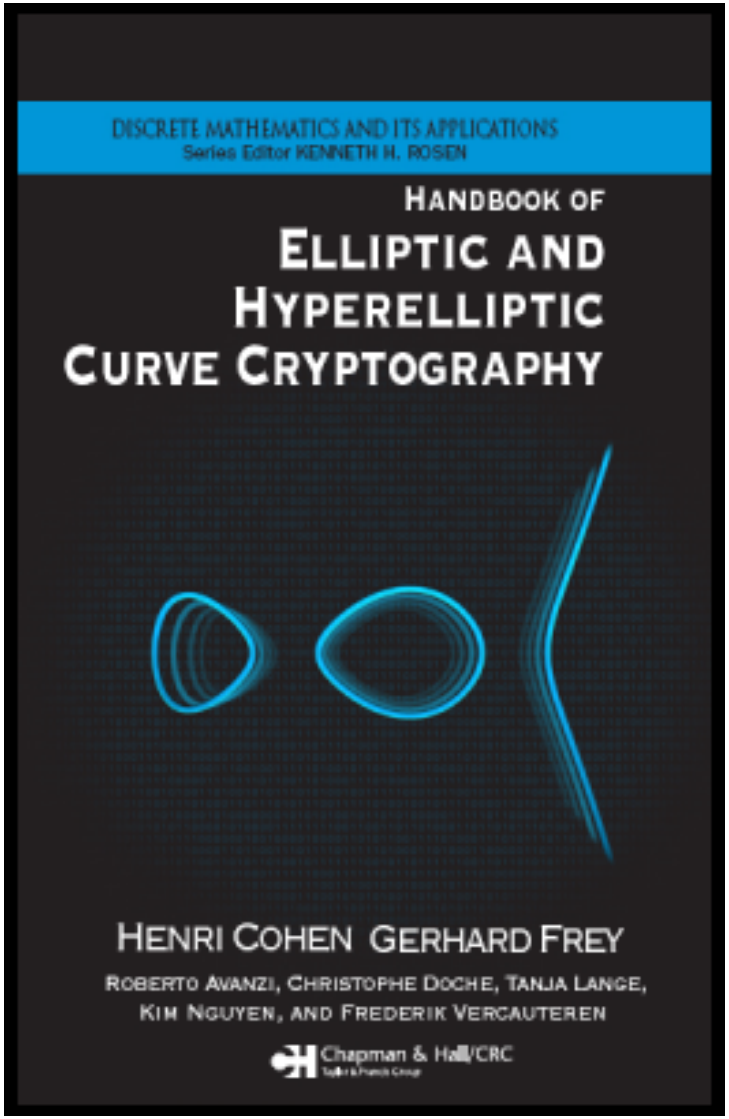
Elliptic and Hyperelliptic Curve Cryptography

Renate Scheidler

Research supported in part by NSERC of Canada

Comprehensive Source

Handbook of Elliptic and Hyperelliptic Curve Cryptography



Overview

- Motivation
- Elliptic Curve Arithmetic
- Hyperelliptic Curve Arithmetic
- Point Counting
- Discrete Logarithm Algorithms
- Other Models

Motivation — Why (Hyper-)Elliptic Cryptography?

Requirements on groups for discrete log based cryptography

- Large group order (plus other restrictions)
- Compact representation of group elements
- Fast group operation
- Hard Diffie-Hellman/discrete logarithm problem

Motivation — Why (Hyper-)Elliptic Cryptography?

Requirements on groups for discrete log based cryptography

- Large group order (plus other restrictions)
- Compact representation of group elements
- Fast group operation
- Hard Diffie-Hellman/discrete logarithm problem

Elliptic and low genus hyperelliptic curves do well on all of these!

Elliptic Curves

Let K be a field (in crypto, $K = \mathbb{F}_q$ with q prime or $q = 2^n$)

Elliptic Curves

Let K be a field (in crypto, $K = \mathbb{F}_q$ with q prime or $q = 2^n$)

Weierstraß equation over K:

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

with $a_1, a_2, a_3, a_4, a_6 \in K$

Elliptic Curves

Let K be a field (in crypto, $K = \mathbb{F}_q$ with q prime or $q = 2^n$)

Weierstraß equation over K:

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

with $a_1, a_2, a_3, a_4, a_6 \in K$

Elliptic curve: Weierstraß equation & **non-singularity** condition: there are no simultaneous solutions to $(*)$ and

$$\begin{aligned} 2y + a_1x + a_3 &= 0 \\ a_1y &= 3x^2 + 2a_2x + a_4 \end{aligned}$$

Elliptic Curves

Let K be a field (in crypto, $K = \mathbb{F}_q$ with q prime or $q = 2^n$)

Weierstraß equation over K:

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

with $a_1, a_2, a_3, a_4, a_6 \in K$

Elliptic curve: Weierstraß equation & **non-singularity** condition: there are no simultaneous solutions to $(*)$ and

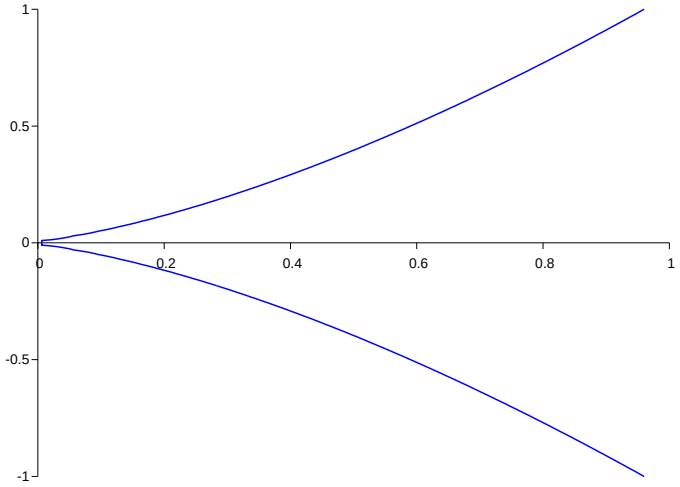
$$\begin{aligned} 2y + a_1x + a_3 &= 0 \\ a_1y &= 3x^2 + 2a_2x + a_4 \end{aligned}$$

Non-singularity $\iff$ $\Delta \neq 0$ where Δ is the **discriminant** of E

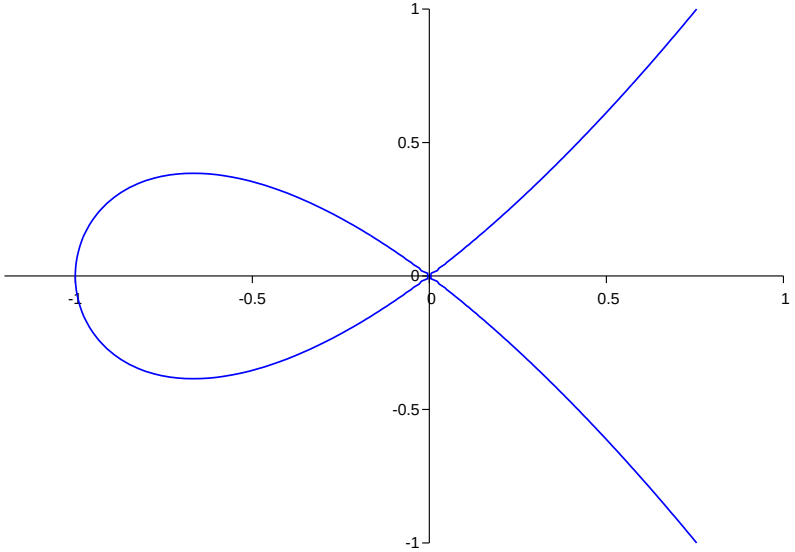
Non-Examples

Two Weierstraß equations with a singularity at $(0,0)$

$$y^2 = x^3$$

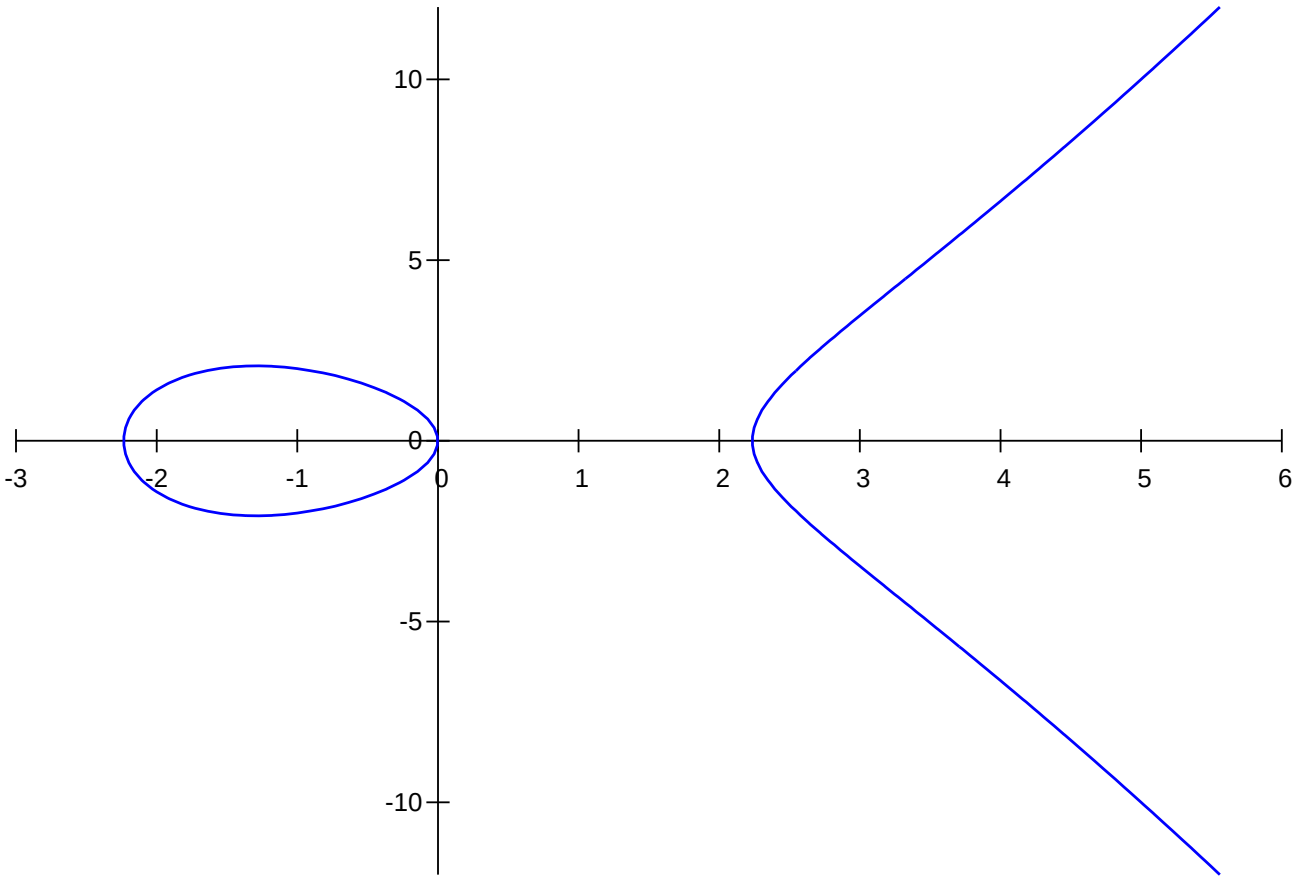


$$y^2 = x^2(x-1)$$



An Example

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$



Elliptic Curves, $\mathrm{char}(K) \neq 2, 3$

The variable transformations

$$y \to y - (a_1 x + a_3)/2, \text{ then } x \to x - (a_1^2 + 4a_2)/12:$$

yield an elliptic curve in **short** Weierstraß form:

$$E \ : \ \boxed{y^2 = x^3 + Ax + B} \qquad (A, B \in K)$$

Discriminant $\Delta = 4A^3 + 27B^2 \neq 0$ (cubic in x has distinct roots)

Elliptic Curves, $\mathrm{char}(K) \neq 2, 3$

The variable transformations

$$y \to y - (a_1 x + a_3)/2, \text{ then } x \to x - (a_1^2 + 4a_2)/12:$$

yield an elliptic curve in **short** Weierstraß form:

$$E \ : \ \boxed{y^2 = x^3 + Ax + B} \qquad (A, B \in K)$$

Discriminant $\Delta = 4A^3 + 27B^2 \neq 0$ (cubic in x has distinct roots)

For any field L with $K \subseteq L \subseteq \overline{K}$:

