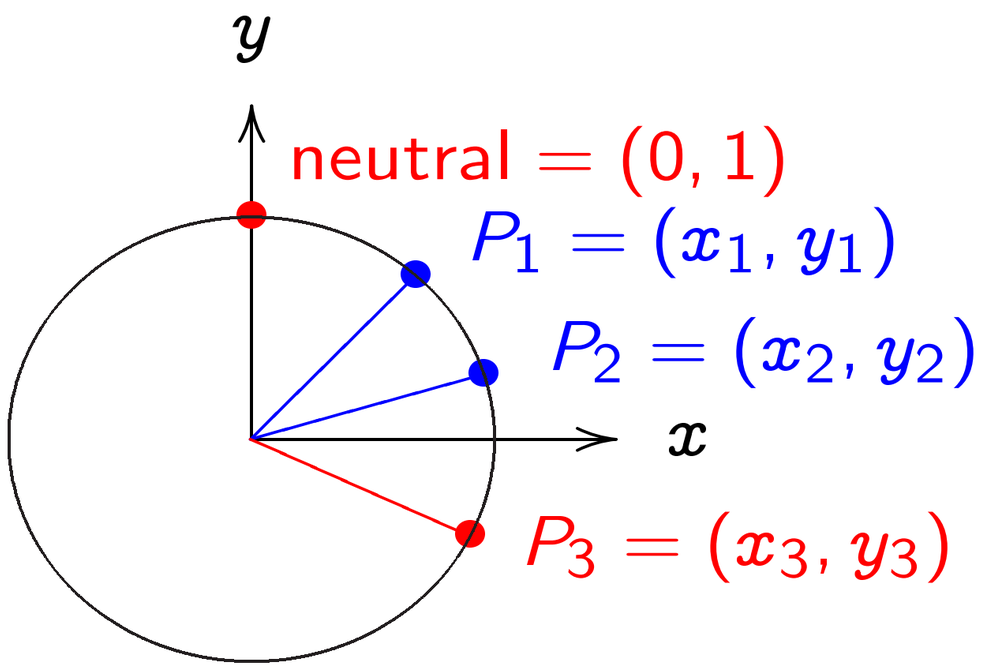
Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4})$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

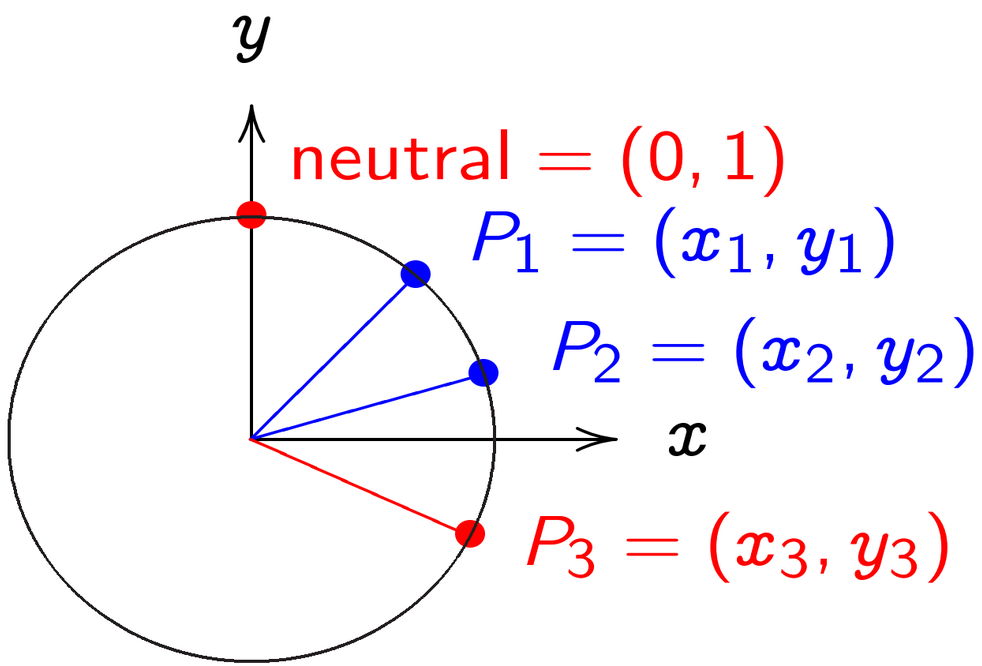
Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

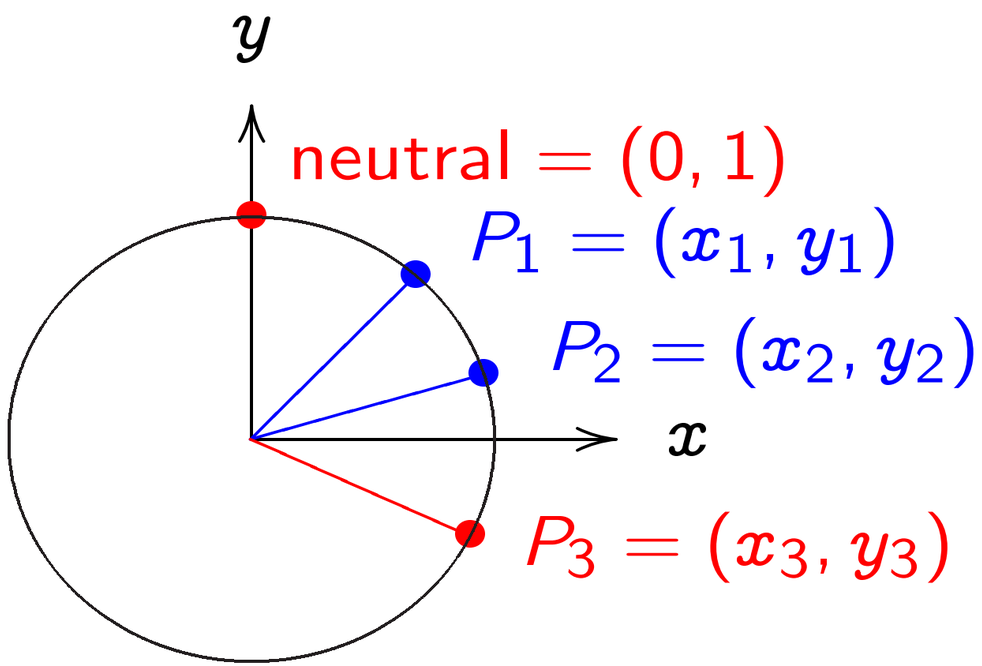
$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

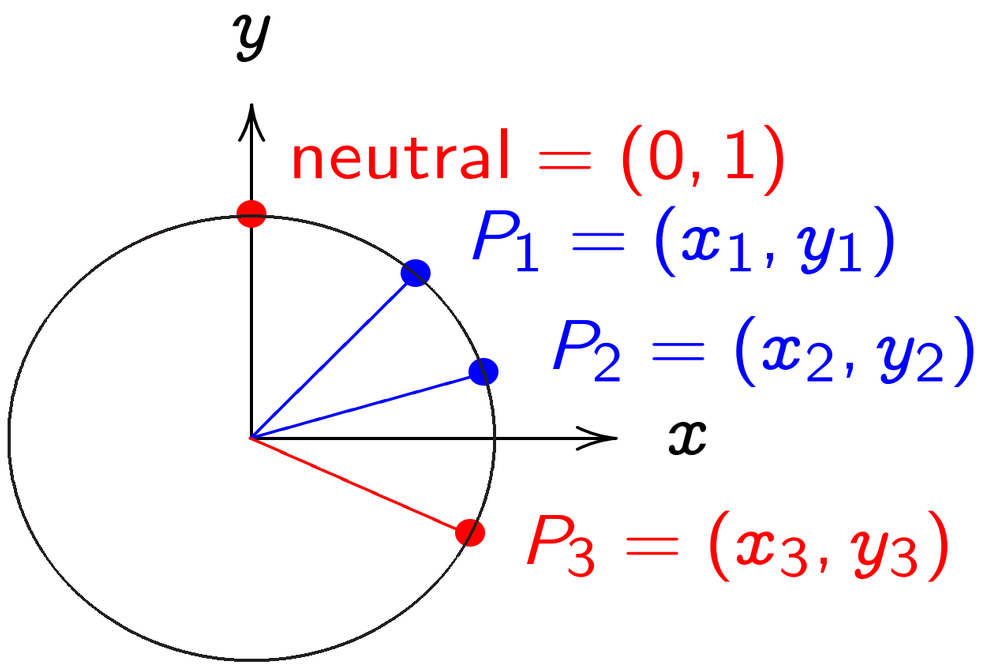
$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

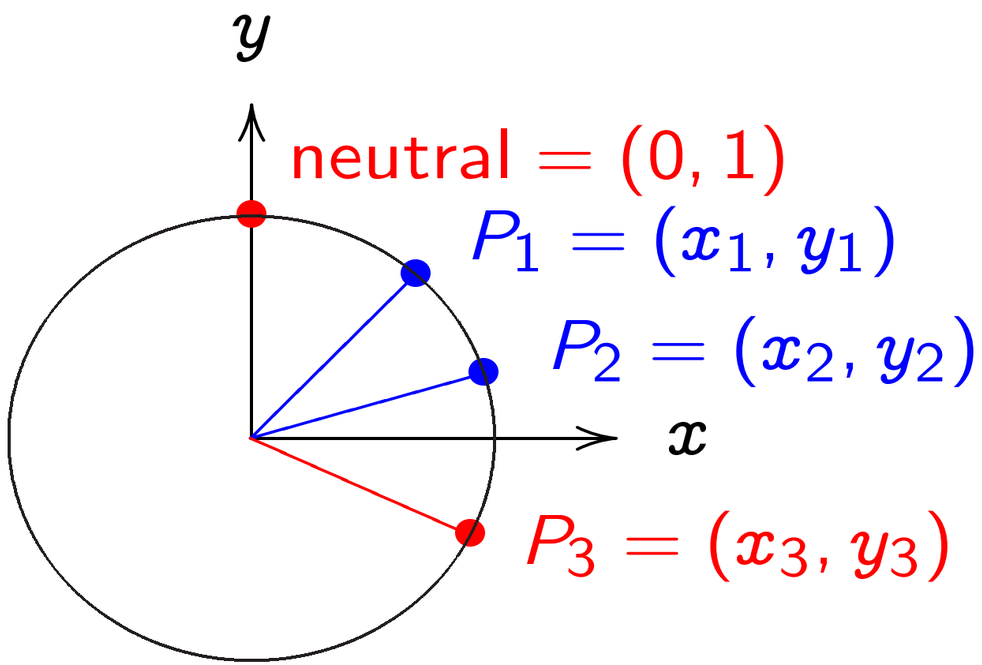
"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$2\left(\frac{3}{5}, \frac{4}{5}\right) =$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

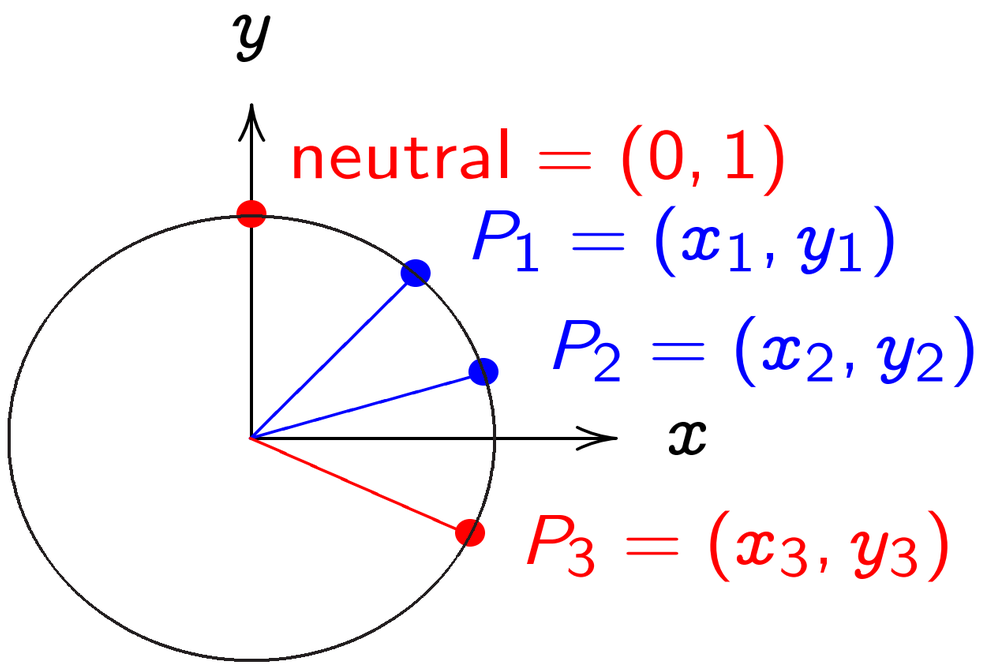
"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

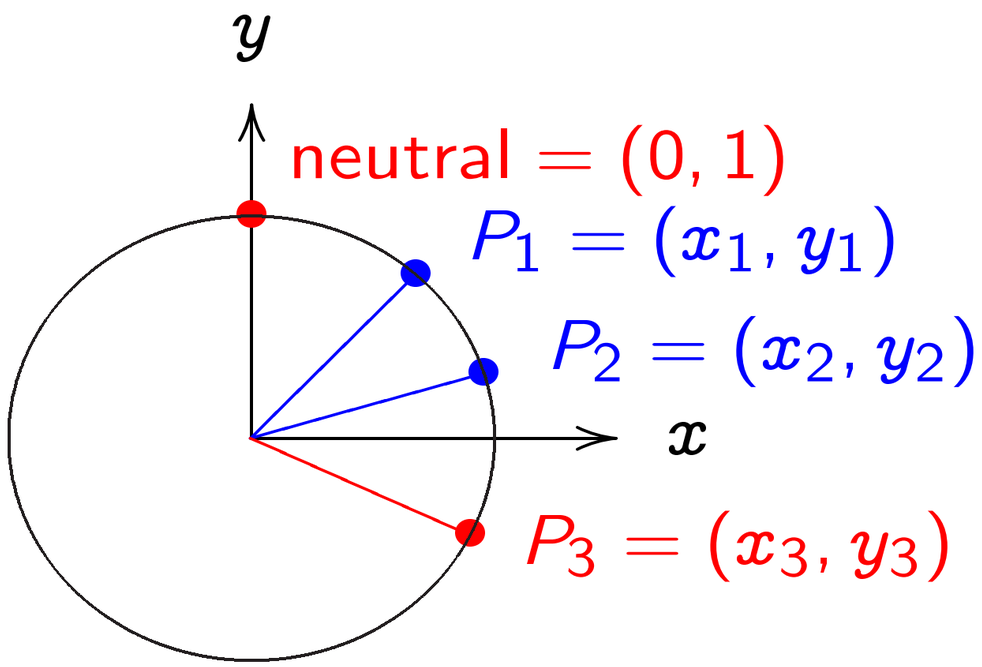
$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

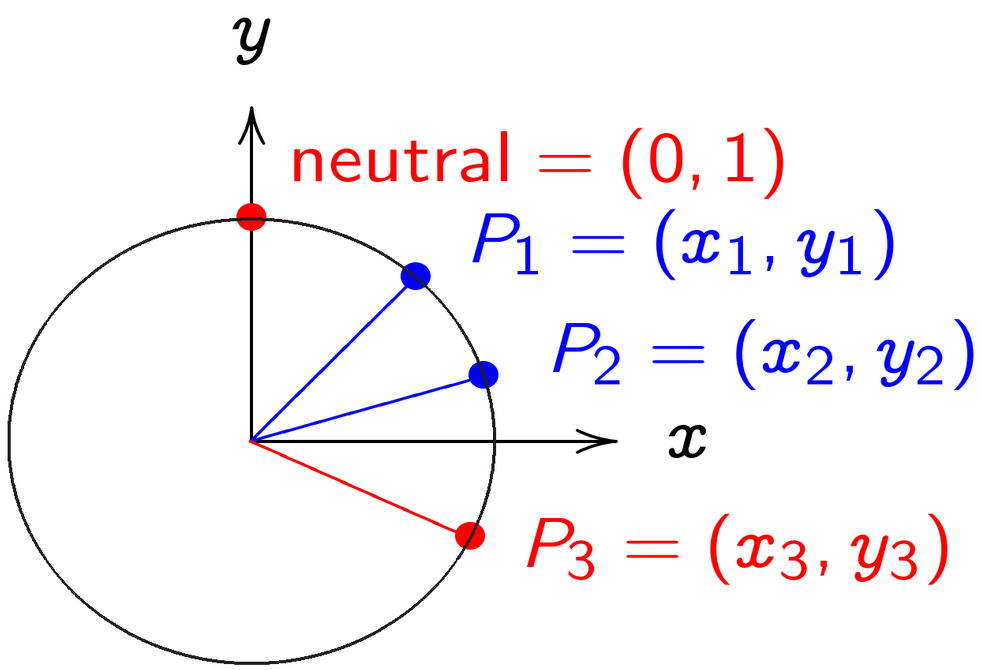
$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

