Elliptic-curve cryptography I

Diffie-Hellman and clocks

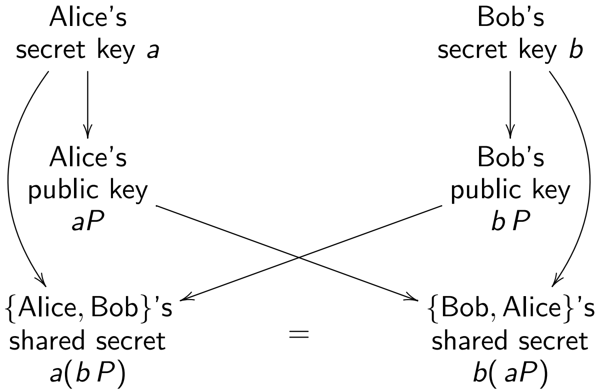
Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

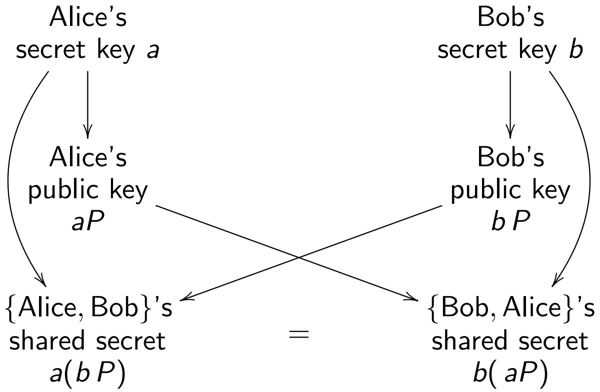
Diffie-Hellman key exchange

Pick some *generator* P, i.e., some group element
(using additive notation here).



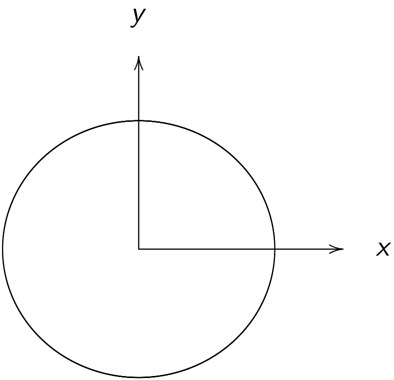
Diffie-Hellman key exchange

Pick some *generator* P, i.e., some group element (using additive notation here).



What does P look like? How to compute $P + Q$?

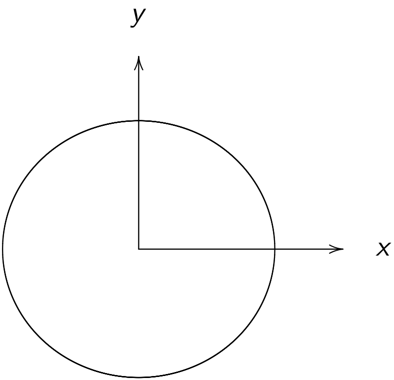
The clock



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

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

The clock



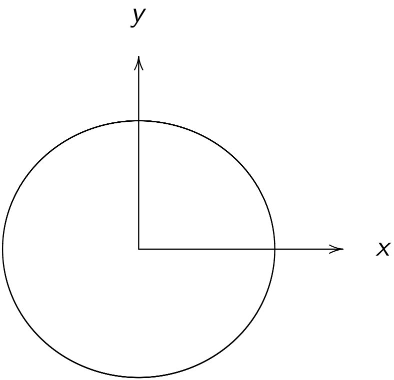
This is the curve $x^2 + y^2 = 1$.

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

Examples of points on this curve:

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

The clock



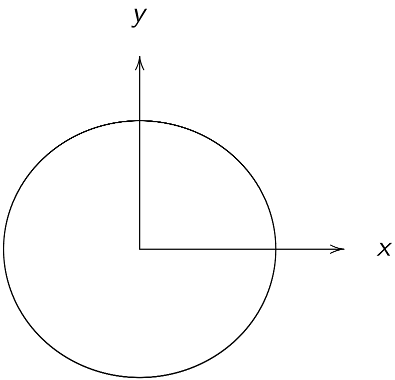
This is the curve $x^2 + y^2 = 1$.

