A course in
Elliptic Curves

Taught by T.A. Fisher

Lent 2013

Last updated: July 10, 2013

Disclaimer

These are my notes from Prof. Fisher's Part III course on elliptic curves, given at Cambridge University in Lent term, 2013. I have made them public in the hope that they might be useful to others, but these are not official notes in any way. In particular, mistakes are my fault; if you find any, please report them to:

Eva Belmont
ekbelmont at gmail.com

A note on the numbering

There are two concurrent numbering schemes in this document: numbers and headings in green refer to Prof. Fisher's numbering system; everything else refers to LaTeX's numbering, induced by setting section numbers = lecture numbers.

Contents

Lecture 1: January 18

Chapter 1: Introduction

References: Silverman – *Arithmetic of Elliptic Curves*; Cassels – *Lectures on Elliptic Curves*; see Milne's graduate lecture notes.

Fermat's method of descent.

Definition 1.1 (Rational, primitive triangles). A right triangle Δ is *rational* if it has rational side lengths $a, b, c \in \mathbb{Q}$. Δ is *primitive* if $a, b, c \in \mathbb{Z}$ are coprime.

Lemma 1.2. (1.1) *Every primitive triangle has side lengths of the form $(u^2 - v^2, 2uv, u^2 + v^2)$ for $u, v \in \mathbb{Z}$ with $u > v > 0$.*

Proof. Let (a, b, c) be a primitive Pythagorean triple (so $a^2 + b^2 = c^2$). a and b can't both be even, because then c would be. If they were both odd, then $a^2 + b^2 \equiv 2 \pmod 4$, which isn't a square. Without loss of generality assume a is odd and b is even; then c is odd. Write $b^2 = c^2 - a^2$. Then

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2} \cdot \frac{c-a}{2}$$

(where both terms on the right are integers).

I claim that $\frac{c+a}{2}$ and $\frac{c-a}{2}$ are coprime: otherwise $p \mid \frac{c+a}{2} + \frac{c-a}{2} = c$ and $p \mid \frac{c+a}{2} - \frac{c-a}{2} = a$, which contradicts our assumption that (a, b, c) is primitive. Suppose $p^2 \mid \left(\frac{b}{2}\right)^2$. Then p divides exactly one of $\frac{c+a}{2}$ and $\frac{c-a}{2}$, since they are coprime. So either $p^2 \mid \frac{c+a}{2}$ or $p^2 \mid \frac{c-a}{2}$. Repeating this for every factor p of $\left(\frac{b}{2}\right)^2$, we find that both $\frac{c+a}{2}$ and $\frac{c-a}{2}$ are squares, say, u^2 and v^2 respectively. Then $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$. ○

Definition 1.3. $D \in \mathbb{Q}_{>0}$ is *congruent* if there is a rational triangle Δ with area D.

Note it suffices to consider square-free $D \in \mathbb{Z}_{>0}$. For example, $D = 5, 6$ are congruent.

Lemma 1.4. (1.2) *$D \in \mathbb{Q}_{>0}$ is congruent iff $Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}$ with $y \neq 0$.*

Proof. By Lemma 1.1, the area of a *primitive* right triangle has the form

$$\frac{1}{2}ab = \frac{1}{2}(u^2 - v^2) \cdot 2uv = uv(u^2 - v^2)$$

so D is congruent iff $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}$ with $w \neq 0$. Set $x = \frac{u}{v}, y = \frac{w}{v^2}$ to get the desired formula. ○

Theorem 1.5 (Fermat). (1.3) *There is no solution to*

$$w^2 = uv(u - v)(u + v) \tag{1.1}$$

in $\mathbb{Z}$ with $w \neq 0$.

Proof. Divide through by common factors to ensure that u, v are coprime. We can assume $u > 0$ (otherwise $(-u, -v, w)$ is a solution), $w > 0$, and $v > 0$ (otherwise $(-v, u, w)$ is a solution). If $u \equiv v \pmod 2$ then replace (u, v, w) by $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$. Now u and v have opposite parity. By now, I can assume that $u, v, u-v, u+v$ are positive, pairwise-coprime integers. (The only place to go wrong, coprime-wise, is with $u-v, u+v$; but if p divides both, then p divides their sum $2u$ and their difference $-2v$. The only prime to worry about is 2, and we just arranged for $u+v$ and $u-v$ both to be odd.)

