

# Elliptic Curves

D. Zack Garza

March 14, 2020

## Contents

<b>1</b>	<b>Wednesday January 8</b>	<b>1</b>
<b>2</b>	<b>Mordell-Weil Groups</b>	<b>2</b>
<b>3</b>	<b>Monday January 13th</b>	<b>4</b>
3.1	Every Abelian Group is a Class Group . . . . .	4
3.2	Proof Sketch . . . . .	4
3.2.1	Step 1 . . . . .	4
3.2.2	Step 2 . . . . .	4
3.2.3	Step 3 . . . . .	5
3.3	Mordell-Weil . . . . .	6
<b>4</b>	<b>Wednesday January 15th</b>	<b>6</b>

## List of Definitions

3.1	Definition – Replete . . . . .	5
3.2	Definition – Weakly Replete . . . . .	5
4.1	Definition . . . . .	8

## List of Theorems

3.1	Theorem – Claborn - Leedham - Green - Clark . . . . .	4
3.2	Theorem – Mordell-Weil . . . . .	6
4.1	Theorem – Height Descent . . . . .	8

## 1 Wednesday January 8

Summary:

1. Mordell-Weil theorem
  - For elliptic curves over global fields (number fields, function fields, finite fields, etc)

- Proof uses Galois cohomology and height functions, essentially one proof!
  - Holds for abelian varieties, but more difficult (need an analog of height functions, i.e. an  $x$ -coordinate)
2. Height functions (possibly)
  3. Elliptic curves over  $\mathbb{Q}_p$  or complete discrete valuation fields (see Silverman for basics, possibly Chapter 5), particularly Tate curves
  4. Weil-Chatelet groups  $E/k$  related to  $H^1(k; E)$  with coefficients in the elliptic curve
  5. Galois representation of  $E/k$  for  $\text{char } k = 0$ , for  $\rho_n g_k \rightarrow \text{GL}(2, \mathbb{Z}/n\mathbb{Z})$  which leads to  $\hat{\rho} : g_k \rightarrow \text{GL}(\hat{\mathbb{Z}})$ .

## 2 Mordell-Weil Groups

Let  $E/k$  be an elliptic curve over a field  $k$ , i.e. a smooth, projective, geometrically integral curve of genus 1 with a  $k$ -rational point  $O$ .

Note: Silverman good for foundations, but assumes  $k$  is perfect! Here we'll assume  $k$  is arbitrary.

**Remark:** If  $k$  is not algebraically closed, such a point  $O$  may not exist.

By Riemann-Roch (easy computation)  $E$  embeds (non-canonically) into  $\mathbb{P}^2/k$  as a Weierstrass cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \Delta \neq 0.$$

This is a smoothness condition, and this equation has a  $k$ -rational point at infinity  $[0 : 1 : 0]$ . The line at infinity is a flex line (?), and so only intersects this curve at one point.

If  $\text{char } k \neq 2, 3$  then  $y^2 = x^3 + Ax + B$ .

Every elliptic curve is given by a Weierstrass equation, although not in a unique way.

**An amazing fact:** The  $k$ -rational points  $E(k)$  forms an abelian group with zero as the identity.

*Proof:*

1. Given any plane cubic  $C/k$  and an origin  $O \in C(k)$ , the chord and tangent process yields a group structure. Note that there is a symmetry in connecting rational points  $a, b$  with a line intersecting at another rational point  $c$  which is not present in most groups, so an additional inversion about  $O$  is needed to actually make this into a group. Proving associativity: difficult!
2. Look at  $\text{Pic}^0 E$ , the degree 0 divisors on  $E$  mod birational equivalence (?), which is equal to the degree 0 line bundles on  $E$  mod bundle isomorphism.

**Exercise:** Show there is a map  $C(k) \rightarrow \text{Pic}^1 C$  given by sending  $p$  to its equivalence class; this is a bijection by Riemann-Roch (straightforward exercise).

We can then compose this with a map  $\text{Pic}^1 \rightarrow \text{Pic}^0 C$  given by  $D \mapsto D - [O]$ , which decreases the degree by 1. This gives a map  $\Phi : C(k) \rightarrow \text{Pic}^0 C$ , just need to check that  $\Phi(P \oplus Q) = \Phi(P) + \Phi(Q)$ .

