London School of Geometry and Number Theory

London Learning Lean

Elliptic curves and the Mordell-Weil theorem

David Ang

Thursday, 26 May 2022

Overview

- Introduction
- Abstract definition
- Concrete definition
- Implementation
- Associativity
- The Mordell-Weil theorem
- Selmer groups
- Future

Introduction — informally

What are elliptic curves?

Introduction — informally

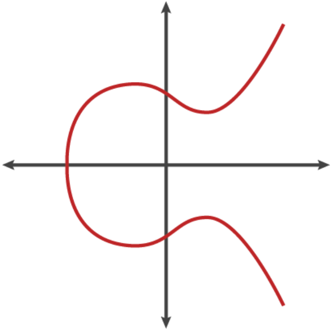
What are elliptic curves?

- A curve — solutions to $y^2 = x^3 + Ax + B$ for fixed A and B.

Introduction — informally

What are elliptic curves?

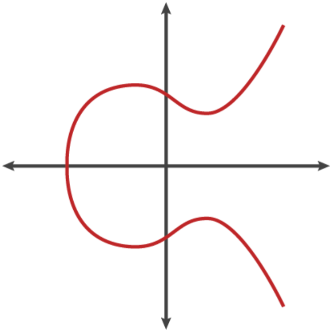
- A curve — solutions to $y^2 = x^3 + Ax + B$ for fixed A and B.



Introduction — informally

What are elliptic curves?

- A curve — solutions to $y^2 = x^3 + Ax + B$ for fixed A and B.



- A group — notion of addition of points!

Introduction — applications

Why do we care?

Introduction — applications

Why do we care?

Make or break cryptography.

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).
- Discrete logarithm problem — solve $nQ = P$ given P and Q (DH).

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).
- Discrete logarithm problem — solve $nQ = P$ given P and Q (DH).
- Post-quantum cryptography (SIDH).

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).
- Discrete logarithm problem — solve $nQ = P$ given P and Q (DH).
- Post-quantum cryptography (SIDH).

Number theory and algebraic geometry.

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).
- Discrete logarithm problem — solve $nQ = P$ given P and Q (DH).
- Post-quantum cryptography (SIDH).

Number theory and algebraic geometry.

- The simplest non-trivial objects in algebraic geometry.
    - Abelian variety of dimension one, projective curve of genus one, etc...

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).
- Discrete logarithm problem — solve $nQ = P$ given P and Q (DH).
- Post-quantum cryptography (SIDH).

Number theory and algebraic geometry.

- The simplest non-trivial objects in algebraic geometry.
  - Abelian variety of dimension one, projective curve of genus one, etc...
- Rational elliptic curve associated to $a^p + b^p = c^p$ is not modular.
  - But modularity theorem — rational elliptic curves are modular!

Introduction — applications

Why do we care?

Make or break cryptography.

- Lenstra's integer factorisation algorithm (RSA).
- Discrete logarithm problem — solve $nQ = P$ given P and Q (DH).
- Post-quantum cryptography (SIDH).

Number theory and algebraic geometry.

- The simplest non-trivial objects in algebraic geometry.
  - Abelian variety of dimension one, projective curve of genus one, etc...
- Rational elliptic curve associated to $a^p + b^p = c^p$ is not modular.
  - But modularity theorem — rational elliptic curves are modular!
- Distribution of ranks of rational elliptic curves.
  - The BSD conjecture — analytic rank equals algebraic rank?

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ {\scriptstyle f}\big\downarrow \\ S \end{array}$$

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ f\big\downarrow \;\; \big\uparrow 0 \\ S \end{array}$$

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ f\big\downarrow \;\; \big\uparrow 0 \\ S \end{array}$$

with a few technical conditions. [1]

[1] f is smooth, proper, and all its geometric fibres are integral curves of genus one

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ f\downarrow \;\; \curvearrowright 0 \\ S \end{array}$$

with a few technical conditions. [1]

For a scheme T over S,

[1] f is smooth, proper, and all its geometric fibres are integral curves of genus one

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ {\scriptstyle f}\downarrow \;\; \uparrow {\scriptstyle 0} \\ S \end{array}$$

with a few technical conditions. [1]

For a scheme T over S, define the **set of** T**-points** of E by

$$E(T) := \mathrm{Hom}_S(T, E),$$

[1] f is smooth, proper, and all its geometric fibres are integral curves of genus one

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ {\scriptstyle f}\downarrow \;\; \uparrow{\scriptstyle 0} \\ S \end{array}$$

with a few technical conditions. [1]

For a scheme T over S, define the **set of** T**-points** of E by

$$E(T) := \mathrm{Hom}_S(T, E),$$

which is naturally identified with a **Picard group** $\mathrm{Pic}^0_{E/S}(T)$ of E.

[1] f is smooth, proper, and all its geometric fibres are integral curves of genus one

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ f\big\downarrow \;\big)\,0 \\ S \end{array}$$

with a few technical conditions. [1]

For a scheme T over S, define the **set of** T**-points** of E by

$$E(T) := \mathrm{Hom}_S(T, E),$$

which is naturally identified with a **Picard group** $\mathrm{Pic}^0_{E/S}(T)$ of E.

This defines a contravariant functor $\mathbf{Sch}_S \to \mathbf{Ab}$ given by $T \mapsto E(T)$.

