ELLIPTIC CURVES

Elliptic curve are algebraic curves that carry a group law. As such, they are objects of algebraic geometry, but they are also of huge significance in number theory; for example, Wiles' proof of the Shimura-Taniyama conjecture for semi-stable elliptic curves over $\mathbb{Q}$ has Fermat's Last Theorem as a consequence. The aim of this course is to introduce some of the basic ideas in this area, and to prove some of the basic theorems.

Tentative list of contents:

Smooth curves in $\mathbb{A}^2$ and $\mathbb{P}^2$. Cubic curves E and the group law (via Riemann-Roch).

Over $\mathbb{C}$, $E = \mathbb{C}/\Lambda$; comparison of group laws. Abel-Jacobi map.

Morphisms and isogenies.

Elliptic curves over finite fields. The Weil conjectures.

Elliptic curves over number fields. Heights and the Mordell-Weil theorem.

The j-invariant.

The Weil pairing on torsion points. Tate modules and the action of Galois.

Good and bad reduction. The Néron model, and Grothendieck's theorem on semi-stable reduction.

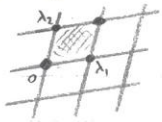
Reference

J. Silverman, Arithmetic of Elliptic Curves.

Elliptic Curves

Start with $\mathbb{C}$. In general, elliptic curves are algebraic varieties, and as such may be defined over a field, eg $\mathbb{C}, \mathbb{Q}, \mathbb{F}_p$, or over something more general, eg. $\mathbb{Z}$. Even to study things over $\mathbb{Q}$, need an understanding of things over $\mathbb{C}, \overline{\mathbb{F}_p}$.

In $\mathbb{C}$, take a lattice Λ, ie $\Lambda \cong \mathbb{Z}^2$ and Λ is discrete. So $\Lambda \cap U$ is finite $\forall$ compact $U \subset \mathbb{C}$



$\{\lambda_1, \lambda_2\}$ is a basis of Λ.

$\mathbb{C}/\Lambda$ is a torus, topologically compact. Λ acts on $\mathbb{C}$ by translation, as a group of holomorphic transformations. So $\mathbb{C}/\Lambda$ is a Riemann surface.
$\mathbb{C}/\Lambda$ also inherits an additive group law from $\mathbb{C}$. $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ descends to $\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, $(z, w) \mapsto z + w$, also holomorphic.
So, $\mathbb{C}/\Lambda$ is a compact Riemann surface with a commutative group law, and the group law is holomorphic.

Aim: find polynomial equations describing $\mathbb{C}/\Lambda$. Ie, have $f(X, Y) = 0$, f a polynomial, with X, Y meromorphic functions in $\mathbb{C}/\Lambda$, and $f = 0$ should be a relation satisfied by X, Y identically.

So, we want meromorphic functions on $\mathbb{C}/\Lambda$, ie, meromorphic functions in $\mathbb{C}$, invariant under $z \mapsto z + \lambda$.
So, define $\wp(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right)$

Remarks: (i) We must allow poles to get something non-constant (Liouville).
(ii) Must have ≥ 2 poles (Residue Theorem).

This series converges in the sense that for any compact $U \subset \mathbb{C}$, we can write $\wp(z) =$ (finitely many terms) + (something absolutely convergent). So $\wp$ is a meromorphic function in $\mathbb{C}$, and can be differentiated term by term.
We get $\wp'(z) = -2 \sum_{\lambda} (z+\lambda)^{-3}$, obviously Λ-invariant.

Lemma: $\wp$ is Λ-invariant.
Proof: Fix $\lambda \in \Lambda$. Let $g(z) = \wp(z+\lambda) - \wp(z)$. So, $g'(z) = \wp'(z+\lambda) - \wp'(z) = 0$, so g is constant. Now, $\wp(-z) = \wp(z)$, so $g(-\frac{1}{2}\lambda) = \wp(\frac{1}{2}\lambda) - \wp(-\frac{1}{2}\lambda) = 0$, so $g(z) \equiv 0$.

So $\wp$ is a meromorphic function on $\mathbb{C}/\Lambda$, as is $\wp'$.
In $\mathbb{C}$, the only poles of $\wp$ are at $\lambda \in \Lambda$. So in $\mathbb{C}/\Lambda$, the only pole of $\wp$ is at 0, and it is a double pole.
Tautologically, $\wp$ defines a holomorphic map $\mathbb{C}/\Lambda \to \mathbb{P}^1_{\mathbb{C}}$ $(= \mathbb{C} \cup \{\infty\} = \hat{\mathbb{C}} = \mathbb{C}_\infty)$, ie, the Riemann sphere, with $0 \mapsto \infty$. The double pole implies $\wp^{-1}(\infty) = 2.0$.

Recall: If X, Y are compact Riemann surfaces and $f: X \to Y$ is holomorphic, non-constant, then $\exists\, n \in \mathbb{N}$, the degree of f, such that $\forall y \in Y$, $f^{-1}(y)$ consists of n points, counted with multiplicity, and f is surjective. For $\mathbb{C}(X) :=$ field of meromorphic functions in X, then $\deg f = [\mathbb{C}(X) : \mathbb{C}(Y)]$.

Take $X = \mathbb{C}/\Lambda$, $Y = \mathbb{P}^1_{\mathbb{C}}$. $\mathbb{C}(Y) = \mathbb{C}(\wp)$, the field of rational functions of $\wp$.
So, $[\mathbb{C}(X) : \mathbb{C}(\wp)] = 2$.
$\wp$ is even as a function of z, so $\wp'$ is odd, so $\wp' \notin \mathbb{C}(\wp)$. So $\mathbb{C}(X) = \mathbb{C}(\wp, \wp')$ and $\wp'^2 \in \mathbb{C}(\wp)$.
In X, $\wp$ has a double pole at 0 and no others, so $\wp'$ has a triple pole at 0 and no others. We have $\wp'^2 = \frac{F(\wp)}{G(\wp)} = \frac{\prod(\wp(z) - a_r)}{\prod(\wp(z) - b_s)}$. If $z_0 \in \mathbb{C}$ such that $\wp(z_0) = b_s$, then $\wp'$ has a pole at z_0, so $z_0 = 0$. #, as $b_s \in \mathbb{C}$ and $\wp(0) = \infty$.
So $G = 1$, and $\wp'^2 = F(\wp) = \sum_{n=0}^{N} A_n \wp^n$. This has a pole of order $2N$.
But LHS has a pole of order 6, so $N = 3$. So $\wp'^2$ is a cubic in $\wp$.
To find this cubic explicitly, take the Laurent expansion of $\wp$.

First, define $G_{2k} = \sum_{\lambda \neq 0} \lambda^{-2k}$, for $k \geq 2$, integer. This is absolutely convergent.
(This is an Eisenstein series).
Then, $\wp(z) = z^{-2} + \sum' ((z+\lambda)^{-2} - \lambda^{-2})$, where $\sum' = \sum_{\lambda \in \Lambda, \lambda \neq 0}$.

$$= z^{-2} + \sum{}' \lambda^{-2}\left[(1 + z/\lambda)^{-2} - 1\right] = z^{-2} + \sum{}' \lambda^{-2} \sum_{n \geq 1} (n+1)(-1)^n z^n \lambda^{-n}.$$

$$= z^{-2} + \sum_{n \geq 1} (-1)^n (n+1) z^{n} \cdot \sum{}' \lambda^{-n-2} = z^{-2} + \sum_{m \geq 1} (2m+1) z^{2m} \cdot G_{2m+2} \quad (n = 2m).$$

So, $\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \dots$, so $\wp'(z) = -2z^{-3} + 6G_4 z + 20 G_6 z^3 + \dots$
So, $\wp^3$ has constant term $= 15 G_6$, and $\wp'^2$ has constant term $= 2.(-2).20G_6 = -80G_6$.

$\wp'^2 = 4z^{-6} + \dots$, $\wp^3 = z^{-6} + \dots$, so $\wp'^2 = 4\wp^3 +$ lower order terms.
In fact, $\wp'^2 = 4\wp^3 - g_2\wp - g_3$, where $g_2 = 60 G_4$, $g_3 = 140 G_6$.
Proof: Recall that the Laurent series for $\wp$ is: $\wp(z) = z^{-2} + \sum_{m \geq 1} (2m+1) z^{2m} G_{2m+2}$.
So $\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \dots$, and $\wp'(z) = -2z^{-3} + 6G_4 z + 20G_6 z^3 + \dots$
So, $\wp(z)^3 = z^{-6} + 9G_4 z^{-2} + 15 G_6 + \dots$, and $\wp'(z)^2 = 4z^{-6} - 24 G_4 z^{-2} - 80 G_6 + \dots$
$\Rightarrow \wp'^2 - 4\wp^3 = -60 G_4 z^{-2} - 140 G_6 + \dots$ - and this is at most cubic in $\wp$.
Consider most negative powers of z. Since RHS is a polynomial in $\wp$, it must be linear in $\wp$. Considering coefficients of z^{-2} and the constant term, we get $\wp'^2 - 4\wp^3 = -60G_4\wp - 140 G_6$.

Put $X = \wp$, $Y = \wp'$: $Y^2 = 4X^3 - g_2 X - g_3$ is the Weierstrass Normal Form of $\mathbb{C}/\Lambda$.

Lemma: The cubic, call it f, has no repeated roots.
Proof: Suppose $f = r^2 s$. Then $[Y/r]^2 = s$, r, s linear in X. Let $E = \mathbb{C}/\Lambda$.
Then, $\mathbb{C}(E) = \mathbb{C}(X, Y) = \mathbb{C}(S, Y) = \mathbb{C}(s) = \mathbb{C}(\mathbb{P}^1_{\mathbb{C}})$.
Basic fact about Riemann surfaces and smooth algebraic projective curves.
Given two such, say A, B, $A \cong B \Leftrightarrow \mathbb{C}(A) = \mathbb{C}(B)$. But E is a torus and $\mathbb{P}^1_{\mathbb{C}}$ is a sphere. $\left[\mathrm{disc}\,(X^3 - \frac{1}{4}g_2 X - \frac{1}{4}g_3) = -4(-\frac{g_2}{4})^3 - 27(-\frac{g_3}{4})^2 = \frac{1}{16}(g_2^3 - 27g_3^2) \neq 0\right]$

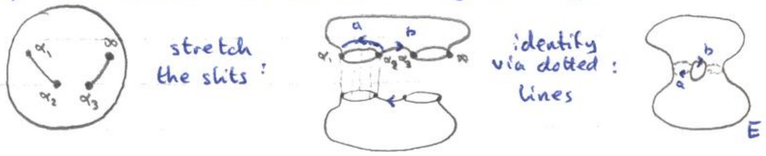
Conversely: start with $y^2 = f(x)$, f cubic, no repeated roots. Put $\omega = \frac{dx}{y} = \frac{dx}{\sqrt{f}}$

Put $z = \int_0^u \frac{dx}{y} = z(u)$. Jacobi: invert this equation: $u = u(z)$. $\frac{dz}{du} = \frac{1}{y(u)}$.

So, $\frac{du}{dz} = y(u) = \sqrt{f(u)}$, so $u'^2 = f(u)$.

Construct a Riemann Surface of y. Ie, a Riemann Surface where y is single-valued.

Say zeroes of f are $\alpha_1, \alpha_2, \alpha_3$.



E = Riemann Surface of y, by construction, $\mathbb{C}(E) = \mathbb{C}(\mathbb{P}^1_{\mathbb{C}})(y = \sqrt{f(x)}) = \mathbb{C}(x, y)$.

Aim: prove $E = \mathbb{C}/\Lambda$, some Λ.

ω is a single-valued 1-form on E. A priori ω is meromorphic. But local calculations $\Rightarrow$ ω is holomorphic everywhere in E, including at ∞. (Exercise).

Define $\lambda_1 = \int_a \omega$, $\lambda_2 = \int_b \omega$. (In fact, $\lambda_1 = 2\int_{\alpha_2}^{\alpha_1} \frac{dx}{y}$, $\lambda_2 = 2\int_{\alpha_2}^{\alpha_3} \frac{dx}{y}$).

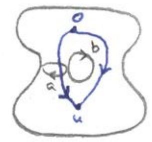
Set $\Lambda = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2 \subseteq \mathbb{C}$.

Lemma: Λ is a lattice, ie, λ_1, λ_2 are linearly independent over the reals.

Proof: Postponed.

Define $\alpha: E \to \mathbb{C}/\Lambda$, $u \mapsto \int_0^u \omega$. (Fix base point $0 \in E$).

Any two paths from 0 to u differ by something homologous to $ma + nb$, with $m, n \in \mathbb{Z}$. So $\int_0^u \omega$ is defined modulo $m\int_a \omega + n\int_b \omega \in \Lambda$. So α is defined, and is holomorphic



~~Claim: have $\beta: \mathbb{C}/\Lambda \to E$, $z \mapsto (\wp(z), \wp'(z))$.~~

We will prove later that α is an isomorphism.

Focus now on cubic equation, $y^2 = 4x^3 - g_2 x - g_3$, where disc (RHS) $\neq 0$.

This defines a curve in $\mathbb{C}^2$. More generally, if $g_2, g_3 \in$ field k, then we get a curve in $k^2 = \mathbb{A}^2_k$.

Introduce $\mathbb{P}^2_k$: This is an object with 3 coordinates, ie a point $p = (x, y, z)$, where $(x, y, z) = (\lambda x, \lambda y, \lambda z)$ for any $\lambda \in k^* = k - \{0\}$, and x, y, z are not all zero.

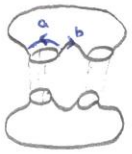
ie, $\mathbb{P}^2_k = (k^3 - \{0\})/k^*$.

$\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$: $(x, y) \mapsto (x, y, 1)$. $= \{(x, y, z) : z \neq 0\}$.

Also, $\mathbb{P}^2 - \{\alpha x + \beta y + \gamma z = 0\} \cong \mathbb{A}^2$, with $\alpha, \beta, \gamma \in k$, not all zero. Ie, given any homogeneous polynomial $F(x, y, z)$, the equation $F = 0$ makes sense in $\mathbb{P}^2$ and defines a curve there.

$\mathbb{P}^1 - (\text{point}) \cong \mathbb{A}^1$, $\mathbb{P}^2 - \mathbb{P}^1 \cong \mathbb{A}^2$.

Recall that if E is the Riemann Surface of $y^2 = f(x)$, $\deg f = 3$, distinct roots, then E is a torus:

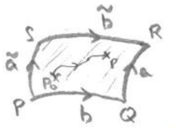


$\omega = \frac{dx}{y}$, a holomorphic 1-form on E (no poles).

$\lambda_1 = \int_a \omega$, $\lambda_2 = \int_b \omega$, $\in \mathbb{C}$.

Need to prove: λ_1, λ_2 linearly independent over $\mathbb{R}$, so $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ is a lattice in $\mathbb{C}$.

Proof: E is topologically a torus; cut it open along a, b to get E^*, which is simply connected, so $\exists$ a holomorphic function f in E^*.



$\omega = df$. $\left(f(p) = \int_{P_0}^{P} \omega \right)$.

$\lambda_2 = \int_b \omega = \int_b df = \int_{\tilde{b}} df$, $\lambda_1 = \int_a \omega = \int_a df = \int_{\tilde{a}} df$.

Let $\gamma = \partial E^* = b + a - \tilde{b} - \tilde{a}$.

Compute $\int_\gamma \bar{f}\omega = \int_a - \int_{\tilde{a}} + \int_b - \int_{\tilde{b}}$. Parametrize $a, \tilde{a}$ simultaneously by t, a by $\delta = \delta(t)$, $\tilde{a}$ by $\tilde{\delta} = \tilde{\delta}(t)$.

Then $f(\delta(t)) - f(\tilde{\delta}(t))$ is constant, so $= f(Q) - f(P) = \lambda_2$.

So, $\int_a \bar{f}\omega - \int_{\tilde{a}} \bar{f}\omega = \bar{\lambda}_2 \int_a \omega = \bar{\lambda}_2 \lambda_1$. Similarly, $\int_b \bar{f}\omega - \int_{\tilde{b}} \bar{f}\omega = -\bar{\lambda}_1 \lambda_2$.

So, $\int_\gamma \bar{f}\omega = \bar{\lambda}_2 \lambda_1 - \bar{\lambda}_1 \lambda_2 = 2i\,\mathrm{Im}(\lambda_1 \bar{\lambda}_2)$.

Compute LHS: say $f = u + iv$, so $\omega = du + i dv$. Then $\bar{f}\omega = \frac{d(u^2+v^2)}{2} + i(u dv - v du)$.

Green's Theorem: $\int_\gamma \bar{f}\omega = 0 + i \int_\gamma (u dv - v du) = i \int_{E^*} du dv$.

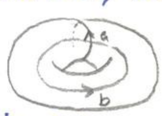
Now suppose z is a local complex coordinate at a point in E^*, say $z = x + iy$. Then, $du dv = \left| \frac{df}{dz} \right| dx dy$. So $\int_{E^*} du dv > 0$. So $\mathrm{Im}(\lambda_1 \bar{\lambda}_2) \neq 0$, ie, λ_1, λ_2 are linearly independent over $\mathbb{R}$. So Λ is a lattice.

We then defined $\varphi : E \to \mathbb{C}/\Lambda$ as follows: fix a base point $P_0 \in E$, and then $\varphi(p) = \int_{P_0}^{P} \omega$.

Proposition: φ is an isomorphism.

Proof: $d\varphi = \omega$. Claim: ω is holomorphic and has no zeroes (Proof: exercise).

So $d\varphi$ is never 0. Note that E, $\mathbb{C}/\Lambda$ are 2-dimensional manifolds, and are compact. So $d\varphi$ is an isomorphism at every point.



E is a torus, as is $\mathbb{C}/\Lambda$. So $H_1(E, \mathbb{Z}) \cong \pi_1(E) \cong \mathbb{Z}a \oplus \mathbb{Z}b$.

$\pi_1(\mathbb{C}/\Lambda) = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$. φ induces $\varphi_* : \pi_1(E) \to \pi_1(\mathbb{C}/\Lambda)$, $a \mapsto \lambda_1$, $b \mapsto \lambda_2$, by construction. So φ_* is an isomorphism.

Apply result from topology: If $\varphi : M \to N$ is a morphism of compact manifolds (respectively Riemann surfaces, smooth projective curves) with $d\varphi$ everywhere an isomorphism, and $\varphi_* : \pi_1(M) \to \pi_1(N)$ an isomorphism, then φ is an isomorphism. (Consequence of the theory of covering spaces).

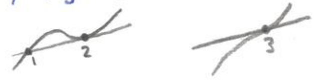
Apply to $\varphi : E \to \mathbb{C}/\Lambda$ - this is an isomorphism.

Return to $\mathbb{P}^2$. K a field, $\mathbb{P}^2_K = \{(a,b,c) : a,b,c \text{ not all zero}\} / (a,b,c) \sim \lambda(a,b,c)$.

$a, b, c \in$ some extension field of K, usually allow $a, b, c \in \bar{K}$, an algebraic closure of K.

Then, homogeneous polynomials, eg $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, define interesting subsets of $\mathbb{P}^2_K$. Have $\mathbb{A}^2 \subset \mathbb{P}^2$, eg $\mathbb{A}^2 = \{Z \neq 0\}$. Here, X, Y, Z are homogeneous coordinates on $\mathbb{P}^2_K$. X, Y, Z are not functions on $\mathbb{P}^2$. Only defined up to simultaneous rescaling. But, eg, X/Y is a function; it is a rational function. Also, $\frac{X^2+YZ}{Y^2+X^2}$ is a rational function.

Bézout's Theorem: If f, g are homogeneous polynomials in X, Y, Z, of degrees d, e respectively, then the curves $(f=0)$, $(g=0)$ intersect in de points, counted with multiplicity. Eg, $d=3, e=1$:



Example: (i) $F = Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3$, $G = Z$. Then $F = G = 0$ is given by $Z = 0 = X^3$. So line G has triple contact with F at the point $(0:1:0)$.
(ii) $F = Y^2Z - 4X^3 + g_2XZ^2$, $G = X$. Then $F = G = 0$ is given by $X = Y^2Z = 0$. So this is $(0:1:0)$ with multiplicity 1, and $(0:0:1)$ with multiplicity 2.

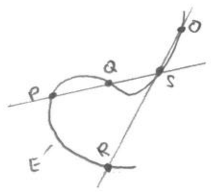
Smoothness: Intuitively, a curve $C \subset \mathbb{P}^2$, given by $F = 0$, is smooth if, at every point $p \in C$ (with coefficients in $\bar{K}$), there is a tangent line.
This turns out to be equivalent to the condition that F and $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ are never simultaneously zero. If $\operatorname{char} K \nmid \deg F$, this is equivalent to saying that $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ are never simultaneously zero.

Definition: Given K, an elliptic curve over K is a smooth cubic curve E in $\mathbb{P}^2_K$, with a fixed point $O \in E$, such that the coordinates of O lie in E. Implicitly, we demand that the equation defining E should have coefficients in K.

Example: $\operatorname{char} K \neq 2, 3$. $F = Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3$, $g_2, g_3 \in K$, disc. $(4X^3 - g_2X - g_3) \neq 0$. This is an elliptic curve, with $O = (0,1,0)$.

Our definition turns out to be equivalent to:
(i) E is a smooth projective curve over K with group law defined over K.
(ii) E is a smooth projective curve over K with a point defined over K, and $g(E) = 1$, ie, the K-vector space of global 1-forms is 1-dimensional.

Group law on a smooth cubic curve E in $\mathbb{P}^2_K$, where E has a point O, defined over K will be $\oplus$, with O as origin. $P \oplus Q = R$, defined as follows:

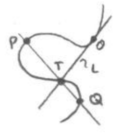


Draw S = third point of intersection of E with line PQ.
Then R = third point of intersection of E with line OR.
(If $P = Q$, for example, take tangent line to E at P).
This is the chord and tangent construction.