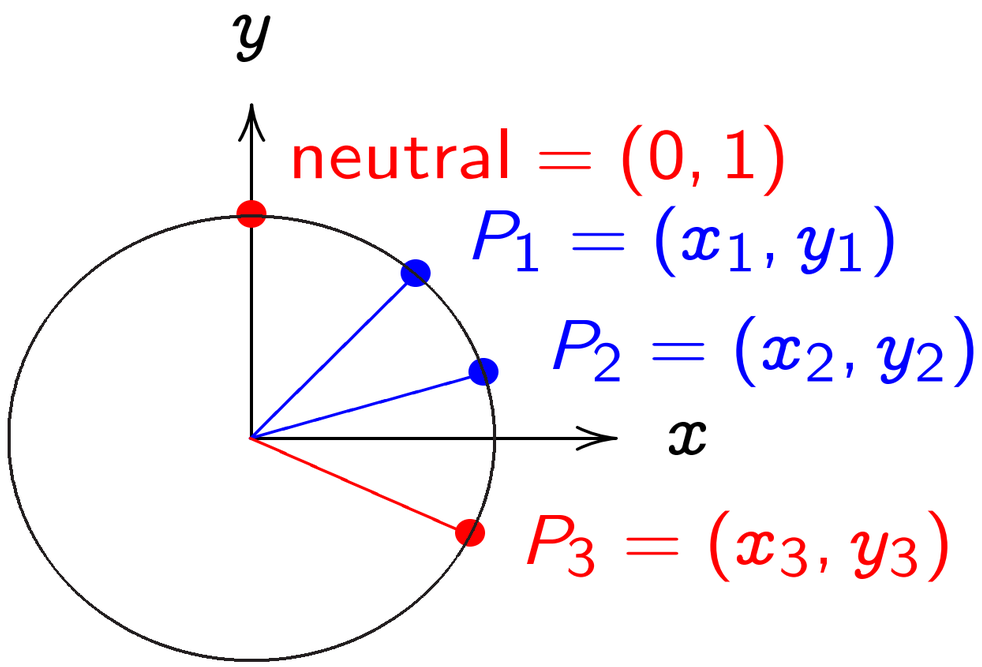
$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) =$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

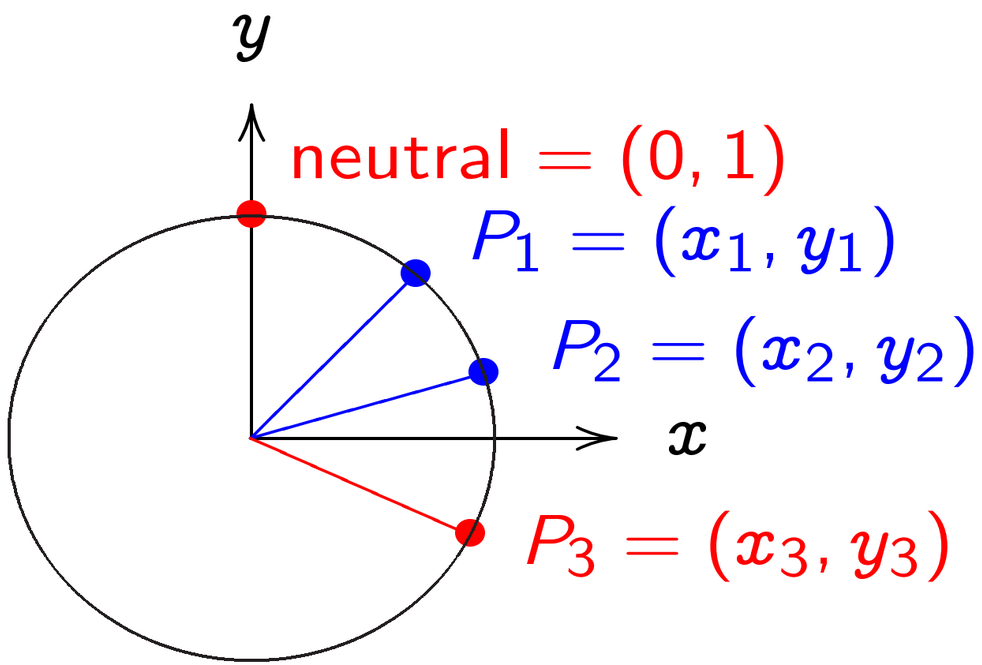
$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) = (x_1, y_1)$.

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

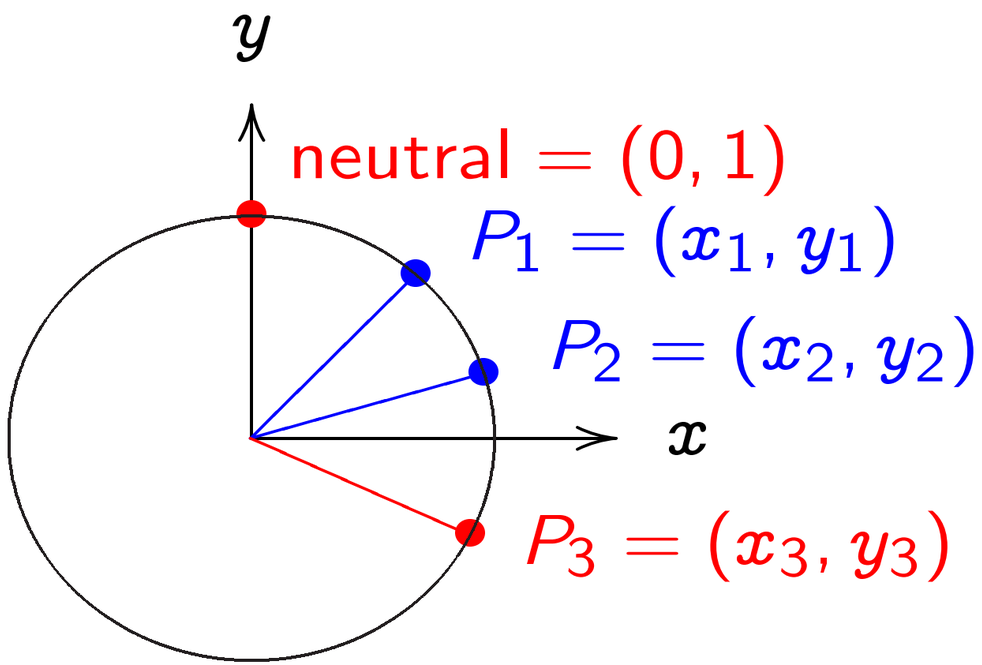
$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) = (x_1, y_1).$

$(x_1, y_1) + (-x_1, y_1) =$

Clock addition



Standard addition formula
for the clock $x^2 + y^2 = 1$:
sum of (x_1, y_1) and (x_2, y_2) is
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"
$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$
$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"
$= (1/2, -\sqrt{3/4}) + (-1, 0)$
$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

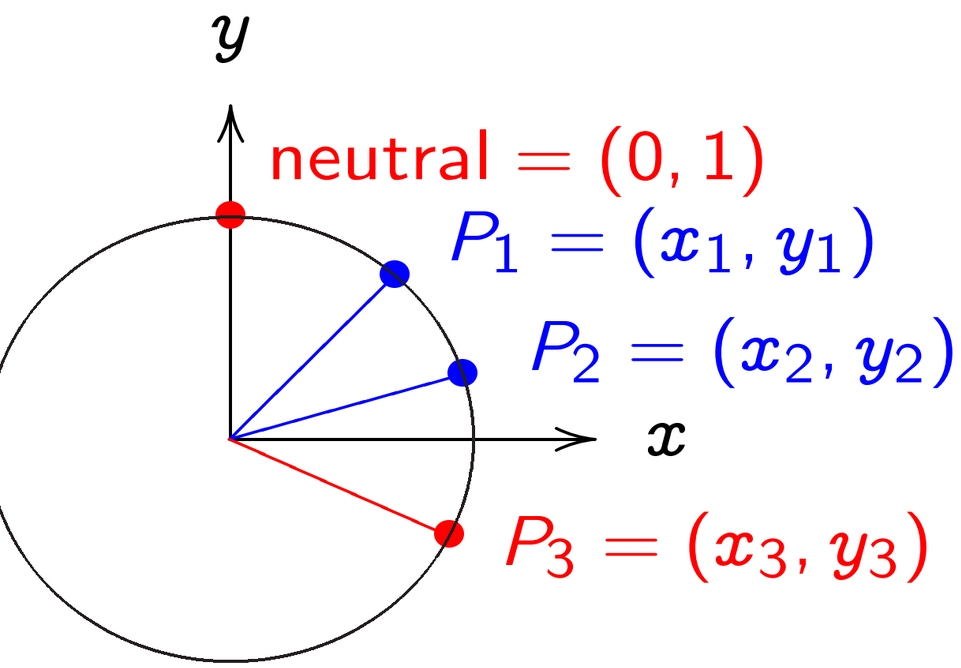
$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) = (x_1, y_1)$.

$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

addition



rd addition formula
clock $x^2 + y^2 = 1$:
(x_1, y_1) and (x_2, y_2) is
$+ y_1x_2, y_1y_2 - x_1x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

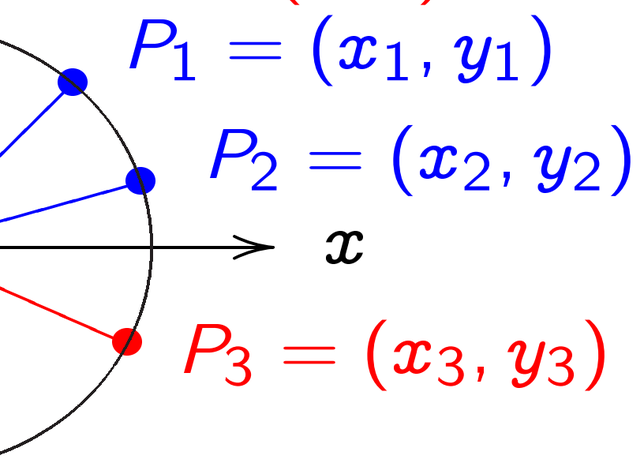
$(x_1, y_1) + (0, 1) = (x_1, y_1)$.

$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

Define
$\{(x, y)$
As usu

Exercis
Prove t
is a co
under

In othe
clock s
clock a
clock a
there is
each el



n formula
$+ y^2 = 1$:
and (x_2, y_2) is
$y_2 - x_1 x_2)$.

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) = (x_1, y_1).$

$(x_1, y_1) + (-x_1, y_1) = (0, 1).$

Define Clock($\mathbf{R}$)
$\{(x, y) \in \mathbf{R} \times \mathbf{R}$
As usual $\mathbf{R} = \{$re

Exercise:
Prove that Clock
is a commutative
under clock addi

In other words:
clock sum is in C
clock addition is
clock addition is
there is a neutral
each element has

$0, 1)$
(x_1, y_1)
$= (x_2, y_2)$
x
$= (x_3, y_3)$

$_2$) is
).

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) = (x_1, y_1).$

$(x_1, y_1) + (-x_1, y_1) = (0, 1).$

Define Clock($\mathbf{R}$) as

$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2$

As usual $\mathbf{R} = \{$real numbe

Exercise:

Prove that Clock($\mathbf{R}$)

is a commutative group

under clock addition.

In other words:

clock sum is in Clock($\mathbf{R}$);

clock addition is commutat

clock addition is associativ

there is a neutral element;

each element has a negativ

Examples of clock addition:

"2:00" + "5:00"

$= (\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$= (-1/2, -\sqrt{3/4}) =$ "7:00".

"5:00" + "9:00"

$= (1/2, -\sqrt{3/4}) + (-1, 0)$

$= (\sqrt{3/4}, 1/2) =$ "2:00".

$$2\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$(x_1, y_1) + (0, 1) = (x_1, y_1).$

$(x_1, y_1) + (-x_1, y_1) = (0, 1).$

Define Clock($\mathbf{R}$) as

$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}.$

As usual $\mathbf{R} = \{$real numbers$\}$.

Exercise:

Prove that Clock($\mathbf{R}$)

is a commutative group

under clock addition.

In other words:

clock sum is in Clock($\mathbf{R}$);

clock addition is commutative;

clock addition is associative;

there is a neutral element;

each element has a negative.

les of clock addition:

$+$ "5:00"

$\sqrt{3/4}, 1/2) + (1/2, -\sqrt{3/4})$

$/2, -\sqrt{3/4}) =$ "7:00".

$+$ "9:00"

$2, -\sqrt{3/4}) + (-1, 0)$

$\sqrt{3/4}, 1/2) =$ "2:00".

$$\left(\frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right).$$

$$\left(\frac{4}{5}\right) = \left(\frac{117}{125}, \frac{-44}{125}\right).$$

$$\left(\frac{4}{5}\right) = \left(\frac{336}{625}, \frac{-527}{625}\right).$$

$) + (0, 1) = (x_1, y_1).$

$) + (-x_1, y_1) = (0, 1).$

Define Clock($\mathbf{R}$) as
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$.
As usual $\mathbf{R} = \{\text{real numbers}\}$.

Exercise:
Prove that Clock($\mathbf{R}$)
is a commutative group
under clock addition.

In other words:
clock sum is in Clock($\mathbf{R}$);
clock addition is commutative;
clock addition is associative;
there is a neutral element;
each element has a negative.

How to

$x^2 + y$

$x = \sin$

$(\sin(\alpha_1$

$(\sin \alpha_1$

$\cos \alpha_1$

k addition:

$+ (1/2, -\sqrt{3/4})$

$\overline{4}) =$ “7:00”.

$+ (-1, 0)$

$=$ “2:00”.

$\left(\frac{}{5}, \frac{7}{25}\right)$.

$\left(\frac{7}{25}, \frac{-44}{125}\right)$.

$\left(\frac{36}{25}, \frac{-527}{625}\right)$.

$= (x_1, y_1)$.

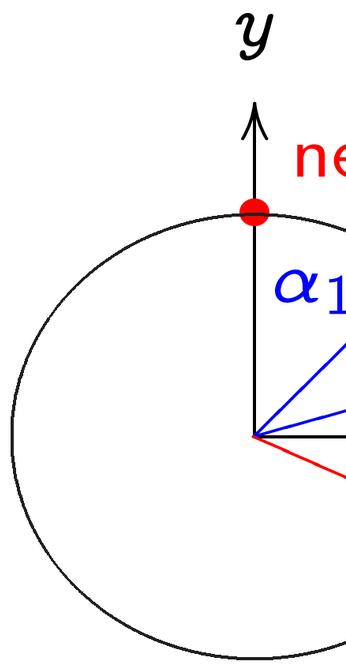
$y_1) = (0, 1)$.

Define Clock($\mathbf{R}$) as
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$.
As usual $\mathbf{R} = \{\text{real numbers}\}$.

Exercise:
Prove that Clock($\mathbf{R}$)
is a commutative group
under clock addition.

In other words:
clock sum is in Clock($\mathbf{R}$);
clock addition is commutative;
clock addition is associative;
there is a neutral element;
each element has a negative.

How to remembe



$x^2 + y^2 = 1$, par

$x = \sin\alpha, \quad y =$

$(\sin(\alpha_1 + \alpha_2), \cos$

$(\sin\alpha_1 \cos\alpha_2 +$

$\cos\alpha_1 \cos\alpha_2 -$

:

$\sqrt{3/4})$

0".

).

.

1).

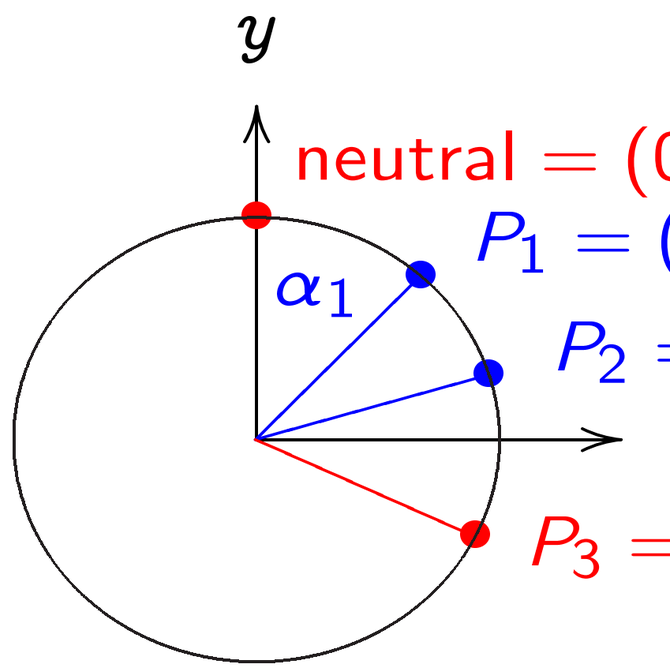
Define Clock($\mathbf{R}$) as
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$.
As usual $\mathbf{R} = \{\text{real numbers}\}$.

Exercise:

Prove that Clock($\mathbf{R}$)
is a commutative group
under clock addition.

In other words:
clock sum is in Clock($\mathbf{R}$);
clock addition is commutative;
clock addition is associative;
there is a neutral element;
each element has a negative.