[1] f is smooth, proper, and all its geometric fibres are integral curves of genus one

Abstract definition — globally

An **elliptic curve** E **over a scheme** S is a diagram

$$\begin{array}{c} E \\ f\downarrow \;\; \uparrow 0 \\ S \end{array}$$

with a few technical conditions. [1]

For a scheme T over S, define the **set of** T**-points** of E by

$$E(T) := \mathrm{Hom}_S(T, E),$$

which is naturally identified with a **Picard group** $\mathrm{Pic}^0_{E/S}(T)$ of E.

This defines a contravariant functor $\mathbf{Sch}_S \to \mathbf{Ab}$ given by $T \mapsto E(T)$.

Good for algebraic geometry, but not very friendly...

[1] f is smooth, proper, and all its geometric fibres are integral curves of genus one

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

[2] or even a ring extension K/F whose class group has no 12-torsion

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

An **elliptic curve** E **over a field** F is a tuple $(E, 0)$.

[2] or even a ring extension K/F whose class group has no 12-torsion

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

An **elliptic curve** E **over a field** F is a tuple $(E, 0)$.

- E is a nice [3] genus one curve over F.

---

[2] or even a ring extension K/F whose class group has no 12-torsion
[3] smooth, proper, and geometrically integral

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

An **elliptic curve** E **over a field** F is a tuple $(E, 0)$.

- E is a nice [3] genus one curve over F.
- 0 is an F-point.

[2] or even a ring extension K/F whose class group has no 12-torsion

[3] smooth, proper, and geometrically integral

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

An **elliptic curve** E **over a field** F is a tuple $(E, 0)$.

- E is a nice [3] genus one curve over F.
- 0 is an F-point.

The Picard group is

$$\mathrm{Pic}^0_{E/F}(K) = \frac{\{\text{degree zero divisors of } E \text{ over } K\}}{\{\text{principal divisors of } E \text{ over } K\}}.$$

[2] or even a ring extension K/F whose class group has no 12-torsion

[3] smooth, proper, and geometrically integral

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

An **elliptic curve** E **over a field** F is a tuple $(E, 0)$.

- E is a nice [3] genus one curve over F.
- 0 is an F-point.

The Picard group is

$$\mathrm{Pic}^0_{E/F}(K) = \frac{\{\text{degree zero divisors of } E \text{ over } K\}}{\{\text{principal divisors of } E \text{ over } K\}}.$$

This defines a covariant functor $\mathbf{Alg}_F \to \mathbf{Ab}$ given by $K \mapsto E(K)$.

[2] or even a ring extension K/F whose class group has no 12-torsion

[3] smooth, proper, and geometrically integral

Abstract definition — locally

Let $S = \mathrm{Spec}\ F$ and $T = \mathrm{Spec}\ K$ for a field extension K/F. [2]

An **elliptic curve** E **over a field** F is a tuple $(E, 0)$.

- E is a nice [3] genus one curve over F.
- 0 is an F-point.

The Picard group is

$$\mathrm{Pic}^0_{E/F}(K) = \frac{\{\text{degree zero divisors of } E \text{ over } K\}}{\{\text{principal divisors of } E \text{ over } K\}}.$$

This defines a covariant functor $\mathbf{Alg}_F \to \mathbf{Ab}$ given by $K \mapsto E(K)$.

Group law is free, but still need equations...

[2] or even a ring extension K/F whose class group has no 12-torsion

[3] smooth, proper, and geometrically integral

Concrete definition – Weierstrass equations

The Riemann-Roch theorem gives **Weierstrass equations**.

Concrete definition – Weierstrass equations

The Riemann-Roch theorem gives **Weierstrass equations**.

Corollary (of Riemann-Roch)

An elliptic curve E over a field F is a projective plane curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_i \in F,$$

Concrete definition – Weierstrass equations

The Riemann-Roch theorem gives **Weierstrass equations**.

Corollary (of Riemann-Roch)

An elliptic curve E over a field F is a projective plane curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_i \in F,$$

with $\Delta \neq 0$. [4]

[4] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Concrete definition – Weierstrass equations

The Riemann-Roch theorem gives **Weierstrass equations**.

Corollary (of Riemann-Roch)

An elliptic curve E over a field F is a projective plane curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_i \in F,$$

with $\Delta \neq 0$. [4]

If $\mathrm{char}\ F \neq 2, 3$, can reduce this to

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \qquad A, B \in F,$$

[4] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Concrete definition – Weierstrass equations

The Riemann-Roch theorem gives **Weierstrass equations**.

Corollary (of Riemann-Roch)

An elliptic curve E over a field F is a projective plane curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_i \in F,$$

with $\Delta \neq 0$. [4]

If $\mathrm{char}\ F \neq 2, 3$, can reduce this to

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \qquad A, B \in F,$$

with $\Delta := 4A^3 + 27B^2 \neq 0$.

[4] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Concrete definition – Weierstrass equations

The Riemann-Roch theorem gives **Weierstrass equations**.

Corollary (of Riemann-Roch)

An elliptic curve E over a field F is a projective plane curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_i \in F,$$

with $\Delta \neq 0$. [4]

If $\mathrm{char}\ F \neq 2, 3$, can reduce this to

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \qquad A, B \in F,$$

with $\Delta := 4A^3 + 27B^2 \neq 0$.

Note the unique **point at infinity** when $Z = 0$! Call this point 0.

---

[4] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Concrete definition — group law

The **group law** from $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$ is reduced to drawing lines.

Concrete definition — group law

The **group law** from $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$ is reduced to drawing lines.