Examples of points on this curve:

$(0, 1) =$ "12:00".
$(0, -1) =$ "6:00".

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

The clock



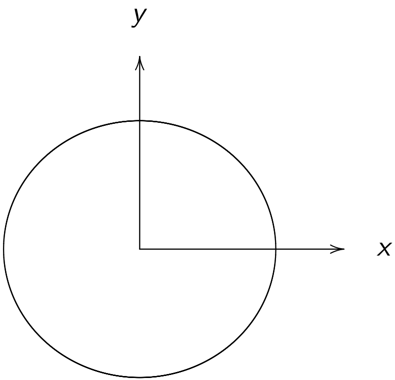
This is the curve $x^2 + y^2 = 1$.

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".

The clock



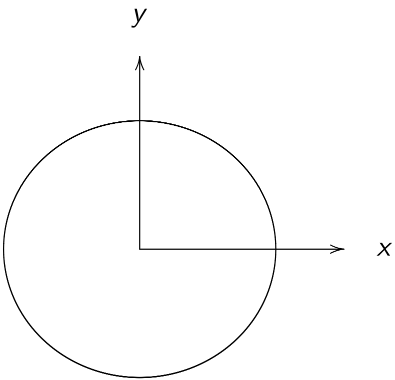
Examples of points on this curve:

$(0,1) =$ "12:00".
$(0,-1) =$ "6:00".
$(1,0) =$ "3:00".
$(-1,0) =$ "9:00".

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

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

The clock



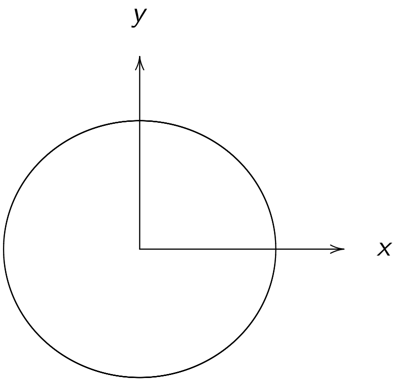
Examples of points on this curve:

$(0,1) =$ "12:00".
$(0,-1) =$ "6:00".
$(1,0) =$ "3:00".
$(-1,0) =$ "9:00".
$(\sqrt{3/4}, 1/2) =$

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

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

The clock



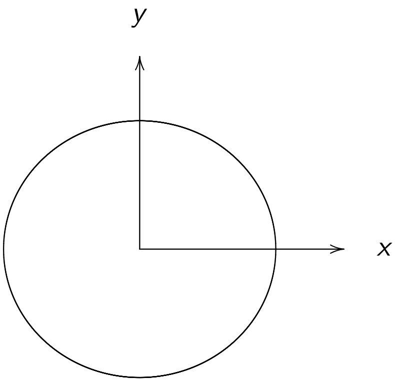
Examples of points on this curve:

$(0, 1) =$ "12:00".
$(0, -1) =$ "6:00".
$(1, 0) =$ "3:00".
$(-1, 0) =$ "9:00".
$(\sqrt{3/4}, 1/2) =$ "2:00".

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

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

The clock



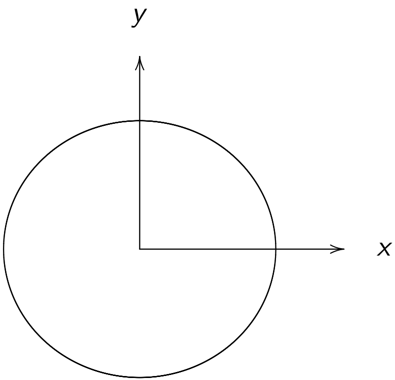
Examples of points on this curve:

$(0,1) =$ "12:00".
$(0,-1) =$ "6:00".
$(1,0) =$ "3:00".
$(-1,0) =$ "9:00".
$(\sqrt{3/4}, 1/2) =$ "2:00".
$(1/2, -\sqrt{3/4}) =$

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

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

The clock



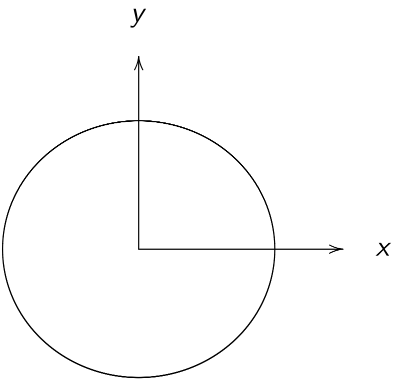
Examples of points on this curve:

$(0, 1) =$ "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".

