2022 Xena Project Undergraduate Workshop

Thursday, 29 September 2022

Elliptic curves and Mordell's theorem

David Ang

London School of Geometry and Number Theory

Integer solutions

Consider Mordell's equation

$$y^2 = x^3 + k, \qquad k \in \mathbb{Z}.$$

What are the integer solutions?

k	$\#\{(x,y) \in \mathbb{Z}^2 : y^2 = x^3 + k\}$
-24	0
-6	0
-5	0
-1	1
7	0
11	0
16	2

- $k = 7$: none (mod 4 and 8)
- $k = 16$: $(0, \pm 4)$ (use UF of $\mathbb{Z}$)
- $k = -1$: $(1, 0)$ (use UF of $\mathbb{Z}[i]$)

Siegel's theorem says that there are only finitely many integer solutions.

Rational solutions

Consider Mordell's equation

$$y^2 = x^3 + k, \qquad k \in \mathbb{Z}.$$

What about the rational solutions?

k	$\#\{(x,y) \in \mathbb{Z}^2 : y^2 = x^3 + k\}$	$\#\{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 + k\}$
-24	0	0
-6	0	0
-5	0	0
-1	1	1
7	0	0
11	0	∞
16	2	2

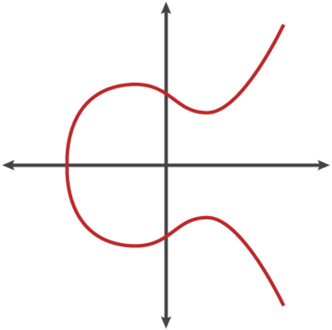
$k = 11$:

$$(-\tfrac{7}{4}, \pm\tfrac{19}{8}), (\tfrac{41825}{5776}, \pm\tfrac{8676719}{438976}), (\tfrac{6179109049}{10788145956}, \pm\tfrac{3747956961949325}{1120521567865896}), \ldots$$

Mordell's theorem says that the rational solutions are finitely generated.

Elliptic curves

If $k \neq 0$, Mordell's equation defines an *elliptic curve*.



More generally, an **elliptic curve** over a field F is a pair $(E, \mathcal{O})$ of

- a smooth projective curve E of genus one defined over F, and
- a distinguished point $\mathcal{O}$ on E defined over F.

Weierstrass equations

By the *Riemann-Roch theorem*, any elliptic curve over a field F is the projective closure of a plane cubic equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in F,$$

where $\Delta \neq 0$, [1] and the distinguished point is the unique point at infinity.

With this definition, an elliptic curve over F is precisely the data of the five coefficients $a_1, a_2, a_3, a_4, a_6 \in F$ and a proof that $\Delta \neq 0$.

```
def Δ_aux {R : Type} [comm_ring R] (a₁ a₂ a₃ a₄ a₆ : R) : R :=
 let
  b₂ := a₁^2 + 4*a₂,
  b₄ := 2*a₄ + a₁*a₃,
  b₆ := a₃^2 + 4*a₆,
  b₈ := a₁^2*a₆ + 4*a₂*a₆ − a₁*a₃*a₄ + a₂*a₃^2 − a₄^2
 in
  −b₂^2*b₈ − 8*b₄^3 − 27*b₆^2 + 9*b₂*b₄*b₆

structure EllipticCurve (R : Type) [comm_ring R] :=
 (a₁ a₂ a₃ a₄ a₆ : R) (Δ : units R) (Δ_eq : ↑Δ = Δ_aux a₁ a₂ a₃ a₄ a₆)
```

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

K-rational points

With this definition, a point on an elliptic curve E over F is either

- the unique point at infinity, or
- the data of its coordinates $x, y \in F$ and a proof that $(x, y) \in E$.

However, it will be important to also consider points defined over a field extension K of F, the K-**rational points** $E(K)$ of E.

Thus, a K-rational point on E is either

- the unique point at infinity, or
- the data of its coordinates $x, y \in K$ and a proof that $(x, y) \in E(K)$.

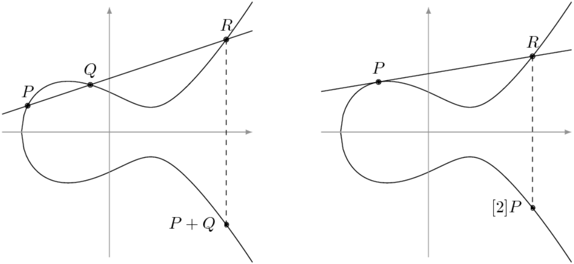
```
variables {F : Type} [field F] (E : EllipticCurve F) (K : Type) [field K] [algebra F K]

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
```

Group law

More importantly, $E(K)$ can be endowed with a group structure.

Group operations are characterised by

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



Note that if $a_1 = a_3 = 0$, then E is symmetric about the x-axis, so (x, y) lies in the the 2-**torsion subgroup** $E[2] := \ker(E \xrightarrow{\cdot 2} E)$ precisely if $y = 0$.

Identity and negation

More importantly, $E(K)$ can be endowed with a group structure.

