Elliptic Curves

D. Zack Garza

February 28, 2020

Contents

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 char $k = 0$, for $\rho_n g_k \longrightarrow \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ which leads to $\widehat{\rho} : g_k \longrightarrow \mathrm{GL}(\widehat{\mathbb{Z}})$.

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 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 an 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 $\mathrm{Pic}^0 E$, 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 $C(k) \longrightarrow \mathrm{Pic}^1 C$ given by sending p is its equivalence class; this is a bijection by Riemann-Roch (straightforward exercise).

We can then compose this with a map $\mathrm{Pic}^1 \longrightarrow \mathrm{Pic}^0 C$ given by $D \mapsto D - [O]$, which decreases the degree by 1. This gives a map $\Phi : C(k) \longrightarrow \mathrm{Pic}^0 C$, 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 $E^0 = E \setminus \{0\}$ 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 $\mathrm{Pic} k[E^0]$, and one can show that

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

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 Pic$k[E^0]$, 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

Theorem (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.

Proof (Sketch): Let E/k be an elliptic curve over a field.

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.

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 $E(k) \cong \oplus_S \mathbb{Z}$. We now want to introduce a process that allows passing to quotients. And $R := k[E^0]$ is the affine coordinate ring of ?, remove the point at infinity (?).

Step 3: Let R be a Dedekind domain. Note it has a fraction field with a certain ideal class group. Let $W \subset \text{maxSpec } (R)$, then $R^W := \displaystyle\bigcap_{\mathfrak{p} \in \text{maxSpec } R \setminus W} R_{\mathfrak{p}}$. Then R^W is Dedekind (and every overring of a Dedekind domain is of this form) and $\text{maxSpec } (R^W) = \text{maxSpec } (R \setminus W)$.

Then $\text{Pic } R^W = \text{Pic } R / \left\langle [\mathfrak{p}] \;\middle|\; \mathfrak{p} \in W \right\rangle$. Note that if $(A, +)$ is a commutative group, writing $A = \displaystyle\bigoplus_S \mathbb{Z}/H$, we have a Dedekind domain $R = k[E^0]$ such that $\text{Pic } R = \displaystyle\bigoplus_S \mathbb{Z}$.

> Note: Pic R is the class group.

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

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

Easy exercise: $K[E^0]$ 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 $W \subset \text{maxSpec } k[E^0]$ such that $\left\langle [p] \;\middle|\; p \in W \right\rangle = H$.

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

■

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 $1 \in \mathbb{Z}$

Claborn's proof: 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 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 $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n \mathbb{Z}/(p^n)$ iff E is ordinary.

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

Theorem (Mordell-Weil): Let k be a global field (extension of $\mathbb{Q}$ or function field over $\mathbb{F}_p$) and E/k and 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 $m \Bigm| n$. So T is generated by at most two elements.

Proof (3 steps)

Step 1: Weak Mordell-Weil theorem.

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

Step 2: Define a height function $h : E(k) \longrightarrow \mathbb{R}$ 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 $h : A \longrightarrow \mathbb{R}$. 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 char k not dividing n, $E(k)/nE(k)$ is finite.

Step 2: Construction of a height function $h : E(K) \longrightarrow \mathbb{R}$ 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 heigh function $h : A \longrightarrow \mathbb{R}$, then A is finitely generated.

Question: What does the weak Mordell-Weil group $E(K)/nE(K)$ tell use 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: Consider $E/\mathbb{C}$, then $E(\mathbb{C}) = S^1 \times S^1$ and $E(\mathbb{C})/nE(\mathbb{C}) = 0$, so the map $x \longrightarrow nx$ 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: 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: 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: 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 $E(K_{v_i})[\text{tors}] \longrightarrow E(\mathbb{F}_{v_i})$
- 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: Fix $n \geq 2$. An n-height function on $(A, +)$ is a map $h : A \longrightarrow \mathbb{R}$ 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 $P \in A$, $h(nP) \geq n^2 h(P) - C_3$

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

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

Proof: Let r be the size of A/nA. Choose coset representatives $Q_1, \cdots, Q_r$ 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: 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 $\{Q_1, \cdots, Q_r\} \bigcup h^{-1}((-\infty, C])$, 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".