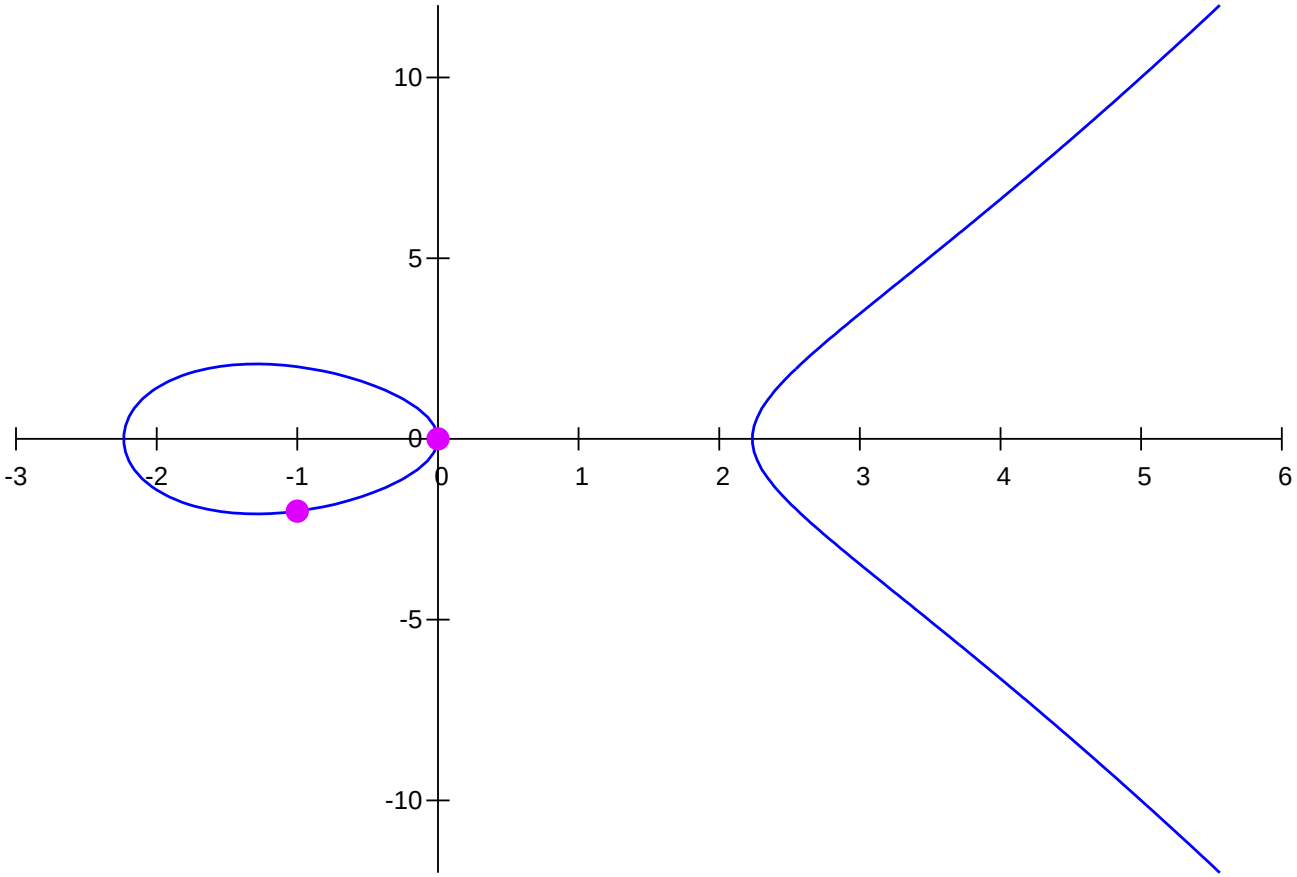
$$\boxed{E(L) \ = \ \{(x_0, y_0) \in L \times L \mid y_0^2 = x_0^3 + Ax_0 + B\} \cup \{\infty\}}$$

set of L-**rational points** on E

An Example

$$E(\mathbb{Q}) = \{(x_0, y_0) \in \mathbb{Q} \times \mathbb{Q} \mid y_0^2 = x_0^3 - 5x_0\} \cup \{\infty\}$$

$$P_1 = (-1, 2),\ P_2 = (0, 0) \ \in \ E(\mathbb{Q})$$



The Mysterious Point at Infinity

In E, replace x by x/z, y by y/z, then multiply by z^3:

$$E_{\text{proj}} \ : \ y^2 z = x^3 + Axz^2 + Bz^3$$

The Mysterious Point at Infinity

In E, replace x by x/z, y by y/z, then multiply by z^3:

$$E_{\text{proj}} \ : \ y^2 z = x^3 + Axz^2 + Bz^3$$

Points on E_{proj}:

$[x : y : z] \neq [0 : 0 : 0]$ normalized so the last non-zero entry is 1

The Mysterious Point at Infinity

In E, replace x by x/z, y by y/z, then multiply by z^3:

$$E_{\text{proj}} \ : \ y^2 z = x^3 + Axz^2 + Bz^3$$

Points on E_{proj}:

$[x : y : z] \neq [0 : 0 : 0]$ normalized so the last non-zero entry is 1

Affine Points		Projective Points
(x, y)	$\leftrightarrow$	$[x : y : 1]$
∞	$\leftrightarrow$	$[0 : 1 : 0]$

Arithmetic on E

Goal: Make $E(L)$ into an additive (Abelian) group

The identity is the point at infinity

Arithmetic on E

Goal: Make $E(L)$ into an additive (Abelian) group

The identity is the point at infinity

By **Bezout's Theorem**, any line intersects E in three points

- Need to count multiplicities
- If one of the points is ∞, the line is "vertical"

Arithmetic on E

Goal: Make $E(L)$ into an additive (Abelian) group

The identity is the point at infinity

By **Bezout's Theorem**, any line intersects E in three points

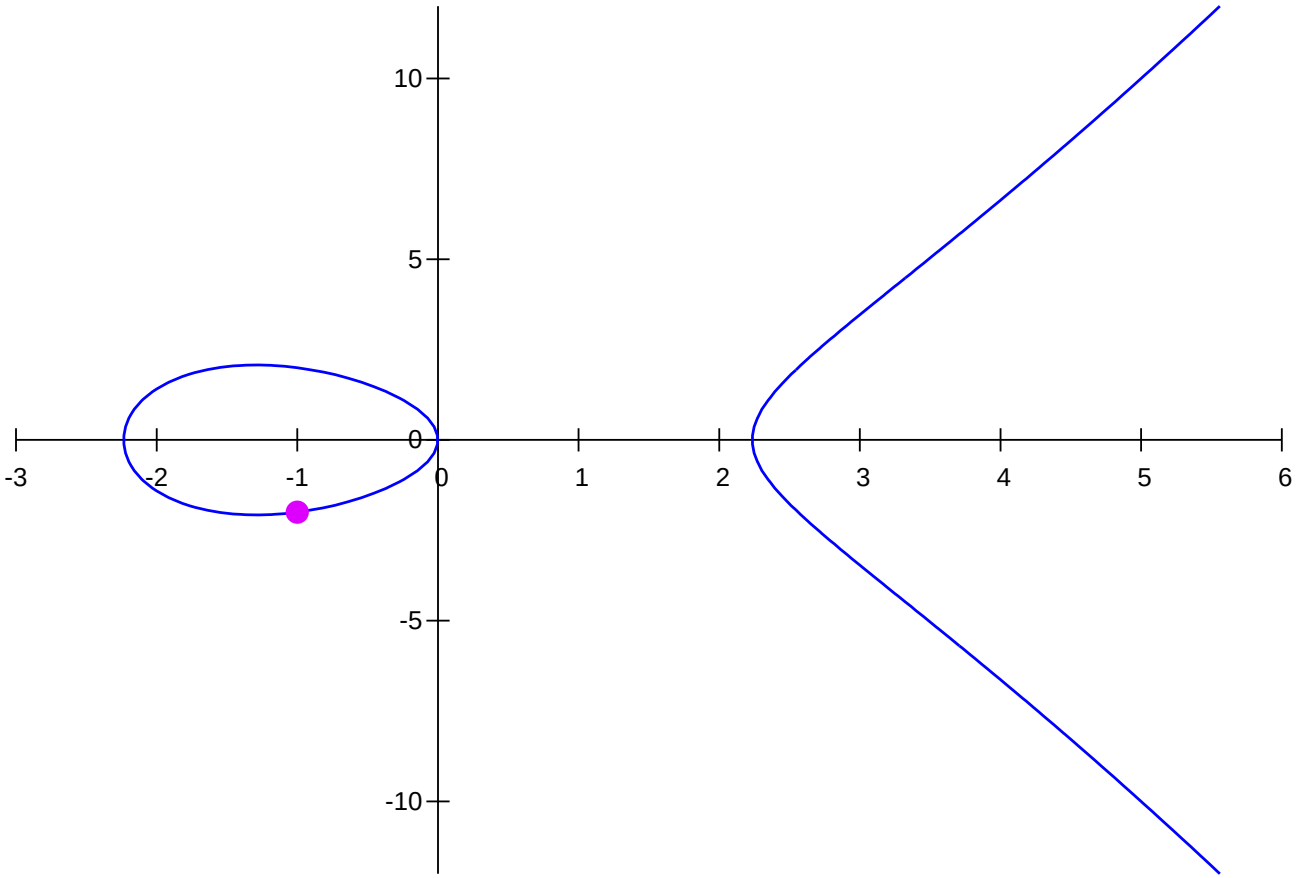
- Need to count multiplicities
- If one of the points is ∞, the line is "vertical"

Motto: "Any three collinear points on E sum to zero"

AKA **Chord & Tangent Addition Law**

Arithmetic on E — Inverses

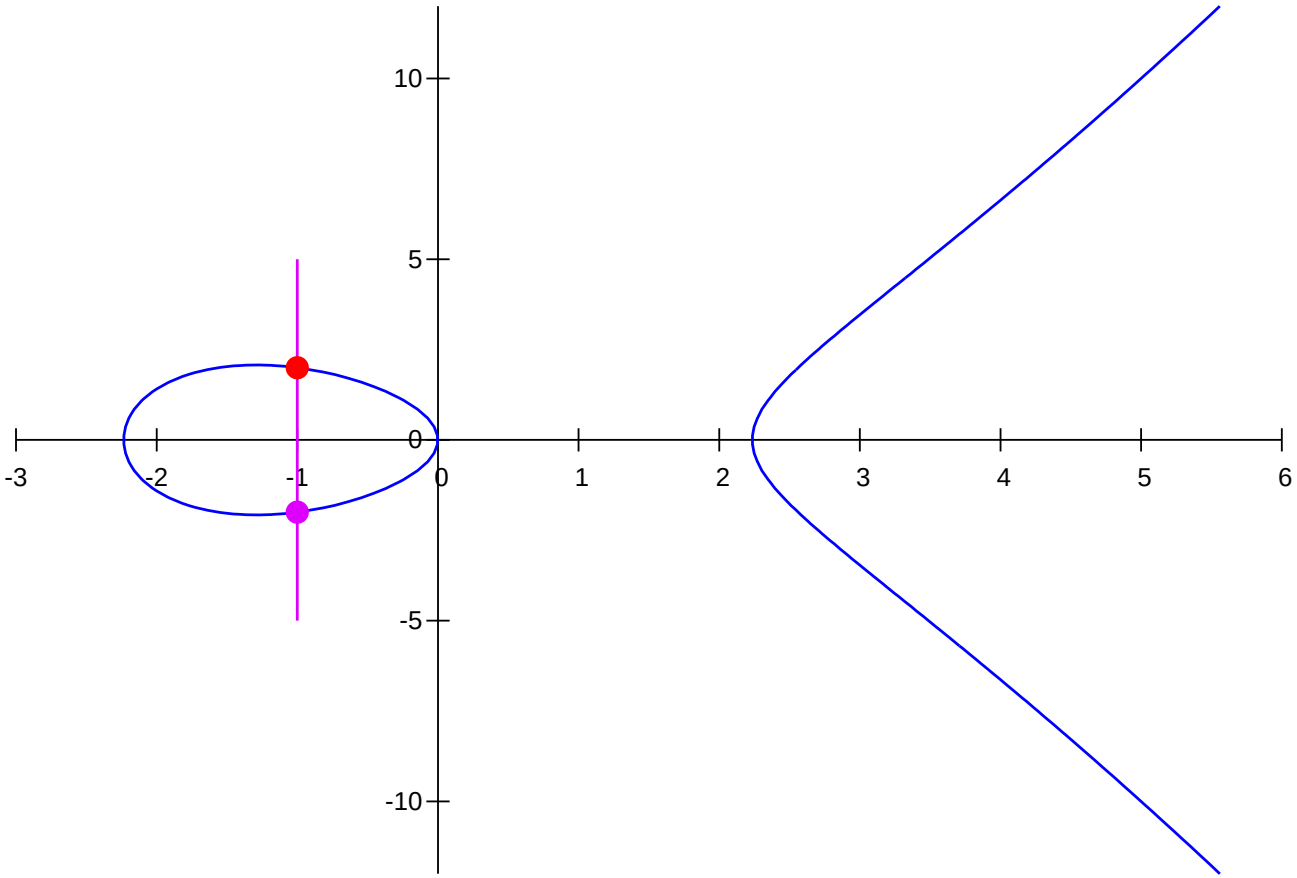
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P = (-1, -2)$



The line through P and ∞ is $\boxed{x = -1}$

Arithmetic on E — Inverses

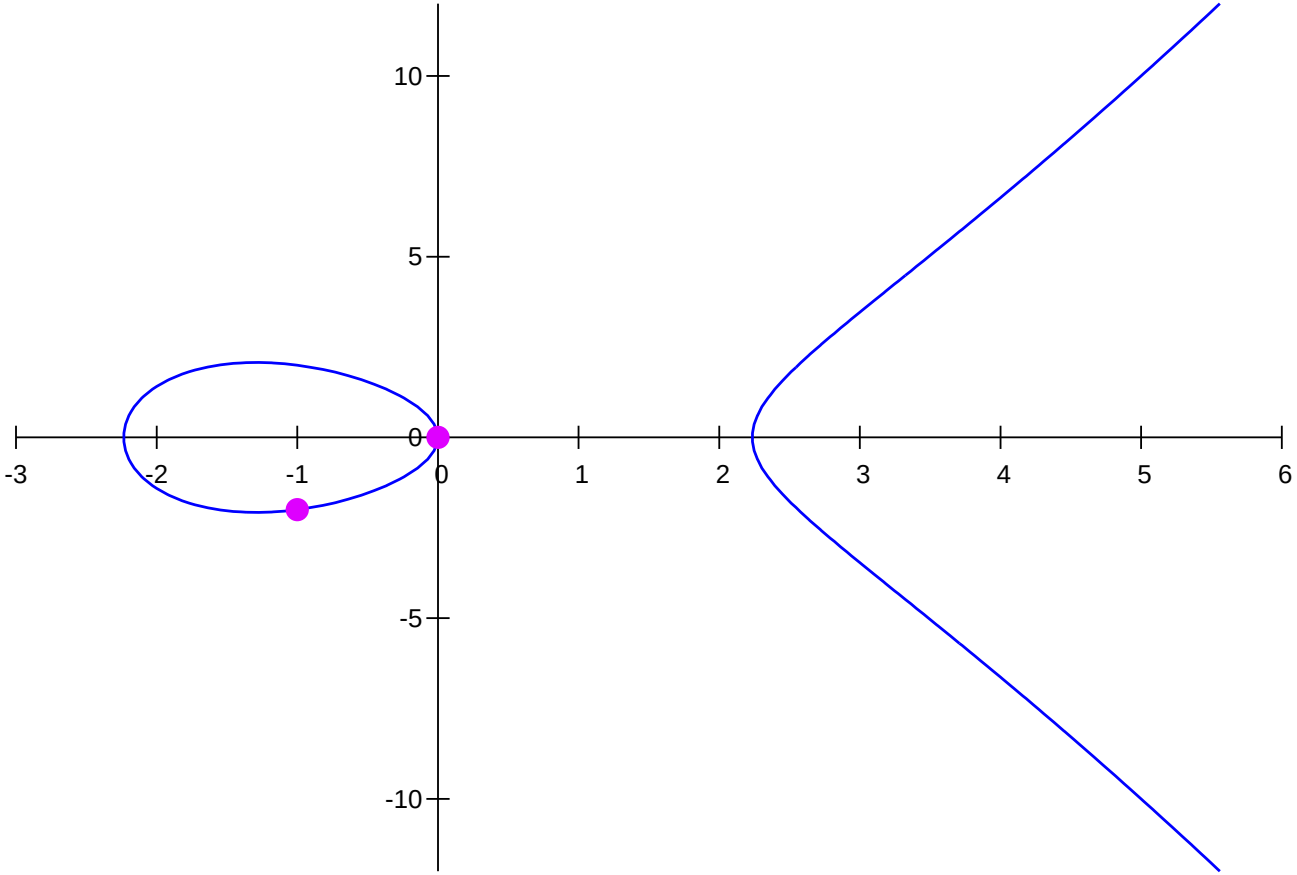
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P = (-1, -2)$