Check that the groups are independent of the  $k$ -rational point chosen, i.e. changing rational points yields isomorphic groups. So the group law itself does actually depend on the rational point, although the structure doesn't.

---

**Exercise:** Let  $(E, O)/k$  be an elliptic curve and define  $E^0 = E \setminus \{O\}$  the (nonsingular, integral) affine curve given by removing the point at infinity. Then the affine coordinate ring  $k[E^0]$  is defined as  $k[x, y]/(y^2 - x^3 - Ax - B)$ , which is a Dedekind ring.

The interesting thing about Dedekind domains: the ideal class group! (i.e. the Picard group)

This has ideal class group  $\text{Pic}[E^0]$ , and one can show that

$$\begin{aligned} \text{Pic}^0 E &\longrightarrow \text{Pic}[E^0] \\ \sum_p n_p \deg(p)[p] &\mapsto \sum_{p \neq 0} n_p [p] = \prod_p p^{n_p} \end{aligned}$$

with the sum ranging over all closed points is an isomorphism.

Just note that the RHS can't have a point at infinity, so we just forget it. The isomorphism follows from some exact sequence with correction terms that vanish.

So the Mordell-Weil group of  $E(k)$  is isomorphic to  $\text{Pic}[E^0]$ , the class group of a dedekind domain (?).

**Definitions:** Let  $G$  be a commutative group.

- $G$  is a *class group* iff there exists a dedekind domain  $R$  such that  $G \cong \text{Pic} R$ .
- $G$  is an (*elliptic*) *Mordell-Weil group* iff there exists a field  $k$  and an elliptic curve  $E/k$  such that  $G \cong E(k)$ .

*Questions:*

1. Which  $G$  are class groups?
2. Which  $G$  are Mordell-Weil groups?

An answer to question 1:

**Theorem (Clayborn, 1966):** Every commutative  $G$  is a class group.

Subsequent proofs: Leetham-Green (1972) and Clark (2008) following Rosen, and uses elliptic curves. See the end of Pete's Commutative Algebra notes!

An answer to question 2:

Consider  $E/\mathbb{C}$ , then  $E(\mathbb{C}) \cong S^1 \times S^1$ , so the torsion subgroup is  $T(1) := (\mathbb{Q}/\mathbb{Z})^2 = \bigoplus_{\ell} (\mathbb{Q}_{\ell}/\mathbb{Z}_{\ell})^2$ .

This in fact holds for any algebraically closed field of characteristic zero.

**Fact:** For any  $E/k$ , the Mordell-Weil group  $E(k)$  is “ $T(1)$ -constrained”, i.e.  $E(k)[\text{tors}] \hookrightarrow T(1)$ .

**Theorem (Clark, 2012):**  $G$  is a Mordell-Weil group  $\iff G$  is  $T(1)$ -constrained.

Note: the analogous statement for abelian varieties, i.e being  $T(g)$  constrained for some other genus  $g \neq 1$ , is open. Fixing  $k = \mathbb{Q}$  still yields very interesting problems. Computing the rank and torsion subgroups is currently open, and the subject of modern research.

---

## 3 Monday January 13th

### 3.1 Every Abelian Group is a Class Group

**Theorem 3.1** (*Claborn - Leedham - Green - Clark*).

Any commutative group is the class group of some Dedekind domain.

Also see: partial re-proof by Rosen that uses elliptic curves. This theorem: mostly a proof in commutative algebra, see end of Pete's commutative algebra notes.

### 3.2 Proof Sketch

Let  $E/k$  be an elliptic curve over a field.

#### 3.2.1 Step 1

Note that  $\text{End}_k(E) \cong_{\mathbb{Z}} \mathbb{Z}^{a(E)}$  where  $a(E) \in \{1, 2, 4\}$ .

Could be  $\mathbb{Z}$  as a  $\mathbb{Z}$ -module, could be an order in the imaginary quadratic field (e.g. a quaternion algebra)

There is a short exact sequence

$$0 \longrightarrow E(k) \longrightarrow E(k(E)) \longrightarrow \text{End}_K(E) \longrightarrow 0.$$

This splits because (as seen above), the RHS term is free and thus projective. So

$$E/k(E) \cong E(k) \oplus \mathbb{Z}^{a(E)}.$$

Note that  $k(E)$  is an extension of  $E_k$  to  $E_{k(E)}$  the field of rational functions over  $k$ ? (function field). To simplify, take  $a(E) = 1$  and  $E(k) = \{0\}$ .