How to remember addition



$x^2 + y^2 = 1$, parametrized

$x = \sin\alpha, \quad y = \cos\alpha.$ Re

$(\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2$

$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha$

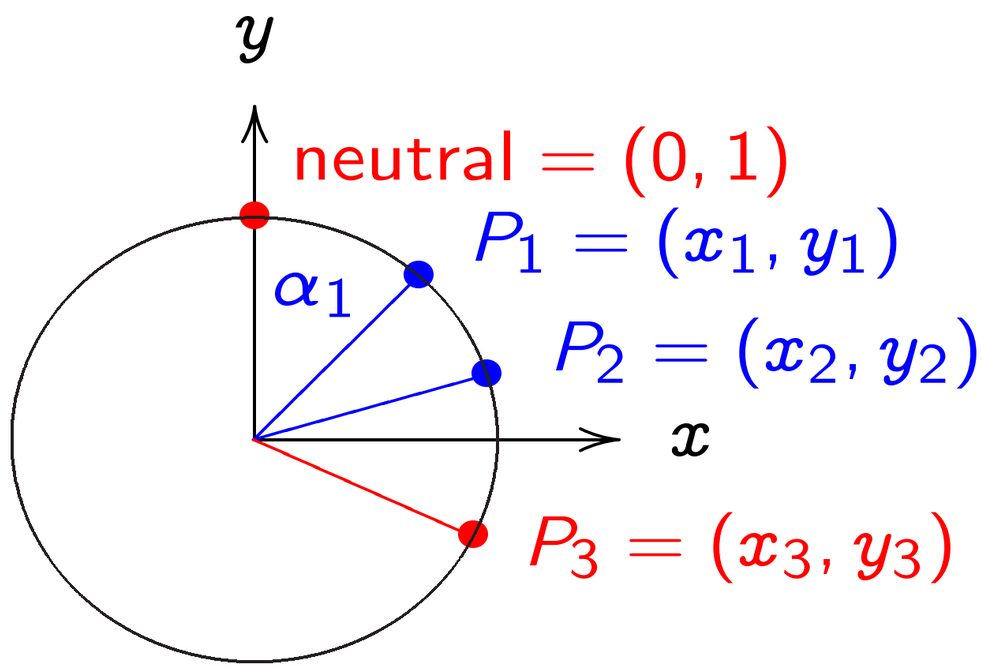
$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha$

Define Clock($\mathbf{R}$) as
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$.
As usual $\mathbf{R} = \{\text{real numbers}\}$.

Exercise:
Prove that Clock($\mathbf{R}$)
is a commutative group
under clock addition.

In other words:
clock sum is in Clock($\mathbf{R}$);
clock addition is commutative;
clock addition is associative;
there is a neutral element;
each element has a negative.

How to remember addition law:



$x^2 + y^2 = 1$, parametrized by
$x = \sin\alpha, \quad y = \cos\alpha$. Recall
$(\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2)) =$
$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$
$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2)$.

Clock(**R**) as

$\in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$.

al $\mathbf{R} = \{$real numbers$\}$.

se:

that Clock(**R**)

mmutative group

clock addition.

er words:

um is in Clock(**R**);

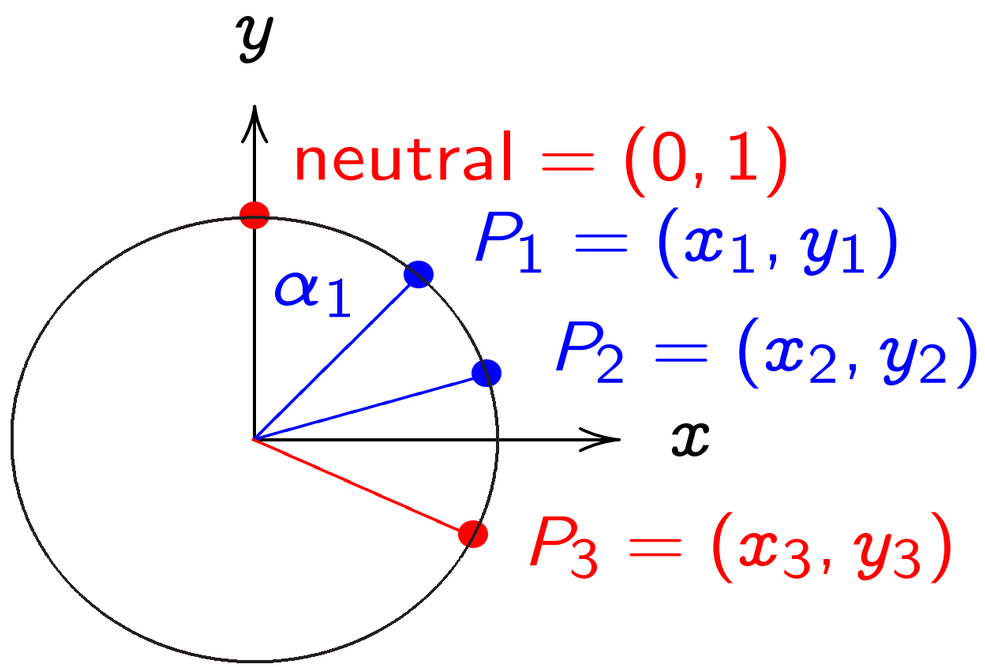
ddition is commutative;

ddition is associative;

s a neutral element;

ement has a negative.

How to remember addition law:



$x^2 + y^2 = 1$, parametrized by

$x = \sin\alpha, \quad y = \cos\alpha$. Recall

$(\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2)) =$

$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$

$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2)$.

Clock(

$\{(x, y)$

Here **F**

$= \{0, 1$

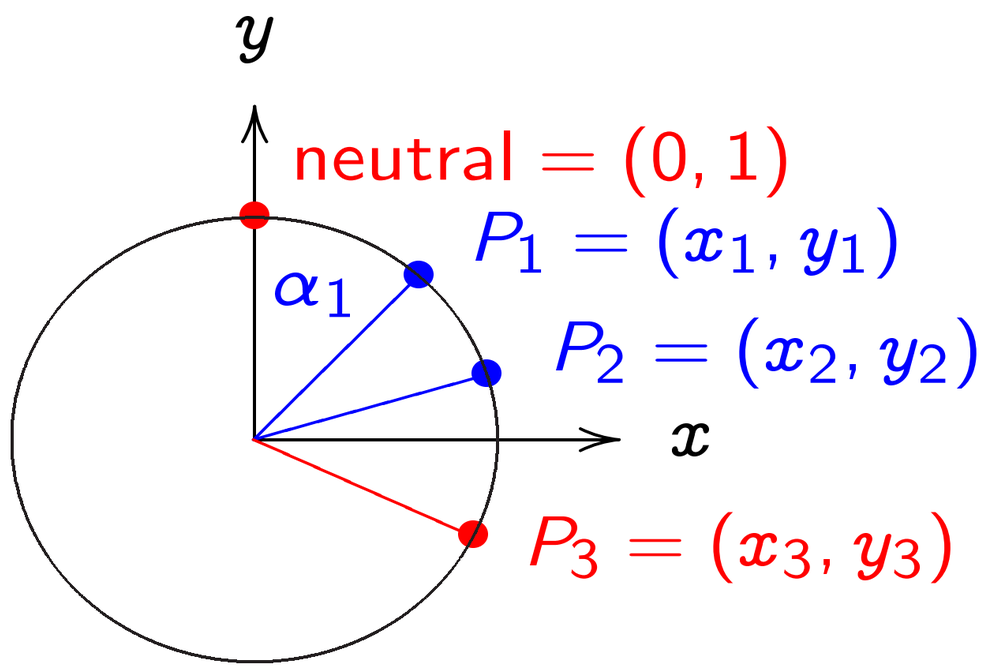
with +

as
$: x^2 + y^2 = 1\}$.
eal numbers}.

$\mathbf{k}(\mathbf{R})$
e group
tion.

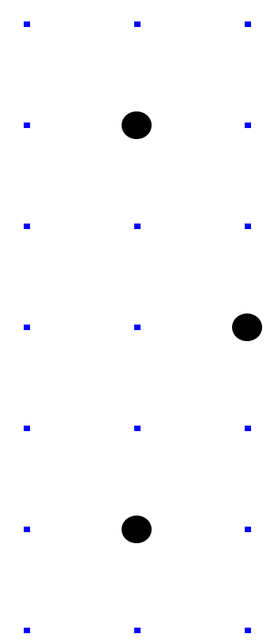
Clock($\mathbf{R}$);
commutative;
associative;
l element;
s a negative.

How to remember addition law:



$x^2 + y^2 = 1$, parametrized by
$x = \sin\alpha, \quad y = \cos\alpha$. Recall
$(\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2)) =$
$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$
$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2)$.

Clocks over finite



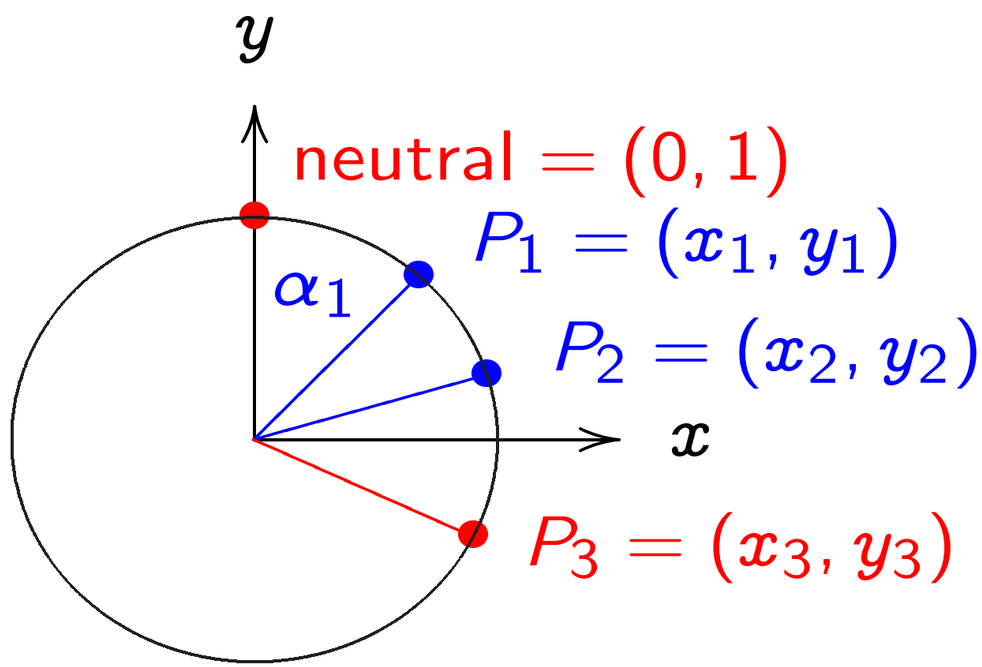
Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}$
Here $\mathbf{F}_7 = \{0, 1,$
$= \{0, 1, 2, 3, -3,$
with $+, -, \times$ mo

$= 1\}$.
rs$\}$.

tive;
e;

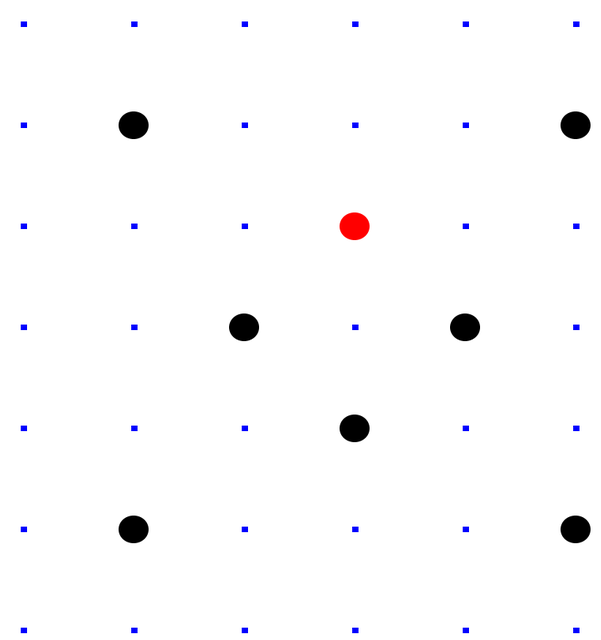
ve.

How to remember addition law:



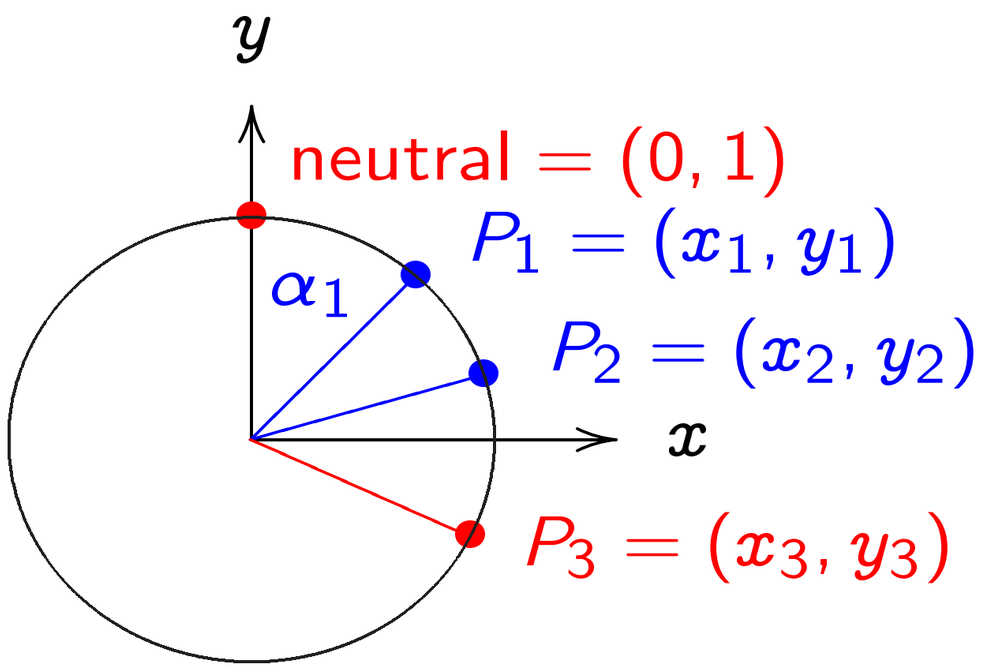
$x^2 + y^2 = 1$, parametrized by
$x = \sin\alpha, \quad y = \cos\alpha$. Recall
$(\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2)) =$
$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$
$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2)$.

Clocks over finite fields



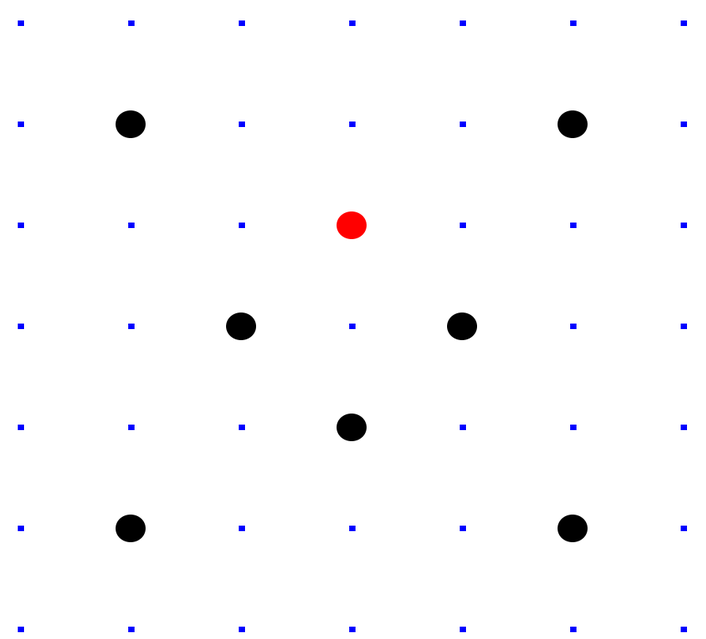
Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y$
Here $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6$
$= \{0, 1, 2, 3, -3, -2, -1\}$
with $+, -, \times$ modulo 7.