It intersects E in the third point $R = (-1, 2) = -P$

Arithmetic on E — Addition

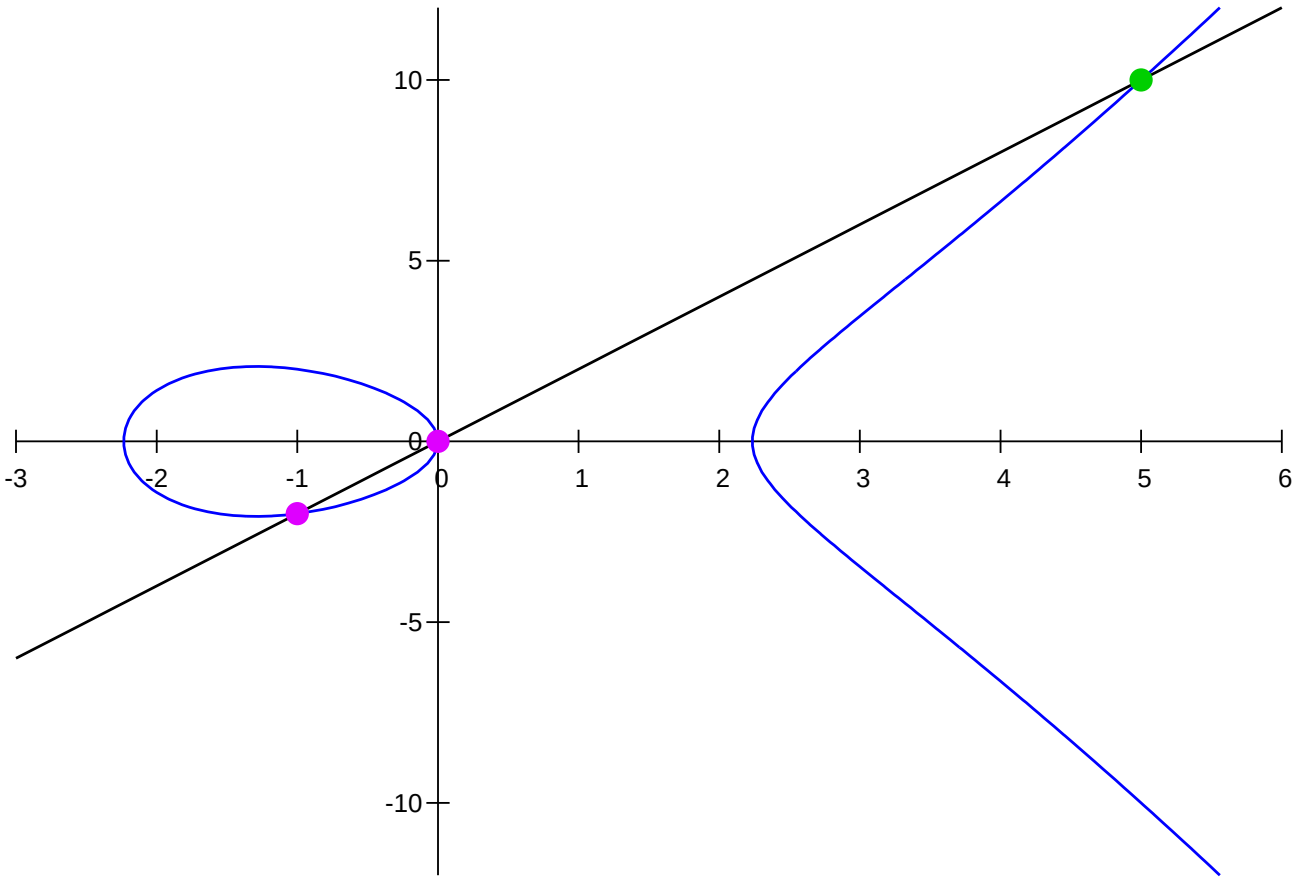
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P_1 = (-1, -2)$, $P_2 = (0, 0)$



The line through P_1 and P_2 is $\boxed{y = 2x}$

Arithmetic on E — Addition

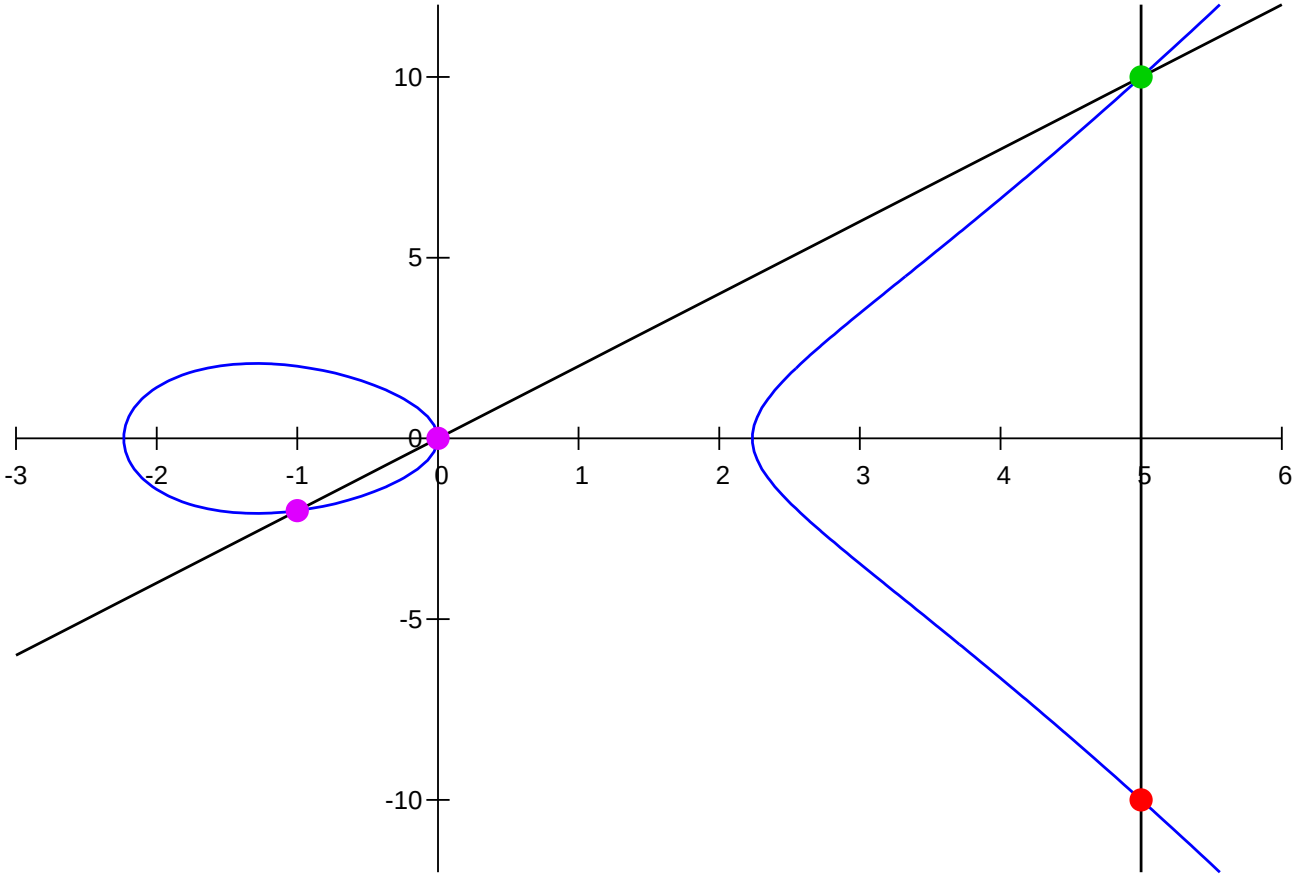
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P_1 = (-1, -2)$, $P_2 = (0, 0)$



It intersects E in the third point $G = (5, 10)$

Arithmetic on E — Addition

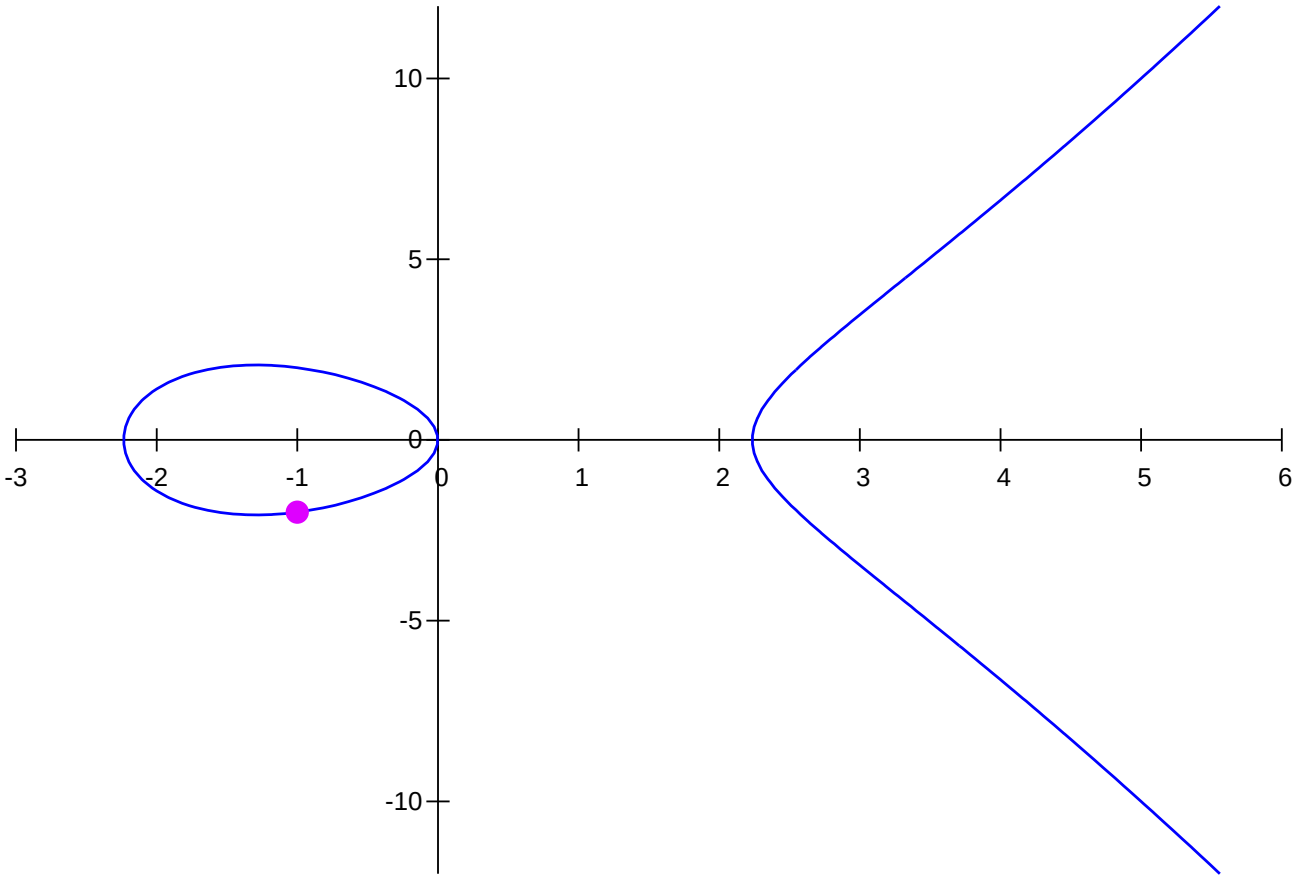
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P_1 = (-1, -2)$, $P_2 = (0, 0)$