Taking  $k = \mathbb{Q}$ , this happens (probably, asymptotically) half of the time. It's easy to write down an elliptic curve that satisfies these conditions

Then  $E/k(E) \cong \mathbb{Z}$ .

Now pass to the field of rational functions over this field, taking  $E(k(E)(E/k(E)))$ . Then  $k^2(E) := k(E)(E/k(E))$ , and inductively define  $k^n(E)$  by passing to function fields. So  $E(k^n(E)) \cong \mathbb{Z}^n$ .

So we can construct elliptic curves that have any free commutative group as their Mordell-Weil group.

#### 3.2.2 Step 2

Loosely speaking, we'll iterate this process transfinitely. Then for any set  $S$ , there exists a field  $k$  and an elliptic curve  $E/k$  such that  $E(k) \cong \bigoplus_S \mathbb{Z}$ . We now want to introduce a process that allows passing to quotients. And  $R := k[E^0]$  is the affine coordinate ring of  $E$ , remove the point at infinity (?).

## 3.2.3 Step 3

Let  $R$  be a Dedekind domain. Note it has a fraction field with a certain ideal class group. Let  $W \subset \max\text{Spec } (R)$ , then

$$R^W := \bigcap_{\mathfrak{p} \in \max\text{Spec } R \setminus W} R_{\mathfrak{p}}.$$

Then  $R^W$  is Dedekind (and every overring of a Dedekind domain is of this form) and  $\max\text{Spec } (R^W) = \max\text{Spec } (R \setminus W)$ .

Then

$$\text{Pic } R^W = \text{Pic } R / \langle [\mathfrak{p}] \mid \mathfrak{p} \in W \rangle.$$

Note that if  $(A, +)$  is a commutative group, writing  $A = \bigoplus_S \mathbb{Z}/H$ , we have a Dedekind domain  $R = k[E^0]$  such that  $\text{Pic } R = \bigoplus_S \mathbb{Z}$ .

Note:  $\text{Pic } R$  is the class group.

**Definition 3.1** (Replete).

A Dedekind domain  $R$  is **replete** iff every element of the class group  $\text{Pic } R$  is the class group  $[\mathfrak{p}]$  of some ideal  $\mathfrak{p} \in \max\text{Spec } (R)$ .

Is every ideal class the class of a prime ideal? For  $k$  a field,  $R = \mathbb{Z}_k$ . This follows from Chebotom (?) Density (most important theorem for arithmetic geometers!)

**Definition 3.2** (Weakly Replete).

A Dedekind domain  $R$  is **weakly replete** iff every subgroup  $H \subset \text{Pic } R$  is generated by classes of prime ideals.

**Exercise (Easy)**  $K[E^0]$  is weakly replete, and an easy application of Riemann-Roch shows that if  $0 \neq p \in E(k) = \text{Pic } k[E^0]$ , then  $[p] \in \text{Pic } k[E^0]$  is generated by a prime ideal.

Note: most applications of Riemann-Roch to elliptic curves are easy! In this case, it gives you an identification  $E \cong \text{Pic } {}^1(E)$ .

So there exists a subset  $W \subset \max\text{Spec } k[E^0]$  such that  $\langle [p] \mid p \in W \rangle = H$ . Then

$$\text{Pic } k[E^0]^W \cong \bigoplus_S \mathbb{Z}/H \cong A.$$

■

Note that Dedekind domains don't have to be replete or even weakly replete. The class group of a Dedekind domain could be  $\mathbb{Z}$ , and the class of every prime ideal could be  $1 \in \mathbb{Z}$

*Proof (Claborn).*

Start with an arbitrary Dedekind domain  $R$  and attach one that's replete.

Can ask for a similar result for abelian varieties, there are conjectures here, few clear results.

Need to get  $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ , since these occur as Mordell-Weil groups. Take a modular curve and a generic point. Look at universal elliptic curves over elliptic curves and take their Mordell-Weil groups (?)

If  $k$  is algebraically closed and  $\text{char } k = p$ , can't have  $\mathbb{Z}(p) \times \mathbb{Z}/(p)$ . Consider the  $p$ -primary torsion  $E_k[p^\infty]$ . It is zero iff  $E$  is supersingular (no points of order  $p$ ). It is  $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim \mathbb{Z}/(p^n)$  iff  $E$  is ordinary.