Claim: (i) $\oplus$ is commutative.

(ii) O is an identity. Say $\overline{PO} \cap E = \{P, O, S\}$. So $\overline{OS} \cap E = \{O, S, P\}$, so third point is P, which we started with.

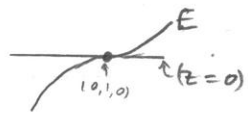
(iii) Each P has an additive inverse. Take tangent line to E at O, say L. Then $L \cap E = O$ (twice) $+ T$, say. Then $-P$ is the third point of $\overline{PT} \cap E$.



Claim: $P \oplus Q = O$. By construction, T is third point of $\overline{PQ} \cap E$, and $\overline{OT}$ meets O twice. So O is the third point of $\overline{OT} \cap E$, so $O = P \oplus Q$.

Natural way of proving associativity is via the Riemann-Roch Theorem.
First, give a direct proof, only valid over $\mathbb{C}$, for E: $Y^2 Z = F(X, Z)$, where F is a homogeneous cubic polynomial in 2 indeterminates. Note that E is the obvious projective model of the curve. $F \in \mathbb{P}^2$. $y^2 = f(x)$ in $\mathbb{A}^2$, where $y = Y/Z$, $x = X/Z$, $f = F/Z^3$.

E = curve $y^2 - f(x)$ with 1 point added, namely $(0,1,0) = P$. The line $z=0$ meets E at P, counted 3 times. (P is a 'flex')



$k = \mathbb{C}$: E is then the Riemann Surface of $y^2 = f(x)$.
So $E \cong \mathbb{C}/\Lambda$.

Theorem: Take $O \in E$ to be $0 \in \mathbb{C}/\Lambda$. Then $\oplus$ in E is the same as $+$ in $\mathbb{C}/\Lambda$.
Proof: Key point turns out to be:

Proposition: Given $P_1, \dots, P_n, Q_1, \dots, Q_n \in \mathbb{C}/\Lambda$, we have $\sum P_i = \sum Q_i \Leftrightarrow \exists$ meromorphic function f in $\mathbb{C}/\Lambda$ such that f has zeroes precisely at the P_i and poles precisely at the Q_i. (Assume $P_i \neq Q_j$)

Proof: Recall $\wp(z) = z^{-2} + \sum'((z+\lambda)^{-2} - \lambda^{-2})$ - this is meromorphic and even, so has no residue. So can construct $\zeta(z) = -\int \wp(u)\,du = z^{-1} - \int_0^z \sum'((z+\lambda)^{-2} - \lambda^{-2})\,dz$.
This is a single-valued function (meromorphic) in $\mathbb{C}$, and $\zeta' = -\wp$.
Can integrate: $\zeta(z) = z^{-1} + \sum'[(z+\lambda)^{-1} + \lambda^{-2}z - \lambda^{-1}]$
Now, $\wp(z+\lambda) = \wp(z)$ $\forall z \in \mathbb{C}$. Fix basis $\{\lambda_1, \lambda_2\}$ of Λ. So, $\zeta(z+\lambda_\alpha) = \zeta(z) + \eta_\alpha$, some constant η_α $(\alpha = 1, 2)$. So the set of poles is invariant under Λ.
So ζ has poles just at points in Λ. At 0, ζ has a simple pole, res $= +1$, so the same is true for all points of Λ.
So, $\int \zeta(z)\,dz$ is multi-valued; its value changes by $\pm 2\pi i$ if path of $\int$ moves across a pole. So, $\sigma(z) := \exp \int \zeta(u)\,du$ is single-valued.
So $\sigma(z) = \exp\left(\log z + \int_0^z (\zeta(u) - u^{-1})\,du\right) = z \exp\left(\sum'(\log(z+\lambda) + \frac{1}{2}\lambda^{-2}z^2 - \lambda^{-1}z - \log\lambda)\right)$
$= z \prod'\left(\frac{(z+\lambda)}{\lambda} \cdot \exp\left(\frac{z^2}{2\lambda^2} - \frac{z}{\lambda}\right)\right)$.
Visibly, σ is holomorphic at 0, and has a zero there. Also, $\prod'$ is even, so $\sigma(-z) = -\sigma(z)$. Certainly, σ is holomorphic away from points in Λ, since ζ is holomorphic away from Λ.
From $\sigma = \exp(\int \zeta)$ and $\zeta(z+\lambda_\alpha) = \zeta(z) + \eta_\alpha$, we get $\sigma(z+\lambda_\alpha) = c.\exp(\eta_\alpha z).\sigma(z)$, c a constant of integration.

Let $z = \frac{1}{2}\lambda_\alpha$. $\sigma(\frac{1}{2}\lambda_\alpha) = -c.\exp(\frac{\eta_\alpha \lambda_\alpha}{2})\sigma(\frac{1}{2}\lambda_\alpha)$, so $c = -\exp(-\frac{\eta_\alpha\lambda_\alpha}{2})$

So, $\sigma(z+\lambda_\alpha) = -\exp(\eta_\alpha(z - \frac{\lambda_\alpha}{2})).\sigma(z)$, so σ has a simple zero at each point in Λ. On $\mathbb{C} - \Lambda$, $\sigma = \exp(\text{holo.})$, so $\neq 0$. So σ is holomorphic in $\mathbb{C}$.

We can now return to the proposition.

($\Rightarrow$): By abuse of notation, write $P_i, Q_i \in \mathbb{C}$, with $\Sigma P_i - \Sigma Q_i = \lambda \in \Lambda$.

Replace P_n by $P_n - \lambda$, so $\Sigma P_i = \Sigma Q_i$ in $\mathbb{C}$. Then define $f(z) = \prod_i \frac{\sigma(z-P_i)}{\sigma(z-Q_i)}$, a meromorphic function on $\mathbb{C}$, with zeroes the P_i, poles the Q_i.

$$f(z+\lambda_\alpha) = \prod_i\left(-\exp(\eta_\alpha(z-P_i-\lambda_\alpha/2)).\sigma(z-P_i)\right) \Big/ \prod_i\left(-\exp(\eta_\alpha(z-Q_i-\lambda_\alpha/2)).\sigma(z-Q_i)\right).$$

$$= \frac{(-1)^n \exp[n\eta_\alpha(z-\lambda_\alpha/2)]\exp(-\eta_\alpha\Sigma P_i).\prod\sigma(z-P_i)}{(-1)^n\exp[n\eta_\alpha(z-\lambda_\alpha/2)].\exp(-\eta_\alpha\Sigma Q_i)\prod.\sigma(z-Q_i)} = f(z).$$

Compare: On $\mathbb{P}^1$, every rational function is $\prod(z-\alpha_i)/\prod(z-\beta_i)$. The Riemann sphere is simpler than a torus – here, we need σ-functions, which are examples of a theta-function.

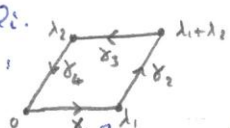
So far, we have proved that if $\Sigma P_i = \Sigma Q_i$ on $\mathbb{C}/\Lambda$, then $\exists$ a meromorphic function f on $\mathbb{C}/\Lambda$. $(f) = \Sigma P_i - \Sigma Q_i$, where (f) = "divisor of f" = (locus of zeroes of f) – (locus of poles of f).

On any Riemann Surface X, the points generate a free abelian group, $\mathrm{Div}(X)$, so $(f) = \Sigma n_P P - \Sigma n_Q Q$. Beware confusion of 2 notations of addition on $\mathbb{C}/\Lambda$, or on any elliptic curve.

So, must now prove: if $(f) = \underbrace{\Sigma P_i - \Sigma Q_i}_{\text{this is in } \mathrm{Div}(\mathbb{C}/\Lambda)}$, then $\underbrace{\Sigma P_i}_{\text{this is in } \mathbb{C}/\Lambda} = \Sigma Q_i$ in $\mathbb{C}/\Lambda$.

Proof: If γ is a simple closed paths in $\mathbb{C}$, and f is meromorphic within and on γ, and there the zeroes of f are at P_i, the poles at Q_i.

$\int_\gamma z.\frac{f'(z)}{f(z)}dz = 2\pi i(\Sigma P_i - \Sigma Q_i)$. Take γ = parallelogram:



$\{\lambda_1, \lambda_2\}$ a basis of Λ.

On γ_3, substitute $u = z - \lambda_2$, $du = dz$. So, $\int_{\gamma_3} = \int_{z=\lambda_1+\lambda_2}^{\lambda_2} = \int_{u=\lambda_1}^{0}(u-\lambda_1)\frac{f'(u-\lambda_1)}{f(u-\lambda_1)}du$

$= \int_{\lambda_1}^{0} u.\frac{f'(u)}{f(u)}du - \lambda_1\int_{\lambda_1}^{0}\frac{f'(u)}{f(u)}du = -\int_{\gamma_1} - \lambda_1[\log f(u)]_{\lambda_1}^{0} = -\int_{\gamma_1} - \lambda_1.2\pi i m$, $m \in \mathbb{Z}$.

So $\lambda_1 + \lambda_3 = 2\pi i m\lambda_1$. Similarly, $\lambda_2 + \lambda_4 = 2\pi i n \lambda_2$. So $\frac{1}{2\pi i}\int_\gamma \in \Lambda$.

So $\Sigma P_i - \Sigma Q_j \in \Lambda$.

Meromorphic functions take us from complex analysis to algebraic geometry.

Recall: If $C \subset \mathbb{P}^2_k$, $(k = \bar{k})$, is a smooth curve of degree d, and suppose $Q_1, .., Q_d \in C$ are collinear, and suppose $P_1, .., P_d \in C$. Then, the P_i are collinear $\Leftrightarrow$ $\exists$ rational function f in C: $(f)_0 = \Sigma Q_i$ and $(f)_\infty = \Sigma P_i$ (ΣQ_i is linearly equivalent to ΣP_i, $\Sigma Q_i \sim \Sigma P_i$).

Proof of ($\Rightarrow$): Suppose $\Sigma Q_i = C \cap (L=0)$, $\Sigma P_i = C \cap (M = 0)$, where L, M are homogeneous linear polynomials. Then $f = (L/M)|_C$.

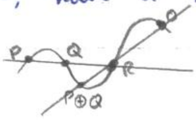
of ($\Leftarrow$): More generally, a similar statement is true for curves C embedded in $\mathbb{P}^n$ by a complete very ample linear system. Any $C \subset \mathbb{P}^2$ is embedded on a complete linear system.

Prove that $\oplus$ on a smooth cubic $C \subset \mathbb{P}^2_{\mathbb{C}}$ is associative, at least when equation of C is $Y^2Z = F(X,Z)$, $\deg F = 3$. In this case, $\pi: C \xrightarrow{\cong} \mathbb{C}/\Lambda$, $p \mapsto \int_0^p dw$, $w = \frac{dx}{y}$, $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.

Lemma: Suppose $P, Q \in \mathbb{C}/\Lambda$, $P \neq Q$. Then $\nexists$ meromorphic function f on $\mathbb{C}/\Lambda$ with $(f)_0 = P$, $(f)_\infty = Q$.

Proof: Any non-constant meromorphic f defines $\mathbb{C}/\Lambda \xrightarrow{f} \mathbb{P}^1_{\mathbb{C}}$. If $(f)_0 = P$, then $f^{-1}(0) = P$, with multiplicity 1, so f has deg 1. Then f is an isomorphism $= \#$, eg. for topological reasons.

On C, have a fixed point O, $\pi(O) = 0$. Claim: $\pi(P \oplus Q) = \pi(P) + \pi(Q)$.

Proof: 

$\exists$ a rational function f on C, with zeroes at P, Q, R and poles at $O, R, P \oplus Q$. Ie, $(f)_0 = P, Q$, $(f)_\infty = O, P \oplus Q$.

So, $P + Q = O + (P \oplus Q)$ in $\mathbb{C}/\Lambda$, by Residue Theorem result.

Ie, $\pi(P) + \pi(Q) = \pi(O) + \pi(P \oplus Q) = \pi(P \oplus Q)$.

So $\oplus$ on C is the same as $+$ on $\mathbb{C}/\Lambda$, and so $\oplus$ is a group law (in particular, associative).

To prove that $\oplus$ is associative over any k, it is enough to do it over $\bar{k}$.

Riemann-Roch for an elliptic curve C over $\bar{k}$, says: If $D = \sum n_P P \in \mathrm{Div}(C)$, $\deg D = \sum n_P = d$, then $\dim L(D) = d$, where $L(D) = \{\text{rational functions } f \text{ in } C : (f) \geqslant D\} \cup \{0\}$, a vector space over k.

The Picard Group of C, $\mathrm{Pic}(C) := \mathrm{Div}(C)/\sim$, where $\sim$ is linear equivalence.

Have a map $\varphi: C \to \mathrm{Pic}^0(C)$, $P \mapsto [P - O]$, where $[D] = D \bmod \sim$, $D \sim E \iff D - E \in (f)$.

Claim: $\varphi(P \oplus Q) = \varphi(P) + \varphi(Q)$.

Proof: $(P \oplus Q) + R + O \sim P + Q + R$ (as in above diagram). So $(P \oplus Q) + O \sim P + Q$.

So, $(P \oplus Q) - O \sim (P - O) + (Q - O)$. So $\varphi(P \oplus Q) = \varphi(P) + \varphi(Q)$.

Claim: φ is 1-1 as a map of sets.

Proof: (i) Suppose $\varphi(P) = \varphi(Q)$. Then $P - O \sim Q - O$, so $P \sim Q$. So $\exists f$ with $(f) = P - Q$.

Get $f: C \to \mathbb{P}^1$. As before, $\deg f = 1$. Basic fact (to be elaborated): C has a 1-form ω with no zeroes and no poles. ω is unique, modulo scalars.

But on $\mathbb{P}^1$, $\nexists$ such a ω. So (i) holds, ie φ is injective.

(ii) Suppose $[D] \in \mathrm{Pic}^0(C)$. $[O = O_C = \text{base-point in } C = \text{origin of } \oplus]$. So $\deg(D + O_C) = 1$.

So by Riemann-Roch, $\exists f$ with $(f) \geqslant D + O_C$. So $D + O_C \sim E$, $E = \sum n_R R$, all $n_R \geqslant 0$.

Ie, $E \geqslant 0$. $\deg E = \deg(D + O_C) = 1$, so $E = R$. Then $[D] = \varphi(R)$, so φ is surjective.

So, via φ, can identify $\oplus$ with $+$. So $\oplus$ is associative.

Over $\mathbb{C}$, gives $C: Y^2Z = f(X,Z)$, get $\oplus$ in C, grouplaw. This result holds for any smooth cubic in $\mathbb{P}^2$, over any k.

Corollary: Over $\mathbb{C}$, the group of points of C dividing n is isomorphic to $(\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$

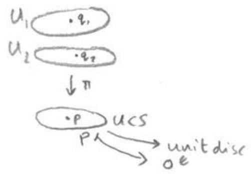
Proof: Group law on C has been identified with $+$ on torus $\mathbb{C}/\Lambda \cong S^1 \times S^1$, and on S^1, the n-torsion points form a copy of $\mathbb{Z}/n\mathbb{Z}$. ie, $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ under multiplication - n^{th} roots of unity.

So, if $E = \mathbb{C}/\Lambda$, then the group $\{x \in E : nx = 0\} \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$, of order n^2.
We know that $\mathbb{C}/\Lambda \cong$ Riemann Surface of $y^2 = f(x)$, f a cubic. Can make $y^2 = f(x)$ into a homogeneous cubic, $Y^2Z = F(X,Z)$, $f(x) = F(X,1)$, $(0,1,0) = 0$.
Have $E \to \mathbb{C}/\Lambda \xrightarrow{\wp} \mathbb{P}^1$, $0 \mapsto 0 \mapsto \infty$. $\hookrightarrow$ This cubic gives a curve $C \subset \mathbb{P}^2_{\mathbb{C}}$, and $0 \in C$.

Lemma: If $C \subset \mathbb{P}^2_k$ is a smooth cubic and $0 \in C$, 0 defined over k, then (provided char $k \neq 2,3$) we can choose homogeneous coordinates in $\mathbb{P}^2$ such that the equation of C is $Y^2Z = F(X,Z)$, F a homogeneous cubic in X, Z.

Proof: An equation $y^2 = f(x)$ exhibits the corresponding curve as a 2-to-1 cover of $\mathbb{P}^1$, branched at 4 points, one being at ∞. ie, take $C \subset \mathbb{P}^2$ given by $Y^2Z = F(X,Z)$, $x = X/Z$, $y = Y/Z$. Have: $\pi: C \to \mathbb{P}^1$, $(X,Y,Z) \mapsto (X,Z)$, or $(x,y) \mapsto x$.

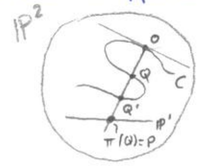
Over $\mathbb{C}$, given $R \xrightarrow{\pi} S$, a holomorphic map of compact Riemann Surfaces, $\deg \pi = 2$.
Given $P \in S$, $\exists$ 2 possibilities for the structure of π in a neighbourhood of P.

(i) 

$\exists$ neighbourhood U of P in S such that $\pi^{-1}(U) = U_1 \cup U_2$, $U_1 \cap U_2 = \phi$, and π induces $U_1, U_2 \xrightarrow{\cong} U$.
$\Leftrightarrow \pi^{-1}(P) = \{P_1, P_2\}$, $P_1 \neq P_2$

(ii) π is branched over $P \Leftrightarrow \pi^{-1}(P) = \{P_1\}$, one point with multiplicity 2.
Then $\exists$ Local coordinates z on S near P and w on R near P_1, such that $z = w^2$.
A Local coordinate on S at P is a function z, analytic on a neighbourhood U of P, such that $z(P) = 0$ and $z'(P) \neq 0$.

Now suppose $C \subset \mathbb{P}^2$, $0 \in C$, C smooth, defined by homogeneous cubic. Projection



from 0 gives $\pi: C \to \mathbb{P}^1$ [with $\pi(0) = (T_0 C) \cap$ (fixed $\mathbb{P}^1$)].
$\pi^{-1}(P) = \{Q, Q'\}$. So $\deg \pi = 2$.

From the Algebraic Geometry course, genus of $C = g(C) = 1$, $g(\mathbb{P}^1) = 0$. We have the Riemann-Hurwitz formula: $2g(C) - 2 = (\deg \pi)(2g(\mathbb{P}^1) - 2) + \sum_{\substack{x \in C \\ \pi \text{ branched} \\ \text{over } \pi(x)}} e_x$, where $e_x = 1$ for such x when $\deg \pi = 2$.

So, $0 = 2(-2) + \underbrace{\#\{x \in C : \pi \text{ is branched over } \pi(x)\}}_{= \#\{y \in \mathbb{P}^1 : \pi \text{ is branched over } y\}}$.

So $\exists$ just 4 points in $\mathbb{P}^1$ over which π is branched.

Choose homogeneous coordinates (X, Z) on $\mathbb{P}^1$ such that one of these points is $(1, 0)$. Then in terms of $x = X/Z$, this point is $x = \infty$. Say other three points are $x = a, b, c$. Then π exhibits C as the Riemann Surface of $y^2 = f(x) = (x-a)(x-b)(x-c)$. $\deg \pi = 2$ means $k(C)$ is a quadratic extension of $k(\mathbb{P}^1) = k(x)$. So $k(C) = k(x, w)$, $w^2 = \varphi(x) = p(x)/q(x)$. Same as $(wq)^2 = pq$. Write $y = wq$, so $y^2 = pq$.

This equation shows that $\pi : C \to \mathbb{P}^1$ is branched at $(pq = 0)$. But we know where π is branched, viz. a, b, c, ∞. So $pq = f$.
So indeed, any smooth cubic $C \subset \mathbb{P}^2$, with $O \in C$, can be written as $y^2 = f(x)$ in certain inhomogeneous coordinates, so as $Y^2 Z = F(X, Z)$ in homogeneous coordinates.
Over $\mathbb{C}$, we started with $y^2 = f(x)$, $\deg f = 3$, and then constructed $\mathbb{C}/\Lambda$ by integrating $\frac{dx}{y} = \frac{dx}{\sqrt{f}}$. So over $\mathbb{C}$, any smooth cubic in $\mathbb{P}^2$ is isomorphic to $\mathbb{C}/\Lambda$.

Given a smooth projective curve C over k, the genus of C is $\dim_k H^0(\Omega^1_C)$, where $H^0(\Omega^1_C)$ is the k-vector space of 1-forms on C with no poles, ie which are regular everywhere
Basic fact: If $C \subset \mathbb{P}^2$ is a smooth cubic, then $g(C) = 1$. Ie, up to scalars, $\exists$ a unique 1-form ω on C. In fact, ω has no zeroes either.

Example: If C is given by $Y^2 Z = F(X, Z)$, then $\omega = \frac{dx}{y}$, where $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.
If C is given by $H(X, Y, Z) = 0$, $\deg H = 3$, then put $h(X, Y) = H(X, Y, 1)$.
So in affine terms, C is given by $h(x, y) = 0$. Then $\omega = \frac{dx}{(\partial h/\partial y)}$.

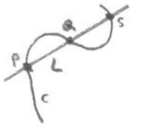
$g(\mathbb{P}^1_k) = 0$. Eg, have inhomogeneous coordinate x. Try $\omega = dx$. This has no zeroes or poles on $\mathbb{P}^1 - \{\infty\}$, but ω has a double pole at ∞. (Calculate in terms of a local coordinate at ∞, eg $1/x$).

$k = \mathbb{C}$: Compact Riemann Surfaces = oriented compact surface, so has 'holes'
$\#$ holes = topological genus.

Families of Elliptic Curves.

Aim: to provide geometric intuition underlying the arithmetic case. Eg, visualise reduction mod p, and the geometry of reduction mod p.