Since the four factors on the RHS of (1.1) are all coprime and their product is a square, they are all squares. Write $u = a^2, v = b^2, u+v = c^2, u-v = d^2$ for some $a, b, c, d \in \mathbb{Z}_{>0}$. Since we're assuming $u \not\equiv v \pmod 2$, c and d are both odd. So $\frac{c+d}{2}$ and $\frac{c-d}{2}$ are integers.

$$\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2}$$

$c^2 + d^2 = 2u$ so this expression is $u = a^2$. So the triple $(\frac{c+d}{2}, \frac{c-d}{2}, a)$ is a primitive triangle, since any prime factor of the first two would divide their sum c and difference d, and we know that c^2 and d^2 are coprime. This triangle has area $\frac{c^2-d^2}{8} = \frac{v}{4} = \left(\frac{b}{2}\right)^2$.

Let $w_1 = \frac{b}{2}$. By Lemma 1.1, $w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$ for some $u_1, v_1 \in \mathbb{Z}$. So we have a new solution to (1.1). I claim this is a smaller solution than what we started with. $4w_1^2 = b^2 = v \mid w^2$. So $w_1 \leq \frac{1}{2} w$ is strictly smaller than w, and is still positive.

Keep repeating this; we get a sequence of strictly decreasing positive integers, which is a contradiction. So there can be no solutions to 1.1.

(A more modern way to phrase this is to assume the first solution you picked is the smallest one, so when you find a smaller one, that's a contradiction.) ○

1.1. A variant for polynomials.

Let K be a field of characteristic $\neq 2$. Let $\overline{K}$ be the algebraic closure.

Lemma 1.6. *(1.4) Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for four distinct points $[\alpha; \beta] \in \mathbb{P}^1$, then $u, v \in K$.*

Proof. We may assume that $K = \overline{K}$. Using Möbius transformations, we may change coordinates on $\mathbb{P}^1$ and assume that the four ratios in question are $[\alpha; \beta] = [1 : 0], [0 : 1], [1, -1], [1; -\lambda]$ for some $\lambda \in K \backslash \{0, 1\}$. Then

$$u = a^2, v = b^2, u - v = (a+b)(a-b), u - \lambda v = (a + \mu b)(a - \mu b)$$

for $\mu = \sqrt{\lambda}$. We know that $(a+b), (a-b)$ are coprime, since a, b are assumed to be coprime. By unique factorization in $K[t]$, $a+b, a-b, a+\mu b, a-\mu b$ are squares.

But $\max(\deg a, \deg b) < \max(\deg u, \deg v)$, unless u, v are constant. We got a new solution from the old one, and the degree has gone down. By Fermat's method of descent, this can't happen unless the original polynomials were constant. ○

Definition 1.7 (elliptic curve, $E(L)$). An *elliptic curve* E/K is the projective closure of a plane affine curve

$$y^2 = f(x)$$

where $f \in K[x]$ is a monic cubic polynomial with distinct roots in $\overline{K}$.

Let L/K be any field extension. Then $E(L) = \{(x,y) : x, y \in L, y^2 = f(x)\} \cup \{0\}$ where 0 is the point at infinity.

The reason we call the point at infinity "0" is that $E(L)$ is naturally an abelian group and this is the identity. In this course we study $E(L)$ when L is a finite field, local field, or number field.

Lemma 1.2 and Theorem 1.3 show that the only rational solutions to $y^2 = x^3 - x$ happen when $y = 0$, so $E(\mathbb{Q}) = \{0, (0,0), (\pm 1, 0)\}$.

Corollary 1.8. *(1.5) Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.*

Proof. Without loss of generality assume $K = \overline{K}$. By a change of coordinates we may assume

$$E : y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \neq 0, 1$ in K. Suppose $(x,y) \in E(K(t))$. Write $x = \frac{u}{v}$ for coprime polynomials $u, v \in K[t]$. Then

$$w^2 = uv(u-v)(u-\lambda v)$$

for some $w \in K[t]$. By the usual trick, the four factors on the right are coprime since u, v are coprime. By unique factorization in $K[t]$, all four factors on the right are squares. Now apply Lemma 1.4, which implies that u and v are constants, and hence $x = \frac{u}{v}$ is constant too. ○

Lecture 2: January 21

Chapter 2: Some remarks on plane curves

In this section we work over an algebraically closed field $K = \overline{K}$ with $\mathrm{char}(K) \neq 2$.

Definition 2.1 (rational algebraic curve, rational parametrization). An algebraic curve is *rational* if it is birational to $\mathbb{P}^1$ (i.e. there is a rational map to $\mathbb{P}^1$ that has a rational inverse).

For example, $C = \{f(x,y) = 0\} \subset \mathbb{A}^2$ is rational if you can find $\varphi(t), \psi(t) \in K(t)$ such that

(1) $f(\varphi(t), \psi(t)) = 0$, and
(2) the map $\mathbb{A}^1 \to \mathbb{A}^2$ given by $t \mapsto (\varphi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus$ finite set.

The pair (φ, ψ) with the above properties is called a *rational parametrization of f*.

