Points

September 27, 2016

An elliptic curve

defined by $V(y^2 = x^3 - x)$

An elliptic curve

defined by $V(y^2 = x^3 - x) \cup \underset{\displaystyle\infty}{\overset{\displaystyle Id_E}{\parallel}}$

An elliptic curve

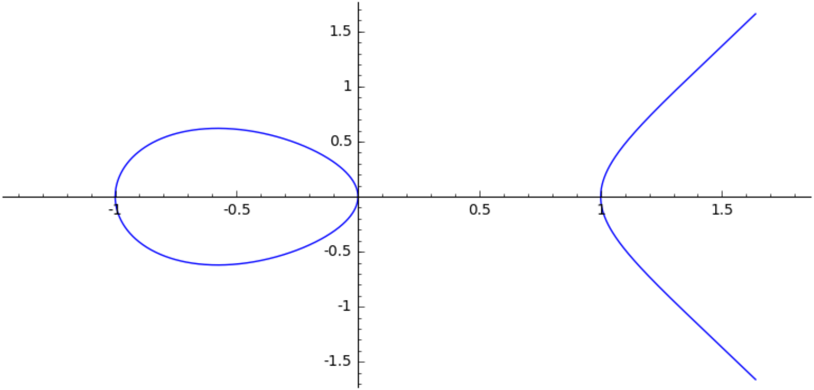
defined by $V(y^2 = x^3 - x) \cup \underset{\substack{\| \\ Id_E}}{\infty}$

$E(\mathbb{R})$:

An elliptic curve

defined by $V(y^2 = x^3 - x) \cup \underset{\substack{\| \\ Id_E}}{\infty}$

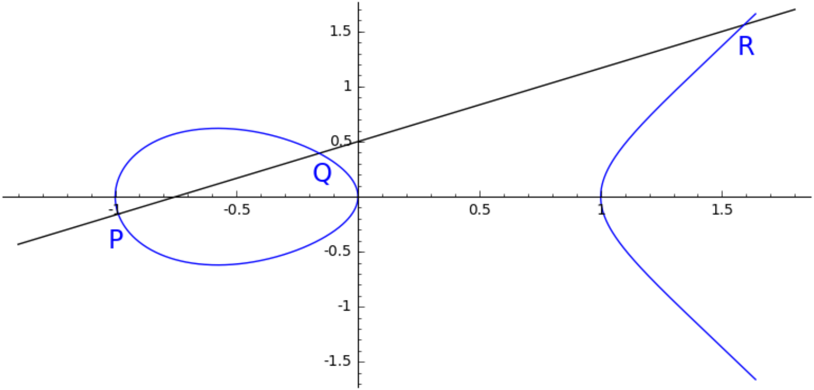
$E(\mathbb{R})$:



An elliptic curve

defined by $V(y^2 = x^3 - x) \cup \underset{\displaystyle \infty}{\overset{Id_E}{\|}}$

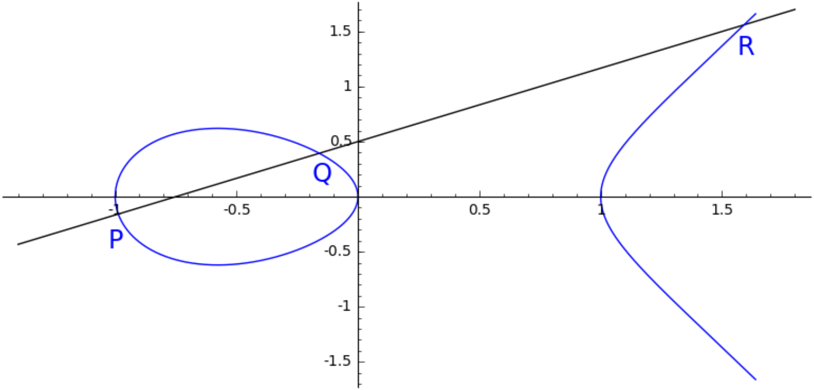
$E(\mathbb{R})$:



An elliptic curve

defined by $V(y^2 = x^3 - x) \cup \overset{Id_E}{\overset{\|}{\infty}}$

$E(\mathbb{R})$:



$$P + Q + R = Id_E$$

Question: how many points are in E ?