The sum R is the inverse of G, i.e. $R = -G = (5, -10) = P + Q$

Arithmetic on E — Doubling

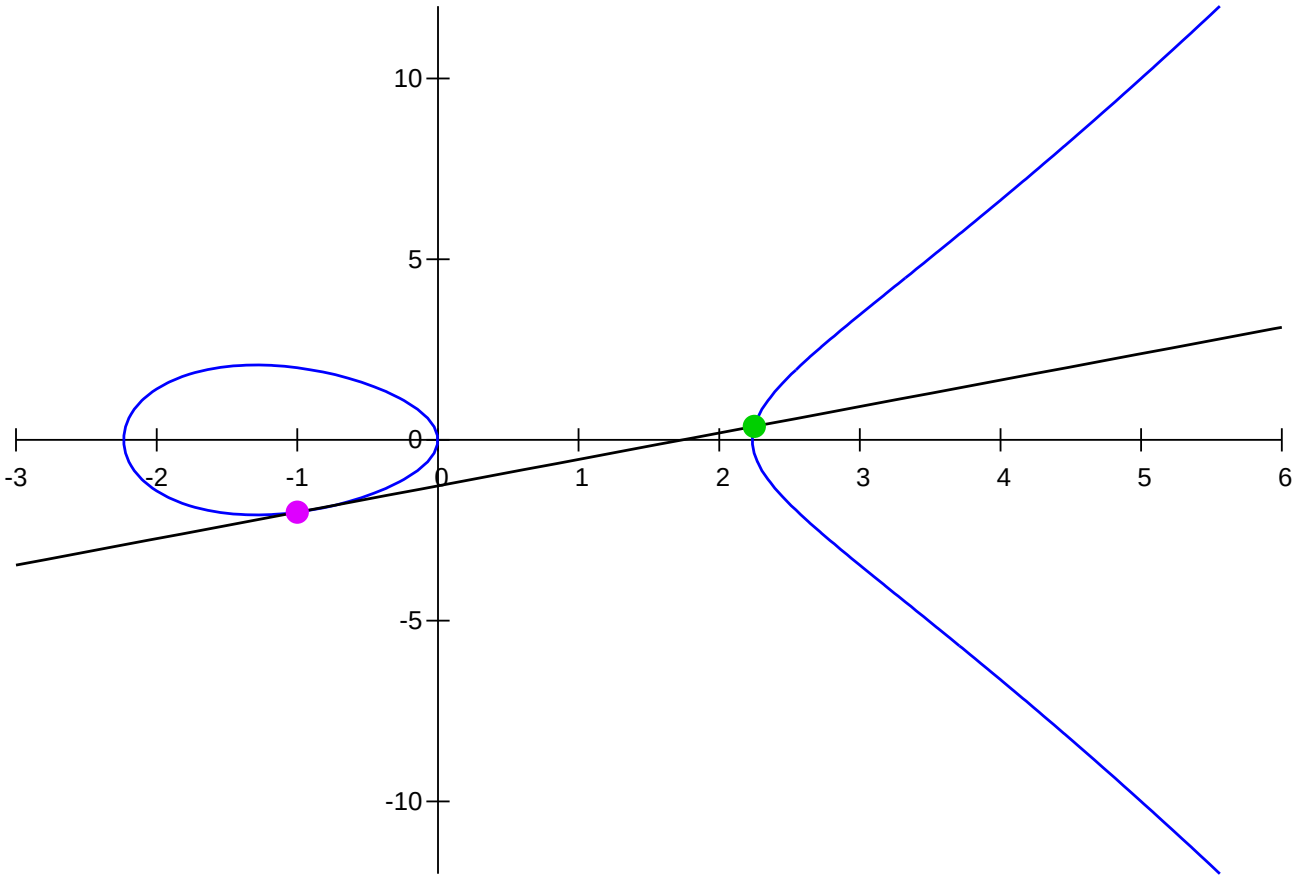
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P = (-1, -2)$



The line tangent to E at P is $\boxed{y = \frac{19}{26}x - \frac{33}{26}}$

Arithmetic on E — Doubling

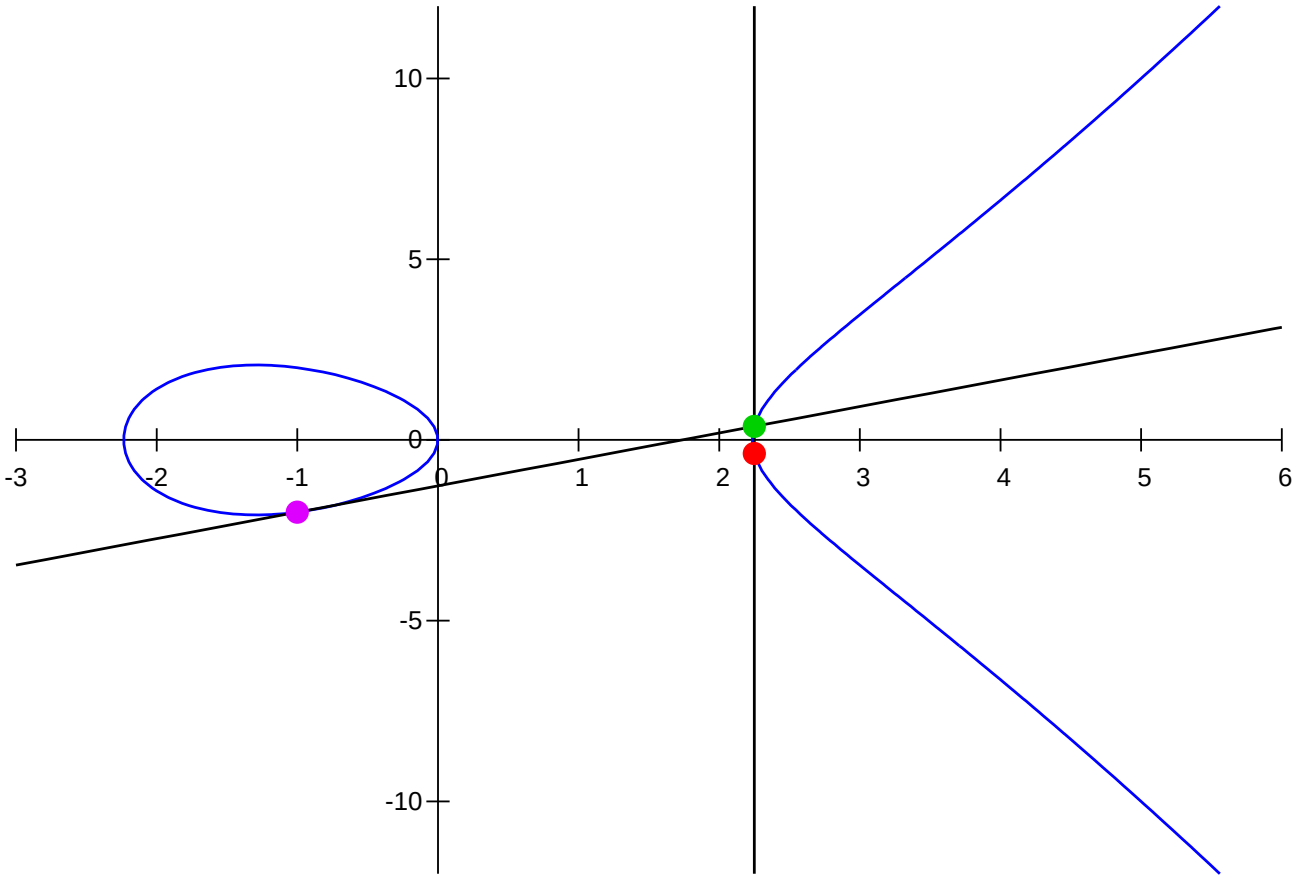
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P = (-1, -2)$



It intersects E in the third point $G = \left(\frac{9}{4}, \frac{3}{8}\right)$

Arithmetic on E — Doubling

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $P = (-1, -2)$



The sum R is the inverse of G, i.e. $R = -G = \left(\frac{9}{4}, -\frac{3}{8}\right) = 2P$

Arithmetic on Short Weierstraß Form — Summary

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2) \qquad (P_1 \neq -P_2;\ P_1, P_2 \neq \infty)$$

$$-P_1 = (-x_1, y_1)$$

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2,\ -\lambda^3 + \lambda(x_1 + x_2) - \mu) \text{ where}$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

$$\mu = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\[2ex] \dfrac{-x_1^3 + A x_1 + 2B}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

Beyond Elliptic Curves

Recall Weierstraß equation:

$$E \ : \ y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}$$

$\deg(f) = 3 = 2 \cdot 1 + 1$ odd

$\deg(h) = 1$ for $\mathrm{char}(K) = 2$; $h = 0$ for $\mathrm{char}(K) \neq 2$

Beyond Elliptic Curves

Recall Weierstraß equation:

$$E \ : \ y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}$$

$\deg(f) = 3 = 2 \cdot 1 + 1$ odd

$\deg(h) = 1$ for $\mathrm{char}(K) = 2$; $h = 0$ for $\mathrm{char}(K) \neq 2$

Generalization: $\deg(f) = 2g + 1, \ \ \deg(h) \leq g$

g is the **genus** of the curve

Beyond Elliptic Curves

Recall Weierstraß equation:

$$E \ : \ y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}$$

$\deg(f) = 3 = 2 \cdot 1 + 1$ odd

$\deg(h) = 1$ for $\mathrm{char}(K) = 2$; $h = 0$ for $\mathrm{char}(K) \neq 2$

Generalization: $\deg(f) = 2g + 1, \ \deg(h) \leq g$

g is the **genus** of the curve

$g = 1$: elliptic curves

$g = 2$: $\deg(f) = 5$, $\deg(h) \leq 2$ — also good for crypto

Hyperelliptic Curves

Hyperelliptic curve of genus g over K:

$$H \ : \ y^2 + h(x)y = f(x)$$

- $h(x), f(x) \in K[x]$
- $f(x)$ monic and $\deg(f) = 2g + 1$ is odd
- $\deg(h) \leq g$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- non-singularity

Hyperelliptic Curves

Hyperelliptic curve of genus g over K:

$$H \ : \ y^2 + h(x)y = f(x)$$

- $h(x), f(x) \in K[x]$
- $f(x)$ monic and $\deg(f) = 2g + 1$ is odd
- $\deg(h) \leq g$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- non-singularity

$\mathrm{char}(K) \neq 2$: $\boxed{y^2 = f(x),}$ $f(x)$ monic, of odd degree, square-free

Hyperelliptic Curves

Hyperelliptic curve of genus g over K:

$$H \ : \ y^2 + h(x)y = f(x)$$

- $h(x), f(x) \in K[x]$
- $f(x)$ monic and $\deg(f) = 2g + 1$ is odd
- $\deg(h) \leq g$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- non-singularity

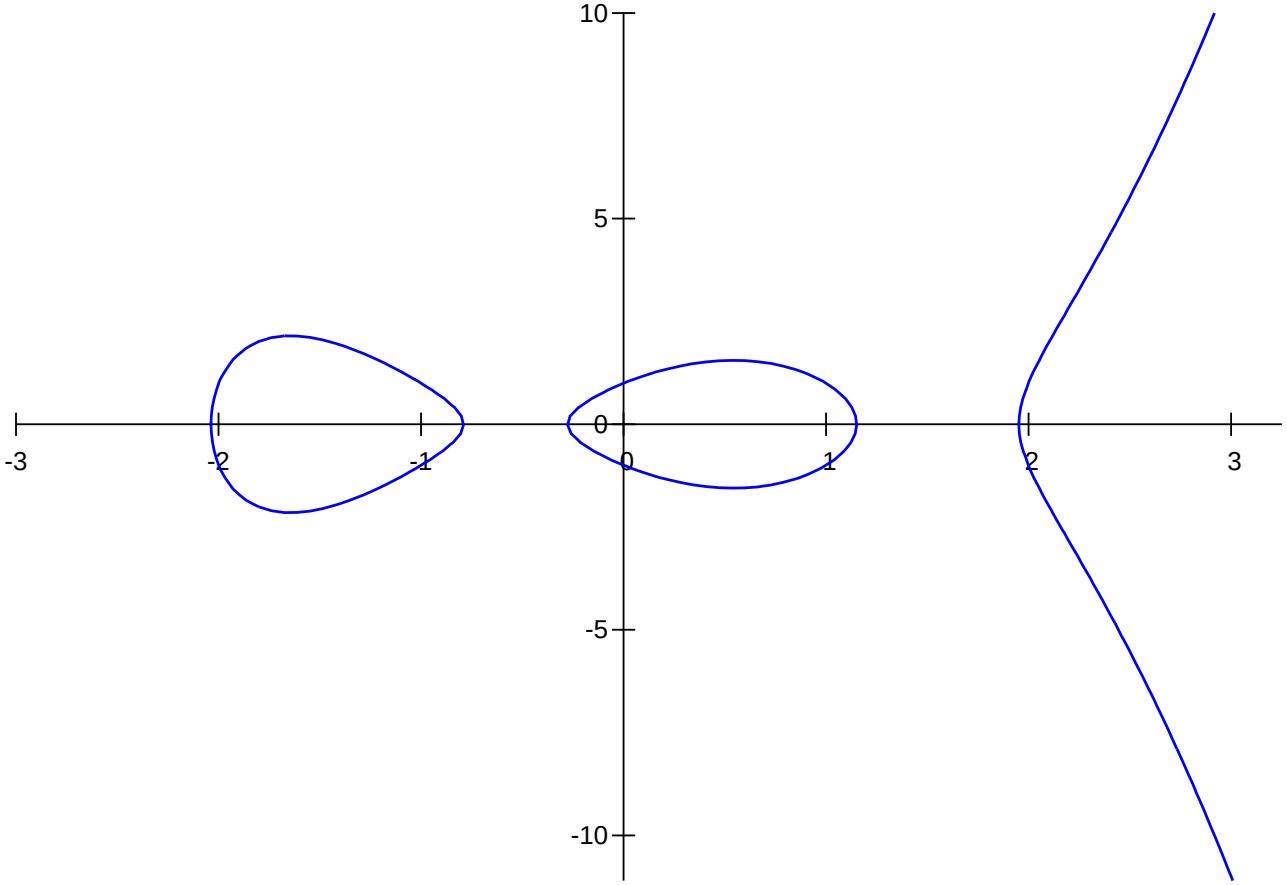
$\mathrm{char}(K) \neq 2$: $\boxed{y^2 = f(x),}$ $f(x)$ monic, of odd degree, square-free