Operations are characterised by

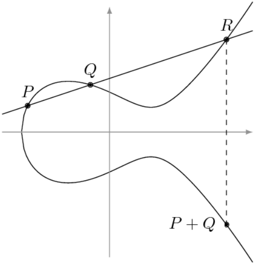
$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$

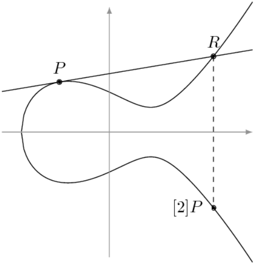
Concrete definition — group law

The **group law** from $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$ is reduced to drawing lines.

Operations are characterised by

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$



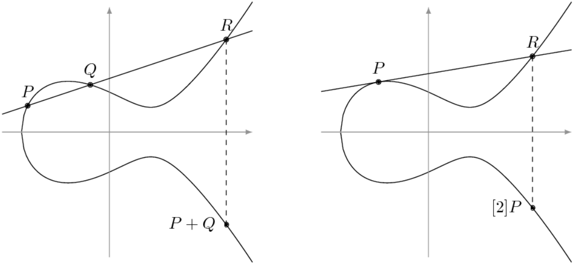


Concrete definition — group law

The **group law** from $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$ is reduced to drawing lines.

Operations are characterised by

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$



Note that $(x, y) \in E[2] := \ker(E \xrightarrow{\cdot 2} E)$ if and only if $y = 0$. [5]

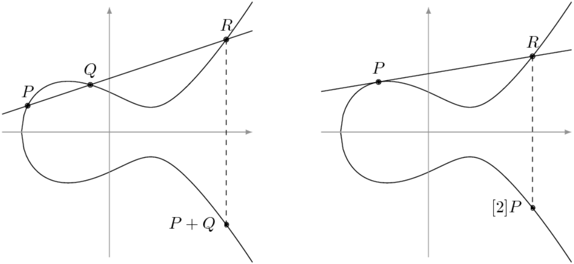
[5] Assume $a_1 = a_3 = 0$.

Concrete definition — group law

The **group law** from $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$ is reduced to drawing lines.

Operations are characterised by

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear.}$$



Note that $(x, y) \in E[2] := \ker(E \xrightarrow{\cdot 2} E)$ if and only if $y = 0$. [5]

Many cases... but all completely explicit!

[5] Assume $a_1 = a_3 = 0$.

Implementation — the curve

Three definitions of elliptic curves:

1. Abstract definition over a scheme
2. Abstract definition over a field
3. Concrete definition over a field

Generality: 1. $\supset$ 2. $\stackrel{\text{RR}}{=}$ 3.

Implementation — the curve

Three definitions of elliptic curves:

1. Abstract definition over a scheme
2. Abstract definition over a field
3. Concrete definition over a field

Generality: 1. $\supset$ 2. $\overset{\text{RR}}{=}$ 3.

- 1. & 2. require much algebraic geometry (properness, genus, ...).

Implementation — the curve

Three definitions of elliptic curves:

1. Abstract definition over a scheme
2. Abstract definition over a field
3. Concrete definition over a field

Generality: 1. $\supset$ 2. $\overset{\text{RR}}{=}$ 3.

- 1. & 2. require much algebraic geometry (properness, genus, ...).
- 2. $=$ 3. also requires algebraic geometry (divisors, differentials, ...).

Implementation — the curve

Three definitions of elliptic curves:

1. Abstract definition over a scheme
2. Abstract definition over a field
3. Concrete definition over a field

Generality: 1. $\supset$ 2. $\stackrel{\text{RR}}{=}$ 3.

- 1. & 2. require much algebraic geometry (properness, genus, ...).
- 2. $=$ 3. also requires algebraic geometry (divisors, differentials, ...).
- 3. requires just five coefficients (and $\Delta \neq 0$)!

Implementation — the curve

Three definitions of elliptic curves:

1. Abstract definition over a scheme
2. Abstract definition over a field
3. Concrete definition over a field

Generality: 1. $\supset$ 2. $\overset{\text{RR}}{=}$ 3.

- 1. & 2. require much algebraic geometry (properness, genus, ...).
- 2. = 3. also requires algebraic geometry (divisors, differentials, ...).
- 3. requires just five coefficients (and $\Delta \neq 0$)!

```
def disc_aux {R : Type} [comm_ring R] (a₁ a₂ a₃ a₄ a₆ : R) : R :=
 -(a₁^2 + 4*a₂)^2*(a₁^2*a₆ + 4*a₂*a₆ - a₁*a₃*a₄ + a₂*a₃^2 - a₄^2)
 - 8*(2*a₄ + a₁*a₃)^3 - 27*(a₃^2 + 4*a₆)^2
 + 9*(a₁^2 + 4*a₂)*(2*a₄ + a₁*a₃)*(a₃^2 + 4*a₆)

structure EllipticCurve (R : Type) [comm_ring R] :=
 (a₁ a₂ a₃ a₄ a₆ : R) (disc : units R) (disc_eq : disc.val = disc_aux a₁ a₂ a₃ a₄ a₆)
```

Implementation — the curve

Three definitions of elliptic curves:

1. Abstract definition over a scheme
2. Abstract definition over a field
3. Concrete definition over a field

Generality: 1. $\supset$ 2. $\overset{\text{RR}}{=}$ 3.