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$$

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ *such that:*

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*
- *$|\alpha| = |\beta| = \sqrt{3}$*

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*
- *$|\alpha| = |\beta| = \sqrt{3}$*

In particular

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*
- $|\alpha| = |\beta| = \sqrt{3}$

In particular

- $\alpha + \beta \in \mathbb{Z}$ and $|\alpha + \beta| \leq 2\sqrt{3}$

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*
- $|\alpha| = |\beta| = \sqrt{3}$

In particular

- $\alpha+\beta \in \mathbb{Z}$ and $|\alpha+\beta| \leq 2\sqrt{3}$
- $\alpha\beta \in \mathbb{Z}$ and $|\alpha\beta| = 3$

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*
- $|\alpha| = |\beta| = \sqrt{3}$

In particular

- $\alpha+\beta \in \mathbb{Z}$ and $|\alpha+\beta| \leq 2\sqrt{3}$
- $\alpha\beta \in \mathbb{Z}$ and $|\alpha\beta| = 3$

$$\Rightarrow P(t) = t^2 + a\,t \pm 3$$

Question: how many points are in $E(\mathbb{F}_{3^d})$?

Theorem

$\#E(\mathbb{F}_{3^d}) = 1^d - \alpha^d - \beta^d + 3^d$ such that:

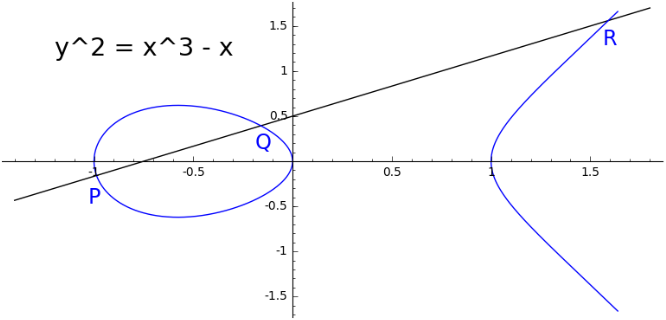
- *$P(t) = (t-\alpha)(t-\beta)$ is a polynomial in $\mathbb{Z}[t]$*
- $|\alpha| = |\beta| = \sqrt{3}$

In particular

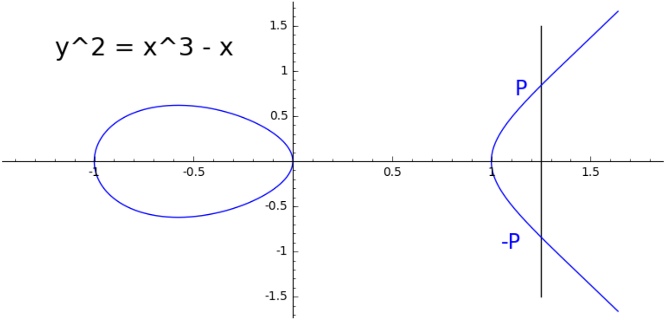
- $\alpha+\beta \in \mathbb{Z}$ and $|\alpha+\beta| \leq 2\sqrt{3}$
- $\alpha\beta \in \mathbb{Z}$ and $|\alpha\beta| = 3$

$$\Rightarrow P(t) = t^2 + a\,t \pm 3 \qquad -3 \leq a \leq 3$$

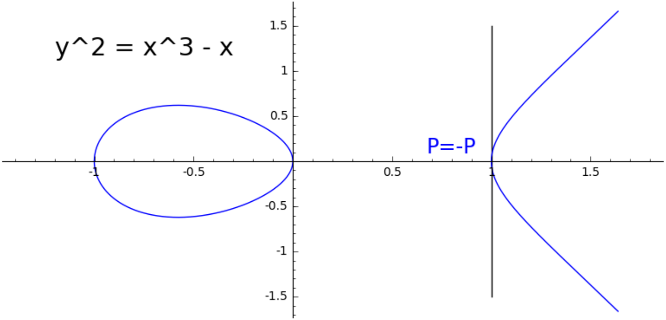
$E[2]$ and $P(t) = t^2 + at \pm 3$ $\quad -3 \leq a \leq 3$