Set of L-**rational** points on H ($K \subseteq L \subseteq \overline{K}$):

$$H(L) \ = \ \{(x_0, y_0) \in L \times L \mid y_0^2 + h(x_0)y = f(x_0)\} \cup \{\infty\}$$

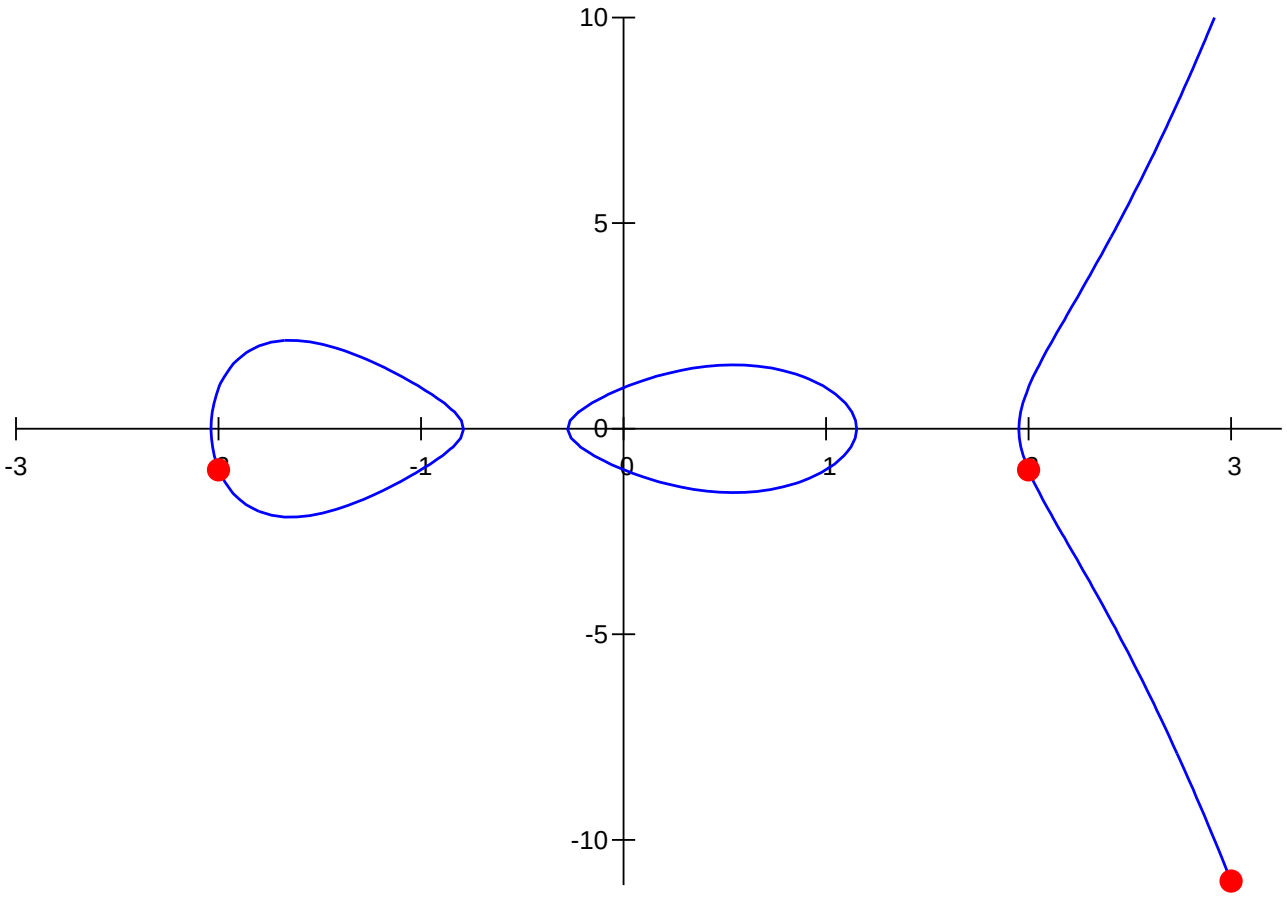
An Example

$H : y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, genus $g = 2$



An Example

$(-2,-1),\ (2,-1),\ (3,-11)\ \in\ H(\mathbb{Q})$



Divisors

- Group of **divisors** on H:

$$\mathrm{Div}_H(\overline{K}) = \langle H(\overline{K}) \rangle = \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z},\ P \in H(\overline{K}) \right\}$$

Divisors

- Group of **divisors** on H:

$$\mathrm{Div}_H(\overline{K}) = \langle H(\overline{K}) \rangle = \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z},\ P \in H(\overline{K}) \right\}$$

- Subgroup of $\mathrm{Div}_H(\overline{K})$ of **degree zero divisors** on H:

$$\mathrm{Div}_H^0(\overline{K}) = \langle [P] \mid P \in H(\overline{K}) \rangle = \left\{ \sum_{\text{finite}} m_P [P] \mid m_P \in \mathbb{Z},\ P \in H(\overline{K}) \right\}$$

where $[P] = P - \infty$

Divisors

- Group of **divisors** on H:

$$\mathrm{Div}_H(\overline{K}) = \langle H(\overline{K}) \rangle = \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z},\ P \in H(\overline{K}) \right\}$$

- Subgroup of $\mathrm{Div}_H(\overline{K})$ of **degree zero divisors** on H:

$$\mathrm{Div}_H^0(\overline{K}) = \langle [P] \mid P \in H(\overline{K}) \rangle = \left\{ \sum_{\text{finite}} m_P [P] \mid m_P \in \mathbb{Z},\ P \in H(\overline{K}) \right\}$$

where $[P] = P - \infty$

- Subgroup of $\mathrm{Div}_H^0(\overline{K})$ of **principal divisors** on H:

$$\mathrm{Prin}_H(\overline{K}) = \left\{ \sum_{\text{finite}} v_P(\alpha)[P] \mid \alpha \in K(x,y),\ P \in H(\overline{K}) \right\}$$

The Jacobian

Jacobian of H: $\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}^0_H(\overline{K})/\mathrm{Prin}_H(\overline{K})$

Motto: "Any complete collection of points on a function sums to zero"

The Jacobian

Jacobian of H: $\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}_H^0(\overline{K})/\mathrm{Prin}_H(\overline{K})$

Motto: "Any complete collection of points on a function sums to zero"

$$H(\overline{K}) \hookrightarrow \mathrm{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P]$$

The Jacobian

Jacobian of H: $\boxed{\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}_H^0(\overline{K})/\mathrm{Prin}_H(\overline{K})}$

Motto: "Any complete collection of points on a function sums to zero"

$$H(\overline{K}) \hookrightarrow \mathrm{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P]$$

For elliptic curves: $E(\overline{K}) \cong \mathrm{Jac}_E(\overline{K})$ $\quad (\Rightarrow\ E(\overline{K})$ is a group$)$

The Jacobian

Jacobian of H: $\boxed{\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}_H^0(\overline{K})/\mathrm{Prin}_H(\overline{K})}$

Motto: "Any complete collection of points on a function sums to zero"

$$H(\overline{K}) \hookrightarrow \mathrm{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P]$$

For elliptic curves: $E(\overline{K}) \cong \mathrm{Jac}_E(\overline{K})$ $\quad (\Rightarrow\ E(\overline{K})$ is a group$)$

Identity: $[\infty] = \infty - \infty$

The Jacobian

Jacobian of H: $\boxed{\mathrm{Jac}_H(\overline{K}) = \mathrm{Div}_H^0(\overline{K})/\mathrm{Prin}_H(\overline{K})}$

Motto: "Any complete collection of points on a function sums to zero"

$$H(\overline{K}) \hookrightarrow \mathrm{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P]$$

For elliptic curves: $E(\overline{K}) \cong \mathrm{Jac}_E(\overline{K}) \quad (\Rightarrow \; E(\overline{K})$ is a group)

Identity: $[\infty] = \infty - \infty$

Inverses: The points

$$P = (x_0, y_0) \quad \text{and} \quad \overline{P} = (x_0, -y_0 - h(x_0))$$

on H both lie on the function $x = x_0$, so

$$-[P] = [\overline{P}]$$

Semi-Reduced and Reduced Divisors

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of P, $\overline{P}$ can appear in the sum (as $[P] + [\overline{P}] = 0$)

Semi-Reduced and Reduced Divisors

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of P, $\overline{P}$ can appear in the sum (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**.

Semi-Reduced and Reduced Divisors

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of P, $\overline{P}$ can appear in the sum (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**. If $\sum m_P \leq g$, then it is **reduced**.

Semi-Reduced and Reduced Divisors

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of P, $\overline{P}$ can appear in the sum (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**. If $\sum m_P \leq g$, then it is **reduced**.

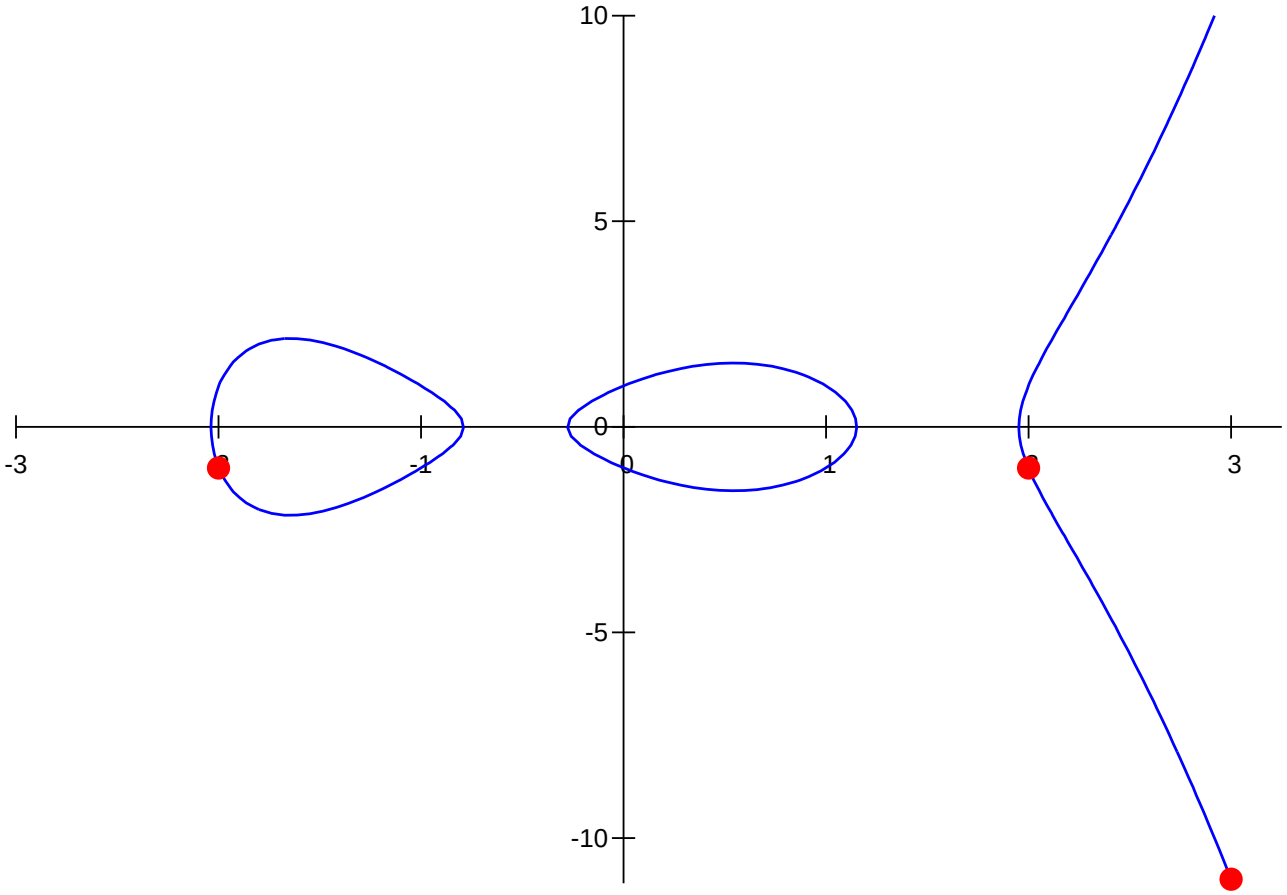
Theorem

Every class in $\mathrm{Jac}_H(\overline{K})$ contains a unique reduced divisor.