- 1. & 2. require much algebraic geometry (properness, genus, ...).
- 2. $=$ 3. also requires algebraic geometry (divisors, differentials, ...).
- 3. requires just five coefficients (and $\Delta \neq 0$)!

```
def disc_aux {R : Type} [comm_ring R] (a₁ a₂ a₃ a₄ a₆ : R) : R :=
 -(a₁^2 + 4*a₂)^2*(a₁^2*a₆ + 4*a₂*a₆ - a₁*a₃*a₄ + a₂*a₃^2 - a₄^2)
 - 8*(2*a₄ + a₁*a₃)^3 - 27*(a₃^2 + 4*a₆)^2
 + 9*(a₁^2 + 4*a₂)*(2*a₄ + a₁*a₃)*(a₃^2 + 4*a₆)

structure EllipticCurve (R : Type) [comm_ring R] :=
 (a₁ a₂ a₃ a₄ a₆ : R) (disc : units R) (disc_eq : disc.val = disc_aux a₁ a₂ a₃ a₄ a₆)
```

This is the *curve* E — what about the *group* $E(K)$?

Implementation — the group

```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

inductive point
  | zero
  | some (x y : K) (w : y^2 + E.a₁*x*y + E.a₃*y = x^3 + E.a₂*x^2 + E.a₄*x + E.a₆)

notation E(K) := point E K
```

Implementation — the group

```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

inductive point
  | zero
  | some (x y : K) (w : y^2 + E.a₁*x*y + E.a₃*y = x^3 + E.a₂*x^2 + E.a₄*x + E.a₆)

notation E(K) := point E K
```

- Identity is trivial!

```
instance : has_zero E(K) := ⟨zero⟩
```

Implementation — the group

```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

inductive point
  | zero
  | some (x y : K) (w : y^2 + E.a₁*x*y + E.a₃*y = x^3 + E.a₂*x^2 + E.a₄*x + E.a₆)

notation E(K) := point E K
```

- Identity is trivial!

```
instance : has_zero E(K) := ⟨zero⟩
```

- Negation is easy.

```
def neg : E(K) → E(K)
  | zero := zero
  | (some x y w) := some x (−y − E.a₁*x − E.a₃) $
    begin
      rw [← w],
      ring
    end

instance : has_neg E(K) := ⟨neg⟩
```

Implementation — the group

```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

inductive point
  | zero
  | some (x y : K) (w : y^2 + E.a1*x*y + E.a3*y = x^3 + E.a2*x^2 + E.a4*x + E.a6)

notation E(K) := point E K
```

- Addition is complicated...

```
def add : E(K) → E(K) → E(K)
  | zero P := P
  | P zero := P
  | (some x1 y1 w1) (some x2 y2 w2) :=
    if x_ne : x1 ≠ x2 then                          -- add distinct points
     let L := (y1 - y2) / (x1 - x2),
         x3 := L^2 + E.a1*L - E.a2 - x1 - x2,
         y3 := -L*x3 - E.a1*x3 - y1 + L*x1 - E.a3
     in some x3 y3 $ by { ... }
    else if y_ne : y1 + y2 + E.a1*x2 + E.a3 ≠ 0 then -- double a point
     ...
    else                                            -- draw vertical line
     zero

instance : has_add E(K) := ⟨add⟩
```

Implementation — the group

```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

inductive point
  | zero
  | some (x y : K) (w : y^2 + E.a₁*x*y + E.a₃*y = x^3 + E.a₂*x^2 + E.a₄*x + E.a₆)

notation E(K) := point E K
```

- Commutativity is... doable.

```
lemma add_comm (P Q : E(K)) : P + Q = Q + P :=
 begin
   rcases ⟨P, Q⟩ with ⟨_ | _, _ | _⟩,
   ... -- six cases
 end
```

Implementation — the group

```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

inductive point
  | zero
  | some (x y : K) (w : y^2 + E.a₁*x*y + E.a₃*y = x^3 + E.a₂*x^2 + E.a₄*x + E.a₆)

notation E(K) := point E K
```

- Commutativity is... doable.

```
lemma add_comm (P Q : E(K)) : P + Q = Q + P :=
 begin
  rcases ⟨P, Q⟩ with ⟨_ | _, _ | _⟩,
  ... -- six cases
 end
```

- Associativity is... impossible?

```
lemma add_assoc (P Q R : E(K)) : (P + Q) + R = P + (Q + R) :=
 begin
  rcases ⟨P, Q, R⟩ with ⟨_ | _, _ | _, _ | _⟩,
  ... -- ??? cases
 end
```

Associativity — explaining the problem

Known to be difficult with several proofs:

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
    - Probably(?) times out with 130,000(!) coefficients.

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
  - Probably(?) times out with 130,000(!) coefficients.
- Uniformisation.
  - Requires theory of elliptic functions.

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
  - Probably(?) times out with 130,000(!) coefficients.
- Uniformisation.
  - Requires theory of elliptic functions.
- Cayley-Bacharach.
  - Requires intersection multiplicity and Bézout's theorem.

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
  - Probably(?) times out with 130,000(!) coefficients.
- Uniformisation.
  - Requires theory of elliptic functions.
- Cayley-Bacharach.
  - Requires intersection multiplicity and Bézout's theorem.
- $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$.
  - Requires divisors, differentials, and the Riemann-Roch theorem.

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
  - Probably(?) times out with 130,000(!) coefficients.
- Uniformisation.
  - Requires theory of elliptic functions.
- Cayley-Bacharach.
  - Requires intersection multiplicity and Bézout's theorem.
- $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$.
  - Requires divisors, differentials, and the Riemann-Roch theorem.

Current status:

- Left as a `sorry`.

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
  - Probably(?) times out with 130,000(!) coefficients.
- Uniformisation.
  - Requires theory of elliptic functions.
- Cayley-Bacharach.
  - Requires intersection multiplicity and Bézout's theorem.
- $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$.
  - Requires divisors, differentials, and the Riemann-Roch theorem.