How to remember addition law:



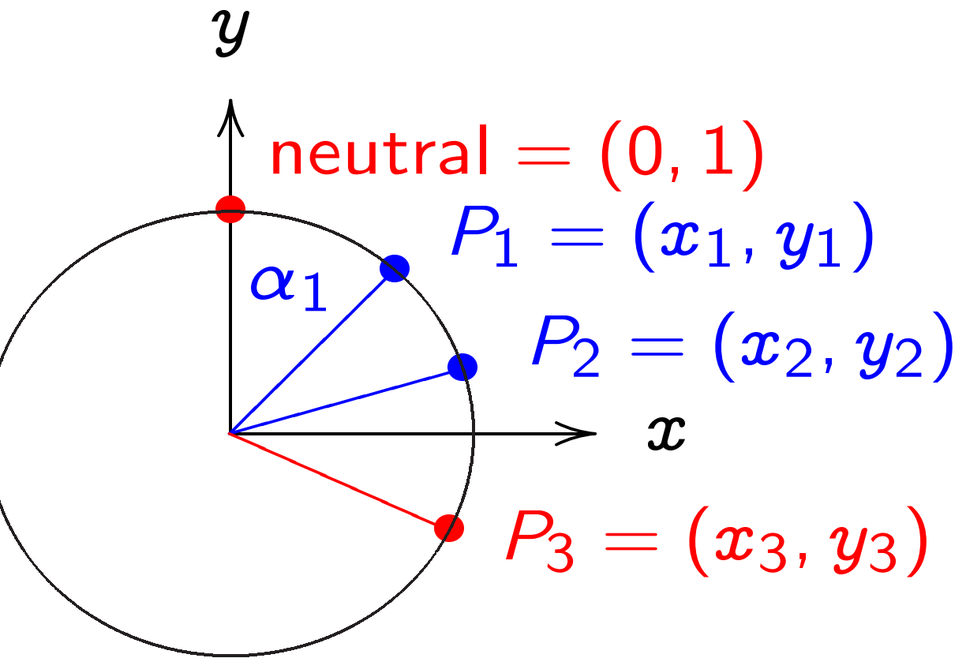
$x^2 + y^2 = 1$, parametrized by
$x = \sin\alpha, \quad y = \cos\alpha$. Recall
$(\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2)) =$
$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$
$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2)$.

Clocks over finite fields



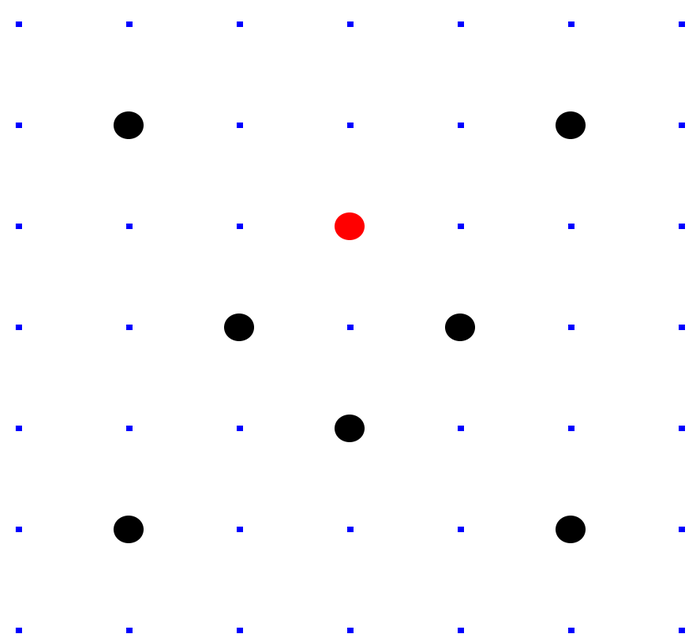
Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Here $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$= \{0, 1, 2, 3, -3, -2, -1\}$
with $+, -, \times$ modulo 7.

o remember addition law:



$^2 = 1$, parametrized by
$\sin\alpha, \quad y = \cos\alpha$. Recall
$_1 + \alpha_2), \cos(\alpha_1 + \alpha_2)) =$
$\cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$
$\cos\alpha_2 - \sin\alpha_1 \sin\alpha_2).$

Clocks over finite fields



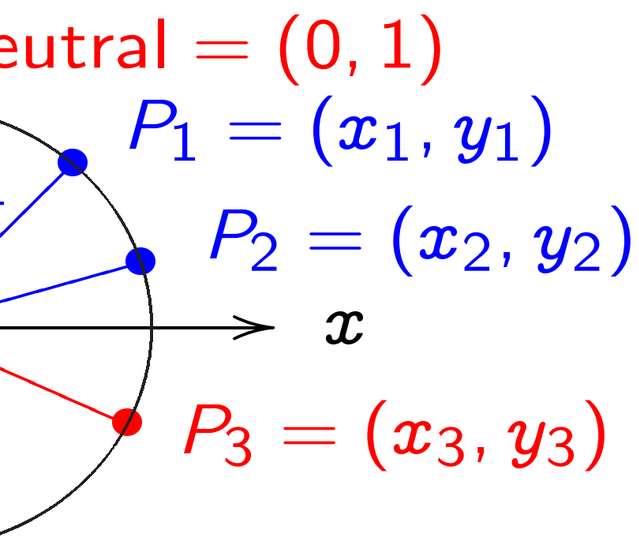
Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Here $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$= \{0, 1, 2, 3, -3, -2, -1\}$
with $+, -, \times$ modulo 7.

Clock(
under t
used fo
$(x_1, y_1$
$(x_1 y_2 +$

Similar
finite g
for eac

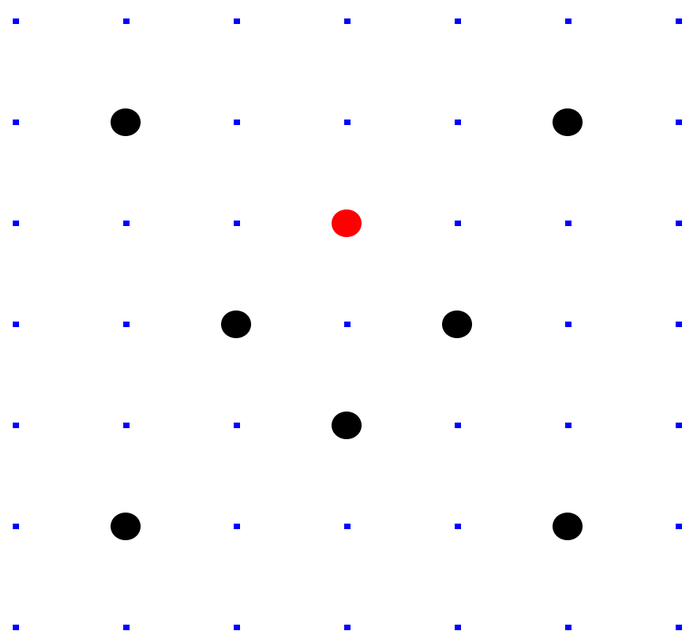
Clock(
"Index-
discrete
exp($O($

er addition law:



ametrized by
$\cos\alpha$. Recall
$\cos(\alpha_1 + \alpha_2)) =$
$\cos\alpha_1 \sin\alpha_2$,
$\sin\alpha_1 \sin\alpha_2$).

Clocks over finite fields



Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Here $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$= \{0, 1, 2, 3, -3, -2, -1\}$
with $+, -, \times$ modulo 7.

Clock($\mathbf{F}_7$) is a gr
under the same a
used for Clock($\mathbf{R}$
$(x_1, y_1) + (x_2, y_2$
$(x_1 y_2 + y_1 x_2, y_1$

Similarly constru
finite group Cloc
for each prime po

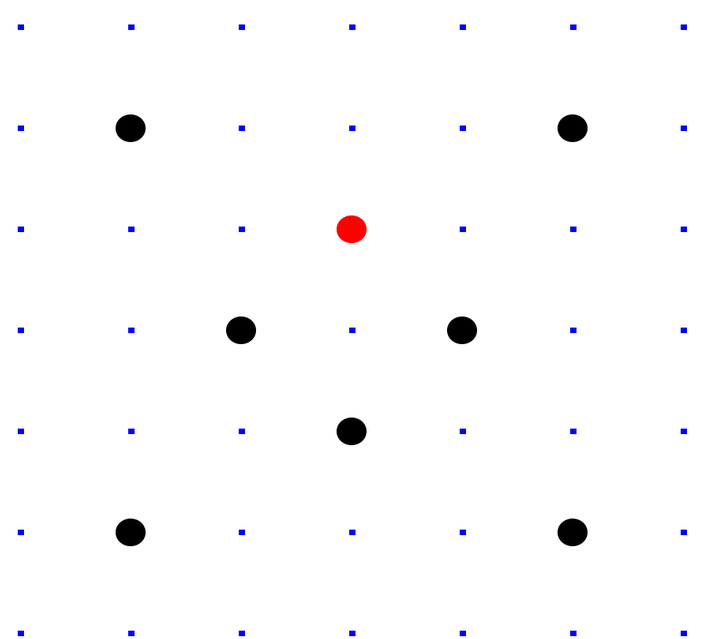
Clock($\mathbf{F}_q$) has $\approx$
"Index-calculus"
discrete logs in C
$\exp(O((\log q)^{1/3}$

law:

$0, 1)$
(x_1, y_1)
$= (x_2, y_2)$
x
$= (x_3, y_3)$

by
ecall
$_2)) =$
$x_2,$
$x_2).$

Clocks over finite fields



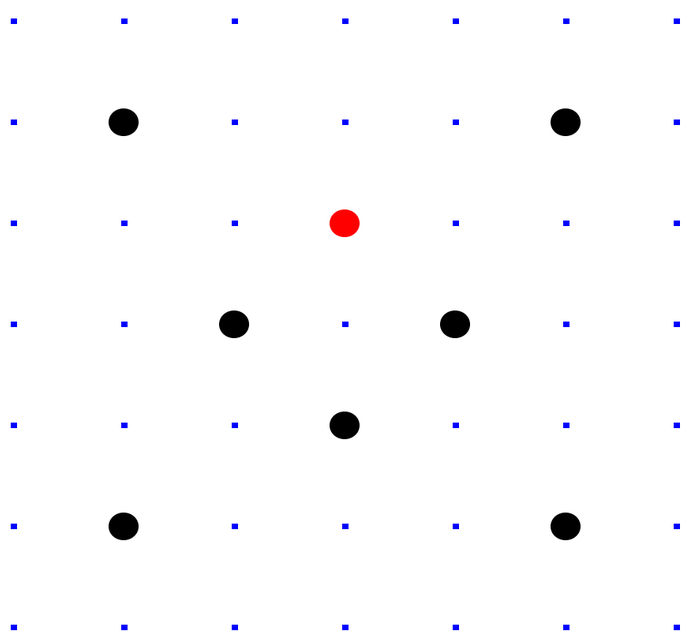
Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Here $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$= \{0, 1, 2, 3, -3, -2, -1\}$
with $+, -, \times$ modulo 7.

Clock($\mathbf{F}_7$) is a group
under the same addition la
used for Clock($\mathbf{R}$):
$(x_1, y_1) + (x_2, y_2) =$
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2$

Similarly construct a
finite group Clock($\mathbf{F}_q$)
for each prime power q.

Clock($\mathbf{F}_q$) has $\approx q$ element
"Index-calculus" attacks fi
discrete logs in Clock($\mathbf{F}_q$) i
$\exp(O((\log q)^{1/3}(\log\log q)^2$

Clocks over finite fields



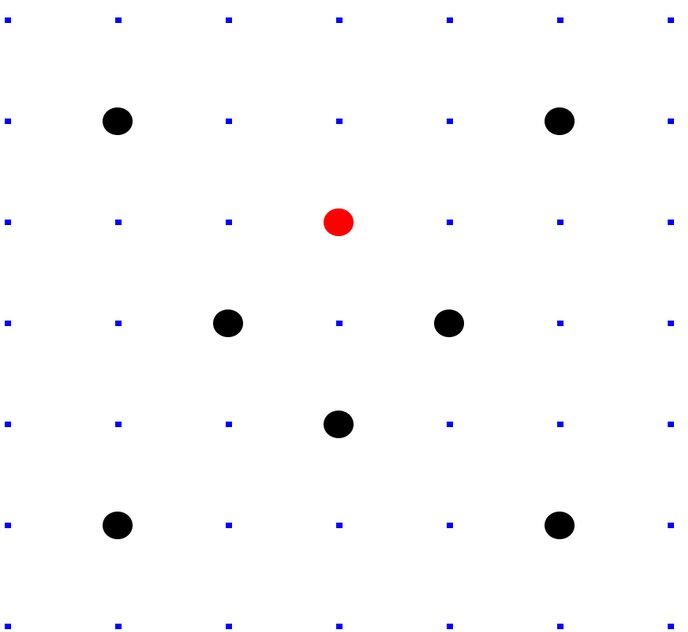
Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Here $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$= \{0, 1, 2, 3, -3, -2, -1\}$
with $+, -, \times$ modulo 7.

Clock($\mathbf{F}_7$) is a group
under the same addition law
used for Clock($\mathbf{R}$):
$(x_1, y_1) + (x_2, y_2) =$
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Similarly construct a
finite group Clock($\mathbf{F}_q$)
for each prime power q.

Clock($\mathbf{F}_q$) has $\approx q$ elements.
"Index-calculus" attacks find
discrete logs in Clock($\mathbf{F}_q$) in time
$\exp(O((\log q)^{1/3}(\log \log q)^{2/3}))$.

over finite fields



$\mathbf{F}_7) =$

$\in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}.$

$_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$, 2, 3, -3, -2, -1\}$

$, -, \times$ modulo 7.

Clock($\mathbf{F}_7$) is a group
under the same addition law
used for Clock($\mathbf{R}$):
$(x_1, y_1) + (x_2, y_2) =$
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Similarly construct a
finite group Clock($\mathbf{F}_q$)
for each prime power q.

Clock($\mathbf{F}_q$) has $\approx q$ elements.
"Index-calculus" attacks find
discrete logs in Clock($\mathbf{F}_q$) in time
$\exp(O((\log q)^{1/3}(\log \log q)^{2/3}))$.

Can us

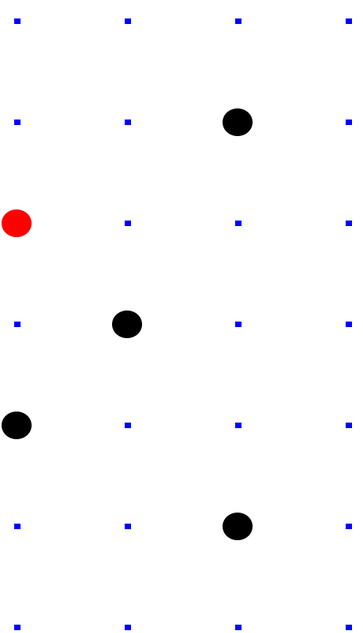
But ne
so neec
so neec

This m

Alterna
indepe
Switch
to an '

As far
index c
against
so can

e fields



$_7 : x^2 + y^2 = 1\}$.
$2, 3, 4, 5, 6\}$
$-2, -1\}$
dulo 7.

Clock($\mathbf{F}_7$) is a group
under the same addition law
used for Clock($\mathbf{R}$):
$(x_1, y_1) + (x_2, y_2) =$
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Similarly construct a
finite group Clock($\mathbf{F}_q$)
for each prime power q.

Clock($\mathbf{F}_q$) has $\approx q$ elements.
"Index-calculus" attacks find
discrete logs in Clock($\mathbf{F}_q$) in time
$\exp(O((\log q)^{1/3}(\log\log q)^{2/3}))$.

Can use Clock($\mathbf{F}$

But need hard di
so need very slow
so need very larg

This makes arith

Alternative (1985
independently 19
Switch from $\mathbf{F}_q^*$,
to an "elliptic cu

As far as we can
index calculus do
against most ellip
so can use much

$^2 = 1\}$.
$6\}$

Clock($\mathbf{F}_7$) is a group
under the same addition law
used for Clock($\mathbf{R}$):
$(x_1, y_1) + (x_2, y_2) =$
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Similarly construct a
finite group Clock($\mathbf{F}_q$)
for each prime power q.

Clock($\mathbf{F}_q$) has $\approx q$ elements.
"Index-calculus" attacks find
discrete logs in Clock($\mathbf{F}_q$) in time
$\exp(O((\log q)^{1/3}(\log\log q)^{2/3}))$.

Can use Clock($\mathbf{F}_q$) for cryp

But need hard discrete logs
so need very slow index cal
so need very large q.

This makes arithmetic slow

Alternative (1985 Miller,
independently 1987 Koblitz
Switch from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$)
to an "elliptic curve."

As far as we can tell,
index calculus doesn't work
against most elliptic curves
so can use much smaller q.

Clock($\mathbf{F}_7$) is a group
under the same addition law
used for Clock($\mathbf{R}$):
$(x_1, y_1) + (x_2, y_2) =$
$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.

Similarly construct a
finite group Clock($\mathbf{F}_q$)
for each prime power q.

Clock($\mathbf{F}_q$) has $\approx q$ elements.
"Index-calculus" attacks find
discrete logs in Clock($\mathbf{F}_q$) in time
$\exp(O((\log q)^{1/3}(\log\log q)^{2/3}))$.

Can use Clock($\mathbf{F}_q$) for crypto.

But need hard discrete logs,
so need very slow index calculus,
so need very large q.

This makes arithmetic slow.

Alternative (1985 Miller,
independently 1987 Koblitz):
Switch from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$), etc.
to an "elliptic curve."

As far as we can tell,
index calculus doesn't work
against most elliptic curves,
so can use much smaller q.

$\mathbf{F}_7$) is a group
the same addition law
or Clock($\mathbf{R}$):
$) + (x_2, y_2) =$
$+ y_1x_2, y_1y_2 - x_1x_2)$.

ly construct a
group Clock($\mathbf{F}_q$)
h prime power q.