Example — Reduction

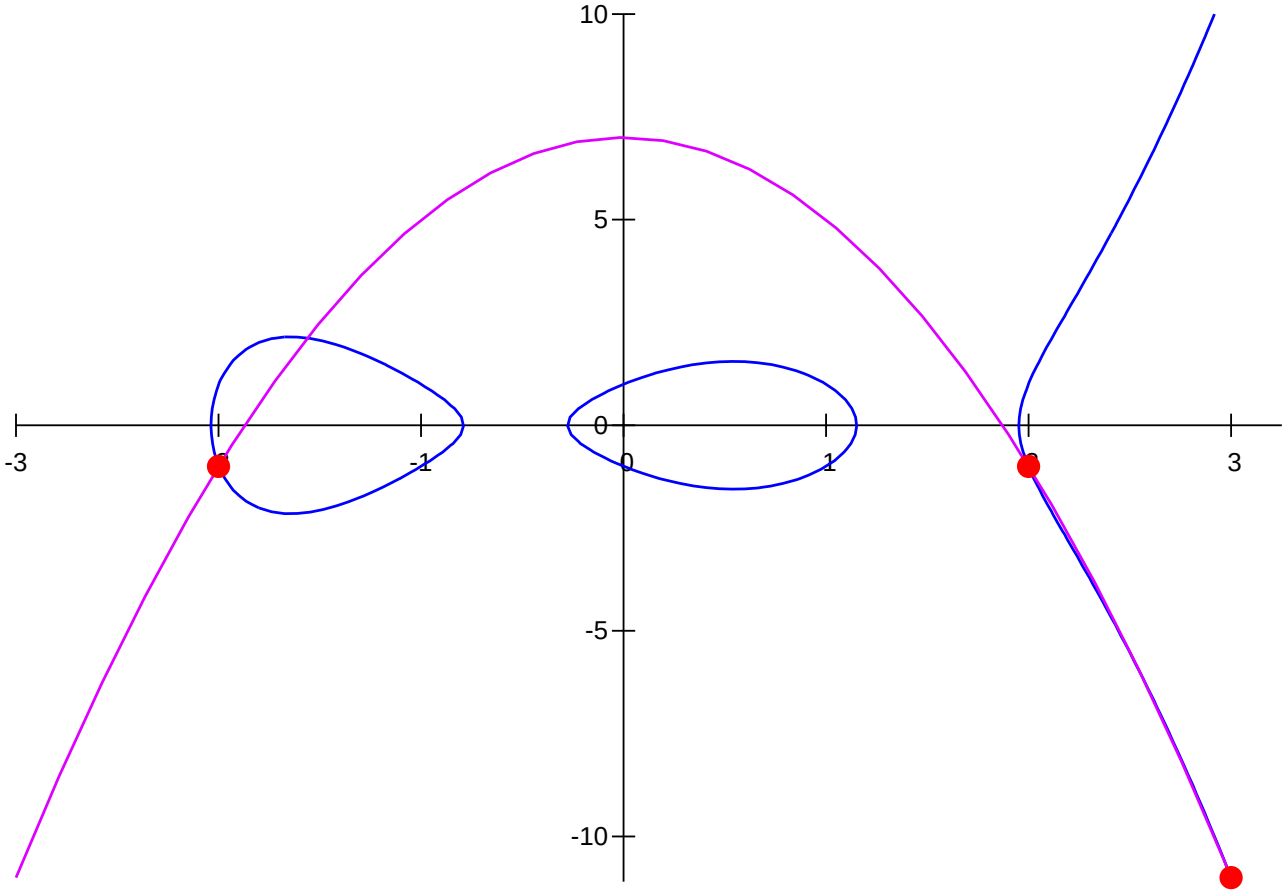
$H : y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, $D = [R_1] + [R_2] + [R_3]$ with

$R_1 = (-2, -1)$, $R_2 = (2, -1)$, $R_3 = (3, -11)$



Example — Reduction

R_1, R_2, R_3 all lie on the quadratic $y = -2x^2 + 7$

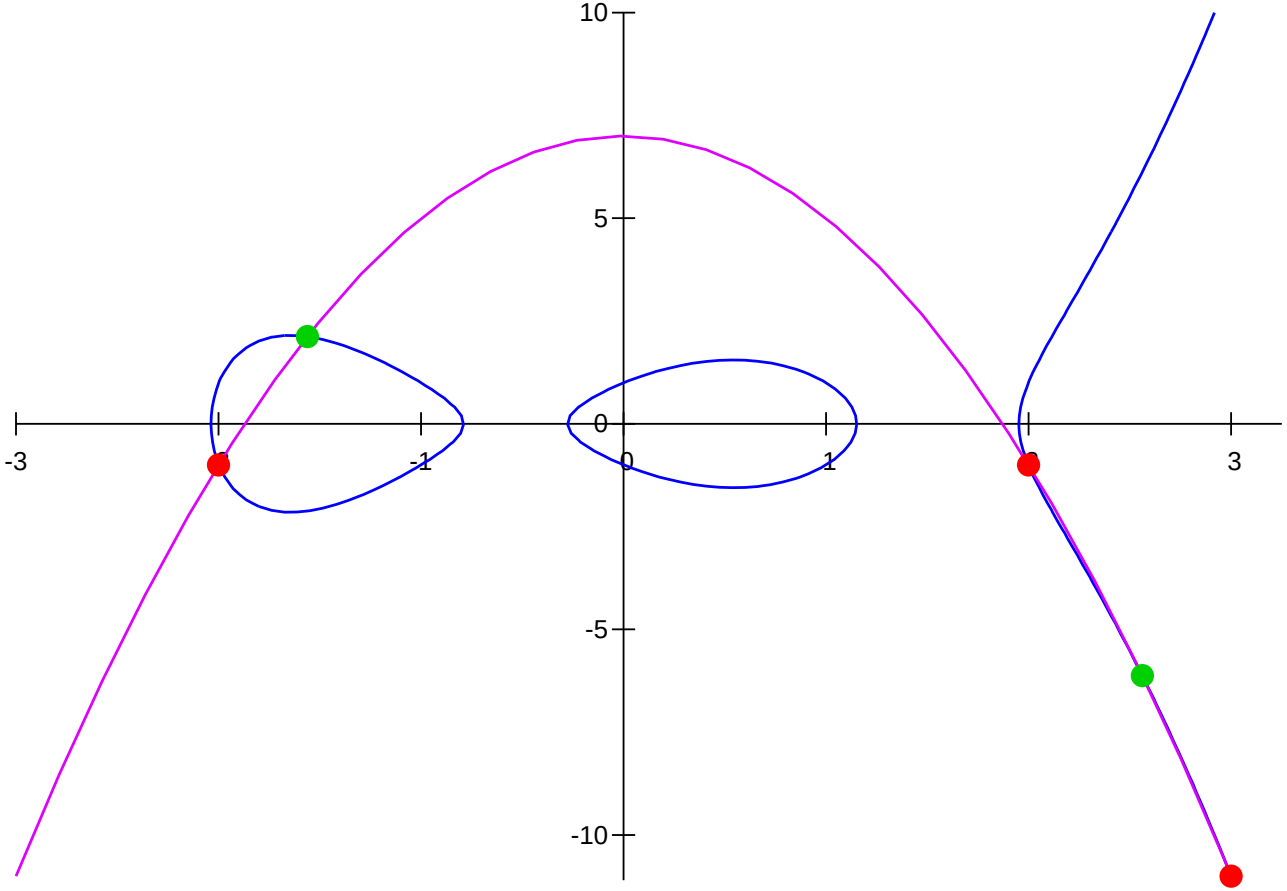


Example — Reduction

This quadratic meets H in the two additional points G_1, G_2 where

$$G_1 = \left(\tfrac{1}{2}(1+\sqrt{17}), -2-\sqrt{17}\right), \quad G_2 = \left(\tfrac{1}{2}(1-\sqrt{17}), -2+\sqrt{17}\right)$$

Thus, $[R_1] + [R_2] + R_3] + [G_1] + [G_2] = 0$ in $\mathrm{Jac}_H(\mathbb{Q})$

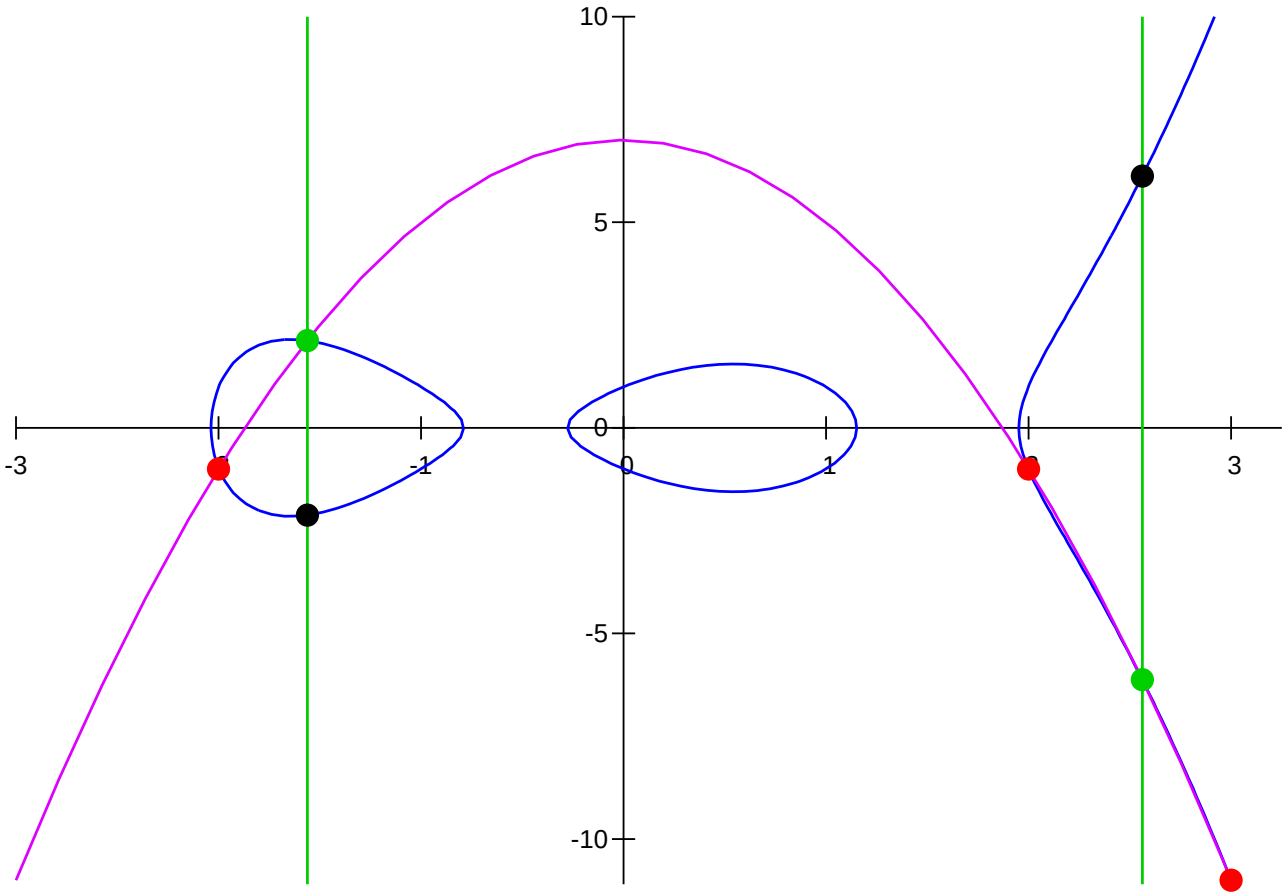


Example — Reduction

$[R_1] + [R_2] + R_3] = [B_1] + [B_2]$ with $B_1 = [\overline{G_1}]$, $B_2 = [\overline{G_2}]$

The reduced divisor in the class of D is $E = [B_1] + B_2]$ where

$B_1 = \left(\frac{1}{2}(1+\sqrt{17}), 2+\sqrt{17}\right)$, $B_2 = \left(\frac{1}{2}(1-\sqrt{17}), 2-\sqrt{17}\right)$,



Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The r points P_i all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The r points P_i all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

$v(x)^2 + h(x)h(x) = f(x)$ polynomial of degree $\max\{2r - 2, 2g + 1\}$

Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The r points P_i all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

$v(x)^2 + h(x)h(x) = f(x)$ polynomial of degree $\max\{2r - 2, 2g + 1\}$

Case $r \geq g + 2$: replace the r points $P_1, \ldots, P_r$ in D by the inverses of the other $(2r - 2) - r = r - 2$ points on this degree $2r - 2$ polynomial

Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The r points P_i all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

$v(x)^2 + h(x)h(x) = f(x)$ polynomial of degree $\max\{2r - 2, 2g + 1\}$

Case $r \geq g + 2$: replace the r points $P_1, \ldots, P_r$ in D by the inverses of the other $(2r - 2) - r = r - 2$ points on this degree $2r - 2$ polynomial

Case $r = g + 1$: replace the $g + 1$ points $P_1, \ldots, P_r$ in D by the inverses of the other $2g + 1 - (g + 1) = g$ points on this degree $2g + 2$ polynomial

Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The r points P_i all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

$v(x)^2 + h(x)h(x) = f(x)$ polynomial of degree $\max\{2r - 2, 2g + 1\}$

Case $r \geq g + 2$: replace the r points $P_1, \ldots, P_r$ in D by the inverses of the other $(2r - 2) - r = r - 2$ points on this degree $2r - 2$ polynomial

Case $r = g + 1$: replace the $g + 1$ points $P_1, \ldots, P_r$ in D by the inverses of the other $2g + 1 - (g + 1) = g$ points on this degree $2g + 2$ polynomial

After $\left\lceil \frac{r - g}{2} \right\rceil$ steps a reduced divisor is obtained ☺

Mumford Representation

Let $D = \sum_{i=1}^{r} m_i[P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$

The **Mumford representation** of D is $D = (u(x), v(x))$ where

$$u(x), v(x) \in \overline{K}[x], \quad u \text{ monic}, \quad \deg(v) < \deg(u), \quad u \mid v^2 + hv - f$$

Mumford Representation

Let $D = \sum_{i=1}^{r} m_i[P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$

The **Mumford representation** of D is $D = (u(x), v(x))$ where

$$u(x), v(x) \in \overline{K}[x], \quad u \text{ monic}, \quad \deg(v) < \deg(u), \quad u \mid v^2 + hv - f$$

$$u(x) = \prod_{i=1}^{r} (x - x_i)^{m_i}$$

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{x=x_i} = 0 \qquad (0 \le j \le m_i - 1)$$

So $u(x_i) = 0$ and $v(x_i) = y_i$ with multiplicity m_i for $1 \le i \le r$

Mumford Representation

Let $D = \sum_{i=1}^{r} m_i[P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$

The **Mumford representation** of D is $D = (u(x), v(x))$ where

$$u(x), v(x) \in \overline{K}[x], \quad u \text{ monic}, \quad \deg(v) < \deg(u), \quad u \mid v^2 + hv - f$$

$$u(x) = \prod_{i=1}^{r} (x - x_i)^{m_i}$$

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{x=x_i} = 0 \qquad (0 \le j \le m_i - 1)$$

So $u(x_i) = 0$ and $v(x_i) = y_i$ with multiplicity m_i for $1 \le i \le r$

Mumford representation uniquely determines D

Mumford Representation

Let $D = \sum_{i=1}^{r} m_i[P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$