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

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

The clock



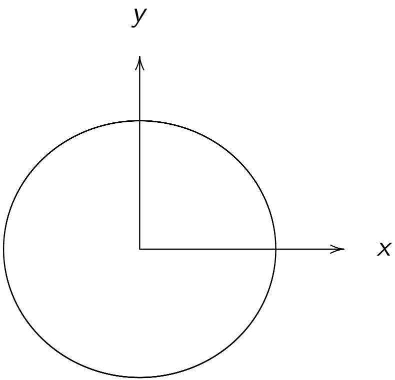
This is the curve $x^2 + y^2 = 1$.

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

The clock



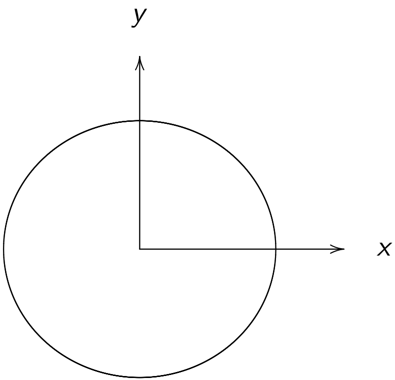
This is the curve $x^2 + y^2 = 1$.

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".

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

The clock



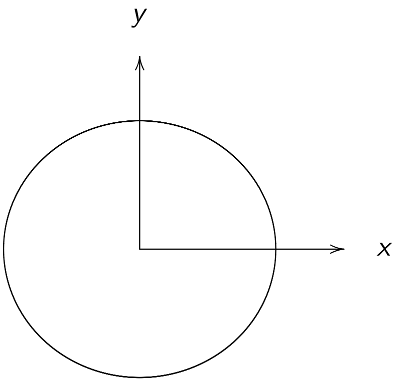
This is the curve $x^2 + y^2 = 1$.

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



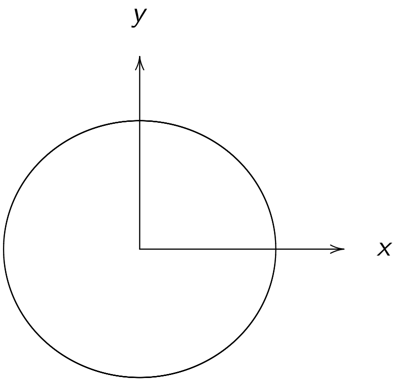
This is the curve $x^2 + y^2 = 1$.

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



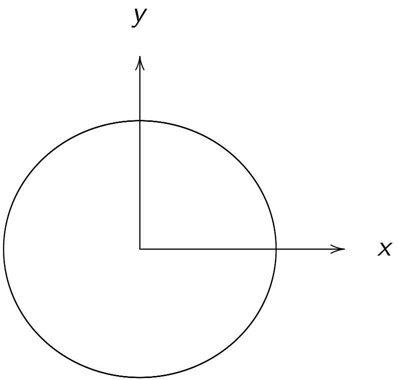
This is the curve $x^2 + y^2 = 1$.

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

The clock



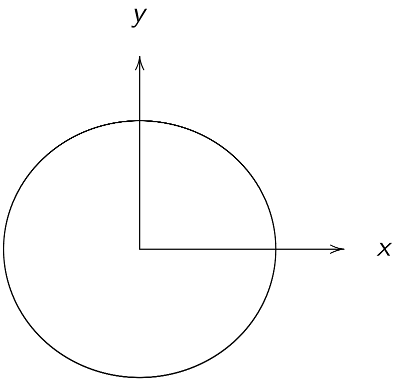
This is the curve $x^2 + y^2 = 1$.