Can sometimes reduce to cases where  $k = \mathbb{C}$  and do things analytically. ■

### 3.3 Mordell-Weil

#### Theorem 3.2 (Mordell-Weil).

Let  $k$  be a global field (extension of  $\mathbb{Q}$  or function field over  $\mathbb{F}_p$ ) and  $E/k$  an elliptic curve. Then  $E(k) \cong \mathbb{Z}^r \oplus T$  (by classification of abelian groups) where  $T$  is finite, and  $T \cong \mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$  for  $m \mid n$ . So  $T$  is generated by at most two elements.

*Proof (3 steps).*

**Step 1:** Weak Mordell-Weil theorem.

Take any  $n \geq 2$  and  $\text{char } k$  not dividing  $n$ . Show that  $E(k)/nE(k)$  is finite.

**Step 2:** Define a height function  $h : E(k) \rightarrow \mathbb{R}$  satisfying 3 properties (see next time). This is approximately a quadratic form.

Decompose at places of a number field, see Number Theory II.

**Step 3:** For any commutative group  $A$ , there is a notion of a height function

$$h : A \rightarrow \mathbb{R}.$$

Show the Height Descent Theorem: if  $A$  admits a height function and  $A/nA$  is finite for some  $n \geq 2$ , then  $A$  is finitely generated.

Also how you'd prove this theorem for abelian varieties, more difficulty defining  $h$ . ■

## 4 Wednesday January 15th

Recall that we're trying to prove the Mordell-Weil theorem. Let  $K$  be a global field, so it's the field of functions over some nice curve. Then the Mordell-Weil group  $E(K)$  is finitely generated.

**Step 1:** The weak Mordell-Weil theorem for all  $n \geq 2$  with  $\text{char } k$  not dividing  $n$ ,  $E(k)/nE(k)$  is finite.

**Step 2:** Construction of a height function  $h : E(K) \rightarrow \mathbb{R}$  that is "trying" to be a quadratic form.

**Step 3 (Today):** The Height Descent Theorem, i.e. if  $(A, +)$  is a commutative group such that  $A/nA$  is finite for some  $n \geq 2$  and it admits a height function  $h : A \rightarrow \mathbb{R}$ , then  $A$  is finitely generated.

*Question:* What does the weak Mordell-Weil group  $E(K)/nE(K)$  tell us about  $E(K)$ ?

---

Note that we'll inject this into a larger group, which we'll show is finite, but this isn't great for learning about the size.

**Example 4.1.**

Consider  $E/\mathbb{C}$ , then  $E(\mathbb{C}) = S^1 \times S^1$  and  $E(\mathbb{C})/nE(\mathbb{C}) = 0$ , so the map  $x \rightarrow nx$  is a surjective map and  $E(K)$  is  $n$ -divisible here. In general, whenever  $K = \overline{K}$  is algebraically closed, then  $x \mapsto nx$  is again surjective and the weak Mordell-Weil group is trivial. So knowing this is small doesn't tell us much about  $E(K)$  at all.

**Example 4.2.**

For  $E/\mathbb{R}$ ,  $E(\mathbb{R})$  is either  $S^1$  (cubic with one real root,  $\Delta = 0$ ) or  $S^1 \times \mathbb{Z}/(2)$  (cubic with three real roots,  $\Delta > 0$ ) are the two possible group structure.

Then

$$\begin{cases} 0 & n \text{ odd} \\ 0 & n \text{ even and } \Delta < 0. \\ \mathbb{Z}/(2) & n \text{ even and } \Delta > 0 \end{cases}$$

**Example 4.3.**

Consider  $E/\mathbb{Q}_p$ , then for all  $\ell \gg 0$   $E(\mathbb{Q}_p) \xrightarrow{[\ell]} E(\mathbb{Q}_p)$  with  $E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) = 0$  while  $E(\mathbb{Q}_p)/pE(\mathbb{Q}_p)$  is not zero.

Note: here is an example of a Boolean space, that ends up being homeomorphic to a Cantor set.