Current status:

- Left as a `sorry`.
- Ongoing attempt (by Marc Masdeu) to bash it out.

Associativity — explaining the problem

Known to be difficult with several proofs:

- Just do it!
  - Probably(?) times out with 130,000(!) coefficients.
- Uniformisation.
  - Requires theory of elliptic functions.
- Cayley-Bacharach.
  - Requires intersection multiplicity and Bézout's theorem.
- $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$.
  - Requires divisors, differentials, and the Riemann-Roch theorem.

Current status:

- Left as a `sorry`.
- Ongoing attempt (by Marc Masdeu) to bash it out.
- Proof in Coq (by Evmorfia-Iro Bartzia and Pierre-Yves Strub [6]) that $E(K) \cong \mathrm{Pic}^0_{E/F}(K)$ but only for $\mathrm{char}\ F \neq 2, 3$.

[6] A Formal Library for Elliptic Curves in the Coq Proof Assistant (2015)

Associativity — ignoring the problem

Modulo associativity, what has been done?

Associativity — ignoring the problem

Modulo associativity, what has been done?

- Functoriality $\mathbf{Alg}_F \to \mathbf{Ab}$.

```
def point_hom (φ : K →ₐ[F] L) : E(K) → E(L)
  | zero := zero
  | (some x y w) := some (φ x) (φ y) $ by { . . . }

lemma point_hom.id (P : E(K)) : point_hom (K→[F]K) P = P

lemma point_hom.comp (P : E(K)) :
 point_hom (L→[F]M) (point_hom (K→[F]L) P) = point_hom ((L→[F]M).comp (K→[F]L)) P
```

Associativity — ignoring the problem

Modulo associativity, what has been done?

- Functoriality $\mathbf{Alg}_F \to \mathbf{Ab}$.

```
def point_hom (φ : K →ₐ[F] L) : E(K) → E(L)
  | zero := zero
  | (some x y w) := some (φ x) (φ y) $ by { . . . }

lemma point_hom.id (P : E(K)) : point_hom (K→[F]K) P = P

lemma point_hom.comp (P : E(K)) :
  point_hom (L→[F]M) (point_hom (K→[F]L) P) = point_hom ((L→[F]M).comp (K→[F]L)) P
```

- Galois module structure $\mathrm{Gal}(L/K) \curvearrowright E(L)$.

```
def point_gal (σ : L ≃ₐ[K] L) : E(L) → E(L)
  | zero := zero
  | (some x y w) := some (σ · x) (σ · y) $ by { . . . }

variables [finite_dimensional K L] [is_galois K L]

lemma point_gal.fixed :
  mul_action.fixed_points (L ≃ₐ[K] L) E(L) = (point_hom (K→[F]L)).range
```

Associativity — ignoring the problem

Modulo associativity, what has been done?

- Isomorphisms $(x, y) \mapsto (u^2 x + r, u^3 y + u^2 s x + t)$.

```
variables (u : units F) (r s t : F)

def cov : EllipticCurve F :=
{ a₁ := u.inv*(E.a₁ + 2*s),
  a₂ := u.inv^2*(E.a₂ − s*E.a₁ + 3*r − s^2),
  a₃ := u.inv^3*(E.a₃ + r*E.a₁ + 2*t),
  a₄ := u.inv^4*(E.a₄ − s*E.a₃ + 2*r*E.a₂ − (t + r*s)*E.a₁ + 3*r^2 − 2*s*t),
  a₆ := u.inv^6*(E.a₆ + r*E.a₄ + r^2*E.a₂ + r^3 − t*E.a₃ − t^2 − r*t*E.a₁),
  disc := ⟨u.inv^12*E.disc.val, u.val^12*E.disc.inv, by { ... }, by { ... }⟩,
  disc_eq := by { simp only, rw [disc_eq, disc_aux, disc_aux], ring } }

def cov.to_fun : (E.cov u r s t)(K) → E(K)
  | zero := zero
  | (some x y w) := some (u.val^2*x + r) (u.val^3*y + u.val^2*s*x + t) $ by { ... }

def cov.inv_fun : E(K) → (E.cov u r s t)(K)
  | zero := zero
  | (some x y w) := some (u.inv^2*(x − r)) (u.inv^3*(y − s*x + r*s − t)) $ by { ... }

def cov.equiv_add : (E.cov u r s t)(K) ≃+ E(K) :=
  ⟨cov.to_fun u r s t, cov.inv_fun u r s t, by { ... }, by { ... }, by { ... }⟩
```

Associativity — ignoring the problem

Modulo associativity, what has been done?

- 2-division polynomial $\psi_2(x)$.

```
def ψ₂_x : cubic K := ⟨4, E.a₁^2 + 4*E.a₂, 4*E.a₄ + 2*E.a₁*E.a₃, E.a₃^2 + 4*E.a₆⟩

lemma ψ₂_x.disc_eq_disc : (ψ₂_x E K).disc = 16*E.disc
```

Associativity — ignoring the problem

Modulo associativity, what has been done?