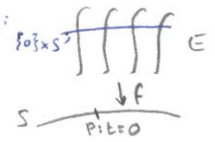
$Y^2 Z = F(X, Z) = 4X^3 - g_2 X Z^2 - g_3 Z^3$ $(\circledast)$, giving $C \subset \mathbb{P}^2_{\mathbb{R}}$, with $g_2, g_3 \in \mathbb{R}$. Have a group law $\oplus$ on C, with $O = (0, 1, 0)$ as origin. $C \times C \xrightarrow{\oplus} C$, $(P, Q) \mapsto P \oplus Q$. $\oplus$ is a morphism of algebraic varieties. Ie, the homogeneous coordinates of $P \oplus Q$ are polynomial functions of the homogeneous coordinates of P, Q.



Suppose ξ, η are homogeneous coordinates on $L \cong \mathbb{P}^1_k$. Then, $L \cap C$ is given by $G(\xi, \eta) = 0$, a homogeneous cubic. If $P = (\xi = a, \eta = b)$ and $Q = (\xi = A, \eta = B)$. Then $G = (b\xi - a\eta)(B\xi - A\eta)(\beta\xi - \alpha\eta)$, so $\alpha, \beta \in k$.

But $S = (\xi = \alpha, \eta = \beta)$. Coordinates of S are then rational, or indeed polynomial, functions of the coefficients of the equation defining C, and the homogeneous coordinates of P and Q.
Similarly, coordinates of $P \oplus Q$ are rational functions of those of O and S, and so of P and Q.

Now suppose $g_2 = g_2(t)$, $g_3 = g_3(t)$, either holomorphic or polynomial functions of t. t is a coordinate on S, some Riemann Surface, or on some smooth algebraic curve, eg, $\mathbb{A}^1$.

Picture: 

E is something 2-dimensional. Explicitly, $E \hookrightarrow \mathbb{P}^2 \times S$, with $f: E \to S$ defined by the given equation.
$\dim E = \dim S + \dim(\text{fibre}) = 1 + 1$
Given $P \in S$, the fibre of f over P is $f^{-1}(P)$.

In affine coordinates, equation $y^2 = 4x^3 - g_2 x - g_3$, defining $E \hookrightarrow \mathbb{A}^2 \times S$ (Assume $S = \mathbb{A}^1$, for simplicity), so $E \hookrightarrow \underset{(x,y)}{\mathbb{A}^2} \times \underset{t}{\mathbb{A}^1} \cong \underset{(x,y,t)}{\mathbb{A}^3}$, $E_0 \hookrightarrow E$, open.

Notation: For each value $t = t_0$, let E_{t_0} be the corresponding curve, given by $Y^2 Z = 4X^3 - g_2(t_0) XZ^2 - g_3(t_0) Z^3$. This is also the fibre over the point $t = t_0$ on S.
Have an origin O on each E_{t_0}. Consider $\{O\} \times S \ (\cong S) \hookrightarrow \mathbb{P}^2 \times S$.
Every point of $\{O\} \times S$ satisfies the given equation ⊛ (end of last page)
To prove this, set $X = 0 = Z$ in ⊛. You get $0 = 0$, true $\forall t$. So $\{O\} \times S \subset E$.
So the origins on the fibres, the elliptic curves, E_{t_0} have been fitted together into $\{O\} \times S$, a copy of S.

Also, the group laws fit together. For $C \subset \mathbb{P}^2_k$ (ie, case where $g_2, g_3 \in K$), $P \oplus Q$ is a rational function of P, Q. In the case where g_2, g_3 are functions of t, have the same formula for the coordinates of $P \oplus Q$ in terms of the coordinates of P, Q. In this formula, it doesn't matter if g_2, g_3 are constant or variable.

Consider $E \times_S E = \{(P,Q) \in E \times E : f(P) = f(Q)\} \hookrightarrow E \times E$. Then have $E \times_S E \xrightarrow{F} S$, $(P,Q) \mapsto f(P) = f(Q)$. $\forall \sigma \in S$, $F^{-1}(\sigma) = f^{-1}(\sigma) \times f^{-1}(\sigma)$. We have

$$\begin{tikzcd} E \times_S E \arrow[r, "\oplus"] \arrow[dr, "F"'] & E \arrow[d, "f"] \\ & S \end{tikzcd}$$

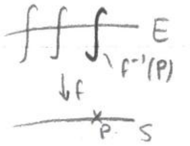
From $\oplus$, get multiplication maps $C \xrightarrow{[m]} C$, $P \mapsto mP$, m a fixed integer.
Suppose $k = \mathbb{C}$. We have seen that $\ker[m] = (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$, so $\deg[m] = m^2$.
Also, $[m]: C \to C$ is unramified. (Eg, via Riemann-Hurwitz, $2g(C) - 2 = \deg[m](2g(C) - 2) + \deg R$. $R = 0 \iff [m]$ is unramified everywhere. And, $g(C) = 1$, so $\deg R = 0$, so $R = 0$).
Or topologically, $C \cong S^1 \times S^1$. Picture of $S^1 \xrightarrow{[m]} S^1$, $m = 2$: 

Definition: $f: A \to B$, a morphism of smooth algebraic varieties, is unramified, if f induces $T_x A \xrightarrow{\cong} T_{f(x)} B$ $\forall x \in A$. (So then f is locally (in some sense) an isomorphism).

Now let k be some algebraically closed field, char $k = 0$. Then ("Lefschetz principle"), exactly same is true. But if $k \neq \bar{k}$, then $[m]$ is still unramified, still of degree m^2, but individual points of $\ker[m]$ may fail to be define over k.

Now pass to our family, $f: E \to S$. Have
$$\begin{tikzcd} E \arrow[r, "{[m]}"] \arrow[dr, "f"'] & E \arrow[d, "f"] \\ & S \end{tikzcd}$$
Ie, the multiplications $[m]$ on each fibre fit together. Then $\ker[m] \subset E$, and is an unramified cover of S of degree m^2.

Recall we had:



The group laws on each fibre $f^{-1}(P)$ fit together as a group law on the family.

Reason: if $R = P \oplus Q$, then the coordinates of R are polynomial functions of the coordinates of P, Q. These functions will involve g_2, g_3.

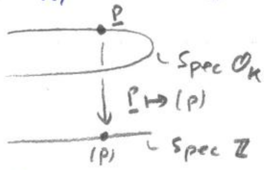
Fix $p \in S$. The condition that $f^{-1}(P)$ is smooth is that $\Delta(t) := -27g_2^2 - 9g_3^2 \neq 0$.
If $\Delta(p) = 0$, then delete P, ie, delete P if the equation giving $f^{-1}(P)$ defines a non-smooth curve.
So now, for example, $S = \mathbb{A}^1 - \{\text{finite set, where } \Delta = 0\}$.
We make take for granted that the formula for $R = P \oplus Q$ does not involve terms like $1/g_2$.
So we do have a group law on "the whole family".
Conversely, given $P \in S$, recover an elliptic curve $f^{-1}(P)$ with origin and group law.

Aim: do the same sort of thing, replacing S by the ring of algebraic integers in an algebraic number field.

Suppose we have $K/\mathbb{Q}$. Have
$$\begin{tikzcd} \mathbb{Q} \arrow[r, hook] & K \\ \mathbb{Z} \arrow[u, hook] \arrow[r, hook] & \mathcal{O}_K \arrow[u, hook] \end{tikzcd}$$
We had:

Consider $S = \operatorname{Spec} \mathcal{O}_K$, $T = \operatorname{Spec} \mathbb{Z}$. Points are the non-zero prime ideals, and (0).

If $\underline{P}$ is a prime ideal in $\mathcal{O}_K$, then $\underline{P} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.
Say $\underline{P} \cap \mathbb{Z} = (p)$, $\underline{P} \mid p$.



Ramification: $(p)\mathcal{O}_K = \underline{P}_1^{e_1} \cdots \underline{P}_r^{e_r}$, unique factorisation into prime ideals.
Then p ramifies in $\mathcal{O}_K$ <=> some $e_i > 1$. <=> in the local ring $(\mathcal{O}_K)_{\underline{P}_i}$, p generates the unique maximal ideal $(\underline{P}_i)_{\underline{P}_i}$.
<=> the $\mathbb{F}_p$-vector space $(p)/(p)^2$ generates the $k(\underline{P}_i)$-vector space $\underline{P}_i/\underline{P}_i^2$, the cotangent space to $\operatorname{Spec} \mathcal{O}_K$ at $\underline{P}_i$. [Where $k(p) = \mathbb{Z}/(p) = \mathbb{F}_p$, and $k(\underline{P}_i) = \mathcal{O}_K/\underline{P}_i = \mathbb{F}_{p^m}$, some m].

There is an obvious map, $(p)/(p)^2 \longrightarrow \underline{P_i}/\underline{P_i}^2$ induced by $(p) \hookrightarrow \underline{P_i}$. This induces a linear map of $k(\underline{P_i})$-vector spaces, $(p)/(p)^2 \otimes_{\mathbb{F}_p} k(\underline{P_i}) \longrightarrow \underline{P_i}/\underline{P_i}^2$.
Dually, this gives: $(\underline{P_i}/\underline{P_i}^2)^\vee \to ((p)/(p)^2)^\vee \otimes k(\underline{P_i})$. This is: (tangent space at $\underline{P_i}$) $\to$ (tangent space at (p)).
Eg: $k(\underline{P_i}) = \mathbb{F}_p$. Just get $\mathbb{F}_p$-linear maps $(p)/(p)^2 \to \underline{P_i}/\underline{P_i}^2$ and $(p)/(p)^2 \leftarrow (\underline{P_i}/\underline{P_i}^2)^\vee$
This induced map in tangent spaces is an isomorphism $\Leftrightarrow e_i = 1$.

Spec $\mathbb{Z}$, Spec $\mathcal{O}_K$ are 1-dimensional in the sense that $\mathbb{Z}$, $\mathcal{O}_K$ are 1-dimensional.
Ie, every non-zero prime ideal is maximal.

Suppose E is an elliptic curve over $\mathbb{Q}$, $Y^2Z = F(X,Z)$, coefficients in $\mathbb{Q}$. E has a point O (eg, $(0,1,0)$), defined over $\mathbb{Q}$. Clearing denominators, we may assume that E has $\mathbb{Z}$-coefficients. Can reduce modulo p. Get a curve E_p, cubic, in $\mathbb{P}^2_{\mathbb{F}_p}$, defined over $\mathbb{F}_p$.

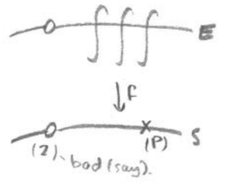
Fact: except for finitely many p, E_p is smooth. E_p contains O. So E_p has a group law.

(Eg: $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$, $g_2, g_3 \in \mathbb{Z}$. Suppose $\Delta(\text{this}) \neq 0$. $\Delta = -27g_2^3 - 9g_3^2$. Then, the bad p are $\{2, 3, p \mid \Delta\}$)

Get
$$\begin{tikzcd} E \arrow[r, hook] \arrow[dr, "f"'] & \mathbb{P}^2_{\mathbb{Z}} \arrow[d] \\ & \operatorname{Spec}\mathbb{Z} \end{tikzcd}$$
. Let $S = \operatorname{Spec}\mathbb{Z} - \{\text{bad primes}\}$. Eg, if $\{2, 3, 17\}$ are bad, then $S = \operatorname{Spec}\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{17}]$.

Start with $k[t]$. Then $\mathbb{A}^1_k = \operatorname{Spec} k[t]$. Conversely, $k[t]$ is recovered as the ring of polynomial functions on $\mathbb{A}^1_k$.
Start with $\mathbb{Z}$. Construct Spec $\mathbb{Z}$: "$\mathbb{Z}$ is the ring of functions on Spec $\mathbb{Z}$".

Picture of $E \to S$:



Have group law $E \times E \xrightarrow{\oplus} E$, which reduces mod every p to the group law on E_p.

Recall: we took k, a number field, and $\mathcal{O}_k \subset k$ the ring of integers.
Suppose $C = C_k \hookrightarrow \mathbb{P}^2_k$, $Y^2Z = F(X,Z)$ is an elliptic curve with coefficients in k. Then we may clear denominators to get an equation with coeffecients in $\mathcal{O}_k$. Then, for almost all prime ideals, $\underline{P}$, of $\mathcal{O}_k$, reducing mod $\underline{P}$ gives a smooth cubic curve $C_{k(\underline{P})}$ over field $k(\underline{P}) = \mathcal{O}_k/\underline{P}$. These are the primes of good reduction.
$\exists$ ring R, $\mathcal{O}_k \hookrightarrow R \hookrightarrow k$, obtained by deleting bad primes. The prime ideals of R are the good primes. R is finitely generated as an $\mathcal{O}_k$-algebra.

Example: $k = \mathbb{Q}$, say $2, 3, 17$ are bad primes. Then $R = \mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{17}]$.

This is a little more complicated if $\mathcal{O}_k$ is not a PID. We may at times also delete a finite set of good primes.

Get
$$\begin{tikzcd} C_R \arrow[r, hook] \arrow[dr, "f"'] & \mathbb{P}^2_R \arrow[d] \\ & \operatorname{Spec} R \end{tikzcd}$$
$\leftarrow$ points are the good primes, plus (0).

Reducing mod (0) means passing back to k. Have O. This O sits inside C_R as a copy of $\operatorname{Spec} R$.

The group laws on C_k, $C_{k(\underline{p})}$ fit together into a group law on C_R.
Fix $m \in \mathbb{N}$. Then the map "multiplication by m" gives a morphism $C_R \xrightarrow{[m]} C_R$.
We know, over $\bar{k}$, $[m]$ is surjective, and $\ker[m]$ has order m^2.
C_R is projective over $\operatorname{Spec} R$, ie it lives in $\mathbb{P}^n_R$, defined by many homogeneous polynomials.

* <u>Theorem</u>: If X_R, Y_R are projective over $\operatorname{Spec} R$, and $g: X_R \to Y_R$ is a morphism, then the image of g $(\subseteq Y_R)$ is also projective over $\operatorname{Spec} R$. *

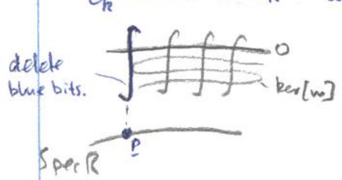
<u>Note</u>: False for affine varieties. For example, take $X = (xy = 1) \hookrightarrow \mathbb{A}^2_k$, (x, y)
$$\begin{tikzcd} X \arrow[r, hook] \arrow[dr, "f"'] & \mathbb{A}^2_k \arrow[d] & (x,y) \arrow[d, mapsto] \\ & \mathbb{A}^1_k & x \end{tikzcd}$$
Then, $\operatorname{im} f = \mathbb{A}^1_k - \{0\}$.

What does $[m]$ do to $C_{k(\underline{p})}$, $\underline{p} \neq (0)$?

<u>Proposition</u>: $[m]$ is surjective on every $C_{k(\underline{p})}$.
<u>Proof</u>: Suppose not, then $[m]$ collapses $C_{k(\underline{p})}$ to a point, (the only proper subvariety of a curve). Say D_R = image of C_R under $[m]$. Have
$$\begin{tikzcd} D_R \arrow[r, hook] \arrow[dr] & C_R \arrow[d] \\ & \operatorname{Spec} R \end{tikzcd}$$
D_R is closed, by Theorem. Over $\underline{p}$, $D_{k(\underline{p})}$ is a point.
Over k, D_k is a point or C_k. We know that over $\bar{k}$, $D_{\bar{k}} = C_{\bar{k}}$
(Think of $R \hookrightarrow \bar{k}$. $D_{\bar{k}}$ means: think of D_R as giving something defined over $\bar{k}$).
So $D_k = C_k$. So $D_R \to \operatorname{Spec} R$ has fibre D_k of dimension 1, and fibre $D_{k(\underline{p})}$ of dimension 0. This is absurd, by the following theorem. So we've done.

* <u>Theorem</u>: If we reduce something projective modulo $\underline{p}$, then the dimension can only go up. "The upper semi-continuity of fibre dimension". *

<u>Next aim</u>: Define $\ker[m] = m^{-1}(0) \hookrightarrow C_R$. Let S, $\mathcal{O}_k \hookrightarrow R \hookrightarrow S \hookrightarrow k$, be obtained by deleting all primes $\underline{p}$ with $\operatorname{char} k(\underline{p}) \mid m$. (This is a finite set).
Then there are finitely many algebraic number field $L_i \supseteq k$, and a diagram
$$\begin{tikzcd} \mathcal{O}_{L_i} \arrow[r, hook] & T_i \arrow[r, hook] & L_i \\ \mathcal{O}_k \arrow[r, hook] \arrow[u, hook] & S \arrow[r, hook] \arrow[u, hook] & k \arrow[u, hook] \end{tikzcd}$$
such that T_i is an f.g. S-module and is unramified over S, and $\coprod \operatorname{Spec} T_i = \ker[m] \cap C_S$.



Eg. one of these $L_i = k$, say L_0, and then $\operatorname{Spec} T_0 = O$.

Shall achieve this aim by showing: (i) over each good $(\mathfrak{p})$, char $k(\mathfrak{p}) \nmid m$, $\ker[m] \cap C_{k(\mathfrak{p})}$ has degree m^2, and moreover, $\ker[m] \cap C_{\overline{k(\mathfrak{p})}}$ consists of m^2 distinct points. (ii) Deduce that over $\operatorname{Spec} S$, $\ker[m]$ is unramified.
(iii) Deduce aim by some commutative algebra.

Proof of (i): Know $[m] : C_R \to C_R$ is surjective on each fibre. Pick prime $\mathfrak{p}$, and $x \in C_{\overline{k(\mathfrak{p})}}$. Then $[m]^{-1}(x) \subseteq C_{\overline{k(\mathfrak{p})}}$ is closed (in Zariski sense, ie defined by polynomial equations), so it is either finite or the whole curve, $C_{\overline{k(\mathfrak{p})}}$
Surjectivity of $[m] \Rightarrow [m]^{-1}(x)$ is finite.
Similarly for $x \in C_{\bar{k}}$: $[m]^{-1}(x)$ consists of m^2 points.
So have $[m] : C_R \to C_R$, and for all "geometric points" x, ie defined over $\bar{k}$ or over $\overline{k(\mathfrak{p})}$, $[m]^{-1}(x)$ is finite.

* Theorem: If X_R, Y_R are projective over $\operatorname{Spec} R$, if $f : X_R \to Y_R$ is a morphism and for every geometric point x, $f^{-1}(x)$ is finite, then f is finite. *

Note: "f is finite" has a strong technical meaning:
If $Z_R \hookrightarrow Y_R$, $Z_R \to \operatorname{Spec} R$ an isomorphism, then $f^{-1}(Z_R) = \operatorname{Spec} A$, where A is a ring which is fg as an R-module.

So, in our situation, we have $\mathcal{O}_S \hookrightarrow C$, $\mathcal{O}_S \xrightarrow{\cong} \operatorname{Spec}$, $C \to \operatorname{Spec}$. $\mathcal{O}_S$ is a "thickening" of $\mathcal{O} \in C_K$.
$[m]$ finite $\Rightarrow [m]^{-1}(\mathcal{O}_S) = \operatorname{Spec} T$, $S \hookrightarrow T$, T a f.g. S-module.
Also, $[m]^{-1}(\mathcal{O}_S) \cap C_{k(\mathfrak{p})} = \{m\text{-torsion points on } C_{k(\mathfrak{p})}\}$ Ie, the m-torsion points on the individual fibres fit together into $\operatorname{Spec} T$.

By construction, S is a Dedekind domain and all $C_{k(\mathfrak{p})}$ are smooth curves.
$\Rightarrow \forall$ prime ideals $\mathfrak{p} \neq 0$, $S_{\mathfrak{p}}$ is a PID.

If X is a curve over a field k, then X is smooth $\Leftrightarrow \mathcal{O}_{X,P} := \{f \in k(X) : f \text{ regular at } P\}$ is a PID.

These $\Rightarrow$ "C_S is a regular scheme".
$x \in C_S$, $\underbrace{\mathcal{O}_{C_S,x}}_{\text{this is a regular local ring, as in commutative algebra}} := \{f \in k(C_S) : f \text{ is regular at } x\}$, where $k(C_S) := k(C_K)$.
This is the algebraic analogue of smoothness in geometry.

Have $[m] : C_S \to C_S$, finite and surjective. Because C_S is regular, it follows that for all points $x \in C_S$, $[m]^{-1}(x)$ has the same "number of points", counted with multiplicity, ie, $[m]$ has constant degree. Ie, it behaves exactly as a non-constant map of projective curves or compact Riemann Surfaces.
Also, for any $C_\sigma = C_{k(\mathfrak{p})}$ or C_K, ($\sigma \in \operatorname{Spec} S$), $[m] : C_\sigma \to C_\sigma$ has same degree.
We know that for $\sigma = \operatorname{Spec} K$, $[m]$ has degree m^2.
Corollary: $[m]$ has degree m^2 on every $C_{k(\mathfrak{p})}$.

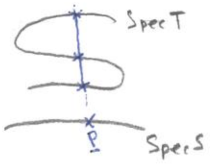
This is true even if char $k(\underline{P}) \mid m^2$.
Also, Spec T has constant degree m^2 over Spec S. So T is purely 1-dimensional.

Now, assume that $p = \text{char}\, k(\underline{P}) \nmid m$, $\forall\, \underline{P}$. Then $[m] : C_{k(\underline{P})} \to C_{k(\underline{P})}$ has degree prime to p, and so it is separable. (ie, $[m]$ induces $k(C_{k(\underline{P})}) \leftarrow k(C_{k(\underline{P})})$, purely inseparable, L, separable)

$\deg(p.i) = p^2$, so $\nexists$ purely inseparable contributions.