5 Friday January 17th

5.1 Continuing Step 3

Recall the Height Descent Theorem (see previous notes). Most important property of height function: the collection of elements under a given height is finite.

> Note that A/nA is the cokernel of multiplication by n.

Proof: Let r be the size of A/nA and choose coset representatives $Q_1, \cdots, Q_r$. For $P \in G$ (?) define $P_0 = P$ and P_k such that $P_{k-1} = nP_k + Q_i$ for any i.

For all positive $k \in \mathbb{Z}$, we have $P = n^k P_k + \sum n^j Q_i$.

Claim: There exists a $c > 0$ such that for all $P \in A$ there exists a $K = K(P)$ such that for all $k \geq K$, $h(P_k) \leq C$. If this holds, A is generated by $\{Q_i\} \bigcup h^{-1}((-\infty, C])$.

Proof of claim: Let $c_2 = \max\limits_{1 \leq i \leq r} c_2(-Q_i)$.

Then

$$
\begin{aligned}
h(P_k) &\le \frac{1}{n^2}(h(nP_k)+c_3) \\
&= \frac{1}{n^2}(h(P_{k-1}-Q_i)+c_3) \\
&\le \frac{1}{n^2}(2h(P_{k-1})+c_2+c_3) \\
&\le \frac{1}{n^2}\left(\frac{2}{n^2}(2h(P_{k-1})+c_2+c_3)+c_2+c_3\right) \quad \text{by repeating} \\
&= \left(\frac{2}{n^2}\right)^2 h(P_{k-2})+(1+\frac{2}{n^2})(c_2+c_3) \\
&= \left(\frac{2}{n^2}\right)^k h(P)+\frac{1}{n^2}\left(1+2/n^2+(2/n^2)^2+\cdots(2/n^2)^k\right)(c_2+c_3) \\
&\le \left(\frac{2}{n^2}\right)^k h(P)+\left(\frac{1}{1-\frac{2}{n^2}}\right)(c_2+c_3),
\end{aligned}
$$

where the last inequality follows because $n \ge 2$ implies the leading term is bounded by 1 and the middle term contains a convergent series.

This proves the claim for any n?

■

Definition: A function $h : A \longrightarrow \mathbb{R}$ from a commutative group is *quadratic* if the associated function $h(x+y)-h(x)-h(y) := B_h : A^2 \longrightarrow \mathbb{R}$ is bilinear. The function h is *linear* iff B_h is constant.

The function h is a *quadratic form* iff h is quadratic and for all $m \in \mathbb{Z}$ and for all $x \in A$, $h(mx) = m^2 h(x)$.

I.e. a degree 2 homogeneous function.

Theorem (Canonical Height Descent): Suppose $(A,+)$ is commutative and $h : A \longrightarrow \mathbb{R}$ is a quadratic form. Suppose

1. A/nA is finite, and
2. $h^{-1}((-\infty, R])$ is finite for all R,

then letting $y_1, \cdots, y_r \in A/nA$ be coset representatives and taking $C = \max h(y_i)$, we can conclude that A is generated by $\left\{x \in A \;\middle|\; h(x) \le C\right\}$.

5.2 Step 4

Theorem (Abstract Weak Mordell-Weil):

Let k be a field, E/k an elliptic curve, choose n such that char k doesn't divide n, and let $k' := k(E[n])$ be k with the n-torsion points of E adjoined. Note that this adjoins finitely many algebraic points to k.

Suppose there exists a Dedekind domain R with fraction field k' with finite class group, so Pic $(R) < \infty$, and $R^\times$ is finitely generated Then $E(k)/nE(k)$ is finite.