- 2-division polynomial $\psi_2(x)$.

```
def ψ₂_x : cubic K := ⟨4, E.a₁^2 + 4*E.a₂, 4*E.a₄ + 2*E.a₁*E.a₃, E.a₃^2 + 4*E.a₆⟩

lemma ψ₂_x.disc_eq_disc : (ψ₂_x E K).disc = 16*E.disc
```

- Structure of $E(K)[2]$.

```
notation E(K)[n] := ((·) n : E(K) →+ E(K)).ker

lemma E₂.x {x y w} : some x y w ∈ E(K)[2] ↔ x ∈ (ψ₂_x E K).roots

theorem E₂.card_le_four : fintype.card E(K)[2] ≤ 4

variables [algebra ((ψ₂_x E F).splitting_field) K]

theorem E₂.card_eq_four : fintype.card E(K)[2] = 4

lemma E₂.gal_fixed (σ : L ≃ₐ[K] L) (P : E(L)[2]) : σ • P = P
```

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.
- $r \in \mathbb{N}$ is the **algebraic rank**.

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.
- $r \in \mathbb{N}$ is the **algebraic rank**.

Proof.

Three steps.

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.
- $r \in \mathbb{N}$ is the **algebraic rank**.

Proof.

Three steps.

- **Weak Mordell-Weil**: $E(K)/2E(K)$ is finite.

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.
- $r \in \mathbb{N}$ is the **algebraic rank**.

Proof.

Three steps.

- **Weak Mordell-Weil**: $E(K)/2E(K)$ is finite.
- **Heights**: $E(K)$ can be endowed with a "height function".

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.
- $r \in \mathbb{N}$ is the **algebraic rank**.

Proof.

Three steps.

- **Weak Mordell-Weil**: $E(K)/2E(K)$ is finite.
- **Heights**: $E(K)$ can be endowed with a "height function".
- **Descent**: An abelian group A endowed with a "height function", such that $A/2A$ is finite, is necessarily finitely generated. □

The Mordell-Weil theorem — statement and proof

Theorem (Mordell-Weil)

Let K be a number field. Then $E(K)$ is finitely generated.

By the structure theorem (Pierre-Alexandre Bazin),

$$E(K) \cong T \oplus \mathbb{Z}^r.$$

- T is a finite **torsion subgroup**.
- $r \in \mathbb{N}$ is the **algebraic rank**.

Proof.

Three steps.

- **Weak Mordell-Weil**: $E(K)/2E(K)$ is finite.
- **Heights**: $E(K)$ can be endowed with a "height function".
- **Descent**: An abelian group A endowed with a "height function", such that $A/2A$ is finite, is necessarily finitely generated. □

The descent step is done (Jujian Zhang).

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.

  Completing the square is an isomorphism

$$\begin{array}{ccc} E(K) & \longrightarrow & E'(K) \\ (x, y) & \longmapsto & (x, y - \frac{1}{2}a_1x - \frac{1}{2}a_3) \end{array}.$$

```
def covm.equiv_add : (E.cov _ _ _ _)(K) ≃+ E(K) := cov.equiv_add 1 0 (−E.a₁/2) (−E.a₃/2)
```

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.

  Completing the square is an isomorphism

$$\begin{array}{ccc} E(K) & \longrightarrow & E'(K) \\ (x, y) & \longmapsto & (x, y - \frac{1}{2}a_1x - \frac{1}{2}a_3) \end{array} .$$

  Thus

$$E(K)/2E(K) \text{ finite} \iff E'(K)/2E'(K) \text{ finite}.$$

```
def cov_m.equiv_add : (E.cov _ _ _ _)(K) ≃+ E(K) := cov.equiv_add 1 0 (−E.a₁/2) (−E.a₃/2)
```

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.

  Completing the square is an isomorphism

$$\begin{array}{ccc} E(K) & \longrightarrow & E'(K) \\ (x, y) & \longmapsto & (x, y - \frac{1}{2}a_1x - \frac{1}{2}a_3) \end{array} .$$

  Thus

$$E(K)/2E(K) \text{ finite} \quad \Longleftrightarrow \quad E'(K)/2E'(K) \text{ finite.}$$

```
def covₘ.equiv_add : (E.cov _ _ _ _)(K) ≃+ E(K) := cov.equiv_add 1 0 (−E.a₁/2) (−E.a₃/2)
```

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.

Let $L = K(E[2])$. Suffices to show

$$E(L)/2E(L) \text{ finite} \qquad \Longrightarrow \qquad E(K)/2E(K) \text{ finite.}$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.

Let $L = K(E[2])$. Suffices to show

$$E(L)/2E(L) \text{ finite} \qquad \Longrightarrow \qquad E(K)/2E(K) \text{ finite.}$$

Suffices to show finiteness of

$$\Phi := \ker(E(K)/2E(K) \to E(L)/2E(L)).$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.

Let $L = K(E[2])$. Suffices to show

$$E(L)/2E(L) \text{ finite} \qquad \Longrightarrow \qquad E(K)/2E(K) \text{ finite.}$$

Suffices to show finiteness of

$$\Phi := \ker(E(K)/2E(K) \to E(L)/2E(L)).$$

Define an injection

$$\kappa : \Phi \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E(L)[2]).$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.