Riemann-Hurwitz applies to separable morphisms.
$g = g(C_{k(\underline{P})}) = 1$. So, $2g-2 = m^2(2g-2) + (\geq 0 \text{ for ramification})$.
So $[m]$ is unramified, ie over $\overline{k(\underline{P})}$. $[m]^{-1}(0) \cap C_{\overline{k(\underline{P})}}$ consists of m^2 distinct points.

<u>Corollary:</u> Spec $T \to$ Spec S is unramified, of degree m^2.



$\forall\, \underline{P} \in$ Spec S, the fibre over $\underline{P}$ in Spec T never coalesces. This is unramified. So $T = T_1 \times \cdots \times T_r$, a product of Dedekind domains, each unramified over S.

<u>Theorem:</u> (i) Suppose $x \in C_K$, x also defined over k. Then, every point y such that $my = x$ is defined over the field $L \supseteq K$, where $[L:K] \leq m^2$, and L/K is unramified outside $\{$primes in K where C_K has bad reduction$\} \cup \{$primes in K that divide $m\} = \Sigma$.
(ie, $[L:K]$ and "ramification data" of L/K are independent of y).
(ii) $\exists$ finite L/K such that $\forall\, x, y$ as in (i), y is defined over L!

...

S a Dedekind domain, $\underline{P} \neq 0$ a prime ideal. Then $S_{\underline{P}}$ has a unique maximal ideal $\underline{P}_{\underline{P}}$ $(= t)$. Suppose $S \hookrightarrow T$, T another Dedekind domain. Take Q a prime of T, $Q \mid \underline{P}$. Say $Q_Q = (u)$. Then $S_{\underline{P}} \hookrightarrow T_Q$.
$t \in (u)$. Say $t = u^e v$, v a unit in T_Q, $e \in \mathbb{N}$. Ramification $\iff e > 1$.

<u>Proof of Theorem:</u> (i) For $x = 0$, this is the statement that Spec T is unramified over Spec S. For arbitrary x, rerun the same discussion, replacing O_S by $x_S \xrightarrow{\cong}$ Spec S. $T = [m]^{-1}(x_S)$.

<u>Recall:</u> We fixed $m \geq 2$. The bad primes include those dividing m.
Have $[m] : C_S \to C_S$, multiplication by m.
Proved: $[m]^{-1}(O_S)$ is finite, of degree m^2, and unramified over Spec S.
So $[m]^{-1}(O_S) =$ Spec T, where $T = T_1 \times \cdots \times T_r$, T_i a Dedekind domain, finite (as a module) over S.

$$\begin{tikzcd} O_S \arrow[r, hook] \arrow[drr, "\cong"'] & C_S \arrow[r, hook] \arrow[dr, "f"] & \mathbb{P}^2_S \arrow[d] \\ & & \text{Spec}\, S \end{tikzcd}$$

Unramified $\Leftrightarrow$ $\forall\, \underline{p} \in \operatorname{Spec} S$, $\underline{p} \neq 0$, $T/\underline{p}T = (T_1/\underline{p}T_1) \times \cdots \times (T_r/\underline{p}T_r)$ $\cong$ a product of finite fields.

(ramified over $\underline{p}$ $\Leftrightarrow$ $T/\underline{p}T$ is non-reduced, ie $\exists \neq 0$ nilpotent elements).

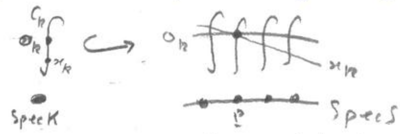
$T/\underline{p}T$ is finite over $S/\underline{p} = k(\underline{p})$. So $T/\underline{p}T$ is finite, so Artinian.

Also, unramified $\Leftrightarrow$ $T \otimes_S \overline{k(\underline{p})} \cong$ a product of m^2 copies of $k(\underline{p})$.

Now return to:

Theorem (ii): $\exists$ finite field extension L/K such that $\forall\, x = x_k \in C_k$ defined over k, every point $y \in C_k$ such that $my = x$, is defined over L.

Proof: The same argument as before shows that $[m]^{-1}(x_S)$ is finite, of degree m^2, and unramified over $\operatorname{Spec} S$.



$x_k = O_k$ modulo $\underline{p}$

$[m]^{-1}(x_S) = \operatorname{Spec} R$, $R = R_1 \times \cdots \times R_s$, R_i a Dedekind domain, finite over S.

Then $\forall\, y$ with $my = x$, the field of definition of y (ie $K(y) = K(\frac{X}{Z}, \frac{Y}{Z})$ if $y = (X:Y:Z) \in \mathbb{P}^2$) is the field of fractions of some R_i.

[Get from 2-dimensional picture over $\operatorname{Spec} S$ back to 1-d picture over $\operatorname{Spec} K$ by $-\otimes_S K$. Go in other direction by: given something on $C_k \hookrightarrow \mathbb{P}^2_k$, clear denominators to get the corresponding object in $C_S \hookrightarrow \mathbb{P}^2_S$.]

Equivalently, take Zariski closure, eg: $\operatorname{Spec} K \hookrightarrow \operatorname{Spec} S$. Its Zariski closure is $\operatorname{Spec} S$. $\mathbb{P}^2_k \hookrightarrow \mathbb{P}^2_S$ Zariski closure $= \mathbb{P}^2_S$.

$$\left.\begin{array}{ccccc} O_k & \hookrightarrow & C_k & \hookrightarrow & \mathbb{P}^2_k \\ \downarrow & & \downarrow & & \downarrow \\ O_S & \hookrightarrow & C_S & \hookrightarrow & \mathbb{P}^2_S \end{array}\right\} \text{take Zariski closure.}$$

So $[k(y):k] \leq m^2$, and $k(y)/k$ is unramified outside the fixed finite set of bad primes.

Theorem (Hermite, Minkowski): Given algebraic number field K, $d \in \mathbb{N}$, and given a finite set Σ of primes in $\mathcal{O}_K$, $\exists$ only finitely many fields L/K such that $[L:K] \leq d$ and L is unramified over K outside Σ.

Ie, given d, Σ, can bound the size of the discriminant, and apply the more usual version of this theorem.

Part (ii) above follows at once.

Aim: Prove the Mordell-Weil Theorem: Given E defined over K, the group $E(K)$ of points of E defined over K is finitely generated.

Theorem: (Weak Mordell-Weil): Fix $m \geq 2$. Assume that all points of $[m]^{-1}(0)$ are defined over K. (via a finite extension of K). Then $E(K)/mE(K)$ is a finite group.

Proof: We know $\exists$ finite L/K such that $\forall\, x \in E(K)$ and y with $my = x$, y is defined over L. Wlog L/K is Galois. $E_m := [m]^{-1}(0)$ consists of m^2 points, all defined over K. Shall construct $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E_m)$, which will prove the theorem.

Pick $x \in E(K)$. Let $\sigma \in \mathrm{Gal}(L/K)$, and pick $y \in E(L)$ with $my = x$

$\sigma(y) \in E(L)$, because σ does not change the coefficients of the polynomial defining $E \hookrightarrow \mathbb{P}^2$. Also, $[m]: E \to E$ is defined over K. So $\sigma(my) = m(\sigma(y))$.

So $m\sigma(y) = x$ also. So $m(\sigma(y) - y) = 0$.

Define $\varphi: E(K) \longrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E_m)$ by $\varphi(x) = (\sigma \mapsto \sigma(y) - y)$.

This is well-defined: Suppose $m\tilde{y} = x$, $\tilde{y} \in E(L)$. $m\tilde{y} = x = my$, so $m(\tilde{y} - y) = 0$.

Ie, $\tilde{y} - y \in E_m$, so (by assumption), $\sigma(\tilde{y} - y) = \tilde{y} - y$.

[Have $d: E \times E \to E$, $(y, z) \mapsto y - z$ is defined over K, so commutes with σ, so $\sigma(y - z) = \sigma(y) - \sigma(z)$.]

So $\sigma(\tilde{y} - y) = \sigma(\tilde{y}) - \sigma(y)$, so φ is well-defined.

Suppose $\varphi(x) = 0$, ie given y with $my = x$, have $\forall \sigma$, $\sigma(y) - y = 0$.

Ie, $y \in E(K)$ since L/K is Galois. So $\ker \varphi = mE(K)$.

Conversely, if $x = my$, $y \in E(K)$, then $\varphi(x) = 0$.

So φ induces $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E_m)$.

Suppose we have an algebraic number field K with $[K:\mathbb{Q}] = d$. $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, $\mathfrak{p} \mid p$, $p \in \mathbb{Z}$. Define $v_\mathfrak{p}: K^* \to \mathbb{Z}$, the valuation corresponding to $\mathfrak{p}$, by $v_\mathfrak{p}(x) = m \iff m$ is the power of $\mathfrak{p}$ appearing in the prime factorisation of (x).

Eg: $K = \mathbb{Q}$, $v_p(p) = 1$.

Define $\|x\|_\mathfrak{p} = (N\mathfrak{p})^{-v_\mathfrak{p}(x)/d} \in \mathbb{R}_{>0}$. If $\sigma: K \hookrightarrow \mathbb{R}$ or $\sigma: K \hookrightarrow \mathbb{C}$, define $\|x\|_\sigma = |\sigma(x)|^{1/d}$.

A place (or prime) of K is a prime ideal or an embedding $\sigma: K \to \mathbb{R}, \mathbb{C}$.

Prime ideal = finite prime/place, embedding $\hookrightarrow \mathbb{R}, \mathbb{C}$ = infinite prime/place.

Exercise: $\|x_1 + \cdots + x_N\|_\mathfrak{p} \leq \sup_i \|x_i\|_\mathfrak{p}$

$\|x_1 + \cdots + x_N\|_\sigma \leq \|N\|_\sigma \cdot \sup_i \|x_i\|_\sigma$.

Write v = a place, finite or infinite.

$\mathfrak{p}$ = a finite place.

σ = an infinite place.

M_K = { places of K }.

Extensions: Given L/K, fix $v \in M_K$. Then $\exists$ finitely many places $w \in M_L$ with $w \mid v$, and $\prod_{w \mid v} \|x\|_w = \|N_{L/K}(x)\|^{1/[L:K]}$ $\forall x \in L^*$. So for $x \in K^*$, $\prod_{w \mid v} \|x\|_w = \|x\|_v$.

Product formula: $\forall x \in K^*$, $\prod_{v \in M_K} \|x\|_v = 1$. This is in fact a finite product, almost all $\|x\|_v = 1$.

<u>Heights</u>: Suppose $P = (x_0, \dots, x_n) \in \mathbb{P}^n$, all $x_i/x_j \in K$, ie P is defined over K.
Then $H_K(P) := \prod_v \sup_i \|x_i\|_v > 0$, $h_K(P) := \log H_K(P)$, the <u>logarithmic height</u>.

<u>Eg</u>: $P = (p, q) \in \mathbb{P}^1$, p, q prime in $\mathbb{Z}$. Then $h_{\mathbb{Q}}(P) = \max(\log p, \log q)$

1. Suppose $\lambda \in K^*$. Then $\max_i \|\lambda x_i\|_v = \|\lambda\|_v \cdot \max_i \|x_i\|_v$. Since $\prod_v \|\lambda\|_v = 1$, get $H_K(\lambda x_0, \dots, \lambda x_n) = H_K(x_0, \dots, x_n)$. So H_K and h_K are well-defined.

2. Suppose $K \hookrightarrow L$. Then $H_L(P) = H_K(P)$ (easy check).
So, have $H: \mathbb{P}^n(\bar{\mathbb{Q}}) \to \mathbb{R}_{>0}$. $\mathbb{P}^n(\bar{\mathbb{Q}})$ = set of all points in $\mathbb{P}^n$ defined over $\bar{\mathbb{Q}}$.
$= \bigcup_{\text{number fields } K} \mathbb{P}^n(K)$.

   $h := \log H$.

3. $h \geq 0$. So need $H \geq 1$. Choose $P \in \mathbb{P}^n(K)$, K dependent on P.
$H(P) = \prod_v \max_i \|x_i\|_v \geq \max_i \prod_v \|x_i\|_v = 1$.

<u>Theorem (Northcott)</u>: Fix $C > 0$, $d \in \mathbb{N}$. Then $\{ P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : P$ is defined over some K with $[K:\mathbb{Q}] \leq d$ and $H(P) \leq C \}$ is finite.

<u>Proof</u>: <u>First assume $n=1$.</u> $P = (1, \alpha)$: P is defined over $K \iff \alpha \in K$

Assume $C \geq H(P) = \prod_v \max(1, \|\alpha\|_v)$. So $\|\alpha\|_v \leq C$ $\forall v$

Say $\alpha = \alpha_1, \dots, \alpha_e$ are conjugates of v. ($e \leq d$). $F(T) := \prod (T - \alpha_i) = T^e - s_1 T^{e-1} + \dots + (-1)^e s_e$, $s_i \in \mathbb{Q}$. $e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

Define $(d,j)_v = \max\left(1, \left\|\binom{d}{j}\right\|_v\right)$. $\|s_j\|_v \leq \begin{cases} \max_{i_1 < \dots < i_j} \|\alpha_{i_1} \cdots \alpha_{i_j}\|_v & (v \text{ finite}) \\ \left\|\binom{d}{j}\right\|_v \cdot \max \|\alpha_{i_1} \cdots \alpha_{i_j}\|_v & (v \text{ infinite}), \end{cases}$

since $s_j = \sum_{i_1 < \dots < i_j} \alpha_{i_1} \cdots \alpha_{i_j}$.

Fix a place u of $\mathbb{Q}$. $\|s_j\|_u = \prod_{v|u} \|s_j\|_v$. The number of v with $v|u$ is $\leq d = [K:\mathbb{Q}]$.

Now, $\|\alpha_{i_1} \cdots \alpha_{i_j}\|_v = \|\alpha_{i_1}\|_v \cdots \|\alpha_{i_j}\|_v$. For each v, the numbers $\|\alpha_1\|_v, \dots, \|\alpha_e\|_v$ are the same as $\|\alpha\|_{v_1}, \dots, \|\alpha\|_{v_{\tilde{e}}}$, where the v_i are the conjugates of v. If u is the place of $\mathbb{Q}$ with $v|u$, then the set of all places of K dividing u, is $v_1, \dots, v_{\tilde{e}}$ ($\tilde{e} \leq e$).

We deduce $\|\alpha_i\|_v \leq C$ $\forall i, \forall v$. So $\|s_j\|_v \leq (d,j)_v C^j$. Fix place u of $\mathbb{Q}$, $\exists \leq e$ $v|u$.

So, $\|s_j\|_u \leq \prod_{v|u} (d,j)_v (C^j)^d$. So $\|s_j\|_u$ is bounded independently of α, $\forall u$.

Say $s_j = a_j/b_j$, $a_j, b_j \in \mathbb{Z}$, coprime. Fix p, say $v_p(b_j) = n$, ie $p^n \| b_j$.
Then $\|s_j\|_p = p^n$. So b_j is bounded independently of α.
Also, $\|s_j\|_\infty$ is bounded. So the number of choices of s_j is bounded, independently of α. So the number of possible $F(T)$ is bounded, so the number of α's is bounded. So done for $n=1$.

<u>General n</u>: Say $P = (1, \alpha_1, \dots, \alpha_n)$. Fix C, d. $L = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq L$.
By hypothesis, $[L:\mathbb{Q}] \leq d$ and $H(P) \leq C$. So $C \geq \prod_v \max_i (1, \|\alpha_i\|_v) \geq \prod_v \max(1, \|\alpha_1\|_v)$.
$[\mathbb{Q}(\alpha_1):\mathbb{Q}] \leq d$, so # possible α_1 is finite (case $n=1$). Similarly, # possible $\alpha_2, \dots, \alpha_n$ is finite.

Corollary: Given C, d, the set $\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : h(P) \leq C, [\mathbb{Q}(P):\mathbb{Q}] \leq d\}$ is finite.
Proof: $h = \log H$ and $h \geq 0$.

In fact, given any smooth projective variety X defined over K ($[K:\mathbb{Q}] < \infty$) and given a linear equivalence class $[D]$ of divisors ~~of~~ in X, shall construct a height function $h_{[D]} : X(\bar{\mathbb{Q}}) \to \mathbb{R}$.
Or rather, we shall construct an equivalence class of such functions, where two functions are equivalent if $f-g$ is bounded. Write $f = g + O(1)$.

Basic tautology in algebraic geometry.

K a field, X a smooth projective variety over K.
A divisor in X is a formal sum $\sum n_i D_i$, $n_i \in \mathbb{Z}$, and the D_i are irreducible subvarieties of codimension 1. ("a prime divisor").

D, E divisors. They are linearly equivalent ($D \sim E$) if $\exists f \in K(X)^*$ with $(f) = D - E$, where $(f) = \sum n_i A_i$, where $n_i =$ order of zero (or pole) of f along A_i.
$[D] =$ equivalence class of D.
$D = \sum n_i D_i$ is effective if all $n_i \geq 0$. Write $D \geq 0$.
1. Let $|D| = \{$ effective divisors E on $X : E \sim D\}$. Can identify $|D| = \{f \in k(X)^* : (f) + D \geq 0\} / k^*$.
(Given $E \in |D|$, have $(f) = E - D$, so $(f) + D = E \geq 0$).

Note: Given $f, g \in k(X)^*$ have $(f) = (g) \iff (f/g) = 0. \iff \frac{f}{g}, \frac{g}{f}$ are regular everywhere in X.

Basic fact about projective varieties: every global function is in k^*, so $f \equiv g \mod k^*$. Conversely, given $f \in k(X)^*$ with $(f) + D \geq 0$, take $E = (f) + D$, so $E - D = (f)$, so $E \sim D$.

2. Giving a morphism $\varphi : X \to \mathbb{P}^n_k$ is equivalent to giving a divisor D in X, and $f_0, \ldots, f_n \in k(X)^*$ such that $(f_i) + D \geq 0$, and *writing $(f_i) + D = E_i$, $\forall x \in X$, x defined over k, since E_i does not contain x.*
Given $f_0, \ldots, f_n$, define $\varphi(x) = (f_0(x), \ldots, f_n(x))$. (+)

Basic fact: X is projective, so $\varphi(X)$ is a projective subvariety of $\mathbb{P}^n_k$.
Dropping the above hypothesis between the asterisks, means that φ, defined by (+), may fail to be defined everywhere. ie, φ would be only a rational map, rather than a morphism.
Conversely, start with $\varphi : X \to \mathbb{P}^n_k$. Then, for any hyperplane $H \subset \mathbb{P}^n$ with $H \not\supseteq \varphi(X)$, gives an effective divisor on X, namely $\varphi^{-1}(\varphi(X) \cap H)$ (given multiplicities appropriately).

Since $\forall x \in X \ \exists H \not\ni \varphi(x)$ then $\varphi^{-1}(\varphi(X) \cap H) \not\ni x$.
Say H_1, given by $l_1 = 0$, H_2 given by $l_2 = 0$, l_1, l_2 given by linear homogeneous polynomials in $z_0, \dots, z_n$, the homogeneous coordinates of $\mathbb{P}^n$. So $\frac{l_1}{l_2} \in k(\mathbb{P}^n)$.
So $\frac{l_1}{l_2} \circ \varphi \in k[X]$

If $D_\alpha = \varphi^{-1}(\varphi(X) \cap H_\alpha)$, then $H_1 - H_2 = (\frac{l_1}{l_2})$ and $D_1 - D_2 = (\frac{l_1}{l_2} \circ \varphi)$
↑ obviously effective.

Eg: X = elliptic curve over $\mathbb{C}$. Given $P \in X$, let $[P]$ be P considered as a divisor. So $[P] + [Q] = [P \oplus Q] + [0]$.
Also, $[P] = [Q] \iff P = Q$.

Consider $D = 2.[0]$.
Define $\varphi : X \to \mathbb{P}^1_{\mathbb{C}}$, $\varphi(z) = (1 : \wp(z))$. Hyperplane H = point.
$\varphi^{-1}(0,1) = 2.[0] = D$. $\varphi^{-1}(H) = [P] + [-P]$, for the various points P on X.
This is true because $\wp(-z) = \wp(z)$
We know $\deg \varphi = 2$, so $\varphi^{-1}(H) \geq [P] + [-P]$ some P, and since both sides have degree 2, so $\varphi^{-1}(H) = [P] + [-P]$.

Conversely, given $P \in X$, have $[P] + [-P] = \varphi^{-1}(1, \wp(P))$. (In notation of ⊕, $f_0 = 1$, $f_1 = \wp$)

~~Suppose X is an elliptic curve over K. Consider $D = 2[0]$.~~

X smooth, projective over K, D a divisor, then $\{f \in K(X)^* : (f) + D \geq 0\} \cup \{0\}$ is a K-vector space, of finite dimension.
If X is an elliptic curve, and $\deg D > 0$, then this dimension $= \deg D$.
(Riemann-Roch for elliptic curves).

Now assume X is an elliptic curve, $D = 2[0]$. So $\deg D = 2$. We have a 2 dimensional vector space, with basis $\{1, f\}$.
Get $\varphi : X \to \mathbb{P}^1$, $\varphi(P) = (1, f(P))$.
For any hyperplane (ie point) H on $\mathbb{P}^1$, $\varphi^{-1}(H) = [P] + [-P]$, some P.

[If X is $Y^2 Z = F(X, Z)$, then $\varphi(P) = (X, Z)$.]