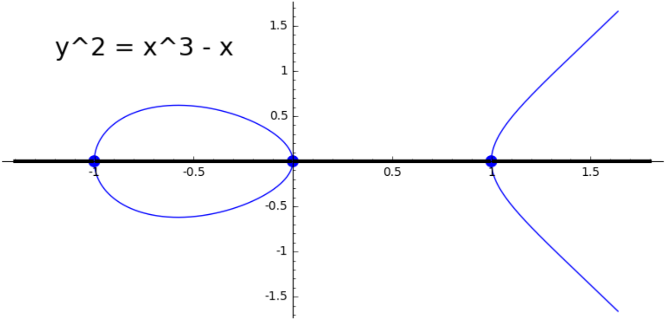
$E[2]$ and $P(t) = t^2 + at \pm 3$ $\quad -3 \le a \le 3$



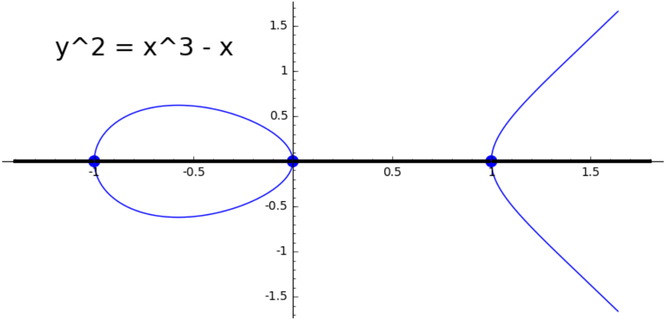
$E[2]$ and $P(t) = t^2 + at \pm 3$ $\quad -3 \leq a \leq 3$



$E[2]$ and $P(t) = t^2 + at \pm 3$ $\quad -3 \leq a \leq 3$

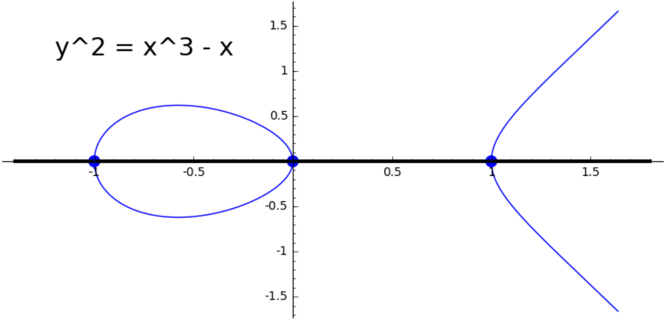


$E[2]$ and $P(t) = t^2 + at \pm 3$ $\quad -3 \leq a \leq 3$



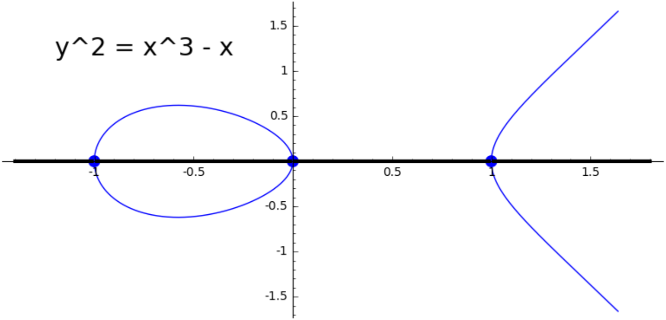
- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{Id_E}{\underset{\infty}{||}}$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \leq a \leq 3$