(Note that there is an unproved assertion here, namely that this definition guarantees the existence of a rational inverse.)

Example 2.2 (circle). Let $C = \{x^2 + y^2 = 1\} \subset \mathbb{A}^2$. To get a parametrization, draw a line through $P = (-1, 0)$ with slope t. This line intersects the circle in exactly one other point, the coordinates of which are given by a rational function.

$$\begin{aligned} y &= t(x+1) \\ x^2 + t^2(x+1)^2 &= 1 \\ (x+1)(x-1+t^2(x+1)) &= 0 \\ x = -1 \text{ or } x &= \frac{1-t^2}{1+t^2} \\ (x,y) &= \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{aligned}$$

The same method works for any conic, as long as you can find a rational point.

Proposition 2.3. *Any singular plane cubic is rational.*

Proof. Consider a line of slope t through the singular point. Normally, a line would intersect the cubic three times, but the singular point "counts double", so there is just one more intersection point. Now we can use the above method to obtain a parametrization. ○

For example, $y^2 = x^3$ (cubic with a cusp) has a parametrization $(x, y) = (t^2, t^3)$.

Exercise: find a rational parametrization of $y^2 = x^2(x + 1)$ (cubic with a node).

Theorem 2.4. (2.1) *Let $C \subset \mathbb{P}^2$ be a smooth plane cubic. Then we can change coordinates such that*

$$C : Y^2Z = X(X-Z)(X-\lambda Z)$$

for some $\lambda \in K\backslash\{0, 1\}$.

This is called Legendre form.

Remark 2.5. Putting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ this is $y^2 = x(x-1)(x-\lambda)$ (i.e. the definition of an elliptic curve).

Remark 2.6. Saying "a cubic with distinct roots" is the same as "a cubic with roots $0, 1, \lambda$ (for $\lambda \neq 0, 1$)" (up to change of coordinates).

By Corollary 1.5, elliptic curves are not rational.

By Theorem 2.1 we deduce

Corollary 2.7. (2.2) *No smooth plane cubic is rational.*

To prove Theorem 2.1, we need to quote the following result:

THEOREM 2.8 (Bezout's Theorem). *Let $C, D \subset \mathbb{P}^2$ be plane curves of degrees of m, n with no common components (i.e. there are only finitely many points of intersection), then they meet in exactly mn points when counted with multiplicity. Write this as:*

$$mn = \sum_{P \in C \cap D} (C.D)_P.$$

Lots of the work of the proof involves defining the intersection multiplicity $(C.D)$ properly. But we can quote some properties:

PROPOSITION 2.9 (Properties of intersection multiplicity).

(1) *If $P \in C \cap D$ then $(C\ .\ D)_P \geq 1$ with equality iff the curves* meet transversely *at P (i.e. P is a smooth point on both curves C and D, and $T_P C \neq T_P D$, where $T_P C$ is the tangent line to C through P).*

(2) *If $C = \{F = 0\} \subset \mathbb{P}^2$ for some homogeneous polynomial F and D is the line through P and P', then*

$$(C\ .\ D)_P = \operatorname{ord}_{t=0} F(P + tP')$$

where ord *is the order of vanishing.*

(Note the abuse of notation in (2), since P, P' are projective points and $P + tP'$ is only a polynomial up to scalar multiples. But this doesn't affect the order.)

DEFINITION 2.10 (Flex/ point of inflection). A smooth point $P \in C$ is a *flex (point of inflection)* if $(C\ .\ T_P C)_P \geq 3$.

DEFINITION 2.11. Let $C = \{F(X_1, X_2, X_3) = 0\} \subset \mathbb{P}^2$ be a smooth plane curve of degree d. The *Hessian* is the polynomial

$$H(X_1, X_2, X_3) = \det\left(\frac{\partial^2 F}{\partial X_i \partial X_j}\right)_{i,j=1,2,3}.$$

Note that this has degree $3(d-2)$ in the variables X_1, X_2, X_3.

LEMMA 2.12. *(2.3) Assume* $\operatorname{char}(K) \nmid 2(d-1)$. *Let $P \in C$. Then P is a flex point iff $H(P) = 0$.*

Proof. Let $P = (P_1, P_2, P_3)$ be a point on the curve, and also write $X = (X_1, X_2, X_3)$. Do a Taylor series expansion at the point P:

$$F(P + X) = F(P) + \sum_{i=1}^{3} \frac{\partial F}{\partial X_i}(P) X_i + \frac{1}{2} \sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(P) X_i X_j + \cdots$$

The first term is zero because P is on the curve. Name the first- and second-degree parts:

$$L = \left\{\sum_{i=1}^{3} \frac{\partial F}{\partial X_i}(P) X_i = 0\right\} = T_P C$$

$$Q = \Big\{ \underbrace{\sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(P) X_i X_j}_{G} = 0 \Big\}$$

Then L is the tangent line, and Q is a conic. If P is an inflection point, then Q vanishes. So

$$P \in C \text{ is a flex } \iff L \subset Q$$

In the rank 3 case you get a smooth curve (does not contain any lines). So $L \subset Q$ means that Q is singular, which is equivalent to $H(P) = 0$. That is,

$$P \in C \text{ is a flex } \iff L \subset Q \implies Q \text{ singular } \iff H(P) = 0$$

We need to turn the $\implies$ into an $\iff$.