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

The clock



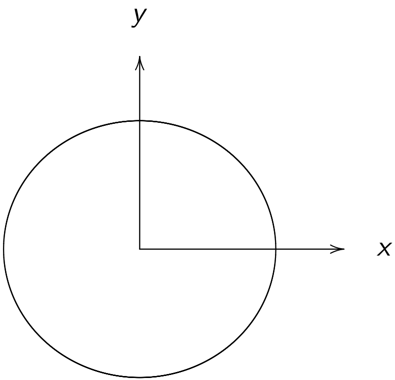
This is the curve $x^2 + y^2 = 1$.

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

The clock



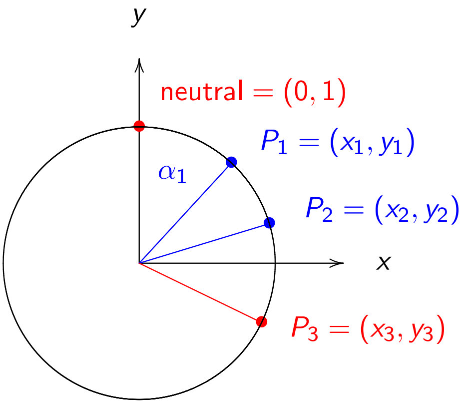
This is the curve $x^2 + y^2 = 1$.

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.

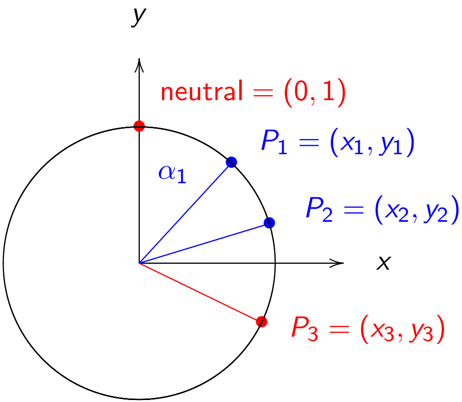
Addition on the clock



Neutral element: $(0, 1)$
at angle $\alpha = 0^\circ$.

Adding two points $\cong$
adding angles α_1 and α_2
(taken modulo 360°).

Addition on the clock

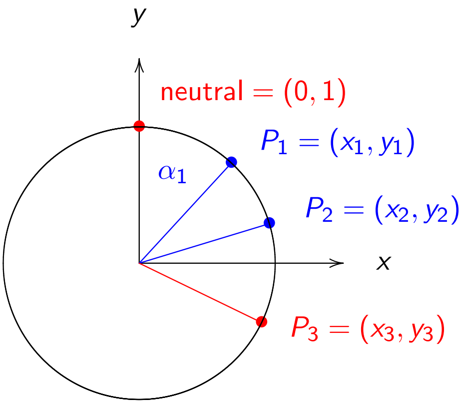


Neutral element: $(0, 1)$
at angle $\alpha = 0°$.

Point $(0, -1)$ has $\alpha = 180°$
thus has order 2.

Adding two points $\cong$
adding angles α_1 and α_2
(taken modulo 360°).

Addition on the clock



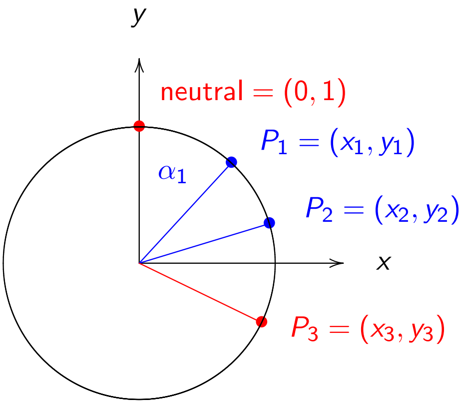
Adding two points $\cong$ adding angles α_1 and α_2 (taken modulo 360°).

Neutral element: $(0, 1)$ at angle $\alpha = 0°$.

Point $(0, -1)$ has $\alpha = 180°$ thus has order 2.

$(1, 0), (0, 1)$ have order 4 with $\alpha = \pm 90°$.

Addition on the clock



Adding two points $\cong$
adding angles α_1 and α_2
(taken modulo 360°).