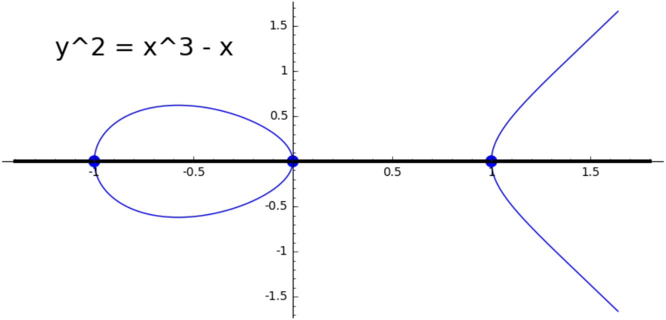
- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{Id_E}{\overset{||}{\infty}} \ \simeq \ (\mathbb{Z}/2\mathbb{Z})^2$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \le a \le 3$



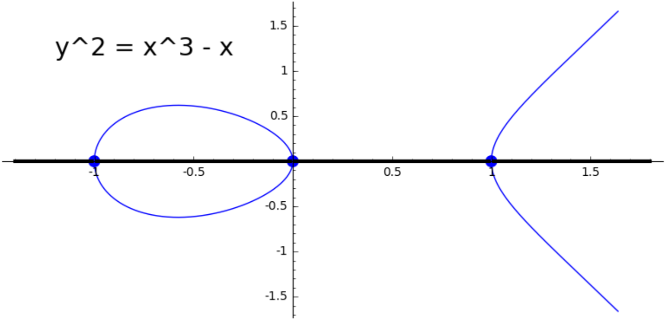
- $E[2] = \; (0,0),\; (1,0),\; (-1,0),\; \underset{\substack{||\\ Id_E}}{\infty} \;\simeq\; (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$

$E[2]$ and $P(t) = t^2 + at \pm 3$ $\quad -3 \leq a \leq 3$



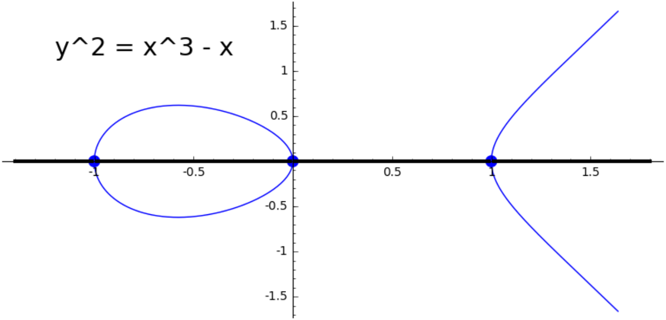
- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{Id_E}{\overset{||}{\infty}} \ \simeq \ (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$
- $Frob_{E[2]}$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \leq a \leq 3$



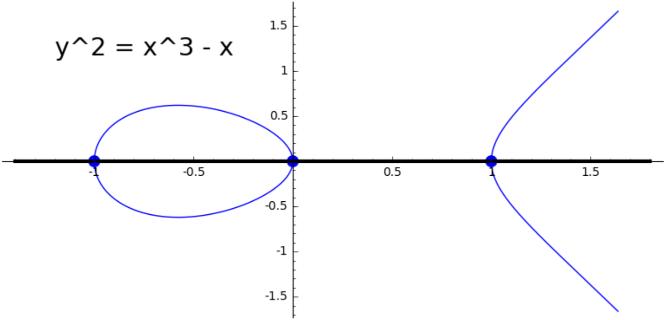
- $E[2] = \; (0,0), \; (1,0), \; (-1,0), \; \underset{\infty}{\overset{Id_E}{||}} \; \simeq \; (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$
- $Frob_{E[2]} = Id$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \leq a \leq 3$



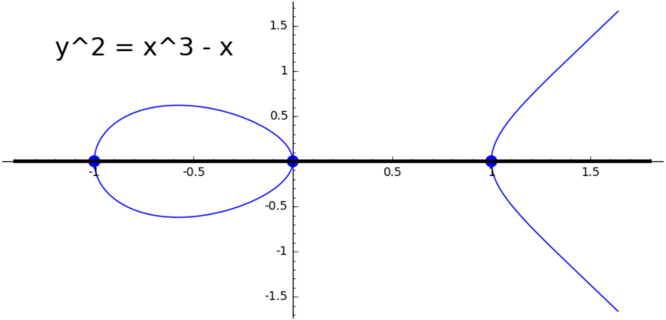
- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{Id_E}{\overset{||}{\infty}} \ \simeq \ (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$
- $Frob_{E[2]} = Id \qquad\qquad \in GL_2(\mathbb{Z}/2\mathbb{Z})$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \leq a \leq 3$