The **Mumford representation** of D is $D = (u(x), v(x))$ where

$$u(x), v(x) \in \overline{K}[x], \quad u \text{ monic}, \quad \deg(v) < \deg(u), \quad u \mid v^2 + hv - f$$

$$u(x) = \prod_{i=1}^{r} (x - x_i)^{m_i}$$

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{x=x_i} = 0 \qquad (0 \le j \le m_i - 1)$$

So $u(x_i) = 0$ and $v(x_i) = y_i$ with multiplicity m_i for $1 \le i \le r$

Mumford representation uniquely determines D

Example: If $P = (x_0, y_0)$, then $D = [P] = (x - x_0, y_0)$

Divisor Reduction Using Mumford Representations

Input: $D = (u, v)$

Output: The reduced divisor $D' = (u', v')$ in the class of D

Divisor Reduction Using Mumford Representations

Input: $D = (u, v)$

Output: The reduced divisor $D' = (u', v')$ in the class of D

while $\deg(u) > g$ *do*

$$u' = \frac{f - vh - v^2}{u}, \quad v' \equiv -v - h \pmod{u'}$$

$$u = u', \quad v = v'$$

end while

return(u', v')

Divisor Reduction — Example

$H \ : \ y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$

$D = [(-2, -1)] + [(2, 1)] + [(3, -11)] = (u, v)$

Divisor Reduction — Example

$H \ : \ y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$

$D = [(-2,-1)] + [(2,1)] + [(3,-11)] = (u,v)$ with

$$\begin{aligned} u(x) &= (x+2)(x-2)(x-3) = x^3 - 3x^2 - 4x + 2 \\ v(x) &= -2x^2 + 7 \quad \text{(from before)} \end{aligned}$$

Divisor Reduction — Example

$H \ : \ y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$

$D = [(-2,-1)] + [(2,1)] + [(3,-11)] = (u,v)$ with

$$\begin{aligned} u(x) &= (x+2)(x-2)(x-3) = x^3 - 3x^2 - 4x + 2 \\ v(x) &= -2x^2 + 7 \quad \text{(from before)} \end{aligned}$$

$$\begin{aligned} u'(x) &= \frac{(x^5 - 5x^3 + 4x - 1) - (-2x^2 + 7)^2}{x^3 - 3x^2 - 4x + 2} = x^2 - x - 4 \\ v'(x) &\equiv -(-2x^2 + 7) \pmod{x^2 - x - 4} = 2x + 1 \end{aligned}$$

$D' = (u', v')$ is the reduced divisor in the class of D

Divisor Reduction — Example

$H \ : \ y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$

$D = [(-2,-1)] + [(2,1)] + [(3,-11)] = (u,v)$ with

$$\begin{aligned} u(x) &= (x+2)(x-2)(x-3) = x^3 - 3x^2 - 4x + 2 \\ v(x) &= -2x^2 + 7 \quad \text{(from before)} \end{aligned}$$

$$\begin{aligned} u'(x) &= \frac{(x^5 - 5x^3 + 4x - 1) - (-2x^2 + 7)^2}{x^3 - 3x^2 - 4x + 2} = x^2 - x - 4 \\ v'(x) &\equiv -(-2x^2 + 7) \pmod{x^2 - x - 4} = 2x + 1 \end{aligned}$$

$D' = (u', v')$ is the reduced divisor in the class of D

Recall $D' = \left[\left(\frac{1}{2}(1+\sqrt{17}),\, 2+\sqrt{17}\right)\right] + \left[\left(\frac{1}{2}(1-\sqrt{17}),\, 2-\sqrt{17}\right)\right]$

Divisor Addition Using Mumford Representations

$D_1 = (u_1, v_1),\ D_2 = (u_2, v_2)$ divisors on $H : y^2 + h(x)y = f(x)$

Divisor Addition Using Mumford Representations

$D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ divisors on $H : y^2 + h(x)y = f(x)$

Simplest case: for any $[P]$ occurring in D_1, $[\overline{P}]$ does not occur in D_2 and vice versa — then $D_1 + D_2$ is semi-reduced

Divisor Addition Using Mumford Representations

$D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ divisors on $H : y^2 + h(x)y = f(x)$

Simplest case: for any $[P]$ occurring in D_1, $[\overline{P}]$ does not occur in D_2 and vice versa — then $D_1 + D_2$ is semi-reduced

Then $D_1 + D_2 = (u, v)$ where $u = u_1 u_2$ and $v = \begin{cases} v_1 \pmod{u_1} \\ v_2 \pmod{u_2} \end{cases}$

Divisor Addition Using Mumford Representations

$D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ divisors on $H : y^2 + h(x)y = f(x)$

Simplest case: for any $[P]$ occurring in D_1, $[\overline{P}]$ does not occur in D_2 and vice versa — then $D_1 + D_2$ is semi-reduced

Then $D_1 + D_2 = (u, v)$ where $u = u_1 u_2$ and $v = \begin{cases} v_1 \pmod{u_1} \\ v_2 \pmod{u_2} \end{cases}$

In general: suppose $P = (x_0, y_0)$ occurs in D_1 and $\overline{P}$ occurs in D_2.

Divisor Addition Using Mumford Representations

$D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ divisors on $H : y^2 + h(x)y = f(x)$

Simplest case: for any $[P]$ occurring in D_1, $[\overline{P}]$ does not occur in D_2 and vice versa — then $D_1 + D_2$ is semi-reduced

Then $D_1 + D_2 = (u, v)$ where $u = u_1 u_2$ and $v = \begin{cases} v_1 \pmod{u_1} \\ v_2 \pmod{u_2} \end{cases}$

In general: suppose $P = (x_0, y_0)$ occurs in D_1 and $\overline{P}$ occurs in D_2.

Then $u_1(x_0) = u_2(x_0) = 0$ and $v_1(x_0) = y_0 = -v_2(x_0) - h(x_0)$, so $x - x_0 \mid u_1(x),\ u_2(x),\ v_1(x) + v_2(x) + h(x)$

Divisor Addition Using Mumford Representations

$D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ divisors on $H : y^2 + h(x)y = f(x)$

Simplest case: for any $[P]$ occurring in D_1, $[\overline{P}]$ does not occur in D_2 and vice versa — then $D_1 + D_2$ is semi-reduced

Then $D_1 + D_2 = (u, v)$ where $u = u_1 u_2$ and $v = \begin{cases} v_1 \pmod{u_1} \\ v_2 \pmod{u_2} \end{cases}$

In general: suppose $P = (x_0, y_0)$ occurs in D_1 and $\overline{P}$ occurs in D_2.

Then $u_1(x_0) = u_2(x_0) = 0$ and $v_1(x_0) = y_0 = -v_2(x_0) - h(x_0)$, so $x - x_0 \mid u_1(x),\ u_2(x),\ v_1(x) + v_2(x) + h(x)$

$$d = \gcd(u_1, u_2, v_1 + v_2 + h) = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h)$$
$$u = \frac{u_1 u_2}{d^2}$$
$$v \equiv \frac{1}{d}\big(s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)\big) \pmod{u}$$

(In the simplest case above, $d = 1$ and $s_3 = 0$)

Arithmetic in $\mathrm{Jac}_H(\overline{K})$

Input: $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ reduced

Output: The reduced divisor $D' = (u', v')$ in the class of $D_1 + D_2$

Arithmetic in $\mathrm{Jac}_H(\overline{K})$

Input: $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ reduced

Output: The reduced divisor $D' = (u', v')$ in the class of $D_1 + D_2$

1. Addition: compute a semi-reduced divisor $D = (u, v)$ in the class of $D_1 + D_2$
2. Reduction: compute the reduced divisor $D' = (u', v')$ in the class of D

Arithmetic in $\mathrm{Jac}_H(\overline{K})$

Input: $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ reduced

Output: The reduced divisor $D' = (u', v')$ in the class of $D_1 + D_2$

1. Addition: compute a semi-reduced divisor $D = (u, v)$ in the class of $D_1 + D_2$
2. Reduction: compute the reduced divisor $D' = (u', v')$ in the class of D

Methods

- "Vanilla" method just discussed
- Cantor's algorithm ("improved vanilla")
- NUCOMP
- Explicit formulas (if g is small, say $g = 2, 3, 4$)

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

ϕ acts on points on H: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

ϕ acts on points on H: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$
ϕ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

ϕ acts on points on H: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$
ϕ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor D is **defined over** K if $\phi(D) = D$

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

ϕ acts on points on H: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$
ϕ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor D is **defined over** K if $\phi(D) = D$

Example:

$$\begin{aligned} D &= (x^2 - x - 4,\, 2x + 1) \quad \text{on } H : y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q} \\ &= \left[\left(\frac{1}{2}(1+\sqrt{17}),\, 2+\sqrt{17}\right)\right] + \left[\left(\frac{1}{2}(1-\sqrt{17}),\, 2-\sqrt{17}\right)\right] \end{aligned}$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{17} \mapsto -\sqrt{17}$)

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

ϕ acts on points on H: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$
ϕ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor D is **defined over** K if $\phi(D) = D$

Example:

$$\begin{aligned} D &= (x^2 - x - 4,\, 2x + 1) \quad \text{on } H : y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q} \\ &= \left[\left(\frac{1}{2}(1+\sqrt{17}),\, 2+\sqrt{17}\right)\right] + \left[\left(\frac{1}{2}(1-\sqrt{17}),\, 2-\sqrt{17}\right)\right] \end{aligned}$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{17} \mapsto -\sqrt{17}$)

Theorem

$D = (u, v)$ is defined over K if and only if $u(x), v(x) \in K[x]$.

Divisors defined over K

Let $\phi \in \mathrm{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

ϕ acts on points on H: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$
ϕ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor D is **defined over** K if $\phi(D) = D$

Example:

$$\begin{aligned} D &= (x^2 - x - 4,\, 2x + 1) \quad \text{on } H : y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q} \\ &= \left[\left(\frac{1}{2}(1+\sqrt{17}),\, 2+\sqrt{17}\right)\right] + \left[\left(\frac{1}{2}(1-\sqrt{17}),\, 2-\sqrt{17}\right)\right] \end{aligned}$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{17} \mapsto -\sqrt{17}$)

Theorem

$D = (u, v)$ is defined over K if and only if $u(x), v(x) \in K[x]$.

Corollary

The group $Jac_H(\mathbb{F}_q)$ of divisor classes defined over $\mathbb{F}_q$ is finite.

Group Structure and Size

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1)$$

Group Structure and Size

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1)$$

Via a hand-wavy argument, $y^2 = f(x)$ should have $\approx q + 1$ points

Group Structure and Size

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1)$$

Via a hand-wavy argument, $y^2 = f(x)$ should have $\approx q+1$ points

Hasse: $|E(\mathbb{F}_q)| = q + 1 - t$ with $|t| \leq 2\sqrt{q}$

Hasse-Weil: $|H(\mathbb{F}_q)| = q + 1 - t$ with $|t| \leq 2g\sqrt{q}$

Serre: $|t| \leq g\lfloor 2\sqrt{q} \rfloor$

Group Structure and Size

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1)$$

Via a hand-wavy argument, $y^2 = f(x)$ should have $\approx q+1$ points

Hasse: $|E(\mathbb{F}_q)| = q + 1 - t$ with $|t| \leq 2\sqrt{q}$

Hasse-Weil: $|H(\mathbb{F}_q)| = q + 1 - t$ with $|t| \leq 2g\sqrt{q}$

Serre: $|t| \leq g\lfloor 2\sqrt{q} \rfloor$

For the Jacobian:

$$(\sqrt{q} - 1)^{2g} \leq |\mathrm{Jac}_H(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g}$$

So $\boxed{|\mathrm{Jac}_H(\mathbb{F}_q)| \approx q^g}$

Group Structure and Size

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1)$$

Via a hand-wavy argument, $y^2 = f(x)$ should have $\approx q+1$ points

Hasse: $|E(\mathbb{F}_q)| = q + 1 - t$ with $|t| \leq 2\sqrt{q}$

Hasse-Weil: $|H(\mathbb{F}_q)| = q + 1 - t$ with $|t| \leq 2g\sqrt{q}$

Serre: $|t| \leq g\lfloor 2\sqrt{q} \rfloor$

For the Jacobian:

$$(\sqrt{q} - 1)^{2g} \leq |\mathrm{Jac}_H(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g}$$

So $|\mathrm{Jac}_H(\mathbb{F}_q)| \approx q^g$

If we want $q^g \approx 2^{160}$:

g	1	2	3	4
q	2^{160}	2^{80}	$2^{53.33}$	2^{40}

Point Counting Algorithms

Stay for next week's workshop to learn more . . .

Point Counting Algorithms

Stay for next week's workshop to learn more ...

$K = \mathbb{F}_q$, $q = p^n$

- **Square Root Methods**

  Pollard kangaroo
  Cartier-Manin

- ℓ-**adic Methods** ($n = 1$, polynomial in $\log(p)$)

  SEA and generalizations

- p-**adic Methods** (p small, polynomial in n)

  Canonical lifts (Satoh, AGM)
  Deformation theory
  Cohomology

Point Counting Algorithms

Stay for next week's workshop to learn more ...

$K = \mathbb{F}_q$, $q = p^n$

- **Square Root Methods**

  Pollard kangaroo
  Cartier-Manin

- ℓ-**adic Methods** ($n = 1$, polynomial in $\log(p)$)

  SEA and generalizations

- p-**adic Methods** (p small, polynomial in n)

  Canonical lifts (Satoh, AGM)
  Deformation theory
  Cohomology

Point counting on certain curves is easy (e.g. Koblitz curves)

Point Counting Algorithms

Stay for next week's workshop to learn more ...