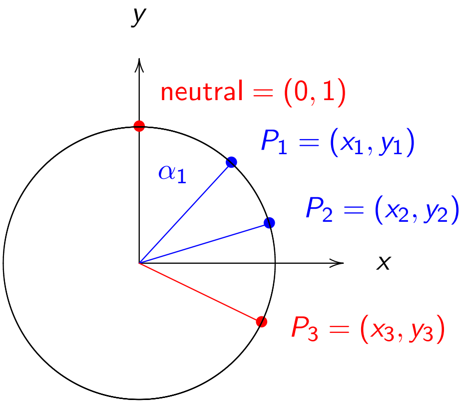
Neutral element: $(0, 1)$
at angle $\alpha = 0°$.

Point $(0, -1)$ has $\alpha = 180°$
thus has order 2.

$(1, 0), (0, 1)$ have order 4
with $\alpha = \pm 90°$.

Inverse of point with α
is point with $-\alpha$
since $\alpha + (-\alpha) = 0$.

Addition on the clock



Adding two points $\cong$
adding angles α_1 and α_2
(taken modulo 360°).

Neutral element: $(0, 1)$
at angle $\alpha = 0°$.

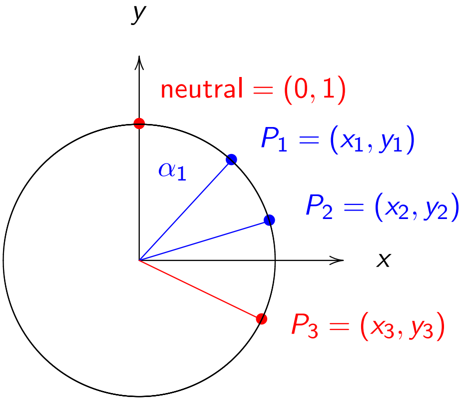
Point $(0, -1)$ has $\alpha = 180°$
thus has order 2.

$(1, 0), (0, 1)$ have order 4
with $\alpha = \pm 90°$.

Inverse of point with α
is point with $-\alpha$
since $\alpha + (-\alpha) = 0$.

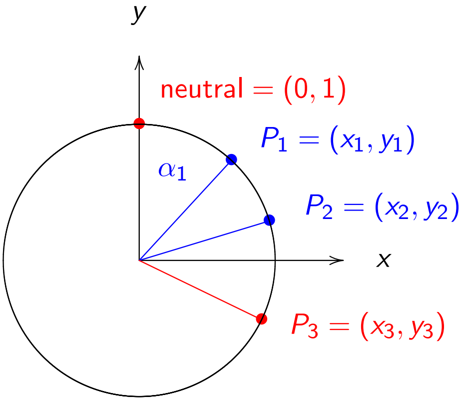
Points form group under addition of angles.

Addition on the clock



This works fine for "nice" α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

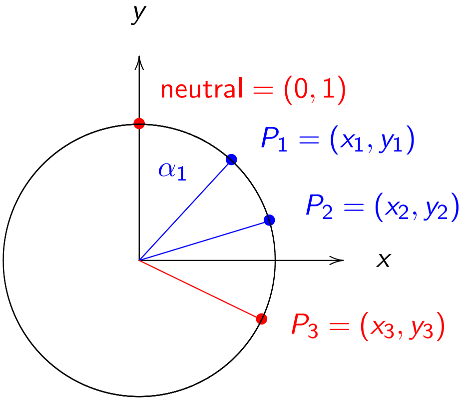
Addition on the clock



Curve $x^2 + y^2 = 1$,
$x = \sin\alpha$, $y = \cos\alpha$.

This works fine for “nice” α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

Addition on the clock

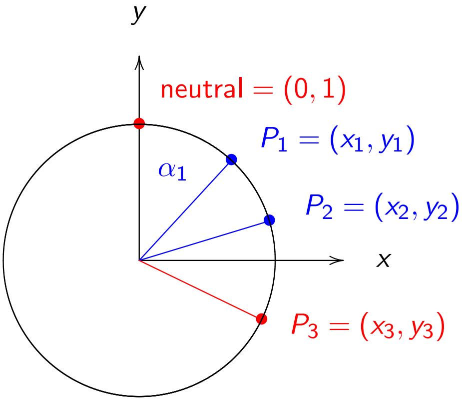


Curve $x^2 + y^2 = 1$,
$x = \sin\alpha$, $y = \cos\alpha$.