$\mathbf{F}_q$) has $\approx q$ elements.
-calculus" attacks find
e logs in Clock($\mathbf{F}_q$) in time
$(\log q)^{1/3}(\log\log q)^{2/3}))$.

Can use Clock($\mathbf{F}_q$) for crypto.

But need hard discrete logs,
so need very slow index calculus,
so need very large q.

This makes arithmetic slow.

Alternative (1985 Miller,
independently 1987 Koblitz):
Switch from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$), etc.
to an "elliptic curve."

As far as we can tell,
index calculus doesn't work
against most elliptic curves,
so can use much smaller q.

Additio

$x^2 + y$
Sum of
$((x_1y_2$
$(y_1y_2$

roup
addition law
):
$_2) =$
$y_2 - x_1x_2)$.

ct a
k($\mathbf{F}_q$)
ower q.

q elements.
attacks find
Clock($\mathbf{F}_q$) in time
$(\log\log q)^{2/3}))$.

Can use Clock($\mathbf{F}_q$) for crypto.

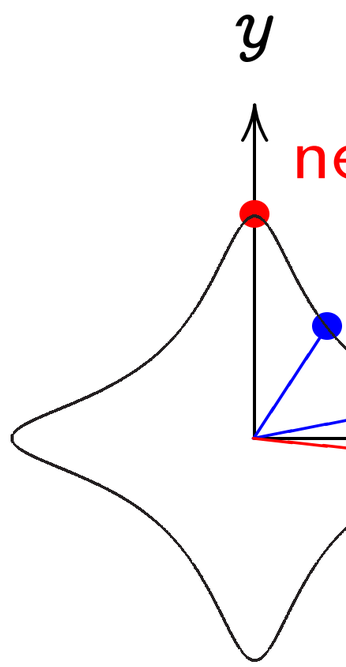
But need hard discrete logs,
so need very slow index calculus,
so need very large q.

This makes arithmetic slow.

Alternative (1985 Miller,
independently 1987 Koblitz):
Switch from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$), etc.
to an "elliptic curve."

As far as we can tell,
index calculus doesn't work
against most elliptic curves,
so can use much smaller q.

Addition on an E



$x^2 + y^2 = 1 - 30$
Sum of (x_1, y_1) a
$((x_1y_2+y_1x_2)/(1$
$(y_1y_2-x_1x_2)/(1$

w

).

ts.

nd

in time

$^{2/3}$)).

Can use Clock($\mathbf{F}_q$) for crypto.

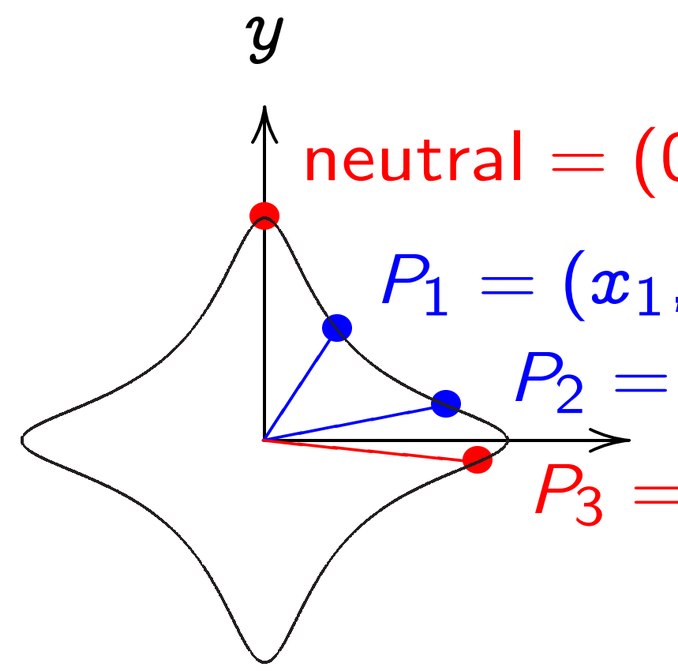
But need hard discrete logs,
so need very slow index calculus,
so need very large q.

This makes arithmetic slow.

Alternative (1985 Miller,
independently 1987 Koblitz):
Switch from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$), etc.
to an "elliptic curve."

As far as we can tell,
index calculus doesn't work
against most elliptic curves,
so can use much smaller q.

Addition on an Edwards cu



$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and $(x_2, y$

$((x_1y_2+y_1x_2)/(1-30x_1x_2$

$(y_1y_2-x_1x_2)/(1+30x_1x_2$

Can use Clock($\mathbf{F}_q$) for crypto.

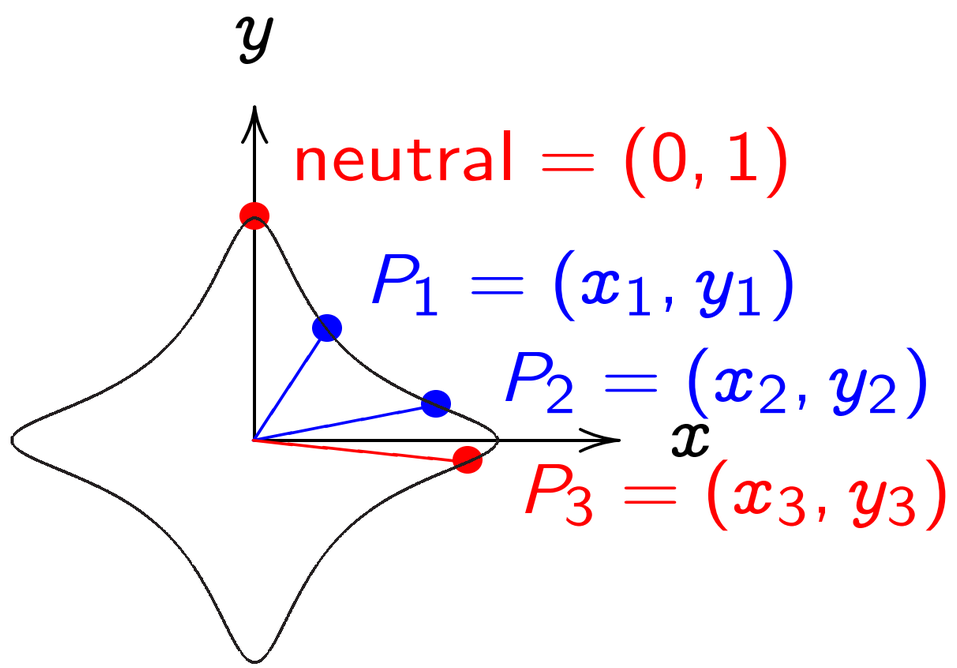
But need hard discrete logs,
so need very slow index calculus,
so need very large q.

This makes arithmetic slow.

Alternative (1985 Miller,
independently 1987 Koblitz):
Switch from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$), etc.
to an "elliptic curve."

As far as we can tell,
index calculus doesn't work
against most elliptic curves,
so can use much smaller q.

Addition on an Edwards curve



$x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2)$,
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

e Clock($\mathbf{F}_q$) for crypto.

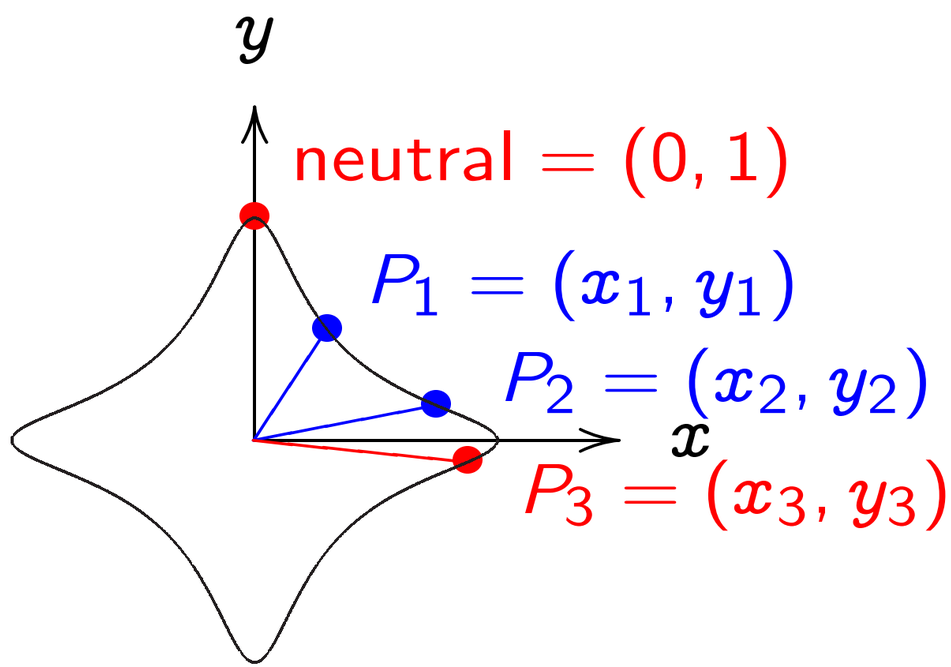
ed hard discrete logs,
d very slow index calculus,
d very large q.

akes arithmetic slow.

ative (1985 Miller,
ndently 1987 Koblitz):
from $\mathbf{F}_q^*$, Clock($\mathbf{F}_q$), etc.
"elliptic curve."

as we can tell,
calculus doesn't work
most elliptic curves,
use much smaller q.

Addition on an Edwards curve



$x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2)$,
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The cl

$x^2 + y$
Sum of
$(x_1y_2 +$
$y_1y_2 +$

$_q$) for crypto.

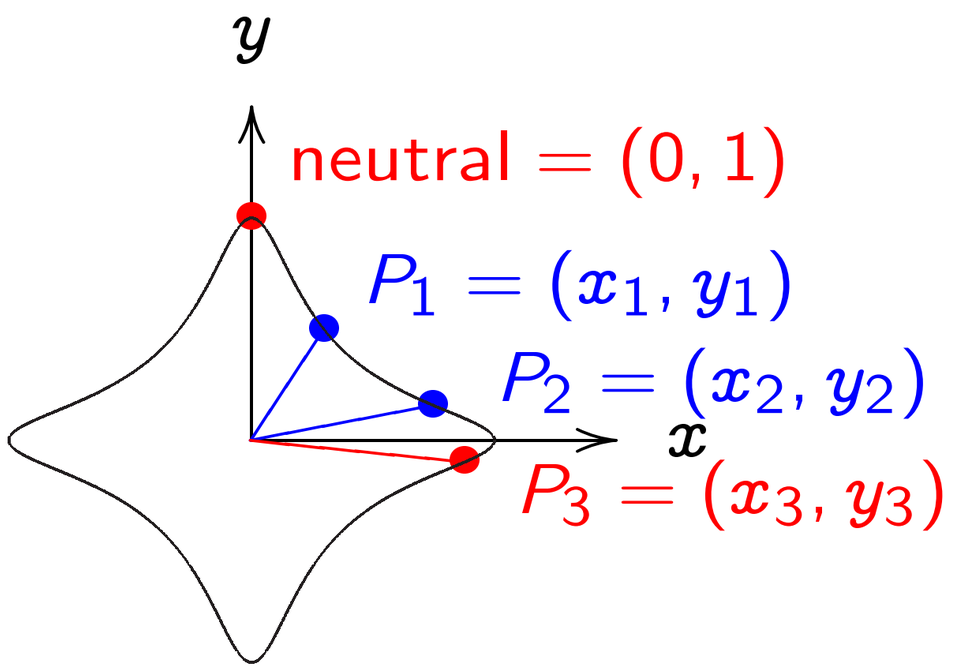
screte logs,
v index calculus,
e q.

metic slow.

5 Miller,
087 Koblitz):
Clock($\mathbf{F}_q$), etc.
rve."

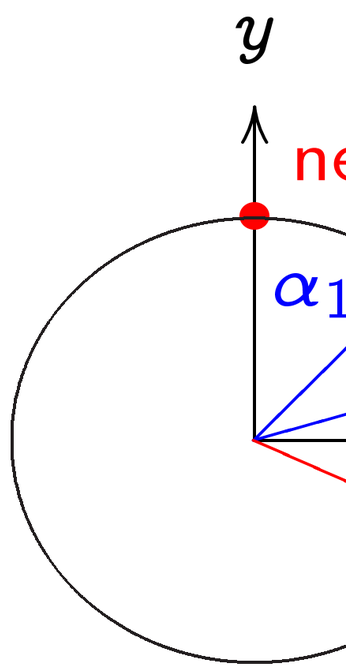
tell,
oesn't work
otic curves,
smaller q.

Addition on an Edwards curve



$x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2)$,
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again,



$x^2 + y^2 = 1$.
Sum of (x_1, y_1) a
$(x_1y_2 + y_1x_2,$
$y_1y_2 - x_1x_2)$.

pto.

s,

lculus,

v.

z):

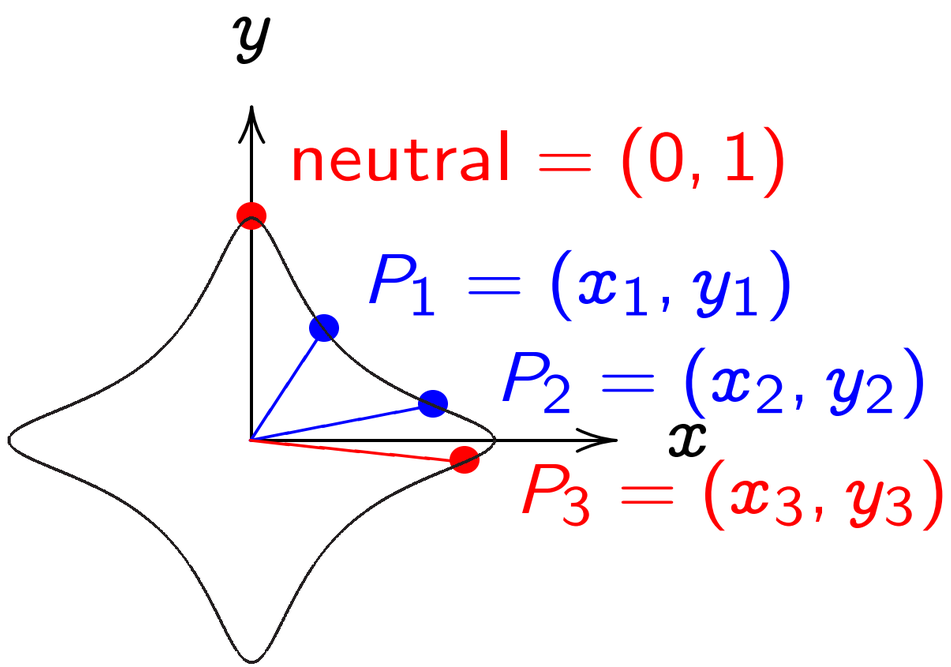
, etc.

k

s,

.

Addition on an Edwards curve



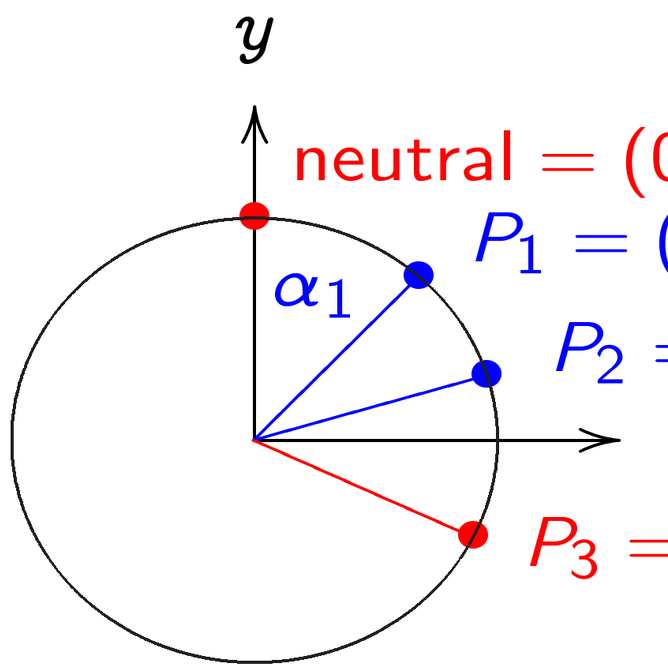
$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2)$,

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, for compa



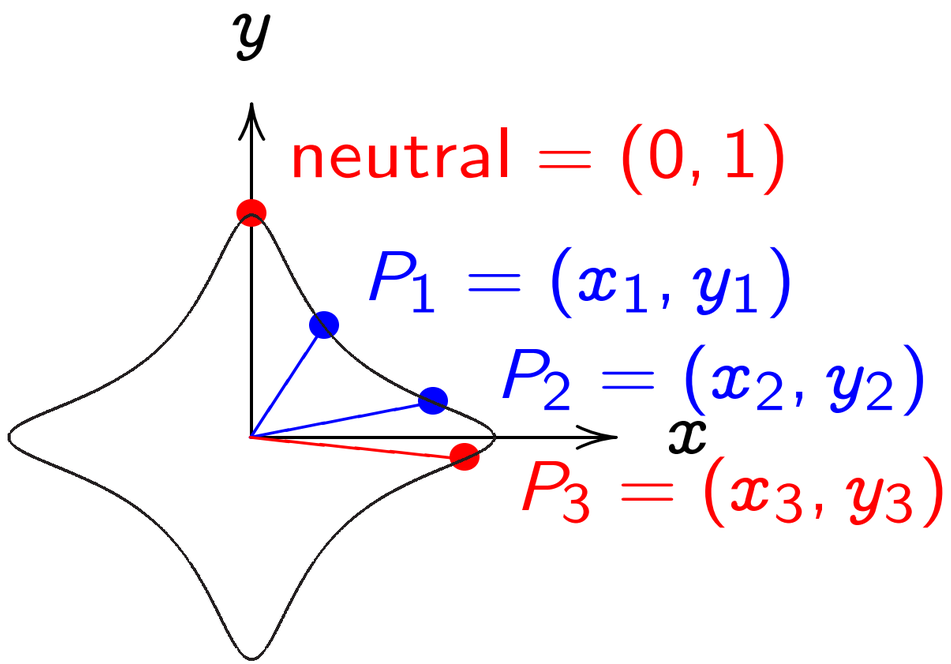
$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and $(x_2, y$

$(x_1y_2 + y_1x_2$,

$y_1y_2 - x_1x_2)$.