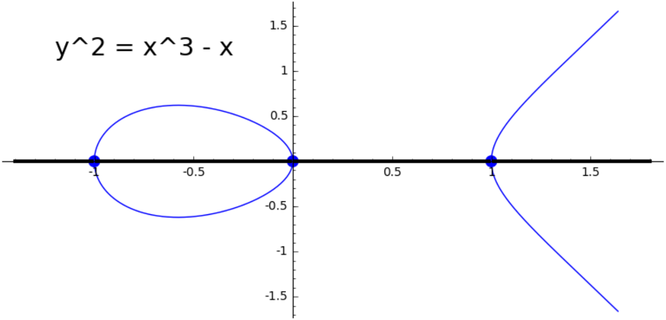
- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{Id_E}{\overset{\|}{\infty}} \ \simeq \ (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$
- $Frob_{E[2]} = Id \qquad\qquad \in GL_2(\mathbb{Z}/2\mathbb{Z})$
- $char(Frob_{E[2]}) = t^2 + 1$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \le a \le 3$



- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{Id_E}{\overset{||}{\infty}} \ \simeq \ (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$
- $Frob_{E[2]} = Id \qquad\qquad \in GL_2(\mathbb{Z}/2\mathbb{Z})$
- $char(Frob_{E[2]}) = t^2 + 1 \qquad \in (\mathbb{Z}/2\mathbb{Z})[t]$

$E[2]$ and $P(t) = t^2 + at \pm 3 \qquad -3 \leq a \leq 3$



- $E[2] = \ (0,0),\ (1,0),\ (-1,0),\ \overset{\overset{Id_E}{||}}{\infty} \ \simeq \ (\mathbb{Z}/2\mathbb{Z})^2$
- $(Frob(x), Frob(y)) = (x^3, y^3)$
- $Frob_{E[2]} = Id \qquad\qquad \in GL_2(\mathbb{Z}/2\mathbb{Z})$
- $char(Frob_{E[2]}) = t^2 + 1 \qquad \in (\mathbb{Z}/2\mathbb{Z})[t]$
- $\Rightarrow P(t) \equiv t^2 + 1$ modulo 2

$E[4]$

$$E : y^2 = x^3 - x$$

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$,

$$E : y^2 = x^3 - x$$

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 = (\text{i, i-1})$, $e_2 = (\text{i+1,i-1})$

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 = $ (i, i-1), $e_2 = $ (i+1,i-1)

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	[0 : 1 : 0]	(i , i–1)	(0,0)	(i , -i+1)
$1e_2$	(i+1, i–1)	(i–1, -i+1)	(-i+1, -i–1)	(-i–1, -i–1)
$2e_2$	(1,0)	(-i , i+1)	(-1,0)	(-i , -i–1)
$3e_2$	(i+1, -i+1)	(-i–1, i+1)	(-i+1, i+1)	(i–1, i–1)

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 = (\text{i}, \text{i-1})$, $e_2 = (\text{i+1,i-1})$

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	$[0:1:0]$	(i , i–1)	(0,0)	(i , -i+1)
$1e_2$	(i+1, i–1)	(i–1, -i+1)	(-i+1, -i–1)	(-i–1, -i–1)
$2e_2$	(1,0)	(-i , i+1)	(-1,0)	(-i , -i–1)
$3e_2$	(i+1, -i+1)	(-i–1, i+1)	(-i+1, i+1)	(i–1, i–1)

$Frob(e_1)$

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 =$ (i, i-1), $e_2 =$ (i+1,i-1)

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	[0 : 1 : 0]	(i , i–1)	(0,0)	(i , -i+1)
$1e_2$	(i+1, i–1)	(i–1, -i+1)	(-i+1, -i–1)	(-i–1, -i–1)
$2e_2$	(1,0)	(-i , i+1)	(-1,0)	(-i , -i–1)
$3e_2$	(i+1, -i+1)	(-i–1, i+1)	(-i+1, i+1)	(i–1, i–1)