X still elliptic, $D = 3.[0]$. We get $\varphi : X \to \mathbb{P}^2_K$, say $\varphi(P) = (Z_0, Z_1, Z_2)$
Every line L in $\mathbb{P}^2_K$ gives a divisor $\varphi^{-1}(\varphi(X) \cap L) \sim 3.[0]$.
(In fact, every effective divisor $E \sim 3[0]$ arises in this way).
So $\varphi(0) = 0$. Then $\exists$ line L cutting $\varphi(X)$ precisely in $3.[0]$:

Tie together heights and morphisms to $\mathbb{P}^n_K$.
Suppose X is smooth and projective over K = number field. Suppose given $\varphi : X \to \mathbb{P}^m$, $\psi : X \to \mathbb{P}^n$, corresponding to the same divisor class $[D]$ on X,

ie $\varphi^{-1}(H_1) \sim \psi^{-1}(H_2)$. H_1 hyperplane in $\mathbb{P}^m$, $H_1 \not\supseteq \varphi(X)$, H_2 in $\mathbb{P}^n$, $H_2 \not\supseteq \psi(X)$.
(Assume all this).
Define $h_\varphi(P) = h(\varphi(P))$, $h_\psi(P) = h(\psi(P))$.

Theorem: $h_\varphi \equiv h_\psi \mod O(1)$.

Ie, $h_\varphi - h_\psi$ is bounded as a function $X(\bar{k}) \to \mathbb{R}$
= set of points on X defined over $\bar{k}$.

Proof: Say $\varphi = (f_0,\dots,f_m)$, $\psi = (g_0,\dots,g_n)$ with $f_i, g_j \in V = \{h \in k(X)^* : (h)+D \geq 0\}$.
Define $w = (f_0,\dots,f_m,g_0,\dots,g_n)$.
Now it's enough to prove the theorem when $\varphi = (f_0,\dots,f_n)$, $\psi = (f_0,\dots,f_n,g)$, $g \in V$.

X, smooth and projective over K. $[D]$, divisor class.
Assume we have morphisms $f: X \to \mathbb{P}^m_K$, $g: X \to \mathbb{P}^n_K$, f, g both associated to $[D]$.
Ie, given hyperplanes $H \subset \mathbb{P}^m$ and $H' \subset \mathbb{P}^n$, $f^* = f^{-1}(X \cap f(X))$, counted with multiplicities, is linearly equivalent to $g^* H'$.
[Recall that if $f(P) = (x_0(P),\dots,x_m(P))$, then $\frac{x_i}{x_j}\cdot f \in K(X)^*$ and $(\frac{x_i}{x_j}\cdot f) + D \geq 0$, where $D \in [D]$]

Look at f: have $f_0,\dots,f_n \in \{\varphi \in K(X)^* : (\varphi)+D \geq 0\}$ and
$f(P) = [f_0(P),\dots,f_m(P)] = [1, \frac{f_1}{f_0}(P),\dots,\frac{f_m}{f_0}(P)]$.
Look at g: have $g_0,\dots,g_m \in \{\text{same}\}$, g defined similarly.
$h_g, h_f : X(\bar{K}) \to \mathbb{R}$, $h_f(P) = h(f(P))$.

Theorem (above): $h_f - h_g$ is bounded.
Proof: We may assume $f = (f_0,\dots,f_n)$, $g = (f_0,\dots,f_n,g_0)$. Important fact about projective X: $f(X)$, $g(X)$ are subvarieties of $\mathbb{P}_K$, ie, they are defined by a bunch of vanishings of homogeneous polynomials.

$$\begin{tikzcd} X \arrow[r, "g"] \arrow[dr, "f"'] & \mathbb{P}^{n+1}_K \arrow[d, dashed, "\pi"] \\ & \mathbb{P}^n_K \end{tikzcd}$$

π = projection from $(0,\dots,0,1) = Q$. By assumption, f is a morphism. So $Q \notin g(X)$, for if $g(x) = Q$ then f would be undefined at x.

We have homogeneous coordinates $z_0,\dots,z_{n+1}$ on $\mathbb{P}^{n+1}$. $\pi(z_0,\dots,z_{n+1}) = (z_0,\dots,z_n)$
$Q \notin g(X)$ means that some homogeneous polynomial vanishing on $g(X)$ is of form $z_{n+1}^D + a_{D-1} z_{n+1}^{D-1} + \dots + a_0$, where $a_{D-j} \in K[z_0,\dots,z_n]$, homogeneous of degree j.
Pick $P \in X(\bar{K})$. Then $P \in X(L)$, some finite L/K.
$x_j := z_j(P)$, $x = z_{n+1}(P)$. Have $x^D + a_{D-1}x^{D-1} + \dots + a_0 = 0$ ⊛, $a_j = \sum_{\Sigma m_i = D-j} \lambda_{j,\underline{m}} x_0^{m_0} \cdots x_n^{m_n}$
Examine places v of L separately.
$v = \underline{P}$, finite. Say $v_{\underline{P}}(x_i) = q_i \in \mathbb{Z}$. ($v_p(p) = 1$ for $p \in \mathbb{Z}$, prime).
$v_p(\lambda_{j,\underline{m}}) = \alpha_{j,\underline{m}}$, independent of P.

So $v_{\underline{P}}(a_i) \geqslant \min_{\underline{m}} (\alpha_{i,\underline{m}} + m_1 q_1 + \dots + m_n q_n) \geqslant \min_{\underline{m}} (\alpha_{i,\underline{m}}) + (D-i) \min_k (q_k)$

From ⊛ $v_{\underline{P}}(x^D) \geqslant v_{\underline{P}}(a_{D-j}\, x^{D-j})$, some j, so $D v_{\underline{P}}(x) \geqslant v_{\underline{P}}(a_{D-j}) + (D-j) v_{\underline{P}}(x)$

So $j v_{\underline{P}}(x) \geqslant v_{\underline{P}}(a_{D-j}) \geqslant \min_{\underline{m}} (\alpha_{D-j,\underline{m}}) + j \min_k (q_k)$

So $v_{\underline{P}}(x) \geqslant \min_k (q_k)$ + (universal constant).

So $\|x\|_{\underline{P}} = (N\underline{P})^{-v_{\underline{P}}(x)/[L:\mathbb{Q}]} \leqslant (N\underline{P})^{[-\min_k v_{\underline{P}}(x_k) - \text{univ. cst.}]/[L:\mathbb{Q}]}$

$$\leqslant \max_k \|x_k\|_{\underline{P}} \, (N\underline{P})^{-(\text{univ. cst})/[L:\mathbb{Q}]} \qquad - \oplus$$

Put $\max_{j,\underline{m}} (N\underline{P})^{-\alpha_{j,\underline{m}}} = C_{\underline{P}}$.

Now either $\lambda_{j,\underline{m}} = 0$ or there are only finitely many $\underline{P}$ with $v_{\underline{P}}(\lambda_{j,\underline{m}}) \neq 0$ ($v_{\underline{P}}(0) = -\infty$, so $\|0\|_{\underline{P}} = 0$). So for almost all $\underline{P}$, $C_{\underline{P}} = 1$ or 0.

But $C_{\underline{P}} = 0$ only if all $\lambda_{j,\underline{m}} = 0$. This implies $x = 0$. If $= z_{n+1}(P) = 0$, then $h_f = h_g$ and there's nothing to do.

So have almost all $C_{\underline{P}} = 1$

Also, $\max_{j \leq n+1} \|x_j\|_{\underline{P}} \leqslant C_{\underline{P}} \cdot \max_{j \leq x} \|x_j\|_{\underline{P}}$, by $\oplus$, for all $\underline{P}$.

Now take $v = \sigma$, infinite.

From ⊛, $\|x\|_\sigma^D \leqslant \|D\|_\sigma \cdot \max_j \|a_j\|_\sigma \cdot \|x\|_\sigma^j$. The number of possible monomials $T_0^{m_0} \cdots T_n^{m_n}$ of degree $D-j$ is $\binom{n+D-j}{n} = \Delta_j$, say.

So $\|a_j\|_\sigma \leqslant \|\Delta_j\|_\sigma \cdot \max_{\underline{m}} \{ \|\lambda_{j,\underline{m}}\|_\sigma \cdot \|x_0\|_\sigma^{m_0} \cdots \|x_n\|_\sigma^{m_n} \}$, where $\Sigma m_i = D-j$.

$$\leqslant \|\Delta_j\|_\sigma \cdot \max_{\underline{m}} \|\lambda_{j,\underline{m}}\| \cdot \max_{k \leq n} \|x_k\|_\sigma^{D-j}$$

Choose $j = j_0$ maximising $\|a_j\|_\sigma \cdot \|x\|_\sigma^j$.

So $\|x\|_\sigma^D \leqslant \|D\|_\sigma \cdot \|\Delta_{j_0}\|_\sigma \cdot \max_{\underline{m}} \|\lambda_{j_0,\underline{m}}\|_\sigma \cdot \max_{k \leq n} \|x_k\|_\sigma^{D-j_0} \cdot \|x\|_\sigma^{j_0}$

So $\exists$ constant C_σ such that $\|x\|_\sigma^{D-j_0} \leqslant C_\sigma^{D-j_0} \cdot \max_{k \leq n} \|x_k\|_\sigma^{D-j_0}$, i.e. $\|x\|_\sigma \leqslant C_\sigma \cdot \max_{k \leq n} \|x_k\|_\sigma$

So $\forall$ places, finite or infinite, $\exists$ constant C_v such that $\|x\|_v \leqslant C_v \cdot \max_{k \leq n} \|x_k\|_\sigma$, and almost all $C_v = 1$.

So $\max_{k \leq n+1} \|x_k\|_v \leqslant C_v \cdot \max_{k \leq n} \|x_k\|_v$. Put $C = \prod_v C_v$. Then $\prod_v \max_{k \leq n+1} \|x_k\|_v \leqslant C \cdot \prod_v \max_{k \leq n} \|x_k\|_v$.

So $H(g(P)) \leqslant C \cdot H(f(P))$. Obviously $H(f(P)) \leqslant H(g(P))$.

So $h(f(P)) \leqslant h(g(P)) \leqslant h(f(P)) + \log C$.

So, given any divisor class $[D]$ on X associated to a morphism $X \to \mathbb{P}_K^n$ we have an equivalence class of height functions. Denote any such function by $h_{[D]}$. ($h \sim h'$ if $h - h'$ is bounded)

$h_{[D]}$ is bounded below. And if $[D]$ is associated to an embedding $X \hookrightarrow \mathbb{P}_K^n$ then $\forall c$ and $\forall d$, $\{P \in X(\bar{K}) : h_{[D]}(P) \leqslant c$ & P is defined over a field L with $[L:K] \leqslant d\}$ is finite

(From Northcott's Theorem).

Last time we showed: X over K projective, given divisor class $[D]$ in X, corresponding to at least one morphism $\varphi: X \to \mathbb{P}^n$, have $h_{[D]}: X(\bar{K}) \to \mathbb{R}$, defined up to addition of a bounded function, and bounded function. Moreover, if φ is finite (give that X is projective, this $\Leftrightarrow$ inverse image of every point in $\mathbb{P}^n(\bar{K})$ is finite, as a set), then by Northcott's Theorem, $\forall\, c, d$, $\#\{P \in X(\bar{K}) : h_{[D]}(P) \le C$ & P is defined over some L with $[L:K] \le d\}$ is finite.

Eg: X a curve, φ non-constant $\Rightarrow \varphi$ is finite, as every $\varphi^{-1}(Q) \subseteq X$.
So either $\dim \varphi^{-1}(Q) = 1$, in which case φ is constant, or $\dim \varphi^{-1}(Q) = 0$, when $\varphi^{-1}(Q)$ is finite and non-empty. (or $\dim \varphi^{-1}(Q) = -\infty$, ie $\varphi^{-1}(Q) = \phi$).

Given divisor classes $[D], [E]$ on X, have $[D+E]$. (If $D = \sum m_i \lambda_i$, $E = \sum n_i \lambda_i$, then $D+E = \sum (m_i + n_i)\lambda_i$)

Lemma: If $[D], [E]$ correspond to morphisms $\varphi: X \to \mathbb{P}^m_k$, $\psi: X \to \mathbb{P}^n_k$, then $[D+E]$ corresponds to a morphism $w: X \to \mathbb{P}_k^{mn+m+n}$, given as follows:
If $\varphi(P) = (x_0, \dots, x_m)$, $x_i = x_i(P)$ and $\psi(P) = (y_0, \dots, y_n)$, $y_j = y_j(P)$, then
$w(P) = (x_0 y_0, \dots, x_m y_n)$

Proof: need to know if all ~~xx~~ $x_i y_j = 0$ simultaneously at $P \in X$, then all $x_i, y_j = 0$ at P.
This is obvious. By assumption that φ, ψ are morphisms, get contradiction.

Proposition: $h_{[D+E]} = h_{[D]} + h_{[E]}$.
Proof: $H_{[D]}(P) = \prod_v \max_i \|x_i(P)\|_v$, $H_{[E]}(P) = \prod_v \max_j \|y_j(P)\|_v$. $(h = \log H)$
So $H_{[D]}(P) H_{[E]}(P) = \prod_v \max_{i,j} \|x_i y_j(P)\|_v$ (as $\max_i \max_j = \max_{i,j}$) $= H_{[D+E]}(P)$.
Take logs.

Now suppose X $(=E=C)$ is an elliptic curve over K. We shall need to compare $h_{[?]}(P)$ and $h_{[?]}(mP)$. ie, $h_{[?]}(P+Q)$ and $h_{[?]}(P)$, $h_{[?]}(Q)$

Recall: given a morphism $f: V \to W$ of smooth projective varieties and a divisor class $[D]$ on W, have $f^*[D] = [f^*D]$ a divisor class on V: if $D = \sum m_i A_i$ then $f^*D = \sum n_i f^* A_i$ where $f^*A_i = f^{-1}(A_i)$, counted with multiplicities.
If V, W are curves, $Q \in W$ say, $f^{-1}(Q) = \{P_1, \dots, P_r\}$ as sets.
Choose a uniformising parameter t in W at Q (ie, generator of maximal ideal m_Q of DVR $\mathcal{O}_{W,Q} = \{\varphi \in K(W) : \varphi$ regular at $Q\}$, $m_Q = \{\varphi \in \mathcal{O}_{W,Q} : \varphi(Q) = 0\}$)
$f(P_i) = Q \Leftrightarrow \mathcal{O}_{W,Q} \subseteq \mathcal{O}_{V,P_i}$, $m_Q \subseteq m_{P_i}$. So $t = u s_i^{n_i}$, $v \in \mathcal{O}_{V,P_i}$, $n_i \in \mathbb{N}$.
$f^*(Q) = \sum n_i \cdot P_i$. All $n_i = 1 \Leftrightarrow f$ is unramified over Q.

Eg: $f = [m]: E \to E$. If $[D] = 0$, then $f^* D =$ the m-torsion points. $[m]$ is unramified everywhere so all multiplicities here are 1.
In general, we want to compare $[m]^*[D]$ and $[D]$.

Basic tool is the "theorem of the cube": Consider $E \times E \times E$, (E elliptic curve over number field K), with maps: $S_{123}, S_{12}, S_{13}, S_{23}, S_1, S_2, S_3 : E \times E \times E \to E$, by:
$S_{123}(P,Q,R) = P+Q+R$, $S_{12}(P,Q,R) = P, Q$, etc...
Then for every divisor class $[D]$ on E, $S_{123}^*[D] + S_1^*[D] + S_2^*[D] + S_3^*[D] \sim S_{12}^*[D] + S_{23}^*[D] + S_{13}^*[D]$

Proof: Invoke basic proposition in algebraic geometry: given a smooth projective variety Z over K, and two divisor classes $[F], [G]$ in Z, have $[F] \sim [G]$ over $K \iff [F] \sim [G]$ over a field $L \supseteq K$.
Ie, $\exists\, \varphi \in K(x)$ with $(\varphi) = F - G \iff \exists\, \psi \in L(x)$ with $(\psi) = F - G$.
So it is enough to prove theorem for E over $\mathbb{C}$.
Assume first that $[D] = [P]$
Consider $\varphi(z_1, z_2, z_3) = \dfrac{\sigma(z_1+z_2+z_3-P)\,\sigma(z_1-P)\,\sigma(z_2-P)\,\sigma(z_3-P)}{\sigma(z_1+z_2-P)\,\sigma(z_1+z_3-P)\,\sigma(z_2+z_3-P)}$

$E = \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$. $\sigma(z+\lambda_\alpha) = \exp\left(i\pi + \eta_\alpha\left(z - \frac{\lambda_\alpha}{2}\right)\right)\sigma(z)$, $(\eta_\alpha \in \mathbb{C})$
Check: $\varphi(z_1+\lambda_\alpha, z_2, z_3) = \varphi(z_1, z_2+\lambda_\alpha, z_3) = \varphi(z_1, z_2, z_3+\lambda_\alpha) = \varphi(z_1, z_2, z_3)$
So φ is a ratio of two holomorphic functions of z_1, z_2, z_3, and so is meromorphic and is invariant wrt $\Lambda^3 = \Lambda \oplus \Lambda \oplus \Lambda \subseteq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} = \mathbb{C}^3$.
So φ is meromorphic in $\mathbb{C}^3/\Lambda^3 = E^3 \times E^3 \times E^3$.
Also, $(\varphi)_0 = S_{123}^* D + S_1^* D + S_2^* D + S_3^* D$ and $(\varphi)_\infty = S_{12}^* D + S_{23}^* D + S_{13}^* D$
[Recall: σ, as function on $\mathbb{C}$, has zeroes only at points of Λ, simple zeroes]
Now, if $[D] = \Sigma n_i [P_i]$, cook up $\varphi = \varphi_{P_i}\ \forall P_i$ and then take $\prod_i \varphi_{P_i}^{n_i}$ to prove theorem.

Definition: Have $[-1]: E \to E$, $P \mapsto -P$. A divisor class $[D]$ on E is symmetric (respectively antisymmetric) if $[-1]^* D \sim D$ (respectively $[-1]^* D \sim -D$).

Eg: If $[D] = [P] + [-P]$ (note: $\deg D = 2$), then $[D]$ is symmetric.
If $[D] = [P] - [-P]$ then $[D]$ is antisymmetric.

Proposition: If D is symmetric, then $[m]^* D \sim m^2 D$
Proof: Induction on m. Obvious for $m=1$. So assume $[n]^* D \sim n^2 D$.
Have $E \to E \times E \times E$, $P \mapsto (nP, P, -P)$.

$$\begin{array}{ccc} E & \longrightarrow & E\times E\times E \\ & {\scriptstyle t\ldots}\searrow & \downarrow {\scriptstyle S\ldots} \\ & & E \end{array}$$

$t_{123}(P) = nP$. $t_{12}(P) = (n+1)P$, etc.
So, $t_{123} = [n]$, $t_{12} = [n+1]$, ..., $t_{23} = 0$, $t_1 = [n]$, $t_2 = [1] = id$, $t_3 = [-1]$
So $[n]^* D + [n]^* D + D + [-1]^* D \sim [n+1]^* D + [n-1]^* D + 0$.
Check $[0]^* D \sim 0$ as divisors.
$E \xrightarrow{[0]} E$, $[0]$ collapses E to $\{0\}$.
Say $D = \Sigma n_P [P]$, no $P = 0$. Then $[0]^* D = \Sigma n_P([0]^{-1}(P))$. But if $P \neq 0$, then $[0]^{-1}(P) = \phi$. So $[0]^* D = 0 = \sum_P 0[P]$.
If some $P = 0$, rewrite D as $D \sim F - G$, $F = \Sigma m_Q Q$, $G = \Sigma q_R R$, no $Q, R = 0$. (always possible). Then $[0]^* D = [0]^* F - [0]^* G = 0$.
More generally if $\varphi: X \to Y$ collapses X to a point then $\varphi^*(D) = 0$ for all divisor classes $[D]$ on Y.

Argue by induction on n. $[1]^*D = D$, since $[1]$ is identity.
Assume $n \geq 1$ and $[n]^*D = n^2 D$. So $2n^2 D + 2D = [n+1]^*D + [n-1]^2 D$, and since $2n^2 + 2 - (n-1)^2 = 2n^2 + 2 - n^2 + 2n - 1 = (n+1)^2$, we are done.

Exercise: If $[-1]^*D = -D$ then $[n]^*D = nD$. (Check $nD + nD = [n+1]^*D + (n-1)D$).

Fix $D = 2[O]$. This is symmetric and corresponds to a morphism $E \xrightarrow{\pi} \mathbb{P}^1$, of degree 2. [If E is $y^2 = f(x)$ in affine terms, then $\pi(x,y) = x$].
Consider $h = h_{[D]}$, defined up to a bounded function. We know h has a finiteness property (Northcott), and that $h_{[D]} + h_{[E]} = h_{[D+E]}$. So $h_{n^2[D]} = n^2 h \quad \forall n \in \mathbb{Z}$.
But $n^2[D] = [n]^*D$.
So $n^2 h(P) = h_{n^2 D}(P) = h_{[n]^*D}(P) = h_D(nP)$. [Recall that for a morphism $\varphi: X \to Y$ and divisor class D in Y, $h_{\varphi^* D}(P) = h_D(\varphi(P))$].
Ie, for given n, $\exists$ constant c such that $|h(nP) - n^2 h(P)| \leq c \quad \forall P \in E(\bar{K})$
So h is a quadratic function, but for a little "noise".
Get rid of noise: fix $m \geq 2$.

Proposition: $\exists$ unique $\hat{h}: E(\bar{K}) \to \mathbb{R}$ such that (a) $\hat{h} - h$ is bounded.
(b) $\hat{h}(mP) = m^2 \hat{h}(P) \quad \forall P \in E(\bar{K})$.