Let $L = K(E[2])$. Suffices to show

$$E(L)/2E(L) \text{ finite} \qquad \Longrightarrow \qquad E(K)/2E(K) \text{ finite.}$$

Suffices to show finiteness of

$$\Phi := \ker(E(K)/2E(K) \to E(L)/2E(L)).$$

Define an injection

$$\kappa : \Phi \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E(L)[2]).$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.

```
variables [finite_dimensional K L] [is_galois K L] (n : ℕ)

lemma range_le_comap_range : n·E(K) ≤ add_subgroup.comap (point_hom _) n·E(L)

def Φ : add_subgroup E(K)/n :=
 (quotient_add_group.map _ _ _ $ range_le_comap_range n).ker

lemma Φ_mem_range (P : Φ n E L) : point_hom _ P.val.out' ∈ n·E(L)

def κ : Φ n E L → L ≃ₐ[K] L → E(L)[n] :=
 λ P σ, ⟨σ · (Φ_mem_range n P).some − (Φ_mem_range n P).some, by { . . . }⟩

lemma κ.injective : function.injective $ κ n

def coker_2_of_fg_extension.fintype : fintype E(L)/2 → fintype E(K)/2
```

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \; : \; E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x,y) \mid y^2 = (x-e_1)(x-e_2)(x-e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Map: $\qquad 0 \longmapsto (\quad 1 \quad , \quad 1 \quad)$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x,y) \mid y^2 = (x-e_1)(x-e_2)(x-e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \longrightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Map:

$$\begin{array}{rcl} 0 & \longmapsto & (\ 1\ ,\ 1\ ) \\ (x,y) & \longmapsto & (\ x-e_1\ ,\ x-e_2\ ) \end{array}$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \longrightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Map:

$$\begin{array}{rcl} 0 & \longmapsto & \left(1 \ , \ 1 \right) \\ (x, y) & \longmapsto & \left(x - e_1 \ , \ x - e_2 \right) \\ (e_1, 0) & \longmapsto & \left(\dfrac{e_1 - e_3}{e_1 - e_2} \ , \ e_1 - e_2 \right) \end{array}$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \longrightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Map:

$$\begin{array}{rcccccc} 0 & \longmapsto & (& 1 & , & 1 &) \\ (x,y) & \longmapsto & (& x - e_1 & , & x - e_2 &) \\ (e_1, 0) & \longmapsto & (& \dfrac{e_1 - e_3}{e_1 - e_2} & , & e_1 - e_2 &) \\ (e_2, 0) & \longmapsto & (& e_2 - e_1 & , & \dfrac{e_2 - e_3}{e_2 - e_1} &) \end{array}$$

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

```
variables (ha₁ : E.a₁ = 0) (ha₃ : E.a₃ = 0) (h3 : (ψ₂_x E K).roots = {e₁, e₂, e₃})

def δ : E(K) → (units K) / (units K)^2 × (units K) / (units K)^2
  | zero := 1
  | (some x y w) :=
   if he₁ : x = e₁ then
    (units.mk0 ((e₁ - e₃) / (e₁ - e₂)) $ by { . . . }, units.mk0 (e₁ - e₂) $ by { . . . })
   else if he₂ : x = e₂ then
    (units.mk0 (e₂ - e₁) $ by { . . . }, units.mk0 ((e₂ - e₃) / (e₂ - e₁)) $ by { . . . })
   else
    (units.mk0 (x - e₁) $ by { . . . }, units.mk0 (x - e₂) $ by { . . . })
```

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

- Prove $\ker \delta = 2E(K)$.

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

- Prove $\ker \delta = 2E(K)$.

Here $\supseteq$ is obvious, while $\subseteq$ is long but constructive.

```
lemma δ.ker : (δ ha₁ ha₃ h3).ker = 2·E(K) :=
 begin
  . . . -- completely constructive proof
 end
```

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x,y) \mid y^2 = (x-e_1)(x-e_2)(x-e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

- Prove $\ker \delta = 2E(K)$.
- Prove $\mathrm{im}\ \delta \leq K(S,2) \times K(S,2)$ for some $K(S,2) \leq K^\times/(K^\times)^2$.

The Mordell-Weil theorem — weak Mordell-Weil

Prove that $E(K)/2E(K)$ is finite with **complete** 2-**descent**.

$$E(K) = \{(x, y) \mid y^2 = (x - e_1)(x - e_2)(x - e_3)\} \cup \{0\}$$

- Reduce to $a_1 = a_3 = 0$.
- Reduce to $E[2] \subset E(K)$.
- Define a **complete** 2-**descent** homomorphism

$$\delta \ : \ E(K) \quad \longrightarrow \quad K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

- Prove $\ker \delta = 2E(K)$.
- Prove $\mathrm{im}\ \delta \leq K(S, 2) \times K(S, 2)$ for some $K(S, 2) \leq K^\times/(K^\times)^2$.

  Here S is a finite set of "ramified" places of K.

```
lemma δ.range_le : (δ ha₁ ha₃ h3).range ≤ K(S, 2) × K(S, 2) := sorry -- ramification theory?
```

Interlude — Selmer groups

Let S be a finite set of places of K.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.

  There is a homomorphism

$$\begin{array}{rcl} K(S,n) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^{|S|} \\ x(K^\times)^n & \longmapsto & (\mathrm{ord}_p(x))_{p\in S} \end{array},$$

  with kernel $K(\emptyset, n)$.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.