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

This works fine for "nice" α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

Addition on the clock

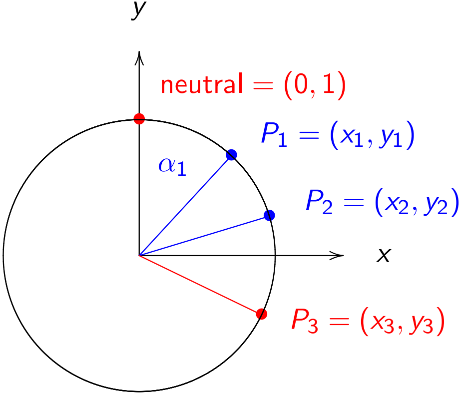


Curve $x^2 + y^2 = 1$,
$x = \sin\alpha$, $y = \cos\alpha$.

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

This works fine for "nice" α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

Addition on the clock

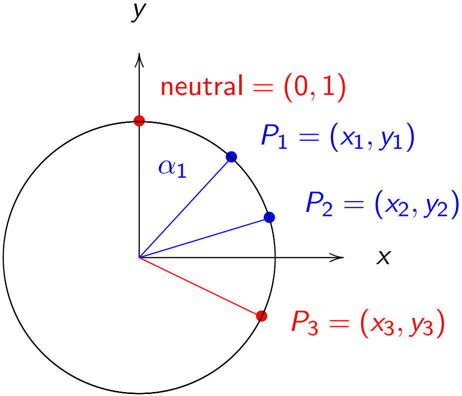


Curve $x^2 + y^2 = 1$,
$x = \sin\alpha$, $y = \cos\alpha$.

Recall
$(\sin(\alpha_1+\alpha_2), \cos(\alpha_1+\alpha_2)) =$
$(\sin\alpha_1\cos\alpha_2 + \cos\alpha_1\sin\alpha_2,$
$\cos\alpha_1\cos\alpha_2 - \sin\alpha_1\sin\alpha_2)$.

This works fine for "nice" α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

Addition on the clock



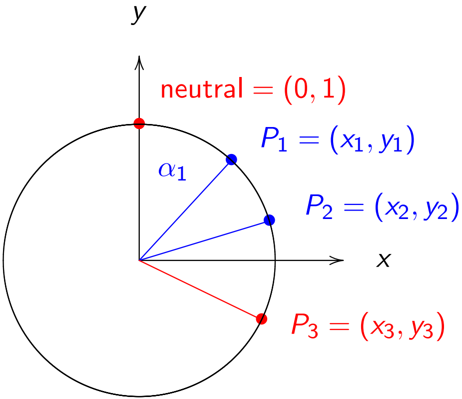
This works fine for "nice" α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

Curve $x^2 + y^2 = 1$,
$x = \sin\alpha$, $y = \cos\alpha$.

Recall
$(\sin(\alpha_1+\alpha_2), \cos(\alpha_1+\alpha_2)) =$
$(\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2,$
$\cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2).$

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

Addition on the clock



Curve $x^2 + y^2 = 1$,
$x = \sin \alpha$, $y = \cos \alpha$.

Recall
$(\sin(\alpha_1+\alpha_2), \cos(\alpha_1+\alpha_2)) =$
$(\sin \alpha_1 \cos \alpha_2 + \cos \alpha_1 \sin \alpha_2,$
$\cos \alpha_1 \cos \alpha_2 - \sin \alpha_1 \sin \alpha_2)$.

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

This works fine for "nice" α;
How about $(3/5, 4/5) + (3/5, 4/5)$?

$$\left(\frac{3}{5}, \frac{4}{5}\right) + \left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{3}{5} \cdot \frac{4}{5} + \frac{4}{5} \cdot \frac{3}{5}, \frac{4}{5} \cdot \frac{4}{5} - \frac{3}{5} \cdot \frac{3}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right)$$

We write $kP = \underbrace{P + P + \cdots + P}_{k \text{ copies}}$ for $k \geq 0$.