Proof: $\exists\, c$ with $|h(mP) - m^2 h(P)| < c \quad \forall P$.
So $|h(m^n P) - m^2 h(m^{n-1}P)| < c \quad \forall P, \forall n \geq 1$. So $\left|\frac{1}{m^{2n}} h(m^n P) - \frac{1}{m^{2n-2}} h(m^{n-1}P)\right| < c/m^{2n}$.
So $\left|\frac{1}{m^{2n}} h(m^n P) - \frac{1}{m^{2(n-r)}} h(m^{n-r}P)\right| < c\left(\frac{1}{m^{2n}} + \dots + \frac{1}{m^{2(n-r+1)}}\right)$

$$< \frac{c}{m^{2(n-r+1)}} \cdot \sum_{s \geq 0} m^{-2s} < \frac{c}{m^{2(n-r+1)}} \cdot \frac{1}{1 - m^{-2}}.$$

So the sequence $\left(\frac{1}{m^{2n}} h(m^n P)\right)_{n \geq 0}$ is a Cauchy sequence, so it is convergent - call its limit $\hat{h}(P)$. This defines $\hat{h}: E(\bar{K}) \to \mathbb{R}$.
Now $\left|\frac{1}{m^{2n}} h(m^n P) - h(P)\right| \leq c \sum \frac{1}{m^{2n}} = \frac{c}{1 - m^{-2}}$. So $\hat{h}(P) - h(P)$ is bounded, independently of P.
So (a) holds.
For (b): $\hat{h}(mP) = \lim_{n \to \infty} \frac{1}{m^{2n}} \hat{h}(m^{n+1}P) = m^2 \lim_{n \to \infty} \frac{1}{m^{2(n+1)}} \cdot \hat{h}(m^{n+1}P) = m^2 \hat{h}(P)$
So (b) holds.
Uniqueness: suppose have $h': E(\bar{K}) \to \mathbb{R}$. $h' - h$ is bounded and $h'(mP) = m^2 h'(P)$.
Then $h' - h$ is bounded and $h'(m^n P) - \hat{h}(m^n P) = m^{2n}(h'(P) - \hat{h}(P))$.
If $h' - \hat{h} \neq 0$, get contradiction to boundedness by $n \to \infty$.

Define $B: E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$, by $B(P,Q) = \frac{1}{2}\left[\hat{h}(P-Q) - \hat{h}(P) - \hat{h}(Q)\right]$.
Aim: prove B is $\mathbb{Z}$-bilinear, wrt structure of $E(\bar{K})$ as an abelian group.

Back to theorem of cube. $S_{123}^* D + S_1^* D + \dots = S_{12}^* D + \dots$.
So $h_{S_{123}^* D} + h_{S_1^* D} + \dots = h_{S_{12}^* D} + \dots$ modulo $O(1)$. But $h_{S_{123}^* D}(P,Q,R) = h_D(P+Q+R)$, etc..
So $h(P+Q+R) + h(P) + h(Q) + h(R) = h(P+Q) + h(P+R) + h(Q+R)$, independent of $P, Q, R \in E(\bar{K})$.
So $\hat{h}(P+Q+R) + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R) = \hat{h}(P+Q) + \hat{h}(P+R) + \hat{h}(Q+R)$.

D is symmetric, $[-1]^* D = D$. So $h(-x) = h(x) + O(1)$, so $\tilde{h}(-x) = \tilde{h}(x)$.
$R = -Q$: $2\tilde{h}(P) + 2\tilde{h}(Q) = \tilde{h}(P-Q) + \tilde{h}(P+Q)$ $\Rightarrow$ B is bilinear.

Recall: we fixed $m \geq 2$, $h = h_{[D]}$; D associated to a morphism, D symmetric.
Eg: $D = 2[O]$. (This D is associated to $E \xrightarrow{\pi} \mathbb{P}^1$, $\deg \pi = 2$. Fibres of P are $\{P\} \cup \{-P\}$).
Then defined $\tilde{h}$, normalised height, by $\tilde{h}(P) = \lim_{n\to\infty} \frac{1}{m^{2n}} h(m^n P)$.
We proved that $\tilde{h} = h + O(1)$, $\tilde{h}(mP) = m^2 \tilde{h}(P)$.

Proposition: $\tilde{h} : E(\bar{K}) \to \mathbb{R}$ is a quadratic form.
Proof: We need to show that $B(P,Q) = \frac{1}{2}\left(\tilde{h}(P+Q) - \tilde{h}(P) - \tilde{h}(Q)\right)$ is bilinear wrt structure of $E(\bar{K})$ as a $\mathbb{Z}$-module.
Cube: $s_{123}^* D + s_1^* D + s_2^* D + s_3^* D \sim s_{12}^* D + s_{13}^* D + s_{23}^* D$. $S_I : E \times E \times E \to E$.
So $h_{s_{123}^* D} + h_{s_1^* D} + \cdots \sim h_{s_{13}^* D} + \cdots + O(1)$. As usual, $h_{f^* D}(P) = h_D(f(P))$.
So $h(P+Q+R) + h(P) + h(Q) + h(R) \sim h(P+Q) + h(Q+R) + h(P+R) + O(1)$, for $P, Q, R \in E(\bar{K})$
$\tilde{h}(P+Q+R) = \lim_{n\to\infty} \frac{1}{m^{2n}} h(m^n P + m^n Q + m^n R)$, etc. So multiply P, Q, R by m^n, divide equation by m^{2n} and let $n \to \infty$.
Get $\tilde{h}(P+Q+R) + \tilde{h}(P) + \tilde{h}(Q) + \tilde{h}(R) = \tilde{h}(P+Q) + \tilde{h}(P+R) + \tilde{h}(Q+R)$.
Then,
$$\begin{aligned} 2B(P+R, Q) &= \tilde{h}(P+Q+R) - \tilde{h}(P+R) - \tilde{h}(Q) \\ &= \tilde{h}(P+Q) + \tilde{h}(P+R) + \tilde{h}(Q+R) - \tilde{h}(P) - \tilde{h}(Q) - \tilde{h}(R) - \tilde{h}(P+R) - \tilde{h}(Q) \\ &= \left(\tilde{h}(P+Q) - \tilde{h}(P) - \tilde{h}(Q)\right) + \left(\tilde{h}(R+Q) - \tilde{h}(R) - \tilde{h}(Q)\right) = 2B(P,Q) + 2B(R,Q). \end{aligned}$$

Lemma: $\tilde{h} \geq 0$.
Proof: h is bounded below, so $\tilde{h}$ is bounded below. If $\tilde{h}(P) < 0$, then $\tilde{h}(m^n P) \to -\infty$ as $n \to \infty$ #

Theorem: For $P \in E(\bar{K})$, $\tilde{h}(P) = 0 \iff P$ is a torsion point.
Proof: Recall that $\tilde{h}$ satisfies the conclusions of Northcott's Theorem. Given $c, d \in \mathbb{N}$, $\{P \in E(\bar{K}) : \tilde{h}(P) \leq c,\ P \text{ defined over } L/K,\ [L:K] \leq d\}$ is finite.
Say $\tilde{h}(P) = 0$, say P defined over L. Then $m^n P \in E(L)$ $\forall n$, and $\tilde{h}(m^n P) = 0$ $\forall n$.
So the set $\{m^n P : n \in \mathbb{N}\}$ is finite. So $m^n P = m^r P$, some $n \neq r$. So P is torsion.
Conversely, P torsion $\Rightarrow$ $m^n P = m^r P$ some $n \neq r$.
Then $m^{2n} \tilde{h}(P) = \tilde{h}(m^n P) = \tilde{h}(m^r P) = m^{2r} \tilde{h}(P)$, so $\tilde{h}(P) = 0$.

Theorem: Given $d \in \mathbb{N}$, the set $\{P \in E(\bar{K}) : P \text{ defined over some } L/K,\ [L:K] \leq d,\ P \text{ a torsion point}\}$ is finite. In particular, $\mathrm{Tors}(E(K)) = \{\text{torsion points}\}$ is finite.
Proof: $\mathrm{Tors}(E(K)) = \{P \in E(\bar{K}) : \tilde{h}(P) = 0\}$. Then apply Northcott.

Theorem (Mordell-Weil): $E(K)$ is a finitely generated Abelian group.
Proof: We know that $\mathrm{Tors}\, E(K)$ is finite. Put $\Gamma = E(K)/\mathrm{Tors}\, E(K)$. Enough to show Γ is f.g.
$E(K) \subseteq E(L)$, for L/K, so we can make any finite extension of K that we like.
Fix $m = 2$: extend K if necessary so that all 2-torsion points of E are defined over K. We use: Weak Mordell-Weil : $\Gamma/2\Gamma$ is f.g.

Notice that $\tilde{h}$ defines a function $\tilde{h} : \Gamma \to \mathbb{R}$ and $\tilde{h}$ is a positive definite quadratic form on Γ. Choose $\gamma_1, \dots, \gamma_r \in \Gamma$ representing the elements of $\Gamma/2\Gamma$. Put $c = \max \tilde{h}(\gamma_i)$. Put $\Sigma = \{x \in \Gamma : \tilde{h}(x) \leq c\}$ We know that Σ is finite.

<u>Claim:</u> Σ generates Γ as an Abelian group.

Suppose this is false, ie $\exists\, x \in \Gamma$ not in group generated by Σ, such that $\tilde{h}(x)$ is minimal. Can write $x = 2y + \gamma_i$, some γ_i. Then $x = 2z - \gamma_i$. $(y, z \in \Gamma)$.

Then $\tilde{h}(x - \gamma_i) = 4\tilde{h}(y)$, $\tilde{h}(x + \gamma_i) = 4\tilde{h}(z)$.

$\tilde{h}(\alpha) = B(\alpha, \alpha)$, so $\tilde{h}(x - \gamma_i) = \tilde{h}(x) + \tilde{h}(\gamma_i) - 2B(x, \gamma_i)$,

$\tilde{h}(x + \gamma_i) = \tilde{h}(x) + \tilde{h}(\gamma_i) + 2B(x, \gamma_i)$.

So $\tilde{h}(x) + \tilde{h}(\gamma_i) = 2\tilde{h}(y) = 2\tilde{h}(z)$. $\tilde{h} \geq 0$. So either $\tilde{h}(y) < \tilde{h}(x)$ or $\tilde{h}(z) < \tilde{h}(x)$, else $\tilde{h}(\gamma_i) \geq 3 \cdot \tilde{h}(x) > 3c$.

$\tilde{h}(x)$ is minimal, so y or z is in subgroup generated by Σ, so x is too.

In general, it is difficult to compute the Mordell-Weil group, due to difficulties of computing the rank. Finding the rank of E/K is very difficult. But finding $\mathrm{Tors}\, E(K)$ is much easier.

<u>Reason:</u> suppose P is a prime ideal of $\mathcal{O}_K$ such that $E \bmod P$ is smooth, ie is an elliptic curve over $K(P) = \mathcal{O}_K/P = \mathbb{F}_q$, say, $q = p^r = NP$. Then the part of $\mathrm{Tors}\, E(K)$ of order prime to p surjects into $E(K(P))$.

We proved earlier that if $p \nmid m$ then $E[m]$, the m-torsion points of E is of degree m^2 over $S = \mathrm{Spec}\,\mathcal{O}_K$ - (bad primes) - (primes dividing m), and is unramified over S. So $E(K)[m] \subseteq E[m]$. $E[m]$ intersects $(E \bmod P)$, the fibre over P, in m^2 distinct points defined over some $\mathbb{F}_{q^s}$. So $E(K)[m]$ intersects $E \bmod p$ in distinct points as required.

<u>Elliptic Curves over $\mathbb{F}_q$ $(q = p^r)$.</u>

Have $E \hookrightarrow \mathbb{P}^2_{\mathbb{F}_q}$, E given by a homogeneous cubic $F = 0$. E is smooth (ie, $F, \frac{\partial F}{\partial x}, \dots$ never vanish simultaneously), and have $O \in E$, O defined over $\mathbb{F}_q$. Then have group law on E, O as origin.

<u>Proposition:</u> For any number field K and a prime ideal P of K such that $\mathcal{O}_{K/P} \cong \mathbb{F}_q^\times$, $\exists$ an elliptic curve $\tilde{E}_K$ defined over K and a ring S, $\mathcal{O}_K \subseteq S \subseteq K$, such that $P \in \mathrm{Spec}\, S = \mathrm{Spec}\, \mathcal{O}_K$ - (finite set), and an elliptic curve $\tilde{E} \hookrightarrow \mathbb{P}^2_S$ $\overset{F}{\searrow} \downarrow \mathrm{Spec}\, S$, such that $(\tilde{E})_K = \tilde{E}_K$ (ie, what I get from $\tilde{E}$ by extending $S \hookrightarrow K$ is just $\tilde{E}_K$) and $\tilde{E} \bmod \underline{P}$ is E, ie E arises by reduction mod $\underline{P}$ from some elliptic curve E defined over some number field K.

Proof: We can choose homogeneous coordinates (X,Y,Z) in $\mathbb{P}^2_{\mathbb{F}_q}$ such that $O=(0,1,0)$. So Y^3 has coefficient zero in the polynomial F. Now choose K and P such that $\mathcal{O}_{K/P} \cong \mathbb{F}_q$. Then choose $\tilde{F} \in \mathcal{O}_K[X,Y,Z]$ such that Y^3 does not appear in F and $\tilde{F} \pmod P = F$.
Consider the equations $\tilde{F} = \frac{\partial \tilde{F}}{\partial X} = \frac{\partial \tilde{F}}{\partial Y} = \frac{\partial \tilde{F}}{\partial Z} = 0$ $(*)$. By assumption, these are insoluble modulo P even after enlarging $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$, so those equations are insoluble in $\bar{K}$. (else $\exists$ simultaneous solution in $\mathcal{O}_L$, some $L \supseteq K$, then there would be a solution in $\mathcal{O}_L/Q$, Q a prime, $Q|P$, #).
So $\tilde{F}=0$ is an elliptic curve $\tilde{E}_K$, origin $(0,1,0)$. To get Spec S, take Spec $\mathcal{O}_K$ and delete the prime ideals modulo which $(*)$ has a solution. (This is a finite set). Now $\tilde{F}=0$ defines: $\tilde{E} \hookrightarrow \mathbb{P}^2_S \to S$

For any $Q \in \operatorname{Spec} S$, we get an elliptic curve $\tilde{E}_{K(Q)}$ over S/Q by reducing $\tilde{F}$ modulo Q. As before, the group laws on the curves $\tilde{E}_{K(Q)}$ "fit together".

Recall corollary: given $m \in \mathbb{N}$ the morphism $[m]: E \to E$ is surjective, finite and of degree m^2 (already proved).

Question: How many points defined over $\mathbb{F}_q$ does E have? Depends on E, but:

Theorem (Hasse): $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$.
Proof uses isogenies. K a field, E_1, E_2 elliptic curves defined over K. Then, an isogeny from E_1 to E_2 is a non-constant morphism $\varphi: E_1 \to E_2$ of algebraic varieties that is also a homomorphism wrt the group laws of E_1, E_2 (over K).

Examples: $[m]: E \to E$ is an isogeny. $\{$isogenies $E_1 \to E_2\} \cup \{0\}$, (0 collapsing E_1 to $O \in E_2$), is an abelian group, denoted $\operatorname{Hom}_K(E_1,E_2)$.
An endomorphism of E is an isogeny $E \to E$. X, Y projective curves, $f: X \to Y$ a morphism. Then $\deg f \in \mathbb{N}$, or $=0$ if f is constant.

Immediate aim: prove that $\deg: \operatorname{Hom}(E_1,E_2) \to \mathbb{Z}$ is a positive definite quadratic form

For this we need the theorem of the cube for $E/\mathbb{F}_q$:
Proof of cube theorem: fix a divisor class $[D]$ on E. $[D] = \sum n_P [P]$, each $[P]$ defined over some $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$. For each P, $\exists$ $L \supseteq K$ such that P lifts to a point $\tilde{P}$ on $\tilde{E}$ defined over L. So we can lift $[D]$ to $[\tilde{D}]$, a divisor class on $\tilde{E}$, maybe after enlarging K, and also maybe enlarging $\mathbb{F}_q$. For $I \subseteq \{1,2,3\}$, $I \neq \emptyset$, have:
$S_I: \tilde{E} \times \tilde{E} \times \tilde{E} \to \tilde{E}$ (S_I gives back the appropriate sum morphism on $\tilde{E}_K$ and on each $\tilde{E}_{K(Q)}$). Put $[\tilde{A}] = S_{123}^*[\tilde{D}] + S_1^*[\tilde{D}] + S_2^*[\tilde{D}] + S_3^*[\tilde{D}] - S_{12}^*[\tilde{D}] - S_{13}^*[\tilde{D}] - S_{23}^*[\tilde{D}]$.
Next, $[\tilde{A}]$ is trivial modulo P. Cube in char $0 \Rightarrow [\tilde{A}]=0$ on $\tilde{E}_K$.
Reduce mod P to get $[A]=0$ where $[A] = S_{123}^*[D] + \cdots$. As before have general statement: if X is a smooth projective variety and $[A]$ a divisor class on X, then $[A]=0$ over K, if $[A]=0$ over $\bar{K}$. So done for $\mathbb{F}_q$.

Theorem: $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form.

Proof: Given $\alpha : E_1 \to E_2$, have $\alpha^* : \{$divisor classes on $E_1\} \to \{$divisor classes on $E_2\}$.

Then $(\deg \alpha).\deg [D] = \deg [\alpha^* D]$ for D in E_2.

Given $\alpha, \beta : E_1 \to E_2$, define $\langle \alpha, \beta \rangle = (\alpha+\beta)^* - \alpha^* - \beta^*$. Have $E_1 \xrightarrow{(\alpha,\beta,\gamma)} E_2 \times E_2 \times E_2$.

So (by cube), $(\alpha+\beta+\gamma)^* + \alpha^* + \beta^* + \gamma^* - (\alpha+\beta)^* - (\alpha+\gamma)^* - (\beta+\gamma)^* = 0$

Follows formally that $\langle \alpha, \beta+\gamma \rangle = \langle \alpha, \beta \rangle + \langle \alpha, \gamma \rangle$. So $\langle , \rangle$ is bilinear.

E_1, E_2 over K. Isogenies $\alpha, \beta, \gamma : E_1 \to E_2$. Define $\langle \alpha, \beta \rangle = (\alpha+\beta)^* - \alpha^* - \beta^*$, where $\alpha^* : \{$divisor classes on $E_2\} \to \{$divisor classes on $E_1\}$.

We proved (via cube), that $\langle \alpha, \beta+\gamma \rangle = \langle \alpha, \beta \rangle + \langle \alpha, \gamma \rangle$.

Define $\deg(\alpha^*)$ by $\deg(\alpha^*[D]) = \deg \alpha^* \deg [D]$.

Ie, over $\bar{K}$, if $D = \sum n_P [P]$, then $\alpha^* D = \sum n_P [\alpha^* P]$ ($\alpha^* P = \alpha^{-1}(P)$, counted with multiplicities)

$= \sum n_P (\deg \alpha) = \deg \alpha . \deg D$. So $\deg \alpha^* = \deg \alpha$.

Theorem: $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive definite quadratic form.

Proof: Note that $\deg \alpha + \deg \beta = \deg \alpha^* + \deg \beta^*$.

[Take $D = \sum n_P [P]$ on E_2, so $\alpha^* D = \sum n_P \alpha^* [P]$, $\beta^* D = \sum n_P \beta^* [P]$.

By definition, $(\alpha^* + \beta^*) D = \alpha^* D + \beta^* D$, so $\deg(\alpha^* + \beta^*) = \deg \alpha^* + \deg \beta^*$.]

Now, $\langle \varphi, \psi \rangle = (\varphi+\psi)^* - \varphi^* - \psi^*$.

So $\deg \langle \varphi, \psi \rangle = \deg(\varphi+\psi) - \deg \varphi - \deg \psi$.

Know $\langle \varphi, \psi + \chi \rangle = \langle \varphi, \psi \rangle + \langle \varphi, \chi \rangle$, so $\deg \langle \varphi, \psi+\chi \rangle = \deg \langle \varphi, \psi \rangle + \deg \langle \varphi, \chi \rangle$.

On the other hand, $\langle \varphi, \varphi \rangle = (2\varphi)^* - 2\varphi^*$. So $\deg \langle \varphi, \varphi \rangle = \deg (2\varphi)^* - 2\deg \varphi^*$.

$2\varphi = [2] \circ \varphi$, so $\deg 2\varphi = \deg [2] . \deg \varphi = 4 \deg \varphi$. [If $X \xrightarrow{f} Y \xrightarrow{g} Z$ are morphisms of curves, then $\deg(gf) = \deg f . \deg g$. cf: Tower Law, Galois Theory].

So $\deg \langle \varphi, \varphi \rangle = 2 \deg \varphi$.

So $\deg$ is the quadratic form associated to the bilinear form, $\frac{1}{2} \deg \langle \varphi, \psi \rangle$.

To get positive definite, just note that any non-constant morphism has degree > 0.

Apply to counting points where $K = \mathbb{F}_q$.

Frobenius: If X is any variety defined over $K = \mathbb{F}_q$, then there is a morphism $F : X \to X$ defined over K as follows: Say X is projective, $X \hookrightarrow \mathbb{P}^n_K$.

Then we have

$$\begin{array}{ccc} X & \xrightarrow{F} & X \\ \downarrow & & \downarrow \\ \mathbb{P}^n_K & \xrightarrow{F} & \mathbb{P}^n_K \end{array} \qquad F(x_0, \ldots, x_n) = (x_0^q, \ldots, x_n^q). \quad -(*)$$

More intrinsically, say $X = \bigcup U_i$, U_i affine. Then U_i has an intrinsic coordinate ring A_i, a K-algebra. ($U_i = \mathrm{Spec}\, A_i$).

Defining $F : U_i \to U_i$ is same as defining $A_i \xleftarrow{F} A_i$, $f^q \mapsfrom f$ - a homomorphism of K-algebras,

and so corresponds to $F_{U_i} : U_i \to U_i$.

These F_{U_i} glue together to give $F : X \to X$.

Given $P \in X(\bar{K})$ we have $F(P) = P \Leftrightarrow P \in X(K)$.