$K = \mathbb{F}_q$, $q = p^n$

- **Square Root Methods**
  - Pollard kangaroo
  - Cartier-Manin
- ℓ-**adic Methods** ($n = 1$, polynomial in $\log(p)$)
  - SEA and generalizations
- p-**adic Methods** (p small, polynomial in n)
  - Canonical lifts (Satoh, AGM)
  - Deformation theory
  - Cohomology

Point counting on certain curves is easy (e.g. Koblitz curves)

Can also **construct** curves with good group orders via CM method (see Thursday's talks by Drew Sutherland and Bianca Viray)

Discrete Logarithms

Elliptic Curve DLP: given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find m

Discrete Logarithms

Elliptic Curve DLP: given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find m

Hyperelliptic Curve DLP: given reduced divisors D, E so that E is equivalent to mD, find m

Discrete Logarithms

Elliptic Curve DLP: given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find m

Hyperelliptic Curve DLP: given reduced divisors D, E so that E is equivalent to mD, find m

Generic Methods — Complexity $O(q^{g/2})$ group operations

- Baby step giant step — also requires $O(q^{g/2})$ space
- Pollard rho
- Pollard lambda (kangaroo)

Discrete Logarithms

Elliptic Curve DLP: given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find m

Hyperelliptic Curve DLP: given reduced divisors D, E so that E is equivalent to mD, find m

Generic Methods — Complexity $O(q^{g/2})$ group operations

- Baby step giant step — also requires $O(q^{g/2})$ space
- Pollard rho
- Pollard lambda (kangaroo)

Index Calculus Methods

- $g \gtrapprox \log(q)$ — sub-exponential
- $3 \leq g \lessapprox \log(q)$ — $O(q^{2-2/g})$

Discrete Logarithms

Elliptic Curve DLP: given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find m

Hyperelliptic Curve DLP: given reduced divisors D, E so that E is equivalent to mD, find m

Generic Methods — Complexity $O(q^{g/2})$ group operations

- Baby step giant step — also requires $O(q^{g/2})$ space
- Pollard rho
- Pollard lambda (kangaroo)

Index Calculus Methods

- $g \gtrapprox \log(q)$ — sub-exponential
- $3 \leq g \lessapprox \log(q)$ — $O(q^{2-2/g})$

For $g = 1, 2$, generic methods are best! (As far as we know . . .)

Other Attacks & Parameter Choices

$K = \mathbb{F}_q$ with $q = p^n$

- **Pohlig-Hellman** — ensure that $|\mathrm{Jac}_H(\mathbb{F}_q)|$ has a large prime factor

Other Attacks & Parameter Choices

$K = \mathbb{F}_q$ with $q = p^n$

- **Pohlig-Hellman** — ensure that $|\mathrm{Jac}_H(\mathbb{F}_q)|$ has a large prime factor
- **Additive Reduction**: if p divides $|\mathrm{Jac}_H(\mathbb{F}_q)|$, then there is an explicit homomorphism $\mathrm{Jac}_H(\mathbb{F}_q)[p] \to (\mathbb{F}_q^{2g-1}, +)$ — ensure that $\gcd(q, |\mathrm{Jac}_H(\mathbb{F}_q)|) = 1$

Other Attacks & Parameter Choices

$K = \mathbb{F}_q$ with $q = p^n$

- **Pohlig-Hellman** — ensure that $|\mathrm{Jac}_H(\mathbb{F}_q)|$ has a large prime factor
- **Additive Reduction**: if p divides $|\mathrm{Jac}_H(\mathbb{F}_q)|$, then there is an explicit homomorphism $\mathrm{Jac}_H(\mathbb{F}_q)[p] \to (\mathbb{F}_q^{2g-1}, +)$ — ensure that $\gcd(q, |\mathrm{Jac}_H(\mathbb{F}_q)|) = 1$
- **Multiplicative Reduction** (MOV): pairings can be used to map the DLP in $\mathrm{Jac}_H(\mathbb{F}_q)$ into $(\mathbb{F}_{q^k}^*, \times)$ where $q^k \equiv 1 \pmod{r}$ for a prime r dividing $|\mathrm{Jac}_H(\mathbb{F}_q)|$ — ensure that k is large

  (For pairing-based crypto, however, we want k small — see Tuesday's and Wednesday's talks)

Other Attacks & Parameter Choices

$K = \mathbb{F}_q$ with $q = p^n$

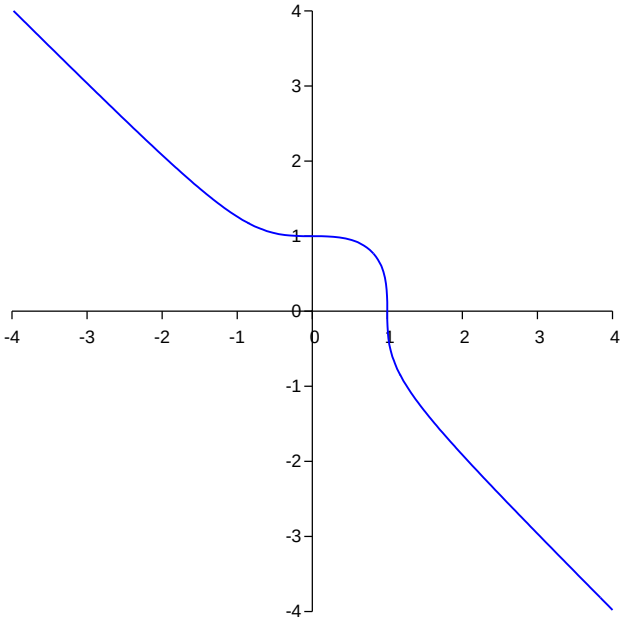
- **Pohlig-Hellman** — ensure that $|\mathrm{Jac}_H(\mathbb{F}_q)|$ has a large prime factor
- **Additive Reduction**: if p divides $|\mathrm{Jac}_H(\mathbb{F}_q)|$, then there is an explicit homomorphism $\mathrm{Jac}_H(\mathbb{F}_q)[p] \to (\mathbb{F}_q^{2g-1}, +)$ — ensure that $\gcd(q, |\mathrm{Jac}_H(\mathbb{F}_q)|) = 1$
- **Multiplicative Reduction** (MOV): pairings can be used to map the DLP in $\mathrm{Jac}_H(\mathbb{F}_q)$ into $(\mathbb{F}_{q^k}^*, \times)$ where $q^k \equiv 1 \pmod{r}$ for a prime r dividing $|\mathrm{Jac}_H(\mathbb{F}_q)|$ — ensure that k is large

  (For pairing-based crypto, however, we want k small — see Tuesday's and Wednesday's talks)
- **Weil Descent**: If $n = kd$ is composite, one may have $\mathrm{Jac}_H(\mathbb{F}_{p^{kd}}) \hookrightarrow \mathrm{Jac}_C(\mathbb{F}_{p^d})$ where C has higher genus — use $n = 1$ or n prime

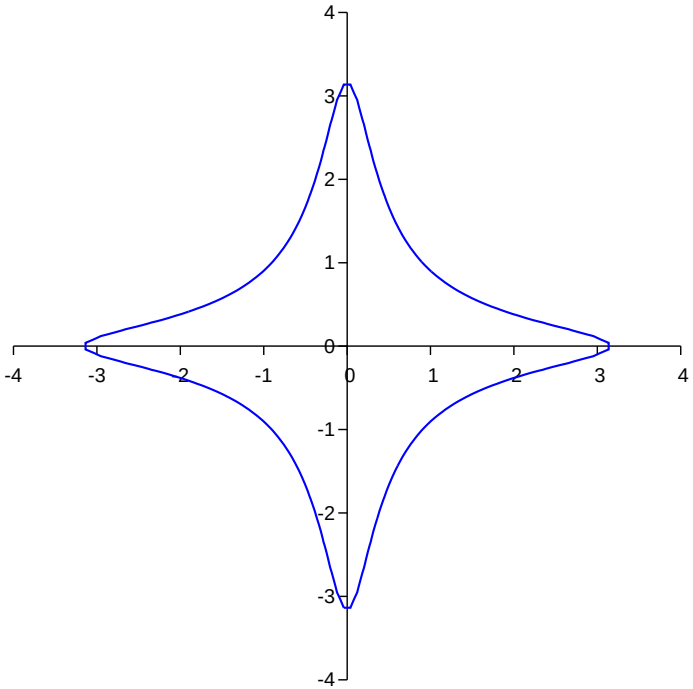
Some Other Models

- **Hessians**: $x^3 + y^3 - 3dxy = 1$
- **Edwards models**: $x^2 + y^2 = c^2(1 + dx^2y^2)$ (q odd) and variations

$x^3 + y^3 = 1$



$x^2+y^2 = 10(1-x^2y^2)$



Even Degree Models

$$H \ : \ y^2 + h(x)y = f(x)$$

- $h(x), f(x) \in K[x]$
- $\deg(h) = g + 1$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- $\deg(f) = 2g + 2$ is even
- $\mathrm{sgn}(f) = s^2 + s$ with $s \in K$ if $\mathrm{char}(K) = 2$; $f(x)$ is monic if $\mathrm{char}(K) \neq 2$
- non-singularity

Even Degree Models

$$H \ : \ y^2 + h(x)y = f(x)$$

- $h(x), f(x) \in K[x]$
- $\deg(h) = g + 1$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- $\deg(f) = 2g + 2$ is even
- $\mathrm{sgn}(f) = s^2 + s$ with $s \in K$ if $\mathrm{char}(K) = 2$; $f(x)$ is monic if $\mathrm{char}(K) \neq 2$
- non-singularity

$\mathrm{char}(K) \neq 2$: $\boxed{y^2 = f(x),}$ $f(x)$ monic, of even degree, square-free

Even Degree Models

$$H \ : \ y^2 + h(x)y = f(x)$$

- $h(x), f(x) \in K[x]$
- $\deg(h) = g + 1$ if $\mathrm{char}(K) = 2$; $h(x) = 0$ if $\mathrm{char}(K) \neq 2$
- $\deg(f) = 2g + 2$ is even
- $\mathrm{sgn}(f) = s^2 + s$ with $s \in K$ if $\mathrm{char}(K) = 2$; $f(x)$ is monic if $\mathrm{char}(K) \neq 2$
- non-singularity

$\mathrm{char}(K) \neq 2$: $y^2 = f(x)$, $f(x)$ monic, of even degree, square-free

Elliptic quartic, $\mathrm{char}(K) \neq 2, 3$:

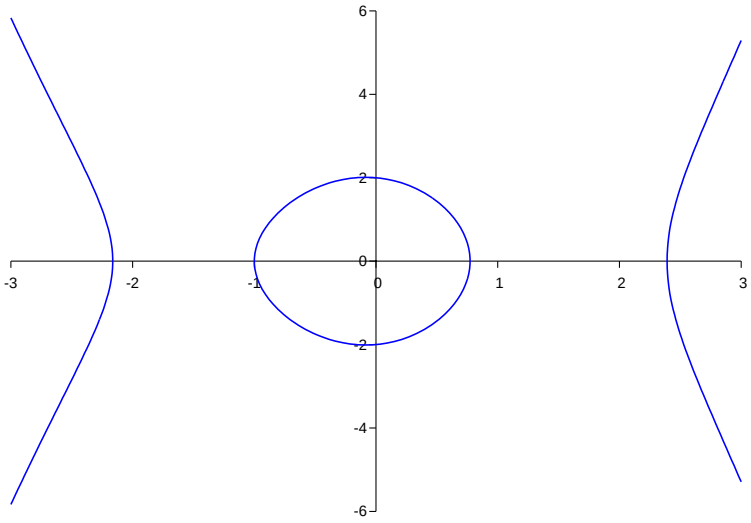
$$y^2 = x^4 + ax^2 + bx + c \quad (a, b, c \in K)$$

($b = 0$: **Jacobi** Quartic)

Examples

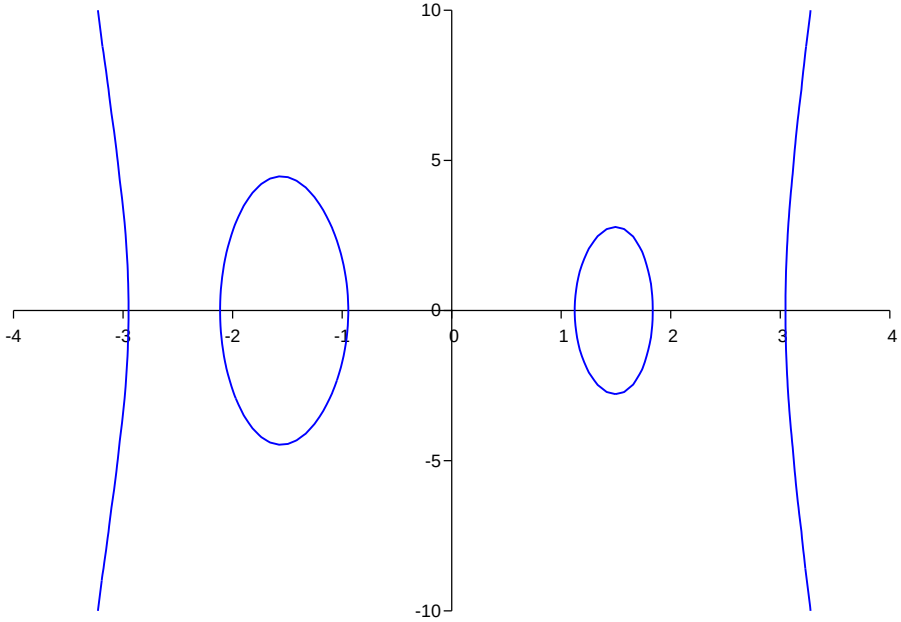
$$E \ : \ y^2 = x^4 - 6x^2 + x + 6$$

$$g = 1$$



$$H \ : \ y^2 = x^6 - 13x^4 + 44x^2 - 4x - 1$$

$$g = 2$$



Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography

Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography
- Use q prime or $q = 2^n$

Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography
- Use q prime or $q = 2^n$
- Good parameter choices are known and easy

Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography
- Use q prime or $q = 2^n$
- Good parameter choices are known and easy
- Cryptographically suitable curves can be constructed in practice

Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography
- Use q prime or $q = 2^n$
- Good parameter choices are known and easy
- Cryptographically suitable curves can be constructed in practice

$*\ *\ *$ **Thank You!** $*\ *\ *$