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⟩
```

Addition

More importantly, $E(K)$ can be endowed with a group structure.

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
    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 ... −− 100 lines
   else if y_ne : y₁ + y₂ + E.a₁*x₂ + E.a₃ ≠ 0 then
    let
     L := (3*x₁^2 + 2*E.a₂*x₁ + E.a₄ − E.a₁*y₁) / (2*y₁ + E.a₁*x₁ + E.a₃),
     x₃ := L^2 + E.a₁*L − E.a₂ − 2*x₁,
     y₃ := −L*x₃ − E.a₁*x₃ − y₁ + L*x₁ − E.a₃
    in
     some x₃ y₃ ... −− 100 lines
   else
    zero

instance : has_add E(K) := ⟨add⟩
```

Group axioms

More importantly, $E(K)$ can be endowed with a group structure.

The remaining group axioms are doable except associativity.

```
lemma zero_add (P : E(K)) : 0 + P = P := ... -- trivial

lemma add_zero (P : E(K)) : P + 0 = P := ... -- trivial

lemma add_left_neg (P : E(K)) : -P + P = 0 := ... -- trivial

lemma add_comm (P Q : E(K)) : P + Q = Q + P := ... -- 100 lines

lemma add_assoc (P Q R : E(K)) : (P + Q) + R = P + (Q + R) := ... -- ?? lines
```

Associativity is known to be mathematically difficult with several proofs.

- Just bash out the algebra!
- Via the *uniformisation theorem* in complex analysis.
- Via the *Cayley-Bacharach theorem* in projective geometry.
- Via identification with the *degree zero Picard group*.

All methods require significant further work.

Functoriality and Galois module structure

Modulo associativity, what basic properties can be stated or proven?

Functoriality from field extensions to abelian groups.

```
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
```

Structure of invariants under a Galois action.

```
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
```

Isomorphism of elliptic curves

Modulo associativity, what basic properties can be stated or proven?

Isomorphism given by an admissible change of variables.

```
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 { ... }⟩
```

2-division polynomial and 2-torsion subgroup

Modulo associativity, what basic properties can be stated or proven?

Polynomial determining points in the 2-torsion subgroup.

```
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 and cardinality of the 2-torsion subgroup.

```
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
```

Mordell's theorem

Modulo associativity, what basic properties can be stated or proven?

Theorem (Mordell)

$E(\mathbb{Q})$ is finitely generated.

```
instance : add_group.fg E(ℚ)
```

As a consequence of the structure theorem, $E(\mathbb{Q})$ can be written as the product of a finite group and a finite number of copies of $\mathbb{Z}$.

Proof of Mordell's theorem.

Three steps.

- **Weak Mordell**: $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.
- **Heights**: $E(\mathbb{Q})$ 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.

□

Weak Mordell

Proof that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

- Reduce to $a_1 = a_3 = 0$, so that $y^2 = x^3 + a_2x^2 + a_4x + a_6$.
- Reduce to $E[2] \subset K$, so that $y^2 = (x - e_1)(x - e_2)(x - e_3)$.
- Define a homomorphism

$$\begin{array}{rcrcc} \delta & : & E(K) & \longrightarrow & K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \\ & & \mathcal{O} & \longmapsto & (1,1) \\ & & (e_1,0) & \longmapsto & ((e_1-e_2)(e_1-e_3), e_1-e_2) \\ & & (e_2,0) & \longmapsto & (e_2-e_1,(e_2-e_1)(e_2-e_3)) \\ & & (x,y) & \longmapsto & (x-e_1, x-e_2) \end{array}.$$

- Prove $\ker(\delta) = 2E(K)$ by an explicit computation.
- Prove $\mathrm{im}(\delta) \subseteq K(S,2)$ by a simple p-adic analysis.
- Prove $K(S,2)$ is finite by classical algebraic number theory.

□

Selmer groups

Here $K(S, 2)$ is a **Selmer group**, more generally given by

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

where S is a finite set of primes of K.

The finiteness of $K(S, n)$ reduces to the finiteness of $K(\emptyset, n)$, which boils down to two fundamental results in classical algebraic number theory.

- The *class group* Cl_K is finite.
- The *unit group* $\mathcal{O}_K^\times$ is finitely generated.

Then $K(\emptyset, n)$ can be nested in a short exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \to K(\emptyset, n) \to \mathrm{Cl}_K[n] \to 0,$$

whose flanking groups are both finite, so $K(\emptyset, n)$ is also finite.

Heights and descent

Proof that $E(\mathbb{Q})/2E(\mathbb{Q})$ finite implies $E(\mathbb{Q})$ finitely generated.

There is a function $h : E(\mathbb{Q}) \to \mathbb{R}$ with the following three properties.

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

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

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

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

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

$$\{P \in E(\mathbb{Q}) : h(P) \leq C_3\}$$

  is finite.

To prove that an abelian group A endowed with such a function, such that $A/2A$ is finite, is finitely generated is an exercise in algebra. □

Future

Potential future projects:

- Generalise 2-division polynomials into n-division polynomials to determine the structure of n-torsion subgroups in general.
- Explore the theory over finite fields and prove the Hasse-Weil bound.
- Verify the correctness of Schoof's and Lenstra's algorithms.
- Explore the theory over local fields via defining formal groups.
- Define the classical Selmer group and the Tate-Shafarevich group with Galois cohomology of elliptic curves.
- Define an elliptic curve as a projective scheme and reprove all results using this definition and some form of the Riemann-Roch theorem.
- Explore the theory over global function fields.
- Explore the complex theory to prove the uniformisation theorem and state some version of the modularity theorem.

Thank you!