Suppose  $E(K)$  is finitely generated, so  $E(K) \cong \mathbb{Z}^r \oplus T$  with  $T$  finite. Then knowing  $E(K)/nE(K)$  gives an upper bound on  $r$ .

**Example 4.4.**

Take  $n = 2$ , then  $E(K)/nE(K) \cong (\mathbb{Z}/(2))^s$  for some  $s \in \mathbb{N}$ . Then  $(\mathbb{Z}^r \oplus T)/2(\mathbb{Z}^r \oplus T) \cong (\mathbb{Z}/(2))^r \oplus T/2T$  for  $r \leq s$ . Then either

- $r = 2$  and  $E(K[2]) = (0)$ .
- $r = 1$  and  $E(K[2]) \cong \mathbb{Z}/(2)$ ,
- $r = 0$  and  $E(K[2]) \cong (\mathbb{Z}/(2))^2$ .

Note that we don't need the Mordell-Weil theorem to compute the torsion subgroups of  $E(k)$ . It is often easier to compute these directly. For all non-archimedean places  $v$  of  $K$ ,  $E(K_v)[\text{tors}]$  is finite (see Silverman?) and embeds into a number of finite things.

To compute  $E(K_v)[\text{tors}]$ ,

1. Find  $N \in \mathbb{Z}^+$  such that  $E(k)[\text{tors}] \subset E[N]$ .
  - Choose 2 different places  $v_0, v_1$  of good reduction (from Weierstrass equation) with different residue characteristics  $\ell_1 \neq \ell_2$

- Consider the map  $E(K_{v_i})[\text{tors}] \rightarrow E(\mathbb{F}_{v_i})$
  - The kernel is a finite  $p_i$ -primary group.
  - Comes down to torsion and formal groups, see first course.
2. Compute  $E[N](K)$  (several algorithms, just checking for rational points on a zero-dimensional variety?)

See division polynomials, can check for roots of polynomials over any global field. Easy to check for rational points on finite fields.

Suppose  $E(K) \cong \mathbb{Z}^r \oplus T$  is finitely generated and we know  $E(K)/nE(K)$  for some  $n$  and we know  $T$ . Then we explicitly know  $r$ .

See Tate Shafarevich group – important! But difficult, a piece of information that helps compute the rank (?).

**Definition 4.1.**

Fix  $n \geq 2$ . An  $n$ -height function on  $(A, +)$  is a map  $h : A \rightarrow \mathbb{R}$  satisfying

1. For all  $R \geq 0$ , the set  $h^{-1}(-\infty, R)$  is finite.
2. For all  $Q \in A$ , there exists a  $C_2 = C_2(A, Q)$  such that for all  $P \in A$ ,  $h(P + Q) \leq 2h(P) + C_2$ .  
(?)
3. There exists a  $C_3 = C_3(A, n)$  such that for all  $P \in A$ ,  $h(nP) \geq n^2h(P) - C_3$

Note: (3) would be an equality for an honest quadratic function, so this deviates in a controlled way.

**Theorem 4.1 (Height Descent).**

Let  $(A, +)$  be a commutative group with an  $n$ -height function  $h : (A, +) \rightarrow \mathbb{R}$ . If  $A/nA$  is finite, then  $A$  is finitely generated.

*Proof:* Let  $r$  be the size of  $A/nA$ . Choose coset representatives  $Q_1, \dots, Q_r$  of  $nA$  in  $A$ . Let  $p \in A$  and define a sequence  $\{P_k\}_{k=0}^\infty$  in  $A$  by  $P_0 = P$  and for  $k \geq 1$ , choose  $P_k$  such that  $P_{k-1} = nP_k + Q_{i_k}$ .

Then for all  $k \in \mathbb{Z}^+$ , it's true that  $P = n^k P_k + \sum_{j=1}^k n^{j-1} Q_{i_j}$ .

**Claim 1.**

There exists a constant  $c > 0$  depending only on  $A, n$  such that for all  $P \in A$ , there exists a  $K = K(P)$  such that for all  $k \geq K$ , we have  $h(P_k) \leq 0$ .

Note that this is sufficient – if so,  $A$  is generated by  $\{Q_1, \dots, Q_r\} \cup h^{-1}((-\infty, C])$ , which are both finite.

Next time: proof of claim.

Note: similar setup goes through for abelian varieties, see Néron–Tate height canonical height, which yields an honest “quadratic form”.