$Frob(e_1) \quad =$ (i^3, $\mathrm{i}^3 - 1^3$)

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 = $ (i, i-1), $e_2 = $ (i+1,i-1)

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	[0 : 1 : 0]	(i , i–1)	(0,0)	(i , -i+1)
$1e_2$	(i+1, i–1)	(i–1, -i+1)	(-i+1, -i–1)	(-i–1, -i–1)
$2e_2$	(1,0)	(-i , i+1)	(-1,0)	(-i , -i–1)
$3e_2$	(i+1, -i+1)	(-i–1, i+1)	(-i+1, i+1)	(i–1, i–1)

$$\begin{aligned} Frob(e_1) &= (\ i^3,\ i^3 - 1^3\ ) \\ &= (\ \text{-}i,\ \text{-}i - 1\ ) \end{aligned}$$

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 = (i, i-1)$, $e_2 = (i+1, i-1)$

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	$[0:1:0]$	$(i, i-1)$	$(0,0)$	$(i, -i+1)$
$1e_2$	$(i+1, i-1)$	$(i-1, -i+1)$	$(-i+1, -i-1)$	$(-i-1, -i-1)$
$2e_2$	$(1,0)$	$(-i, i+1)$	$(-1,0)$	$(-i, -i-1)$
$3e_2$	$(i+1, -i+1)$	$(-i-1, i+1)$	$(-i+1, i+1)$	$(i-1, i-1)$

$$\begin{aligned} Frob(e_1) &= (i^3, i^3 - 1^3) \\ &= (-i, -i-1) \qquad = 3e_1 + 2e_2 \end{aligned}$$

$E[4] \simeq (\mathbb{Z}/4\mathbb{Z})^2$, a basis: $e_1 = (\mathrm{i}, \mathrm{i}\text{-}1)$, $e_2 = (\mathrm{i}+1, \mathrm{i}\text{-}1)$

$$E : y^2 = x^3 - x \qquad (i^2 = -1 \in \mathbb{F}_9)$$

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	$[0 : 1 : 0]$	$(\mathrm{i}, \mathrm{i}-1)$	$(0,0)$	$(\mathrm{i}, -\mathrm{i}+1)$
$1e_2$	$(\mathrm{i}+1, \mathrm{i}-1)$	$(\mathrm{i}-1, -\mathrm{i}+1)$	$(-\mathrm{i}+1, -\mathrm{i}-1)$	$(-\mathrm{i}-1, -\mathrm{i}-1)$
$2e_2$	$(1,0)$	$(-\mathrm{i}, \mathrm{i}+1)$	$(-1,0)$	$(-\mathrm{i}, -\mathrm{i}-1)$
$3e_2$	$(\mathrm{i}+1, -\mathrm{i}+1)$	$(-\mathrm{i}-1, \mathrm{i}+1)$	$(-\mathrm{i}+1, \mathrm{i}+1)$	$(\mathrm{i}-1, \mathrm{i}-1)$

$$\begin{aligned}
Frob(e_1) &= (\mathrm{i}^3, \mathrm{i}^3 - 1^3) \\
&= (-\mathrm{i}, -\mathrm{i} - 1) \qquad = 3\, e_1 + 2\, e_2 \\
Frob(e_2) &= (\mathrm{i}^3 + 1, \mathrm{i}^3 - 1^3) \\
&= (-\mathrm{i}+1, -\mathrm{i} - 1) \qquad = 2\, e_1 + 1\, e_2
\end{aligned}$$

E[4] and $P(t) = t^2 + at \pm 3$

$$\Rightarrow Frob_{E[4]} \qquad = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \quad \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