  There is a homomorphism

$$\begin{array}{ccc} K(S,n) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^{|S|} \\ x(K^\times)^n & \longmapsto & (\mathrm{ord}_p(x))_{p\in S} \end{array},$$

  with kernel $K(\emptyset, n)$. Thus

$$K(S,n) \text{ finite} \iff K(\emptyset,n) \text{ finite.}$$

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.

```
def selmer : subgroup $ (units K) / (units K)^n :=
 { carrier := {x | ∀ p ∉ S, val_of_ne_zero_mod p x = 1},
   one_mem' := by { ... },
   mul_mem' := by { ... },
   inv_mem' := by { ... } }

notation K(S, n) := selmer K S n

def selmer.val : K(S, n) →* S → multiplicative (zmod n) :=
 { to_fun := λ x p, val_of_ne_zero_mod p x,
   map_one' := by { ... },
   map_mul' := by { ... } }

lemma selmer.val_ker : selmer.val.ker = K(∅, n).subgroup_of K(S, n)
```

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset, n) \xrightarrow{g} \mathrm{Cl}_K.$$

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset,n) \xrightarrow{g} \mathrm{Cl}_K.$$

```
def f : units (O K) →* K(∅, n) :=
 { to_fun := λ x, ⟨quotient_group.mk $ ne_zero_of_unit x, λ p _, val_of_unit_mod p x⟩,
   map_one' := rfl,
   map_mul' := λ ⟨⟨_, _⟩, ⟨_, _⟩, _, _⟩ ⟨⟨_, _⟩, ⟨_, _⟩, _, _⟩, rfl } -- lol

lemma f_ker : f.ker = (units (O K))^n

def g : K(∅, n) →* class_group (O K) K := ... -- hmm

lemma g_ker : g.ker = f.range
```

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset,n) \xrightarrow{g} \mathrm{Cl}_K.$$

- Prove Cl_K is finite.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset,n) \xrightarrow{g} \mathrm{Cl}_K.$$

- Prove Cl_K is finite. Done (Baanen, Dahmen, Narayanan, Nuccio).

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset, n) \xrightarrow{g} \mathrm{Cl}_K.$$

- Prove Cl_K is finite. Done (Baanen, Dahmen, Narayanan, Nuccio).
- Prove $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n$ is finite.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset, n) \xrightarrow{g} \mathrm{Cl}_K.$$

- Prove Cl_K is finite. Done (Baanen, Dahmen, Narayanan, Nuccio).
- Prove $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n$ is finite. Suffices to show $\mathcal{O}_K^\times$ is finitely generated.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset, n) \xrightarrow{g} \mathrm{Cl}_K.$$

- Prove Cl_K is finite. Done (Baanen, Dahmen, Narayanan, Nuccio).
- Prove $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n$ is finite. Suffices to show $\mathcal{O}_K^\times$ is finitely generated. Consequence of **Dirichlet's unit theorem (help wanted!)**.

Interlude — Selmer groups

Let S be a finite set of places of K. The n-**Selmer group** of K is

$$K(S,n) := \{x(K^\times)^n \in K^\times/(K^\times)^n \mid \forall p \notin S,\ \mathrm{ord}_p(x) \equiv 0 \mod n\}.$$

Claim that $K(S,n)$ is finite.

- Reduce to $K(\emptyset, n)$.
- Define an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \xrightarrow{f} K(\emptyset, n) \xrightarrow{g} \mathrm{Cl}_K.$$

- Prove Cl_K is finite. Done (Baanen, Dahmen, Narayanan, Nuccio).
- Prove $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n$ is finite. Suffices to show $\mathcal{O}_K^\times$ is finitely generated. Consequence of **Dirichlet's unit theorem (help wanted!)**.

Note the classical n-Selmer group of E is

$$\mathrm{Sel}(K, E[n]) \leq K(S,n) \times K(S,n).$$

The Mordell-Weil theorem — heights

Prove that $E(K)$ can be endowed with a "height function".

The Mordell-Weil theorem — heights

Prove that $E(K)$ can be endowed with a "height function".

A **height function** $h : E(K) \to \mathbb{R}$ satisfies the following.

The Mordell-Weil theorem — heights

Prove that $E(K)$ can be endowed with a "height function".

A **height function** $h : E(K) \to \mathbb{R}$ satisfies the following.

- For all $Q \in E(K)$, there exists $C_1 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$h(P + Q) \leq 2h(P) + C_1.$$

The Mordell-Weil theorem — heights

Prove that $E(K)$ can be endowed with a "height function".

A **height function** $h : E(K) \to \mathbb{R}$ satisfies the following.

- For all $Q \in E(K)$, there exists $C_1 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$h(P + Q) \leq 2h(P) + C_1.$$

- There exists $C_2 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$4h(P) \leq h(2P) + C_2.$$

The Mordell-Weil theorem — heights

Prove that $E(K)$ can be endowed with a "height function".

A **height function** $h : E(K) \to \mathbb{R}$ satisfies the following.

- For all $Q \in E(K)$, there exists $C_1 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$h(P+Q) \leq 2h(P) + C_1.$$

- There exists $C_2 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$4h(P) \leq h(2P) + C_2.$$

- For all $C_3 \in \mathbb{R}$, the set

$$\{P \in E(K) \mid h(P) \leq C_3\}$$

is finite.

The Mordell-Weil theorem — heights

Prove that $E(K)$ can be endowed with a "height function".

A **height function** $h : E(K) \to \mathbb{R}$ satisfies the following.

- For all $Q \in E(K)$, there exists $C_1 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$h(P + Q) \leq 2h(P) + C_1.$$

- There exists $C_2 \in \mathbb{R}$ such that for all $P \in E(K)$,

$$4h(P) \leq h(2P) + C_2.$$

- For all $C_3 \in \mathbb{R}$, the set

$$\{P \in E(K) \mid h(P) \leq C_3\}$$

  is finite.

Ongoing for $K = \mathbb{Q}$. Probably not ready for general K?

Future

Potential future projects:

- n-division polynomials and structure of $E(K)[n]$
- formal groups and local theory
- ramification theory $\implies$ full Mordell-Weil theorem
- Galois cohomology $\implies$ Selmer and Tate-Shafarevich groups
- modular functions $\implies$ complex theory
- algebraic geometry $\implies$ associativity, finally

Thank you!