Addition on an Edwards curve



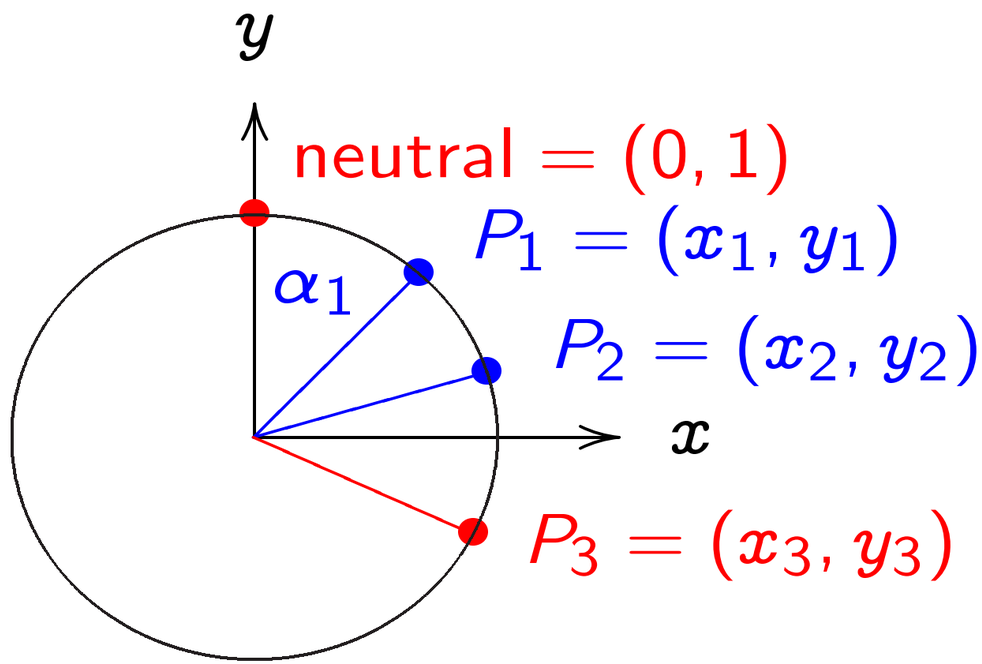
$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2)$,

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, for comparison:



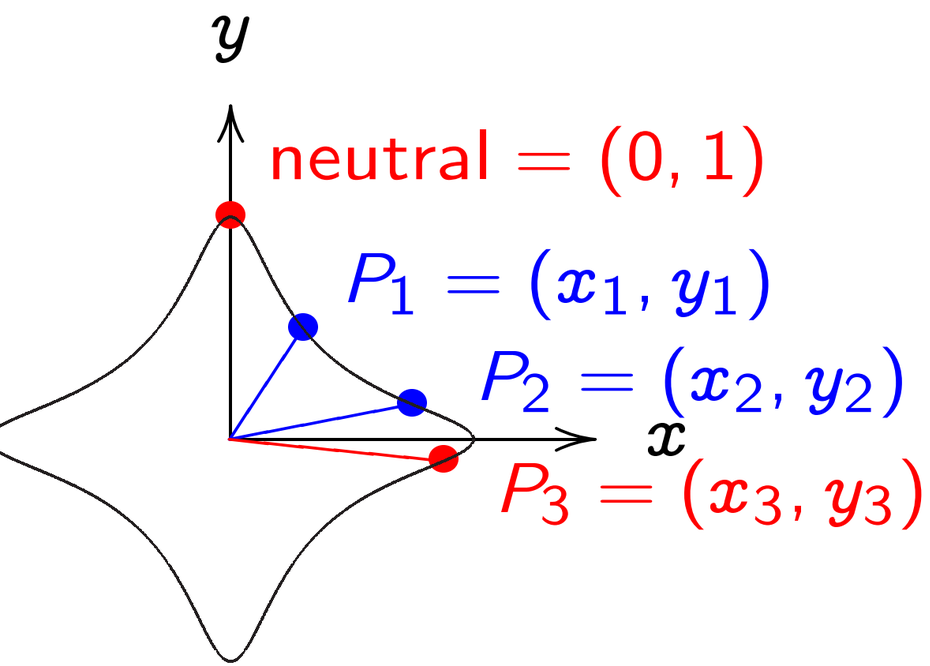
$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

on on an Edwards curve



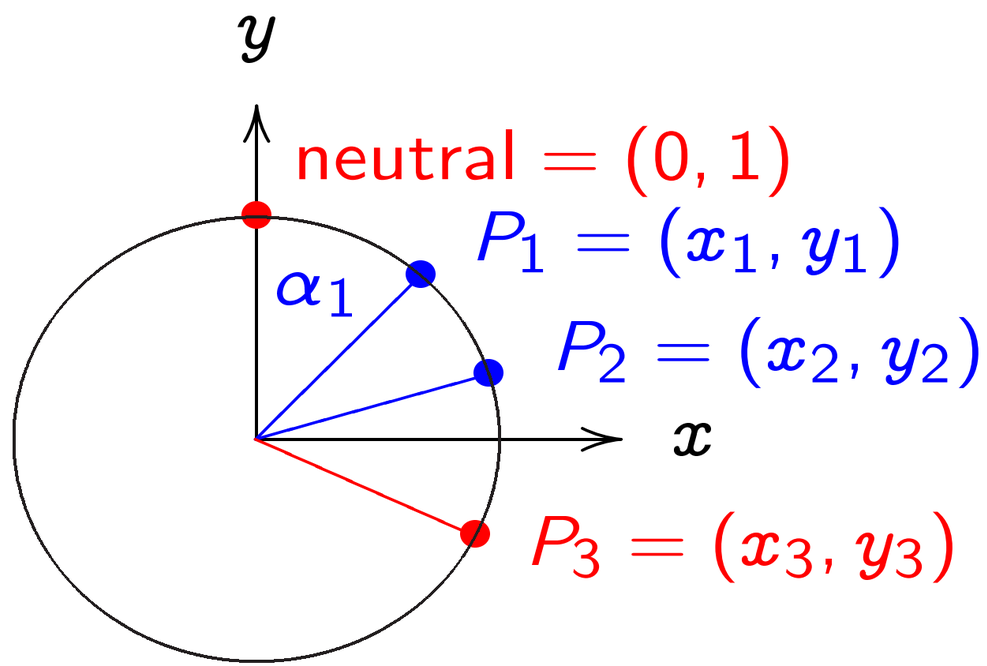
$^2 = 1 - 30x^2y^2$.

f (x_1, y_1) and (x_2, y_2) is

$+y_1x_2)/(1-30x_1x_2y_1y_2)$,

$-x_1x_2)/(1+30x_1x_2y_1y_2)$).

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

"Hey, t

in the

What i

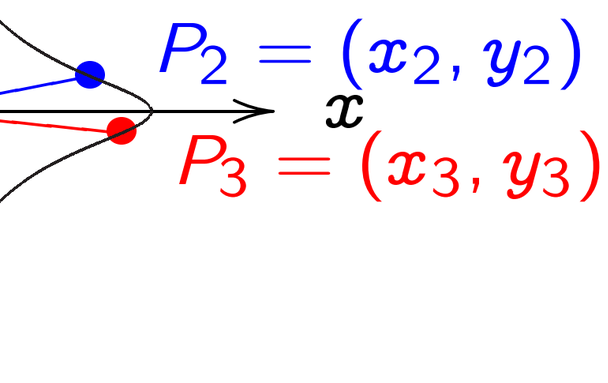
Answer

If $x^2 +$

then 30

so $\sqrt{30}$

Edwards curve



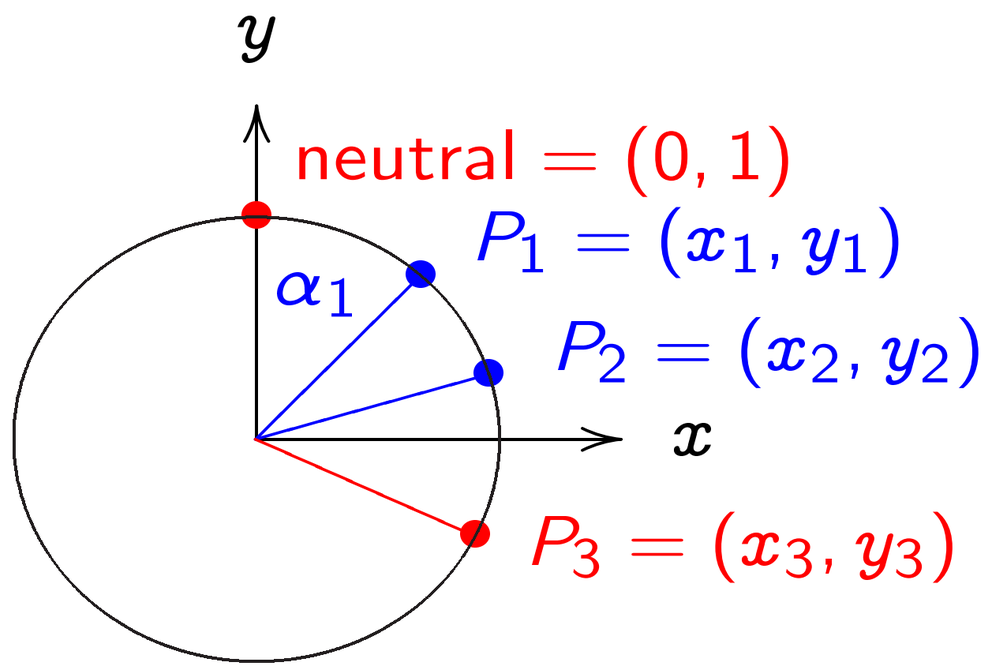
$0x^2y^2$.

and (x_2, y_2) is

$1-30x_1x_2y_1y_2)$,

$1+30x_1x_2y_1y_2)$).

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

"Hey, there were

in the Edwards a

What if the denc

Answer: They ar

If $x^2 + y^2 = 1 -$

then $30x^2y^2 < 1$

so $\sqrt{30}\ |xy| < 1$.

urve

$0, 1)$

$, y_1)$

(x_2, y_2)

x

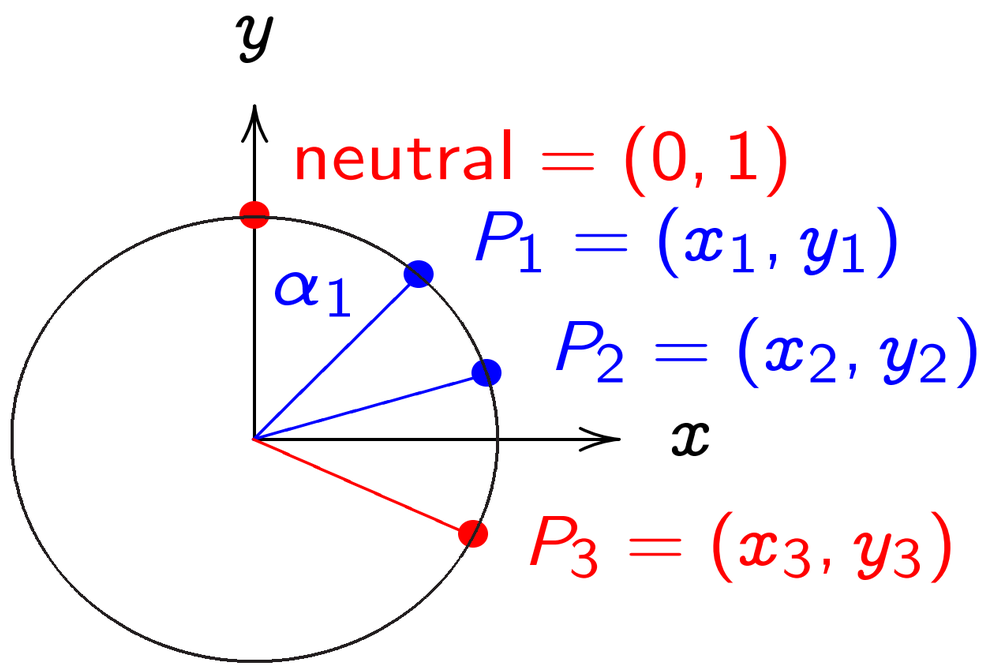
$= (x_3, y_3)$

$_2)$ is

$y_1y_2)$,

$y_1y_2))$.

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

"Hey, there were divisions

in the Edwards addition lav

What if the denominators

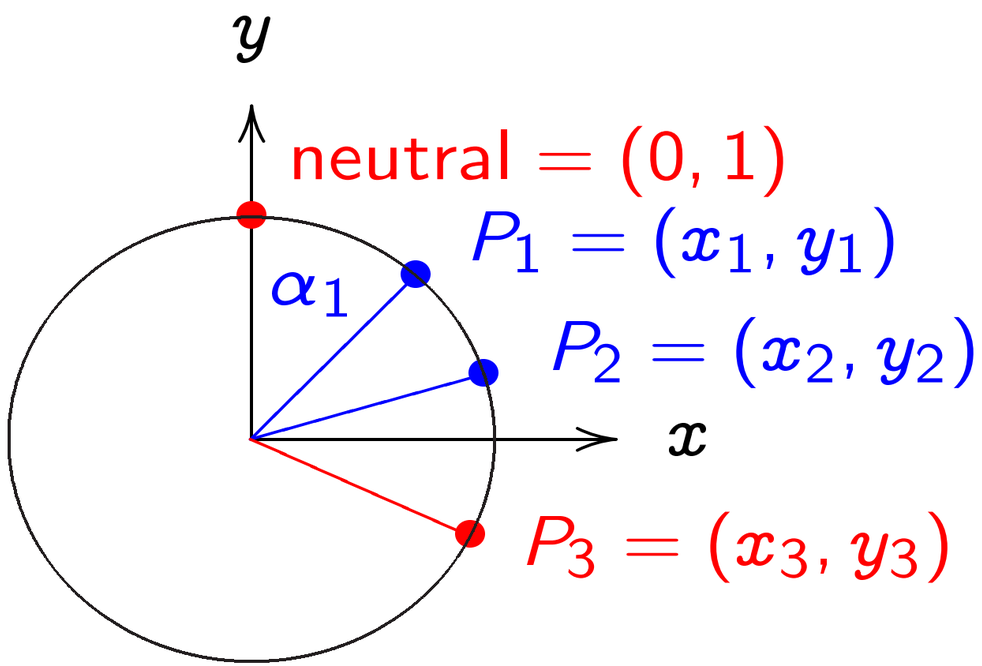
Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$

then $30x^2y^2 < 1$

so $\sqrt{30}\ |xy| < 1$.

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

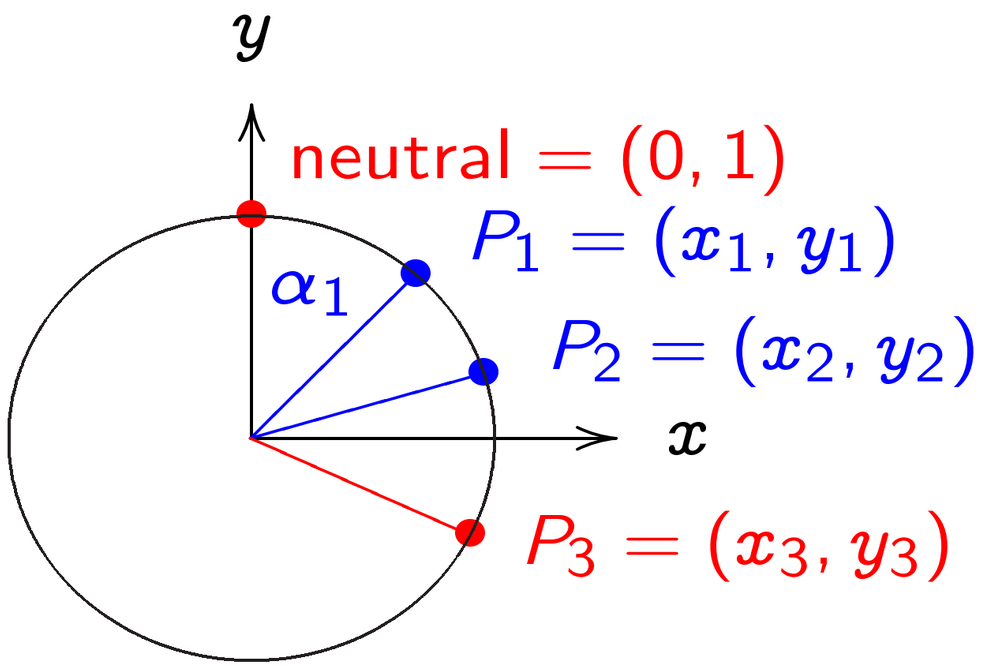
$y_1y_2 - x_1x_2)$.