E[4] and $P(t) = t^2 + at \pm 3$

$$\Rightarrow Frob_{E[4]} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

$$\Rightarrow char(Frob_{E[4]}) = t^2 + 3 \in \mathbb{Z}/4\mathbb{Z}[t]$$

E[4] and $P(t) = t^2 + at \pm 3$

$$\Rightarrow Frob_{E[4]} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

$$\Rightarrow char(Frob_{E[4]}) = t^2 + 3 \in \mathbb{Z}/4\mathbb{Z}[t]$$

$$\Rightarrow P(t) \equiv t^2 + 3 \quad \text{modulo } 4$$

E[4] and $P(t) = t^2 + at \pm 3$

$$\begin{aligned}
&\Rightarrow Frob_{E[4]} && = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} && \in GL_2(\mathbb{Z}/4\mathbb{Z}) \\
&\Rightarrow char(Frob_{E[4]}) && = t^2 + 3 && \in \mathbb{Z}/4\mathbb{Z}[t] \\
&\Rightarrow P(t) && \equiv t^2 + 3 && \text{modulo } 4
\end{aligned}$$

Recall that Theorem $\Rightarrow P(t) = t^2 + ax \pm 3, \quad -3 \leq a \leq 3$

E[4] and $P(t) = t^2 + at \pm 3$

$$\Rightarrow Frob_{E[4]} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/4\mathbb{Z})$$

$$\Rightarrow char(Frob_{E[4]}) = t^2 + 3 \in \mathbb{Z}/4\mathbb{Z}[t]$$

$$\Rightarrow P(t) \equiv t^2 + 3 \quad \text{modulo } 4$$

Recall that Theorem $\Rightarrow P(t) = t^2 + ax \pm 3, \qquad -3 \leq a \leq 3$

$$\Rightarrow P(t) = t^2 + 3$$

$\#E(\mathbb{F}_{3^d})$

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\alpha = \sqrt{-3}, \quad \beta = -\sqrt{-3} = -\alpha$

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$$\alpha = \sqrt{-3}, \qquad \beta = -\sqrt{-3} = -\alpha$$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\alpha = \sqrt{-3}, \quad \beta = -\sqrt{-3} = -\alpha$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$
1	$1 - \alpha + \alpha + 3$	

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\alpha = \sqrt{-3}, \quad \beta = -\sqrt{-3} = -\alpha$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$
1	$1 - \alpha + \alpha + 3$	4

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$$\alpha = \sqrt{-3}, \qquad \beta = -\sqrt{-3} = -\alpha$$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$
1	$1 - \alpha + \alpha + 3$	4
2	$1 - (-3) - (-3) + 9$	

$\#E(\mathbb{F}_{3^d})$

Theorem $\Rightarrow$

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\alpha = \sqrt{-3}, \quad \beta = -\sqrt{-3} = -\alpha$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$
1	$1 - \alpha + \alpha + 3$	4
2	$1 - (-3) - (-3) + 9$	16

$+$	$0e_1$	$1e_1$	$2e_1$	$3e_1$
$0e_2$	[0 : 1 : 0]	(i , i–1)	(0,0)	(i , -i+1)
$1e_2$	(i+1, i–1)	(i–1, -i+1)	(-i+1, -i–1)	(-i–1, -i–1)
$2e_2$	(1,0)	(-i , i+1)	(-1,0)	(-i , -i–1)
$3e_2$	(i+1, -i+1)	(-i–1, i+1)	(-i+1, i+1)	(i–1, i–1)

$\#E(\mathbb{F}_{3^d})$

Theorem

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\Rightarrow \alpha = \sqrt{-3}, \quad \beta = -\alpha$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$
1	$1 - \alpha + \alpha + 3$	4
2	$1 - (-3) - (-3) + 9$	16

$\#E(\mathbb{F}_{3^d})$

Theorem

$$\#E(\mathbb{F}_{q=3^d}) = 1^d - \alpha^d - \beta^d + 3^d,$$

where α, β *are the roots of*

$$P(t) = t^2 + 3.$$

$\Rightarrow \alpha = \sqrt{-3}, \quad \beta = -\alpha$

d	$1^d - \alpha^d - (-\alpha)^d + 3^d$	$\#E(\mathbb{F}_{3^d})$
1	$1 - \alpha + \alpha + 3$	4
2	$1 - (-3) - (-3) + 9$	16
3	$1 - \alpha^3 + \alpha^3 + 27$	28