<u>Proof</u>: Look at $(*)$. So counting K points = counting fixed points under F
$= \sum (-1)^i \operatorname{Tr} F|_{H^i(X,\mathbb{Q})}$ - Lefschetz Fixed Point Theorem.

Grottencheik and Artin constructed $H^i(X, \mathbb{Q}_l)$. $\mathbb{Q}_l$ is characteriste 0, the l-adic numbers.
Proved $\exists$ a Lefschetz fixed point formula.
Deligne: F acts on $H^i(X, \mathbb{Q}_l)$ such that all eigenvalues (X smooth, projective) are algebraic numbers all of whose complex embeddings have absolute value $q^{i/2}$. (analogue of Riemann Hypothesis).

X an elliptic curve over $K = \mathbb{F}_q$. X can be lifted to char 0.

$X_{\mathbb{C}}$

$H^0(X_{\mathbb{C}}, \mathbb{Q}_l) \cong \mathbb{Q}_l$.
$H^1 \cong \mathbb{Q}_l^2$
$H^2 \cong \mathbb{Q}_l$.

We shall construct directly an analogue of H^1 (in fact, $(H^1)^\vee \cong H_1$) in $X/\mathbb{F}_q$, using torsion points.
Postpone this and return to estimating $\# E(\mathbb{F}_q)$. Have $F: E \to E$.

<u>Theorem</u>: F is an isogeny.
<u>Proof</u>: $O \in E(K)$, so $F(O) = O$. We shall prove (later) that any $\varphi: E_1 \to E_2$ with $\varphi(O) = O$ is an isogeny.

Note that $F(P) = P \Leftrightarrow P \in \ker(1-F)$. Shall prove later that $1-F$ is separable.
Then, $\# \ker(1-F) = \deg(1-F)$.
$(1-F): E \to E$. The points in $E(\bar{K})$ that lie in $\ker(1-F)$ are precisely the K-points on E.

By Riemann-Hurwitz, any non-constant separable morphism $E_1 \xrightarrow{f} E_2$ of elliptic curves is everywhere unramified.
So $\forall P \in E_2(\bar{K})$, $\# \{ Q \in E_1(\bar{K}) : f(P) = Q \} = \deg f$.

<u>Claim</u>: $\deg F = q^{\dim E} = q$.
<u>Proof</u>: Look at $F: K(E) \to K(E)$, $f \mapsto f^q$. Trace deg 1 over a perfect field.
Field Theory $\Rightarrow \deg F = q$.

deg is a positive definite quadratic form. $|\deg(\alpha+\beta) - \deg\alpha - \deg\beta| \leq 2\sqrt{\deg\alpha \deg\beta}$.
So $|\deg(1-F) - \overset{=1}{\deg 1} - \overset{=q}{\deg F}| \leq 2\sqrt{q}$.
So $|\# E(K) - (q+1)| \leq 2\sqrt{q}$ [Hasse's Theorem].

Fix prime $l \neq \operatorname{char} K$, K any field. Know $\forall n$, $[l^n]: E \to E$ has degree l^{2n}.
So $[l^n]$ separable gives $p \nmid \deg [l^n]$. So $[l^n]$ is everywhere unramified.
Look at $E(\bar{K})[l^n] = \ker [l^n]$ in $E(\bar{K})$.

We see $E(\bar{K})[\ell^n] = \mathbb{Z}/\ell^n\mathbb{Z} \oplus \mathbb{Z}/\ell^n\mathbb{Z}$ (decomposition not canonical), by induction on n, or by structure theorem for f.g. abelian groups.

Have $E(\bar{K})[\ell^{n+1}] \xrightarrow{[\ell]} E(\bar{K})[\ell^n]$. Must consider then $\forall n$ simultaneously.

Lemma: Suppose $\varphi: E_1 \to E_2$ is a morphism of algebraic varieties, E_1, E_2 elliptic curves over K, with $\varphi(0) = 0$. Then φ is an isogeny.

Proof: Recall: If X is any smooth projective curve, then $\mathrm{Pic}^0(X)$ = group of divisor classes on X of degree 0.

For X an elliptic curve, have
$$X \xrightarrow{i} \mathrm{Pic}^0 X$$
$$P \longmapsto [P] - [0].$$
i is an isomorphism, so giving $\mathrm{Pic}^0 X$ the structure of an algebraic variety, and X the structure of a commutative group.

$[P+Q] - [0] \sim [P] - [0] + [Q] - [0]$, ie, $[P+Q] + [0] \sim [P] + [Q]$.

φ induces $\varphi_*: \mathrm{Pic}^0 E_1 \to \mathrm{Pic}^0 E_2$, $\varphi_*(\Sigma n_p[P]) = \Sigma n_p[\varphi(P)]$, a homomorphism of commutative groups. So get:
$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi} & E_2 \\ {\scriptstyle i_1}\downarrow\cong & & \downarrow {\scriptstyle i_2}, \cong \\ \mathrm{Pic}^0 E_1 & \xrightarrow{\varphi_*} & \mathrm{Pic}^0 E_2 \end{array}$$
$\varphi_* i_1(P) = [\varphi(P)] - [\varphi(0)] = [\varphi(P)] - [0] = i_2\varphi(P)$, so diagram is commutative.

i_1, i_2 are isomorphisms of commutative groups, and φ_* is a homomorphism, so φ is also a homomorphism.

Used this Lemma when φ = Frobenius map, $F: E_1 \to E_2$ over $K = \mathbb{F}_q$.

Check $F(0) = 0$: well, $F(P) = P \iff P \in E(\mathbb{F}_q)$, and $0 \in E(\mathbb{F}_q)$ by definition of an elliptic curve.

Proposition: if $\varphi, \psi: E_1 \to E_2$ are isogenies and ω is a global 1-form in E_2, then $(\varphi+\psi)^*\omega = \varphi^* + \psi^*\omega$.

E is given in affine coordinates by $y^2 = f(x)$, (at least if char $K \neq 2, 3$).

Then $\omega = \frac{dx}{y}$: this has no poles, so is global, and no zeroes.

Even if char $K = 2$ or 3, ω still exists. For any K, ω is unique up to scalars.

What about $\varphi^*\omega$? Suppose $f: X \to Y$ is a morphism of smooth varieties over K. If ω is an r-form on Y, then $\exists$ natural r-form $f^*\omega$ in X. In particular, $f^*: \{1\text{-forms on } Y\} \to \{1\text{-forms on } X\}$. This is dual to the derivative map $f_* = df: T_x \to f^*T_y$. Eg, if $\omega = d\eta$, η a function on Y, then $f^* = d(\eta \circ f)$.

Proof of proposition: have $\omega(0)$, a cotangent vector at the origin $0 \in E_2$, and $(f^*\omega)(0)$ a cotangent vector at $0 \in E_1$. Dually, consider $\varphi_*, \psi_*: T_0 E_1 \to T_0 E_2$. These are Lie algebras, although very boring (1-dimensional, so $[\,,\,] = 0$).

G, H algebraic groups over K. $\varphi, \psi: G \to H$, morphisms of algebraic varieties taking $e_G \to e_H$. Define $\varphi \cdot \psi: G \to H$; $g \mapsto \varphi(g)\psi(g)$. [$\cdot = \oplus$ for elliptic curve].

Compute $(\varphi.\psi)_*: T_eG \to T_eH$ in terms of φ_* and ψ_* as follows.
Suppose $\gamma \in T_eG$. This is $\Leftrightarrow$ $e + \varepsilon\gamma \in G(K[\varepsilon])$

$g|_{t=0} = e$, $\frac{dg}{dt}\Big|_{t=0} = \gamma$.

$$\varphi.\psi(g) = \varphi(e_G + \varepsilon\gamma).\psi(e_G + \varepsilon\gamma) = (e_H + \varepsilon\varphi_*(\gamma))(e_H + \varepsilon.\psi_*(\gamma))$$
$$= e_H + \varepsilon(\varphi_*(\gamma) + \psi_*(\gamma)) = e_H + \varepsilon((\varphi\psi)_*(\gamma))$$

Compare coefficients of ε: $\varphi_*(\gamma) + \psi_*(\gamma) = (\varphi\psi)_*(\gamma)$.
Dually, $(\varphi\psi)^* = \varphi^* + \psi^*$ as maps $T^*_eH \to T^*_eG$.
So if $H = E_2$ and $G = E_1$, then $e = 0$ and $\cdot = +$, so we get
$((\varphi+\psi)^*\omega)(0) = (\varphi^*\omega)(0) + (\psi^*\omega)(0)$, so $(\varphi^*\omega + \psi^*\omega) = (\varphi+\psi)^*\omega$ globally on E_1.

Note that if we have $E_1 \xrightarrow{\varphi} E_2 \xrightarrow{\chi} E_3$, then $(\chi\varphi)^*\omega = \varphi^*\chi^*\omega$, by general stuff about differentiation.

Lemma: On E, $[-1]^*\omega = -\omega$.
Proof: Consider $\varphi: G \to G$, $\varphi(g) = g^{-1}$, where G is an algebraic group.
What is $\varphi_*: T_eG \to T_eG$? Let $\gamma \in T_eG$, so $1 + \varepsilon\gamma \in G(K[\varepsilon])$ $(1 := e)$.
$g = 1 + \varepsilon\gamma \Rightarrow g^{-1} = 1 - \varepsilon\gamma$. So $\varphi(1+\varepsilon\gamma) = 1 - \varepsilon\gamma = 1 + \varepsilon\varphi_*(\gamma)$.
So $\varphi_*(\gamma) = -\gamma$. Dually, $\varphi^*: T^*_eG \to T^*_eG$ is also -1.
So $([-1]^*\omega)(0) = (-\omega)(0)$. So $[-1]^*\omega = -\omega$ globally on E.

Corollary: $1-F$ is separable.
Proof: $[1-F]^*\omega = [1]^*\omega - F^*\omega = \omega - F^*\omega$.
If $f \in K[E]$, then $f \circ F = f^q$. So $F^*df = qf^{q-1}df = 0$. So F^* is 0 on rational differentials in E. So $F^*\omega = 0$, so $(1-F^*)\omega = \omega$.
So $(1-F)_*$ is non-zero on tangent vectors (and so is an isomorphism on tangent spaces), ie $1-F: E \to E$ is a morphism of curves that is $\neq 0$ in tangent spaces. This is equivalent to the definition of separable.
Then by Riemann-Hurwitz, $1-F \neq 0$ everywhere in tangent spaces, ie $1-F$ is everywhere unramified.

Dual Isogenies.
Suppose $\varphi: E_1 \to E_2$ a non-zero isogeny of elliptic curves over K. Say $\deg\varphi = m$.
Maybe φ is inseparable (eg, $K = \mathbb{F}_q$, φ = Frobenius).
But recall Galois theory: $K(E_1) \supseteq K(E_2)$ can be decomposed as: $K(E_1)$ — purely inseparable — $K(E_3)$ — separable — $K(E_2)$.

Then φ can be factored: $E_1 \xrightarrow{\alpha} E_3 \xrightarrow{\beta} E_2$, α purely inseparable, β separable.
$\deg\varphi = \deg\alpha \cdot \deg\beta$. E_3 is an algebraic curve (in fact, elliptic).
[Follows from general theorems about algebraic curves. If $X \to Y$ is a purely inseparable morphism of algebraic curves, then $g(X) = g(Y)$. If X is elliptic,

$g(X)=1$, so $g(Y)=1$, so Y has a K-point $f(0)$. (g = genus = # linearly independent global 1-forms). Any curve of genus 1 with a marked point P is naturally an elliptic curve with P as origin].

α, β are isogenies, as they take O to O.

Claim: $\ker \varphi \subseteq E_1(m)$, and have diagram
$$\begin{tikzcd} E_1 \arrow[rr, "{[m]}"] \arrow[dr, "\varphi"'] & & E_1 \\ & E_2 \arrow[ur] & \end{tikzcd}$$

Proof: (i) Assume φ separable, and that m is prime to char K. Then over $\bar{K}$, $\varphi^{-1}(Q)$ consists of m distinct points. So $\ker\varphi$ consists of m points. So $mP = 0$ $\forall$ $P \in \ker\varphi$, P defined over $\bar{K}$. So $\ker\varphi \subseteq E_1(m)$.
Have
$$\begin{tikzcd} E_1 \arrow[r, "{[m]}"] \arrow[dr, "\varphi"'] & E_1 \\ & E_2 \end{tikzcd}$$

φ, $[m]$ are separable morphisms, and so (by Riemann-Hurwitz) are everywhere unramified.
Given any isogeny $\psi: E_1 \to E_2$, $\ker\psi$ comes with multiplicities. φ, $[m]$ are everywhere unramified, so the structures in $\ker\varphi$ and $\ker[m] = E_1[m]$ are just structures of finite abelian groups. Get $H = E_1[m]/\ker\varphi \hookrightarrow E_2$. H acts on E_2 by translations.
General fact: given a finite group H of automorphisms of an algebraic variety X, there exists a quotient X/H, ie have morphism $\pi: X \to X/H$ of varieties defined over K, whose fibres are the orbits.
Eg: $E_1/E_1[m] \to E_1$. ie, $\pi = [m]: E_1 \to E_1$.

(ii) Assume φ separable, and char $K \mid m$. Picture is the same, but $[m]$ is inseparable (since $[m]^*\omega = m\omega = 0$, ω global 1-form on E_1). Still have $E_1[m]/\ker\varphi \hookrightarrow E_2$, and then construct $E_2 \to E_1$ as quotient by $E_1[m]/\ker\varphi$.

(iii) φ purely inseparable. Can break up φ, with $E_1 \xrightarrow{\varphi_1} E_1' \to \cdots \xrightarrow{\varphi_r} E_2$, each φ_i purely inseparable, of degree p. (If $K = \mathbb{F}_p$, then φ_i = Frobenius: $E_1 \to E_1$. In general, each φ_i is "some version of the Frobenius")

Claim: Have a diagram
$$\begin{tikzcd} E_1 \arrow[r, "{[p]}"] \arrow[dr, "\varphi_1"'] & E_1 \\ & E_1' \arrow[u] \end{tikzcd}$$

$[p]^*\omega = 0$, ie $[p]^*$ kills all tangent vectors. But φ_1 is universal wrt killing tangent vectors. (Given X over K, char $K = p$, $\exists$ $\Phi: X \to X'$, morphism of varieties over K, universal wrt killing tangent vectors. If $K = \mathbb{F}_p$, then Φ = Frob., $\deg\Phi = p^{\dim X}$).

Piecing together (i), (ii), (iii), and second claim, we have proved the first claim.

Basic idea: prove $\ker\varphi \subset E_1[m]$, and construct $E_2 \to E_1$ as quotient by $E_1[m]/\ker\varphi$.

Remark: Given isogeny $\varphi: E_1 \to E_2$, $\varphi \neq 0$, get isogeny $E_1/\ker\varphi \to E_2$.
Given $\varphi: E_1 \to E_2$, $\deg\varphi = m$. Constructed (in outline) $\hat{\varphi}: E_2 \to E_1$ so that
$$\begin{tikzcd} E_1 \arrow[r, "{[m]}"] \arrow[dr, "\varphi"'] & E_1 \\ & E_2 \arrow[u, "\hat{\varphi}"'] \end{tikzcd}$$
is commutative. $\hat{\varphi}$ is the dual isogeny.

Describe φ in terms of divisors. Have $i_\alpha : E_\alpha \to \mathrm{Pic}^\circ E_\alpha$, by $P \mapsto [P]-[0]$.
$\mathrm{Div}^\circ = \{$divisors of degree $0\}$. $\mathrm{Pic}^\circ = \mathrm{Div}^\circ/$(linear equivalence).
Have $\sigma_\alpha : \mathrm{Div}^\circ E_\alpha \to E_\alpha$; $\Sigma n_P[P] \mapsto \Sigma [n_P] P$.

<u>Exercise:</u> σ_α factors through $\mathrm{Pic}^\circ E_\alpha$ so that $E_\alpha \underset{\sigma_\alpha}{\overset{i_\alpha}{\rightleftarrows}} \mathrm{Pic}^\circ E_\alpha$ are inverse. (Abel-Jacobi).

<u>Claim:</u> $\hat{\varphi}$ is the composite $\psi : E_2 \xrightarrow{i_2} \mathrm{Pic}^\circ E_2 \xrightarrow{\varphi^*} \mathrm{Pic}^\circ E_1 \xrightarrow{\sigma_1} E_1$.
<u>Proof:</u> $\hat{\varphi}, \psi$ are defined over K. To show they are equal it's enough to assume $K = \bar{K}$.
Let $Q \in E_2(\bar{K})$. $\psi(Q) = \sigma_1 \varphi^*([Q]-[0]) = \sigma_1 \big(\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)[P] - \sum_{\tau \in \ker\varphi} e_\varphi(\tau)[\tau] \big)$,
where $e_\varphi(P) =$ ramification index of φ at P.
Since φ is a map of elliptic curves, $e_\varphi(P) = \deg_i \varphi$, degree of inseparability of φ. So $m = \deg\varphi = \deg_i \varphi \cdot \#(\ker\varphi)$.
Fix $P_1 \in \varphi^{-1}(Q)$. Get: $\psi(Q) = [\deg_i \varphi] \big(\sum_{P \in \varphi^{-1}(Q)} P - \sum_{\tau \in \ker\varphi} \tau \big)$

$$= [\deg_i \varphi] \big(\sum_\tau (P_1 + \tau) - \sum_\tau \tau \big) = [\deg_i \varphi] . [\#\ker\varphi] P_1 = [m] P_1$$

$\varphi(P_1) = Q$. So $[m]P_1 = \psi(Q) = \psi\varphi(P_1)$, and $\hat{\varphi}\varphi(P_1) = [m]P_1$, both $\forall P_1 \in E_1(K)$.
So $\psi\varphi = \hat{\varphi}\varphi$, so $(\psi - \hat{\varphi})\varphi = 0$. But $\varphi \neq 0$, so $\psi = \hat{\varphi}$.

<u>Theorem:</u> $(\varphi + \psi)^\wedge = \hat{\varphi} + \hat{\psi}$ $\forall \varphi, \psi : E_1 \to E_2$.
<u>Proof:</u> $E_\alpha \xrightarrow{i_\alpha} \mathrm{Pic}^\circ E_\alpha$, isomorphically, via i_1, i_2, $\hat{\varphi}, \hat{\psi}$ corresponding to φ^*, ψ^*.
So need $(\varphi+\psi)^* = \varphi^* + \psi^*$.
$E_1 \to E_2 \times E_2 \times E_2$, $(\varphi + \psi, -\varphi, -\psi)$.
Cube: $\forall D$, $[0]^* D + (\varphi+\psi)^* D + \varphi^*[-1]^* D + \psi^*[-1]^* D \sim \psi^* D + \varphi^* D + (\varphi+\psi)^*[-1]^* D$.

<u>Claim:</u> $D \in \mathrm{Pic}^\circ \Rightarrow D$ is skew-symmetric, ie $[-1]^* D \sim -D$
<u>Proof:</u> Exercise.

Given this claim, get $2(\varphi+\psi)^* D \sim 2\varphi^* D + 2\psi^* D$, so $2(\varphi+\psi)^* = 2(\varphi^* + \psi^*)$
Cancel 2 as before.

<u>Note:</u> In the diagram,

$$\begin{tikzcd} E_1 \arrow[r, "{[m]}"] \arrow[dr, "\varphi"'] & E_2 \\ & E_2 \arrow[u, "\hat{\varphi}"'] \end{tikzcd}$$

, $\ker\varphi$ is a "finite group scheme over K".

$\ker[m] = E[m]$. Over $\mathbb{Q}$, $E[m]$ has degree m^2, but may not have all its points defined over $\mathbb{Q}$.

We showed that under $E \cong \mathrm{Pic}^\circ E$, $P \mapsto [P]-[0]$, $\hat{\varphi}$ is just φ^*.

<u>Complete proof of proposition:</u> $D \sim [z] - [0]$ where $z \in E$. We want to find x such that $[x] - [-x] \sim D \sim [z] - [0]$. Recall $[P+Q] + [0] \sim [P] + [Q]$. We want $[x] + [0] = [-x] + [z]$, ie $x = z - x$. Choose any x such that $2x = z$. This is possible since 2 is surjective. This proves the claim.
Thus $2(\varphi+\psi)^* = 2\varphi^* + 2\psi^*$, ie $2((\varphi+\psi)^* - \varphi^* - \psi^*)$ kills $\mathrm{Pic}^\circ E_2$. So $2(\widehat{(\varphi+\psi)} - \hat{\varphi} - \hat{\psi}) = 0$ is an isogeny $E_2 \to E_1$. But $\mathrm{Hom}(E_2, E_1)$ is a torsion-free $\mathbb{Z}$-module.

Tate modules: Fix a prime l. There is a sequence of $\mathbb{Z}$-modules
$$\cdots \to \mathbb{Z}/l^3\mathbb{Z} \to \mathbb{Z}/l^2\mathbb{Z} \to \mathbb{Z}/l\mathbb{Z} \to 0.$$

Proposition ("l-adic integers): There is a ring $\mathbb{Z}_l$ such that $\mathbb{Z}_l$ is universal for rings R with homomorphisms $R \xrightarrow{\varphi_n} \mathbb{Z}/l^n\mathbb{Z}$ such that
$$\begin{tikzcd} R \arrow[r, "\varphi_m"] \arrow[dr, "\varphi_n"'] & \mathbb{Z}/l^m\mathbb{Z} \arrow[d] \\ & \mathbb{Z}/l^n\mathbb{Z} \end{tikzcd}$$
commutes $\forall m, n$.

$\mathbb{Z}_l$ is a DVR with maximal ideal $(l) = l\mathbb{Z}_l$ and $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(l)} \hookrightarrow \mathbb{Z}_l$. Moreover, $\mathbb{Z}/l^n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_{(l)}/l^n\mathbb{Z}_{(l)} \xrightarrow{\cong} \mathbb{Z}_l/l\mathbb{Z}_l$ and $\mathbb{Z}_l$ is uncountable.