"Hey, there were divisions in the Edwards addition law! What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$ then $30x^2y^2 < 1$ so $\sqrt{30}\ |xy| < 1$.

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

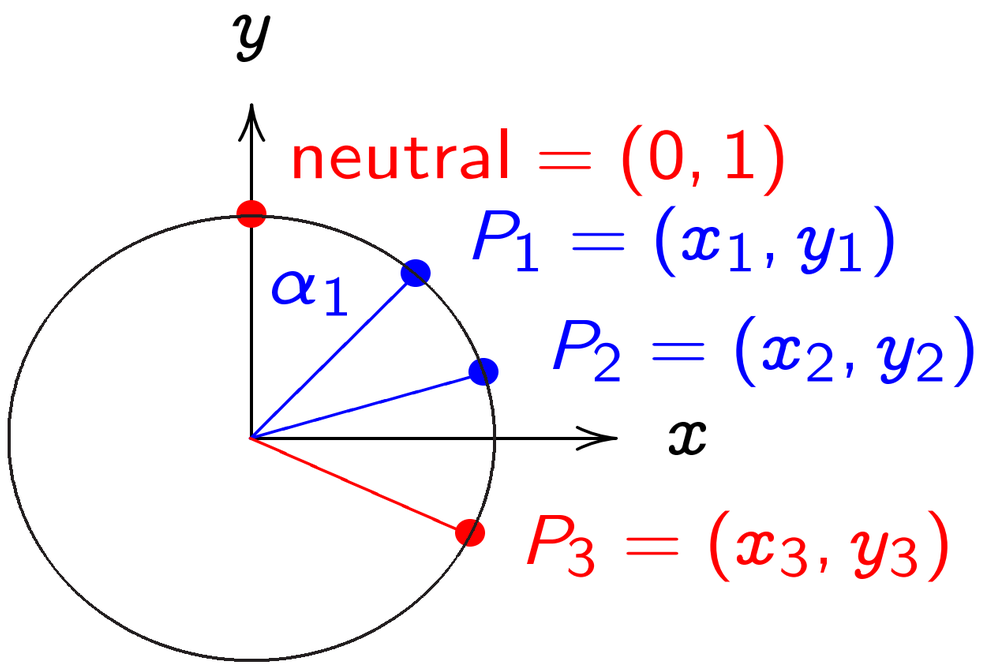
"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

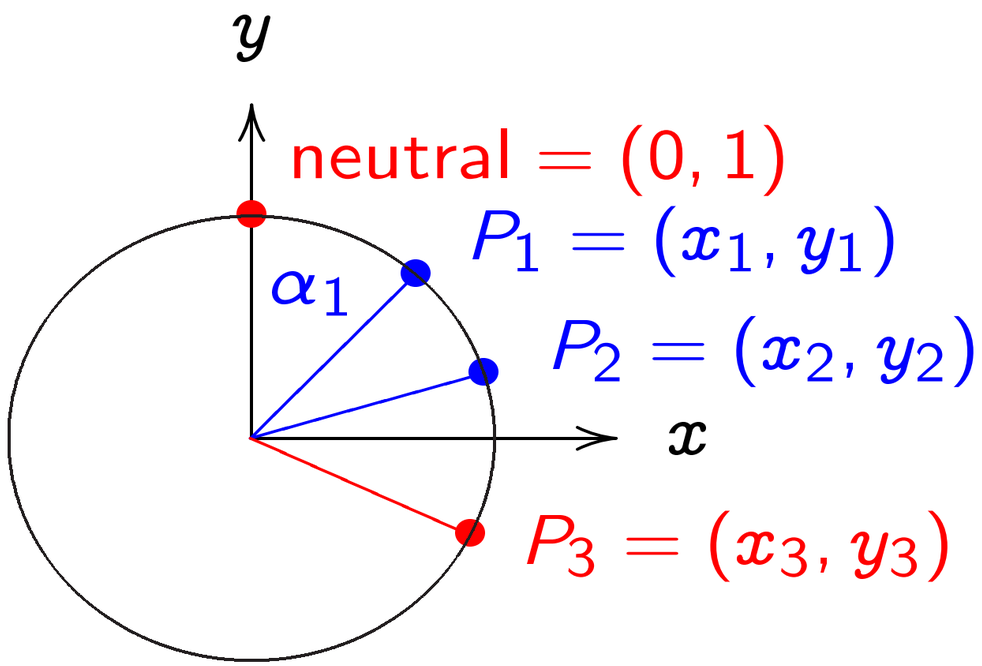
"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$
so $30\,|x_1y_1x_2y_2| < 1$

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

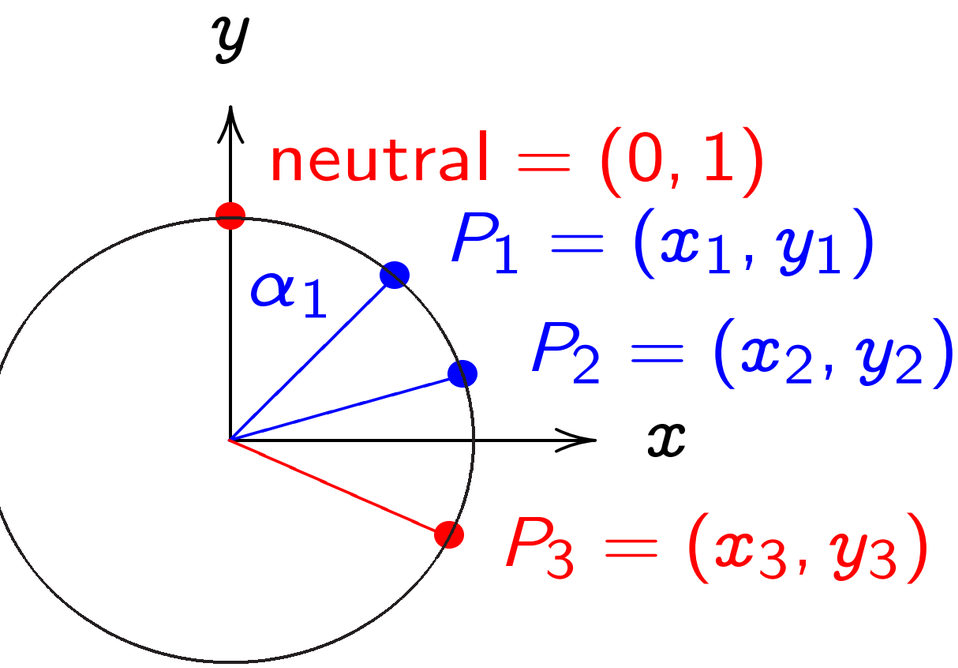
"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$
so $30\,|x_1y_1x_2y_2| < 1$
so $1 \pm 30x_1x_2y_1y_2 > 0$.

ock again, for comparison:



$^2 = 1$.

f (x_1, y_1) and (x_2, y_2) is

$+ y_1x_2$,

$- x_1x_2)$.

"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

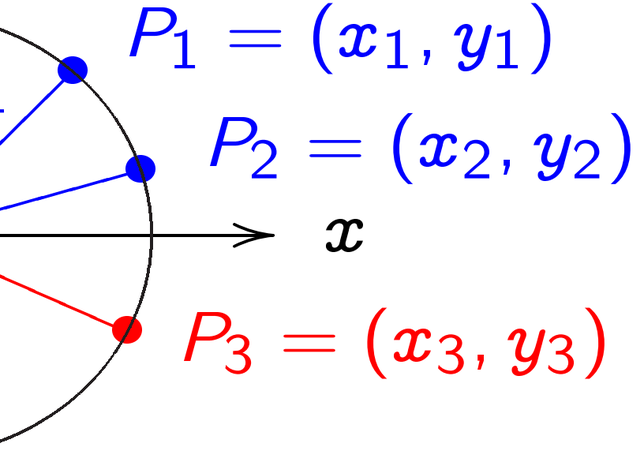
If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$
so $30\,|x_1y_1x_2y_2| < 1$
so $1 \pm 30x_1x_2y_1y_2 > 0$.

The Ed
$(x_1, y_1$
$((x_1y_2$
$(y_1y_2$
is a gro
$x^2 + y$

Some o
additio
additio

Other
additio
$(0, 1)$ i
$(x_1, y_1$

for comparison:



and (x_2, y_2) is

"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$
so $30\,|x_1y_1x_2y_2| < 1$
so $1 \pm 30x_1x_2y_1y_2 > 0$.

The Edwards ad
$(x_1, y_1) + (x_2, y_2$
$((x_1y_2+y_1x_2)/(1$
$(y_1y_2-x_1x_2)/(1$
is a group law fo
$x^2 + y^2 = 1 - 30$

Some calculation
addition result is
addition law is as

Other parts of pr
addition law is co
$(0, 1)$ is neutral e
$(x_1, y_1) + (-x_1,$

arison:

$0, 1)$
(x_1, y_1)
$= (x_2, y_2)$
x
$= (x_3, y_3)$

$_2)$ is

"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$
so $30\,|x_1y_1x_2y_2| < 1$
so $1 \pm 30x_1x_2y_1y_2 > 0$.

The Edwards addition law
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2+y_1x_2)/(1-30x_1x_2$
$(y_1y_2-x_1x_2)/(1+30x_1x_2$
is a group law for the curv
$x^2 + y^2 = 1 - 30x^2y^2$.

Some calculation required:
addition result is on curve;
addition law is associative.

Other parts of proof are ea
addition law is commutativ
$(0, 1)$ is neutral element;
$(x_1, y_1) + (-x_1, y_1) = (0,$

"Hey, there were divisions
in the Edwards addition law!
What if the denominators are 0?"

Answer: They aren't!

If $x^2 + y^2 = 1 - 30x^2y^2$
then $30x^2y^2 < 1$
so $\sqrt{30}\ |xy| < 1$.

If $x_1^2 + y_1^2 = 1 - 30x_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 - 30x_2^2y_2^2$
then $\sqrt{30}\ |x_1y_1| < 1$
and $\sqrt{30}\ |x_2y_2| < 1$
so $30\,|x_1y_1x_2y_2| < 1$
so $1 \pm 30x_1x_2y_1y_2 > 0$.

The Edwards addition law
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$
is a group law for the curve
$x^2 + y^2 = 1 - 30x^2y^2$.

Some calculation required:
addition result is on curve;
addition law is associative.

Other parts of proof are easy:
addition law is commutative;
$(0, 1)$ is neutral element;
$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

there were divisions
Edwards addition law!
f the denominators are 0?"

r: They aren't!

$y^2 = 1 - 30x^2y^2$
$0x^2y^2 < 1$
$\overline{0}\ |xy| < 1.$

$y_1^2 = 1 - 30x_1^2y_1^2$
$+ y_2^2 = 1 - 30x_2^2y_2^2$
$\sqrt{30}\ |x_1y_1| < 1$
$\overline{30}\ |x_2y_2| < 1$
$x_1y_1x_2y_2| < 1$
$30x_1x_2y_1y_2 > 0.$

The Edwards addition law
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$
is a group law for the curve
$x^2 + y^2 = 1 - 30x^2y^2$.

Some calculation required:
addition result is on curve;
addition law is associative.

Other parts of proof are easy:
addition law is commutative;
$(0, 1)$ is neutral element;
$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

<u>More E</u>

Fix an
Fix a n

$\{(x, y)$
x^2

is a co
$(x_1, y_1$
defined

$x_3 = \frac{}{1}$

$y_3 = \frac{}{1}$

divisions
ddition law!
ominators are 0?"

en't!

$30x^2y^2$

$30x_1^2y_1^2$
$- 30x_2^2y_2^2$
< 1
< 1
< 1
$y_2 > 0.$

The Edwards addition law
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$
is a group law for the curve
$x^2 + y^2 = 1 - 30x^2y^2$.

Some calculation required:
addition result is on curve;
addition law is associative.

Other parts of proof are easy:
addition law is commutative;
$(0, 1)$ is neutral element;
$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

More Edwards cu

Fix an odd prime
Fix a non-square

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}$
$x^2 + y^2 = 1$

is a commutative
$(x_1, y_1) + (x_2, y_2$
defined by Edwar

$$x_3 = \frac{x_1y_2 + y_1}{1 + dx_1x_2y}$$

$$y_3 = \frac{y_1y_2 - x_1}{1 - dx_1x_2y}$$

w!

are 0?"

The Edwards addition law
$(x_1, y_1) + (x_2, y_2) =$
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$
is a group law for the curve
$x^2 + y^2 = 1 - 30x^2y^2$.

Some calculation required:
addition result is on curve;
addition law is associative.

Other parts of proof are easy:
addition law is commutative;
$(0, 1)$ is neutral element;
$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

More Edwards curves

Fix an odd prime power q.
Fix a non-square $d \in \mathbf{F}_q$.

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$x^2 + y^2 = 1 + dx^2y^2\}$

is a commutative group wi
$(x_1, y_1) + (x_2, y_2) = (x_3, y$
defined by Edwards additio

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

The Edwards addition law

$(x_1, y_1) + (x_2, y_2) =$

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$

is a group law for the curve

$x^2 + y^2 = 1 - 30x^2y^2$.

Some calculation required:

addition result is on curve;

addition law is associative.

Other parts of proof are easy:

addition law is commutative;

$(0, 1)$ is neutral element;

$(x_1, y_1) + (-x_1, y_1) = (0, 1)$.

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$

$x^2 + y^2 = 1 + dx^2y^2\}$

is a commutative group with

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

defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

dwards addition law

$) + (x_2, y_2) =$

$+y_1x_2)/(1-30x_1x_2y_1y_2),$

$-x_1x_2)/(1+30x_1x_2y_1y_2))$

oup law for the curve

$^2 = 1 - 30x^2y^2$.

calculation required:

n result is on curve;

n law is associative.

parts of proof are easy:

n law is commutative;

s neutral element;

$) + (-x_1, y_1) = (0, 1)$.

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$x^2 + y^2 = 1 + dx^2y^2\}$

is a commutative group with

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

defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denom

But ne

"$x^2 +$

dition law

$_2) =$

$1-30x_1x_2y_1y_2),$

$1+30x_1x_2y_1y_2))$

r the curve

$0x^2y^2.$

required:

on curve;

ssociative.

roof are easy:

ommutative;

element;

$y_1) = (0, 1).$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with

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

defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators ar

But need differen

"$x^2 + y^2 > 0$" d

$y_1y_2)$,
$y_1y_2))$
e

sy:
ve;

1).

More Edwards curves

Fix an odd prime power q.
Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x,y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with
$(x_1,y_1) + (x_2,y_2) = (x_3,y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't wor

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$x^2 + y^2 = 1 + dx^2y^2\}$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$x^2 + y^2 = 1 + dx^2y^2\}$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$

More Edwards curves

Fix an odd prime power q.

Fix a non-square $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Edwards curves

odd prime power q.

on-square $d \in \mathbf{F}_q$.

$\in \mathbf{F}_q \times \mathbf{F}_q$:

$^2 + y^2 = 1 + dx^2y^2\}$

mmutative group with

$) + (x_2, y_2) = (x_3, y_3)$

l by Edwards addition law:

$$\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$\frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Denominators are never 0.

But need different proof;

"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Case 1

$d =$ (

contrad

urves

e power q.
$d \in \mathbf{F}_q$.

$_q$:
$+ dx^2y^2\}$

e group with
$_2) = (x_3, y_3)$
rds addition law:

$\frac{x_2}{y_1y_2}$,

$\frac{x_2}{y_1y_2}$.

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Case 1: $x_2 + y_2$

$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + \right.$

contradiction.

th

$y_3)$

on law:

Denominators are never 0.

But need different proof;

"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + y_2)} \right)^2,$$

contradiction.

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + y_2)} \right)^2,$$

contradiction.

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + y_2)}\right)^2,$$

contradiction.

Case 2: $x_2 - y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \mp y_1}{x_1y_1(x_2 - y_2)}\right)^2,$$

contradiction.

Denominators are never 0.

But need different proof;
"$x^2 + y^2 > 0$" doesn't work.