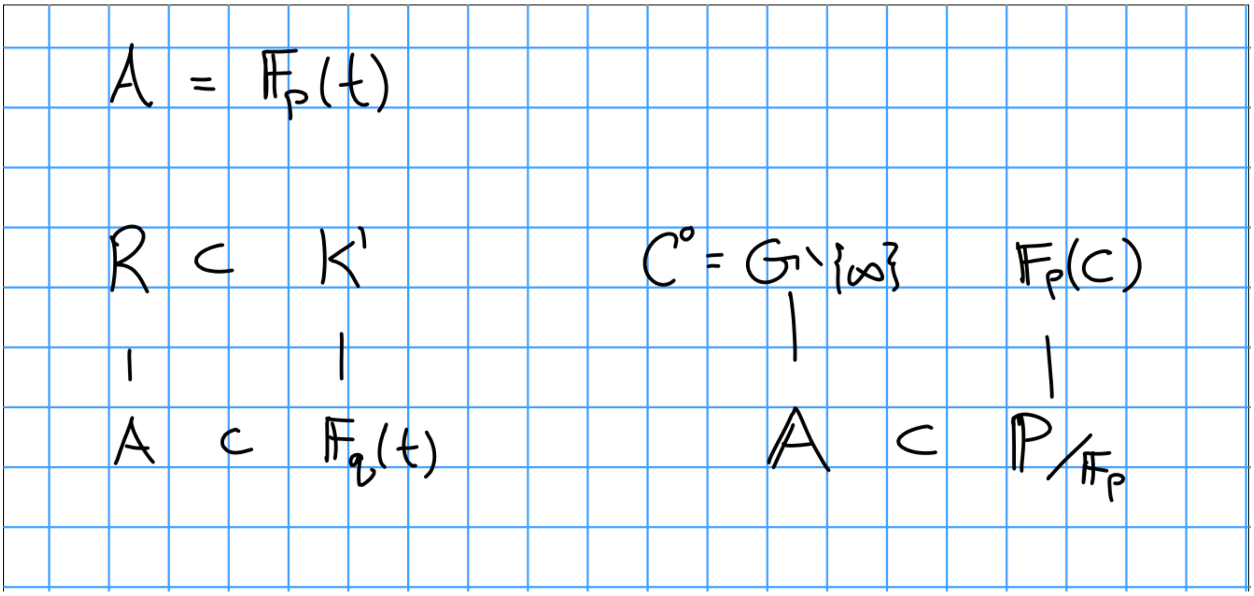

Figure 1: Image

Corollary: Let k be a global field $n \geq 2$, then $E(k)/nE(k)$ is finite.

Proof: k is a number field, so is k'. Pick $k' = \mathbb{Z}_k$, which is a Dedekind domain. By Number Theory I, the hypotheses above are satisfied.

If k is a function field, $k/\mathbb{F}_p(t)$ is finite and separable, so $k'/\mathbb{F}_p(t)$ is finite and separable. For $A = \mathbb{F}_p(t)$, $A \subset \mathbb{F}_q(t)$, then take $R/A \subset k'/\mathbb{F}_q(t)$ the integral closure of A in k'. By Number Theory I, R is a Dedekind domain.

Then $R = \mathbb{F}_p[C^0]$, and by Number Theory II, Pic (R) is finite.

> Removing primes makes unit group larger and the class group smaller.

> Localizing at a prime ideal yields a DVR? This kills the Picard group (since it's a PID?) but blows up the units group.

> Note that the proof for abelian varieties adapts very easily.

■

Sketch of proof:

Step 1: Reduce to the case that E has full n-torsion, i.e. $k' = k$. If L/k is finite Galois (as is k'/k), and $E(L)/nE(L)$ is finite, then $E(k)/nE(k)$ is finite.

Remark: For any extension L/k, there is an injection $E(k) \hookrightarrow E(L)$, but $E(k)/nE(k)$ need not inject into $E(L)/nE(L)$. For counterexamples, take $k = \mathbb{R}$ and $\mathbb{C}/k$, then $E(\mathbb{C})/nE(\mathbb{C})$ can be trivial.

Step 2: Let $L := k([n]^{-1}E(k))$ be the compositum $k[\{P\}]$ over the $P \in E/\overline{k}$ such that $[n]P \in E(k)$ is k-rational. It's straightforward to show that L is separable and Galois (it is an etale covering). That it's galois: if $[n]P$ is rational, so is $[n]\sigma(P)$ for any σ in the galois group. We'll show that this is a finite extension.

Step 3: Construct a Kummer pairing to show that finiteness of $[L : k]$ is equivalent to $E(k)/nE(k)$ being finite.

Step 4: Reduce finiteness of $[L : k]$ to algebraic number theory.