Hensel's Lemma: Suppose $f \in \mathbb{Z}_l[X]$ is monic and that f has a solution modulo l. Then f has a solution in $\mathbb{Z}_l$. (false for $\mathbb{Z}$ or $\mathbb{Z}_{(l)}$).

Starting from an f.g. $\mathbb{Z}$-module M we can form $\cdots \to M/l^3M \to M/l^2M \to M/lM \to 0$, and construct M_l, the l-adic completion of M. There are $\mathbb{Z}_l$-modules not arising naturally from a $\mathbb{Z}$-module.

Example: Let E be an elliptic curve over K. ($K = \bar{K}$). Suppose $l \neq \operatorname{char} K$.
Then $E[l] \cong (\mathbb{Z}/l\mathbb{Z})^2$, $E[l^n] \cong (\mathbb{Z}/l^n\mathbb{Z})^2$, and $[l]: E[l^{n+1}] \to E[l^n]$ is surjective.
We get a sequence $\cdots \to E[l^3] \to E[l^2] \to E[l] \to 0$, giving the l-adic Tate module $T_l(E)$ of E such that
(i) $T_l(E) \cong \mathbb{Z}_l^2$
(ii) There is a natural map $\pi_n : T_l(E) \to E[l^n]$ with $\ker \pi_n = l^n T_l(E)$; and
$$\begin{tikzcd} T_l(E) \arrow[r, "\pi_m"] \arrow[dr, "\pi_n"'] & E[l^m] \arrow[d, "{[l^{m-n}]}"] \\ & E[l^n] \end{tikzcd}$$
, for $m \geq n$ is commutative.
But there is no $\mathbb{Z}$-module $M \cong \mathbb{Z}^2$ giving rise to this naturally.

Aim: To prove $\operatorname{Hom}(E_1, E_2)$ is f.g. of rank ≤ 4 (then $=$ isogeny).

Theorem: The natural map $\operatorname{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \operatorname{Hom}_{\mathbb{Z}_l}(T_l E_1, T_l E_2)$ is injective.
Proof: Any isogeny $E_1 \xrightarrow{\varphi} E_2$ induces a homomorphism $E_1[l^n] \xrightarrow{\varphi_n} E_2[l^n]$ compatible with multiplication by l.
$$\begin{tikzcd} \vdots \arrow[d] & \vdots \arrow[d] \\ E_1[l^{n+1}] \arrow[r, "\varphi_{n+1}"] \arrow[d, "{[l]}"'] & E_2[l^{n+1}] \arrow[d] \\ E_1[l^n] \arrow[r, "\varphi_n"] & E_2[l^n] \\ \vdots & \vdots \end{tikzcd}$$
$T_l E_1$ sits on top of this column $T_l E_2$ on this.

Thus there is a map $\operatorname{Hom}(E_1, E_2) \to \operatorname{Hom}_{\mathbb{Z}_l}(T_l E_1, T_l E_2)$ which is $\mathbb{Z}$-linear,

but which naturally extends to a $\mathbb{Z}_\ell$- linear map,
$\mathrm{Hom}(E_1,E_2)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell E_1, T_\ell E_2)$
Suppose $\varphi_\ell = 0$. Then $\varphi = \sum_{i=1}^{r} a_i\varphi_i$, where $a_i\in\mathbb{Z}_\ell$ and $\varphi_i \in \mathrm{Hom}(E_1,E_2)$
Recall $\mathbb{Z}/(\ell^n) \xrightarrow{\cong} \mathbb{Z}_\ell/(\ell^n)$, so any $a\in\mathbb{Z}_\ell$ can be approximated modulo ℓ^n by $\alpha\in\mathbb{Z}$.
Choose $\alpha_i\in\mathbb{Z}$ such that $\alpha_i \equiv a_i \pmod{\ell^n}$ (continued later).

<u>Note:</u> $E[\ell^n]$ is a f.g. $\mathbb{Z}/(\ell^n)$-module, $\cong \mathbb{Z}/(\ell^n)\oplus\mathbb{Z}/(\ell^n)$. So $E[\ell^n]$ is naturally a $\mathbb{Z}_\ell$-module.
$\alpha_i\big|_{E_1[\ell^n]} = [\alpha_i]\big|_{E_1[\ell^n]}$

Put $\psi = \sum[\alpha_i]\varphi = \sum\alpha_i\varphi_i$. $\varphi_\ell = 0$, so $\sum a_i\varphi_i\big|_{E_1[\ell^n]} = 0$.
So $\psi\big|_{E_1[\ell^n]} = 0$ (ψ approximates $\varphi \pmod{\ell^n}$). ψ kills $E_1[\ell^n]$, so we have a commutative diagram:

$$\begin{tikzcd} E_1 \arrow[r, "\psi"] \arrow[d, "{[\ell^n]}"'] & E_2 \\ E_1 \arrow[ur, "\chi"'] & \end{tikzcd}$$

<u>Lemma</u> (proved later): For any subgroup $M\subseteq \mathrm{Hom}(E_1,E_2)$ define
$M^{div} = \{\gamma: E_1\to E_2 : n\gamma\in M, \text{ some } n\in\mathbb{Z}\}$.
Then $(M^{div})^{div} = M^{div}$, and if M is f.g., so is M^{div}.

<u>Back to proof of Theorem:</u> Apply lemma with M generated by $\varphi_1,\dots,\varphi_r$. Then $\psi\in M^{div}$, and $\psi = \ell^n\chi$, so $\chi\in M^{div}$.
Wlog $M = M^{div}$ (by enlarging the generating set) and $\{\varphi_1,\dots,\varphi_r\}$ is a $\mathbb{Z}$-basis.
Then $\chi = \sum\beta_i\varphi_i$ for certain $\beta_i\in\mathbb{Z}$, so $\alpha_i = \ell^n\beta_i$ $\forall i$, so $a_i\equiv 0 \pmod{\ell^n}$.
Since n was arbitrary, $a_i = 0$ ($\mathbb{Z}_\ell$ is a PID). Hence $\varphi = 0$.

<u>Proof of lemma:</u> deg. is a positive definite quadratic form $\mathrm{Hom}(E_1,E_2)\to\mathbb{Z}$.
Let $M\subseteq\mathrm{Hom}(E_1,E_2)$ be a f.g. $\mathbb{Z}$-module. deg extends to $\deg: M\otimes\mathbb{R}\to\mathbb{R}$ and is still a positive definite quadratic form, so is continuous, on $M\otimes\mathbb{R}$.

$$\begin{array}{ccccccc} M & \subseteq & M^{div} & \subseteq & M\otimes\mathbb{Q} & \subseteq & M\otimes\mathbb{R} \\ & & \cap & & & & \\ & & \mathrm{Hom}(E_1,E_2) & & & & \end{array}$$

$\deg x$ is in $\mathbb{Z}$ $\forall x\in M^{div}$, so $U\cap M^{div} = \{0\}$, so M^{div} is a lattice in $M\otimes\mathbb{R}$, so has a finite $\mathbb{Z}$-basis.

<u>Corollary:</u> $\mathrm{Hom}(E_1,E_2)$ is a f.g. $\mathbb{Z}$-module of rank ≤ 4.
<u>Proof:</u> Let $H = \mathrm{Hom}(E_1,E_2)$ - torsion free. If the result is false then there are $x_1,\dots,x_5\in H$, linearly independent. Then $H\otimes\mathbb{Z}_\ell\to\mathrm{Hom}(T_\ell E_1, T_\ell E_2)$ is not an injection #.

<u>Corollary:</u> $\mathrm{Hom}(E,E)$ is a ring and an f.g. $\mathbb{Z}$-module of rank ≤ 4.

<u>Exercise:</u> Show that if $K=\mathbb{C}$ then $\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}(E,E)\le 2$.
(Rank 4 does occur in char $= p > 0$).

Weil Pairing.

Let E be an elliptic curve over K. Recall $\mu_m(K) = \{\zeta \in \bar{K} : \zeta^m = 1\}$

Theorem: There is a pairing $e_m : E[m] \times E[m] \to \mu_m \bar{K}$ such that

(i) e_m is $\mathbb{Z}$-bilinear,

(ii) e_m is skew-symmetric

(iii) e_m is non-degenerate

(iv) $(e_{mn}(\cancel{m}P, \cancel{m}Q))^n = e_m(nP, nQ)$

(v) if $\varphi : E_1 \to E_2$ is an isogeny then $e_m(\varphi P, Q) = e_m(P, \hat{\varphi} Q)$. $\hat{\varphi}$ is the adjoint.

(vi) taking limits, there is a pairing $e : T_\ell E \times T_\ell E \to T_\ell(\mu \bar{K})$. $(\cong \mathbb{Z}_\ell)$, which is non-degenerate, $\mathbb{Z}_\ell$-bilinear, skew-symmetric.

(vii) e_m and e are equivalent wrt $Gal(\bar{K}:K)$. If $\sigma \in Gal(\bar{K}:K)$, then $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q)$

(viii) If $\varphi : E \to E$ is an isogeny then $\varphi_\ell : T_\ell E \to T_\ell E$ has a determinant $e(\varphi_\ell(X), \varphi_\ell(Y)) = e(X, Y)^{\det \varphi_\ell}$, and $\det \varphi_\ell = \deg \varphi$.

(a) Construction of e_m: use Weil Reciprocity.

Proposition: Let X be a smooth projective algebraic curve over K and $f, g \in K(X)^*$. Let $\operatorname{supp} f = \{$zeroes and poles of $f\}$ and assume $\operatorname{supp} f \cap \operatorname{supp} g = \phi$. Say $(f) = \Sigma n_P P$, $(g) = \Sigma m_Q Q$. Define $f((g)) = \Pi f(Q)^{m_Q} \in K^*$. Then $f((g)) = g((f))$.

Proof: [wlog $K = \bar{K}$]. Step (i): if $X = \mathbb{P}^1$, the result is trivial.

Step (ii): Use that for n sufficiently large $\exists$ a separable morphism $X \xrightarrow{\varphi_n} \mathbb{P}^1$ of degree n. [In fact, by R-R, $n \geq 2g+1$ will do, where $g = g(X)$. Any divisor class of degree $n \geq 2g+1$ corresponds to $X \hookrightarrow \mathbb{P}^N$ of degree n. Construct φ_n as a projection from some general linear space of dimension $N-2$]

If $P \in E[m]$, then $mP = 0$, ie $m[P] - m[0] \sim 0$. Ie $\exists\ f = f_P \in \bar{K}(E)^*$ with $(f) = m([P]-[0])$.
Let $D = [P] - [0]$.
Recall: $\deg D = 0$, so D is antisymmetric in $\operatorname{Pic}^0 E$, so (cube), $[m]^* D \sim mD \sim 0$.
So $\exists\ g = g_P \in \bar{K}(E)^*$ such that $(g) = [m]^* D$. So $(g^m) = m.[m]^* D = [m]^*(mD) = [m]^*(f) = (f \circ [m])$. So $g^m = \lambda f \circ [m]$, $\lambda \in \bar{K}^*$ (global functions on projective varieties are constant. Replacing f by λf, we may assume $\lambda = 1$. So $g^m = f \circ [m]$.
Let $Q \in E[m]$, $X \in E$, arbitrary. Then $g(X+Q)^m = f \circ [m](X+Q) = f(mX + mQ) = f(mX) = g(X)^m$.
Then $\frac{g(X+Q)}{g(X)} \in \bar{K}(E)$, and takes values in μ_m. So on some open piece U of E, $X \to \frac{g(X+Q)}{g(X)}$ is a morphism $U \to \mu_m \subseteq \bar{K} = \mathbb{A}^1_E$. But μ_m is finite and U is connected, so this morphism is constant (ie, independent of X).

So define $e(Q, P) = \frac{g(X+Q)}{g(X)} \in \mu_m$.

(b) e_m is bilinear.

$$e_m(P_1+P_2, Q) = \frac{g_Q(X+P_1+P_2)}{g_Q(X)} = \frac{g_Q((X+P_1)+P_2)}{g_Q(X+P_1)} \cdot \frac{g_Q(X+P_1)}{g_Q(X)} = e_m(P_2, Q)\cdot e_m(P_1, Q).$$

So e_m is bilinear in the first term.

Consider $e_m(S, P_1+P_2)$. Put $P_3 = P_1+P_2$. Ie, $[P_3]+[O] \sim [P_1]+[P_2]$.

So $\exists\, h \in \bar{K}(E)^*$ with $(h) = [P_3]+[O]-[P_1]-[P_2]$. Let $f_i = f_{P_i}$, $g_i = g_{P_i}$.

Then, $\left(\frac{f_3}{f_1 f_2}\right) = m[P_3] - m[O] - m[P_1] + m[O] - m[P_2] + m[O] = m(h)$.

So $f_3 = \lambda f_1 f_2 h^m$, $\lambda \in \bar{K}^*$. So $f_3\circ[m] = \lambda (f_1\circ[m])(f_2\circ[m])(h\circ[m])^m$.

So $g_3^m = \lambda g_1^m g_2^m (h\circ[m])^m$, so $g_3 = \nu g_1 g_2\, h\circ[m]$, $\nu \in \bar{K}^*$.

So $$e(S, P_1+P_2) = e(S, P_3) = \frac{g_3(X+S)}{g_3(X)} = \frac{\nu g_1(X+S)\, g_2(X+S)\, h(mX+\cancelto{0}{mS})}{\nu g_1(X)\, g_2(X)\, h(mX)}$$
$$= e(S, P_1)\, e(S, P_2)$$

(c) Skew-symmetry.

Aim: $e_m(P, P) = 1$.

Let $(f) = m([P]-[O])$ For $z \in E$, define $\tau_z(y+z)$ - "translation by z". $\tau_z : E \to E$ is an isomorphism of varieties, but not an isogeny ($O \not\mapsto O$), if $z \neq 0$.

$(f\circ\tau_{iP}) = m[P-iP] - m[O-iP] = m[(1-i)P] - m[(-i)P]$.

So $\left(\prod_{i=0}^{m-1} f\circ\tau_{iP}\right) = m\sum_i\left([(1-i)P] - [(-i)P]\right) = 0$, by inspection. So $\prod f\circ\tau_{iP}$ is constant.

Choose P' such that $mP' = P$.

Then $(g\circ\tau_{iP'})^m(z) = g(z+iP')^m = f(mz+iP) = f\circ\tau_{iP}\circ[m](z)$.

So $\prod_{i=0}^{m-1}(g\circ\tau_{iP'})^m$ is constant, so $\prod(g\circ\tau_{iP'})$ is constant.

So $\prod(g\circ\tau_{iP'})(X) = \prod g\circ\tau_{iP'}(X+P')$. So $\prod(g\circ\tau_{iP'})(X) = \prod g\circ\tau_{(i+1)P'}(X)$.

Cancel terms: $g(X) = g\circ\tau_{mP'}(X) = g(X+P)$.

So $e(P,P) = \frac{g(X+P)}{g(X)} = 1$, so e is skew-symmetric.

(d) Non-degeneracy

Suppose $e(P, Q) = 1$ $\forall P \in E[m]$. $f = f_Q$, $g = g_Q$, such that $(f) = m([Q]-[O])$, $g^m = f\circ[m]$. $\frac{g(X+P)}{g(X)} = 1$ $\forall P \in E[m]$, so $g(X+P) = g(X)$ $\forall P \in E[m]$.

Ie, g is invariant under translation action of $E[m]$ on E.

$$\begin{tikzcd} & & E \\ E \arrow[r, "\pi"] \arrow[d, "g"'] \arrow[urr, bend left, "{[m]}"] & E/E[m] \arrow[ur, "\cong"'] \arrow[dl, bend left, "h"] & \\ \mathbb{P}^1 & & \end{tikzcd}$$

$g = h\circ\pi$

So $g = h\circ[m]$, some h. So $h^m\circ[m] = g^m = f\circ[m]$. So $f = h^m$.

So $m(h) = (f) = m([Q]-[O])$. This is an equality of divisors, not just divisor classes. So $(h) = [Q]-[O]$

So $Q \neq O \Rightarrow h : E \to \mathbb{P}^1$ is a morphism of degree 1, ie an isomorphism $\divideontimes$. So $Q = O$.

So e_m is non-degenerate.

(e) Adjoints.

Suppose $\varphi: E_1 \to E_2$ is an isogeny, $P \in E_1[m]$, $Q \in [m]$. Then $e_m(\varphi P, Q) = e_m(P, \hat{\varphi} Q)$

Proof: Via $E_i \xrightarrow{\cong} \mathrm{Pic}^0 E_i$, $P \mapsto [P] - [0]$, $\hat{\varphi} = \varphi^*$ ie, $[\hat{\varphi} Q] - [0] \sim \varphi^*([Q] - [0])$ on E_1.

So $\exists\, h \in \bar{K}(E_1)^*$ such that $(h) = \varphi^*[Q] - \varphi^*[0] - [\hat{\varphi} Q] + [0]$. $\quad -(*)$.

Have $f = f_Q$, $g = g_Q \in \bar{K}(E_2)^*$ with $(f) = m([Q] - [0])$, $g^m = f \circ [m]$.

$e(\varphi P, Q) = \dfrac{g(X + \varphi P)}{g(X)}$, any $X \in E_2$.

Consider $\left(\dfrac{f \circ \varphi}{h^m}\right) = (f \circ \varphi) - m(h) = \varphi^*(f) - m(h) = \varphi^* m([Q] - [0]) - m(h)$.

$= m(\varphi^*[Q] - \varphi^*[0] - (h)) = m([\hat{\varphi} Q] - [0])$, by $(*)$

This is an equality of divisors, so $\dfrac{f \circ \varphi}{h^m} = f_{\hat{\varphi} Q}$

Also, $\left(\dfrac{g \circ \varphi}{h \circ [m]}\right)^m = \dfrac{g^m \circ \varphi}{h^m \circ [m]} = \dfrac{f \circ [m] \circ \varphi}{h^m \circ [m]} = \dfrac{f \circ \varphi}{h^m}[m] = f_{\hat{\varphi} Q}[m]$

So $g_{\hat{\varphi} Q} = \dfrac{g \circ \varphi}{h \circ [m]}$

So, $e(P, \hat{\varphi} Q) = \dfrac{g_{\hat{\varphi} Q}(X + P)}{g_{\hat{\varphi} Q}(X)} = \left(\dfrac{g \circ \varphi(X+P)}{h[m](X+P)}\right) \Big/ \left(\dfrac{g \circ \varphi(X)}{h[m](X)}\right) = \dfrac{g(\varphi X + \varphi P)\, h(mX + mP)}{g(\varphi X)\, h(mX)}$

$= \dfrac{g(\varphi X, \varphi P)}{g(\varphi X)} = e(\varphi P, Q)$.

Also, $\forall\, \sigma \in \mathrm{Gal}(\bar{K}/K)$, $\sigma e_m(P, Q) = e_m(\sigma(P), \sigma(Q))$ - easy.

And, $(e_{mn}(P, Q))^n = e_m(nP, nQ)$ - easy.

Fix prime $l \neq \mathrm{char}\, K$. Then the e_{l^n} fit together to give
$e: T_l(E) \times T_l(E) \to T_l(\mu) \underset{\mathbb{Z}_l}{\cong} \mathbb{Z}_l$. e is bilinear, skew-symmetric, non-degenerate, and $\mathrm{Gal}(\bar{K}/K)$ equivariant.

And, if $\varphi: E_1 \to E_2$ is an isogeny, then $e(\varphi_l x, y) = e(x, \hat{\varphi}_l y)$ $\forall\, x \in T_l(E_1)$, $y \in T_l(E_2)$.

And, if $\varphi: E \to E$ is an isogeny, then $\deg \varphi = \det(\varphi_l)$ - $(*)$.

~~Let $K = \mathbb{F}_Q$. $f = \mathrm{Frob} = \mathrm{Frob}_q$. Elliptic curve E over $\mathbb{F}_q$ $F: E \to E$, $\deg F = q$~~

Proof of $(*)$: Say $\deg \varphi = m$. Then $\varphi \hat{\varphi} = [m]$. So $e(x, y)^m = e(mx, y)$

$= e(\hat{\varphi}_l \varphi_l x, y) = e(\varphi_l x, \varphi_l y)$ by adjointness.

Wrt some basis of T_l, φ_l has matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then by bilinearity and skew-symmetry, $e(\varphi_l x, \varphi_l y) = e(x, y)^{\det \varphi_l}$. so $m = \det \varphi_l$.

Know: $\#E(\mathbb{F}_q) = 1 - a_q + q$, $|a_q| \leq 2\sqrt{q}$.

$m, n \in \mathbb{Z}$. $\deg\left(\frac{m}{n} - F\right) = \frac{1}{n^2} \deg(m - nF) \geq 0$. So $\det\left(\frac{m}{n} - \varphi\right) \geq 0$

Lemma: $a_q = \mathrm{Tr}(\varphi_l)$

Proof: Know that $\det \varphi = \deg F = q$. $\det(1 - \varphi) = \deg(1 - F) = \#E(\mathbb{F}_q) = 1 - a_q + q$.

Fact about 2×2 matrices: $\det \varphi - \det(1 - \varphi) = \mathrm{Tr}\, \varphi - 1$. So $\mathrm{Tr}\, \varphi = a_q$.

So, # points on E fixed by F = $1 - \mathrm{Tr}\,\varphi + \det \varphi$.

So can think of $T_\ell(E) \cong H_1(E, \mathbb{Z}_\ell)$ "approximately"

$$\mathbb{Z}_\ell \cong \Lambda^2 T_\ell(E) \cong H_2(E, \mathbb{Z}_\ell)$$

So we have a Lefschetz fixed point formula, for counting the number of points on $E(\mathbb{F}_q)$.