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
and $dx_1x_2y_1y_2 = \pm 1$
then $dx_1^2y_1^2(x_2 + y_2)^2$
$= dx_1^2y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$
$= dx_1^2y_1^2(dx_2^2y_2^2 + 1 + 2x_2y_2)$
$= d^2x_1^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$
$= 1 + dx_1^2y_1^2 \pm 2x_1y_1$
$= x_1^2 + y_1^2 \pm 2x_1y_1$
$= (x_1 \pm y_1)^2$.

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + y_2)}\right)^2,$$

contradiction.

Case 2: $x_2 - y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \mp y_1}{x_1y_1(x_2 - y_2)}\right)^2,$$

contradiction.

Case 3: $x_2 + y_2 = x_2 - y_2 = 0$.
Then $x_2 = 0$ and $y_2 = 0$,
contradiction.

inators are never 0.

ed different proof;

$y^2 > 0$" doesn't work.

$$y_1^2 = 1 + dx_1^2y_1^2$$
$$+ y_2^2 = 1 + dx_2^2y_2^2$$
$$_1x_2y_1y_2 = \pm 1$$
$$x_1^2y_1^2(x_2 + y_2)^2$$
$$y_1^2(x_2^2 + y_2^2 + 2x_2y_2)$$
$$^2y_1^2x_2^2y_2^2 + dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$$
$$dx_1^2y_1^2 \pm 2x_1y_1$$
$$+ y_1^2 \pm 2x_1y_1$$
$$\pm y_1)^2.$$

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + y_2)}\right)^2,$$

contradiction.

Case 2: $x_2 - y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \mp y_1}{x_1y_1(x_2 - y_2)}\right)^2,$$

contradiction.

Case 3: $x_2 + y_2 = x_2 - y_2 = 0$.
Then $x_2 = 0$ and $y_2 = 0$,
contradiction.

This is
(techni

Can us

. . . if i
Need t
If no la
must s
this ve

Also ch
"embe

Safe ex
$q = 2^{25}$

e never 0.

nt proof;

oesn't work.

$dx_1^2y_1^2$

$+ dx_2^2y_2^2$

$= \pm 1$

$+ y_2)^2$

$^2 + 2x_2y_2)$

$+ 1 + 2x_2y_2)$

$dx_1^2y_1^2 + 2dx_1^2y_1^2x_2y_2$

x_1y_1

y_1

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1y_1(x_2 + y_2)}\right)^2,$$

contradiction.

Case 2: $x_2 - y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \mp y_1}{x_1y_1(x_2 - y_2)}\right)^2,$$

contradiction.

Case 3: $x_2 + y_2 = x_2 - y_2 = 0$. Then $x_2 = 0$ and $y_2 = 0$, contradiction.

This is an elliptic

(technically, "mo

Can use this grou

... if it's a "stro

Need to compute

If no large prime

must switch to a

this very often ha

Also check "twist

"embedding degr

Safe example, "C

$q = 2^{255} - 19$; d

rk.

)

$y_2)$

$2x_1^2y_1^2x_2y_2$

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1 y_1 (x_2 + y_2)}\right)^2,$$

contradiction.

Case 2: $x_2 - y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \mp y_1}{x_1 y_1 (x_2 - y_2)}\right)^2,$$

contradiction.

Case 3: $x_2 + y_2 = x_2 - y_2 = 0$. Then $x_2 = 0$ and $y_2 = 0$, contradiction.

This is an elliptic curve (technically, "mod blowups

Can use this group in crypt

. . . if it's a "strong" curve Need to compute group or If no large prime factor in must switch to another d; this very often happens.

Also check "twist security," "embedding degree," et al.

Safe example, "Curve2551 $q = 2^{255} - 19$; $d = 1 - 1/$

Case 1: $x_2 + y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \pm y_1}{x_1 y_1 (x_2 + y_2)} \right)^2,$$

contradiction.

Case 2: $x_2 - y_2 \neq 0$. Then

$$d = \left(\frac{x_1 \mp y_1}{x_1 y_1 (x_2 - y_2)} \right)^2,$$

contradiction.

Case 3: $x_2 + y_2 = x_2 - y_2 = 0$.
Then $x_2 = 0$ and $y_2 = 0$,
contradiction.

This is an elliptic curve
(technically, "mod blowups").

Can use this group in crypto.

. . . if it's a "strong" curve.
Need to compute group order.
If no large prime factor in order,
must switch to another d;
this very often happens.

Also check "twist security,"
"embedding degree," et al.

Safe example, "Curve25519":
$q = 2^{255} - 19$; $d = 1 - 1/121666$.

: $x_2 + y_2 \neq 0$. Then

$$\left(\frac{x_1 \pm y_1}{x_1 y_1 (x_2 + y_2)}\right)^2,$$

diction.

: $x_2 - y_2 \neq 0$. Then

$$\left(\frac{x_1 \mp y_1}{x_1 y_1 (x_2 - y_2)}\right)^2,$$

diction.

: $x_2 + y_2 = x_2 - y_2 = 0$.
$x_2 = 0$ and $y_2 = 0$,
diction.

This is an elliptic curve
(technically, "mod blowups").

Can use this group in crypto.

... if it's a "strong" curve.
Need to compute group order.
If no large prime factor in order,
must switch to another d;
this very often happens.

Also check "twist security,"
"embedding degree," et al.

Safe example, "Curve25519":
$q = 2^{255} - 19$; $d = 1 - 1/121666$.

Histori

1761 E
introdu
for x^2 -
the "le

2007 E
many c
Theore
all ellip

2007 B
Edward
for x^2 -
and giv

$\neq 0$. Then

$$\left(\frac{1}{y_2}\right)^2,$$

$\neq 0$. Then

$$\left(\frac{1}{y_2}\right)^2,$$

$= x_2 - y_2 = 0.$

d $y_2 = 0,$

This is an elliptic curve (technically, "mod blowups").

Can use this group in crypto.

. . . if it's a "strong" curve.
Need to compute group order.
If no large prime factor in order, must switch to another d; this very often happens.

Also check "twist security," "embedding degree," et al.

Safe example, "Curve25519": $q = 2^{255} - 19$; $d = 1 - 1/121666$.

Historical notes:

1761 Euler, 1866
introduced an ad
for $x^2 + y^2 = 1$
the "lemniscatic

2007 Edwards ge
many curves $x^2 +$
Theorem: have n
all elliptic curves

2007 Bernstein–L
Edwards addition
for $x^2 + y^2 = 1$
and gives new EC

n

n

$^2 = 0.$

This is an elliptic curve
(technically, "mod blowups").

Can use this group in crypto.

. . . if it's a "strong" curve.
Need to compute group order.
If no large prime factor in order,
must switch to another d;
this very often happens.

Also check "twist security,"
"embedding degree," et al.

Safe example, "Curve25519":
$q = 2^{255} - 19$; $d = 1 - 1/121666$.

Historical notes:

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic cu

2007 Edwards generalized
many curves $x^2+y^2 = 1+$
Theorem: have now obtain
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is co
for $x^2 + y^2 = 1 + dx^2y^2$ if
and gives new ECC speed

This is an elliptic curve
(technically, "mod blowups").

Can use this group in crypto.

... if it's a "strong" curve.
Need to compute group order.
If no large prime factor in order,
must switch to another d;
this very often happens.

Also check "twist security,"
"embedding degree," et al.

Safe example, "Curve25519":
$q = 2^{255} - 19$; $d = 1 - 1/121666$.

Historical notes:

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curve."

2007 Edwards generalized to
many curves $x^2+y^2 = 1+c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \square$;
and gives new ECC speed records!

an elliptic curve
cally, "mod blowups").

e this group in crypto.

t's a "strong" curve.
o compute group order.
rge prime factor in order,
witch to another d;
ry often happens.

neck "twist security,"
dding degree," et al.

kample, "Curve25519":
$^{55} - 19$; $d = 1 - 1/121666$.

Historical notes:

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curve."

2007 Edwards generalized to
many curves $x^2+y^2 = 1+c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \square$;
and gives new ECC speed records!

(pictur

c curve
od blowups").

up in crypto.

ng" curve.
e group order.
factor in order,
nother d;
appens.

t security,"
ree," et al.

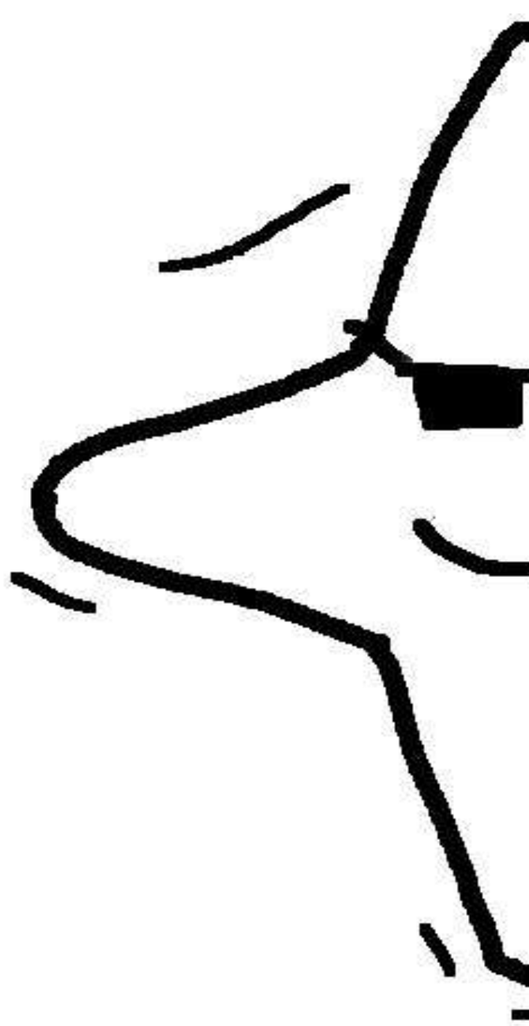
Curve25519":
$= 1 - 1/121666$.

Historical notes:

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curve."

2007 Edwards generalized to
many curves $x^2+y^2 = 1+c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \square$;
and gives new ECC speed records!



(picture courtesy

s").

to.

.

der.

order,

,

.

9":

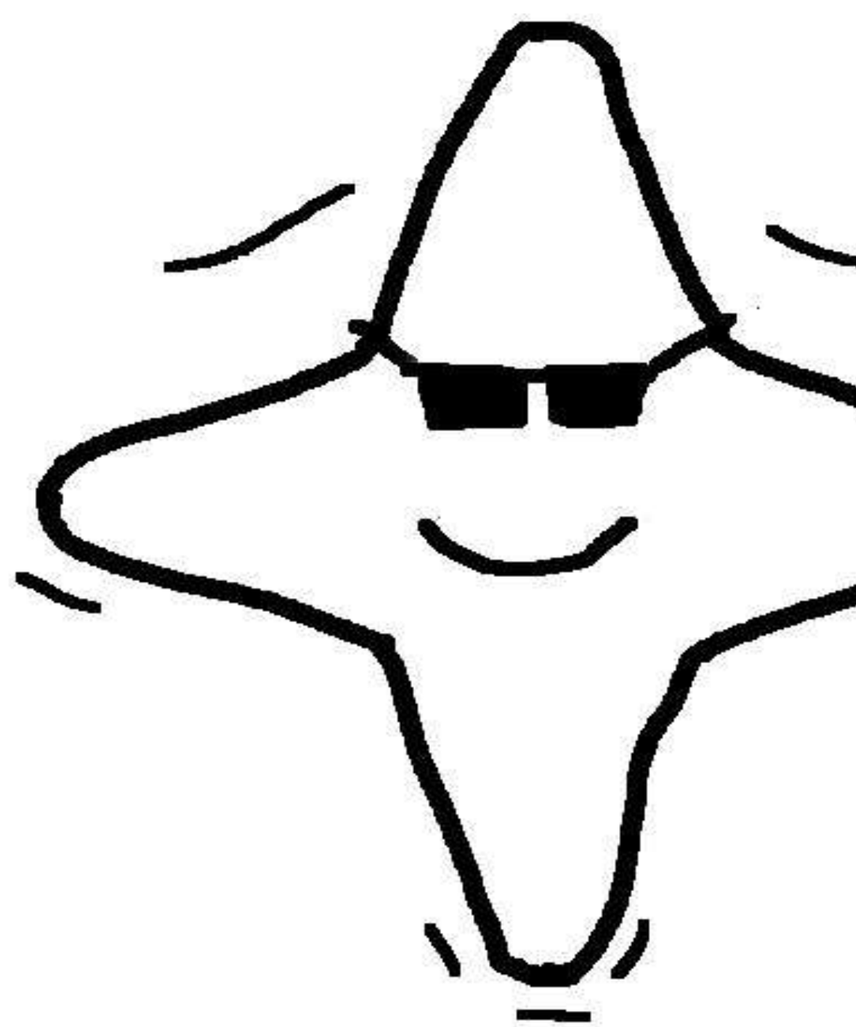
121666.

Historical notes:

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curve."

2007 Edwards generalized to
many curves $x^2+y^2 = 1+c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \square$;
and gives new ECC speed records!



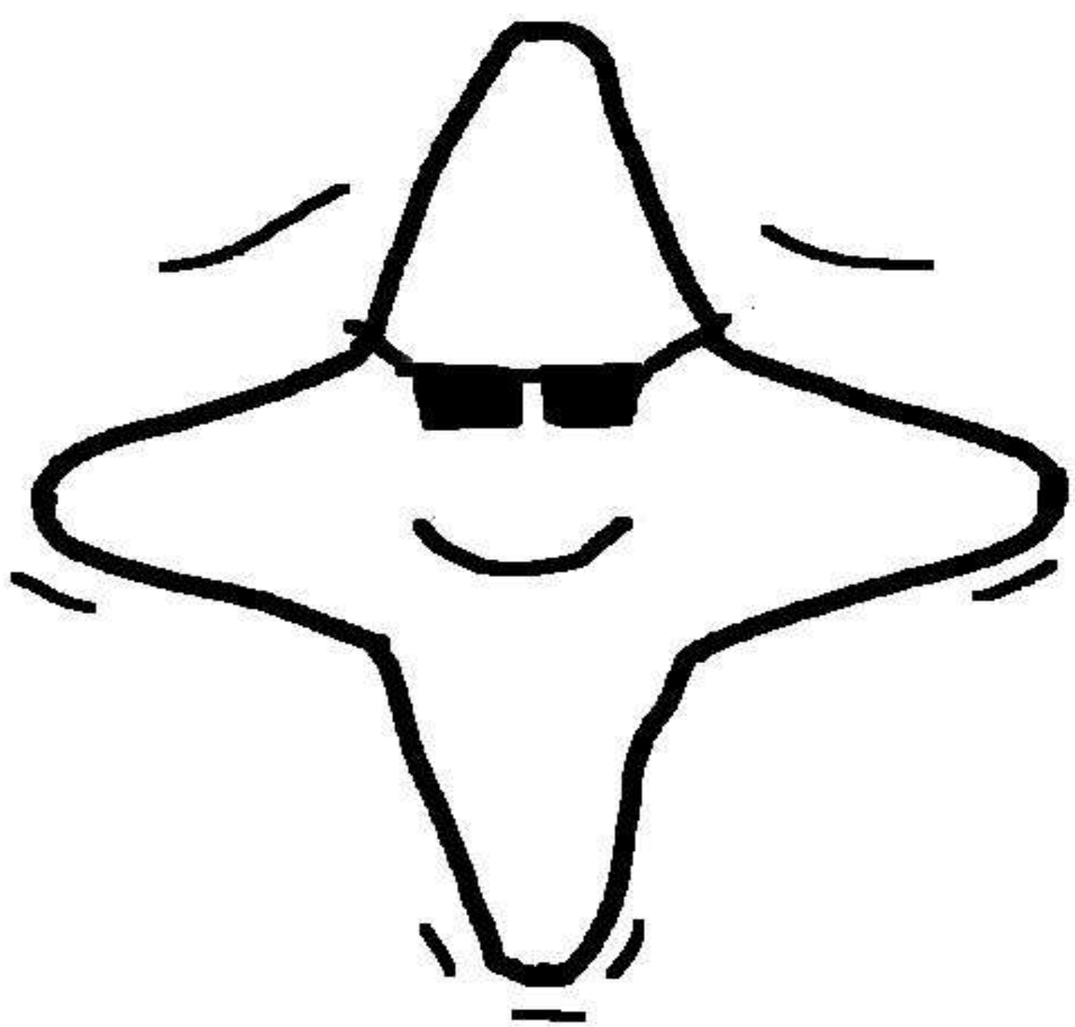
(picture courtesy Tanja La

Historical notes:

1761 Euler, 1866 Gauss
introduced an addition law
for $x^2 + y^2 = 1 - x^2y^2$,
the "lemniscatic elliptic curve."

2007 Edwards generalized to
many curves $x^2+y^2 = 1+c^4x^2y^2$.
Theorem: have now obtained
all elliptic curves over $\overline{\mathbf{Q}}$.

2007 Bernstein–Lange:
Edwards addition law is complete
for $x^2 + y^2 = 1 + dx^2y^2$ if $d \neq \square$;
and gives new ECC speed records!



(picture courtesy Tanja Lange)