Claim 2.13. *P is a smooth point on Q and $T_P Q = L$.*

This suffices: given the claim, if Q is singular, then it's a pair of lines and P is not the singular point. So the line it's on is just L.

Proof of claim. If F is homogeneous of degree d, then $F(\lambda X) = \lambda^d F(X)$. Differentiate with respect to λ:

$$\sum_{i=1}^{3} \frac{\partial F}{\partial X_i}(\lambda X) X_i = d\lambda^{d-1} F(X).$$

Put $\lambda = 1$:

$$\sum_{i=1}^{3} X_i \frac{\partial F}{\partial X_i} = dF(X) \qquad \text{(Euler's identity)}$$

Applying the same result to partial derivatives, if $\frac{\partial F}{\partial X_i}$ is homogeneous of degree $d-1$ then

$$\sum_{j=1}^{3} X_j \frac{\partial^2 F}{\partial X_i \partial X_j} = (d-1)\frac{\partial F}{\partial X_i}. \tag{2.1}$$

To prove the claim, notice that (Euler's identity) implies $P \in L$ and (2.1) implies $P \in Q$.

Recall we've defined $G = \sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(P) X_i X_j$ (the expression in Q).

$$\begin{aligned} \frac{\partial G}{\partial X_i}(P) &= 2 \sum_{j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(P) P_j \\ &= 2(d-1) \frac{\partial F}{\partial X_i}(P) \text{ by Euler's identity} \\ T_P Q &= \Big\{ \sum_{i=1}^{3} \frac{\partial G}{\partial X_i}(P) X_i = 0 \Big\} \end{aligned}$$

Since we assumed $2(d-1) \neq 0$:

$$= \{\sum_{i=1}^{3} \frac{\partial F}{\partial X_i}(P) X_i = 0\}$$
$$= T_P C = L. \qquad \bigcirc$$

Proof of Theorem 2.1. Let

$$C = \{F(X, Y, Z) = 0\} \subset \mathbb{P}^2.$$

Lemma 2.3 and Bezout's theorem show that there is a flex $P \in C$. By a linear change of coordinates in $\mathbb{P}^2$ we may arrange that $P = [0; 1; 0]$, and $T_P C = \{Z = 0\}$. Since P s a flex, $F(t, 1, 0)$ has roots where the tangent line meets the curve. $t = 0$ has to be a triple root, and since we only have degree 3, $F(t, 1, 0) = c \cdot t^3$ for some nonzero constant c. So there are no terms of the form X^2Y, XY^2, Y^3. So

$$F = \left\langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \right\rangle.$$

The coefficient of Y^2Z is nonzero, since otherwise P would be singular. X^3 also has a nonzero coefficient because otherwise the line $\{Z = 0\}$ would be in C, contradicting smoothness. We are free to rescale the coordinates X, Y, Z, so assume the coefficients of Y^2Z and X^3 are 1. So

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Next lecture: put this in the form stated. ○

Lecture 3: January 23

We were proving Theorem 2.1; we showed that we could put C in Weierstrass form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6.$$

Now we want to put it in Legendre form

$$Y^2Z = X(X - Z)(X - \lambda Z).$$

Substituting $Y \leftarrow Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$ (i.e. completing the square), we may assume $a_1 = a_3 = 0$. We get $C : Y^2Z = Z^3 f\left(\frac{X}{2}\right)$ for some cubic f. Since C is smooth, the cubic f has distinct roots; if we're over an algebraically closed field, we can factor f completely. After making some substitutions in X and Z we may assume that the roots are $0, 1, \lambda$. Then

$$C : Y^2Z = X(X - Z)(X - \lambda Z).$$

The genus $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C. We won't define it, but here are some facts:

- If $K = \mathbb{C}$, then the genus is just the genus of the Riemann surface.

- A smooth plane curve $C \subset \mathbb{P}^2$ of degree d has genus
$$g(C) = \frac{(d-1)(d-2)}{2}.$$
So for $d \geq 3$, the genus is positive, and $C \not\cong \mathbb{P}^1$. If we're dealing with smooth projective curves, birational implies isomorphic. So this implies Corollary 2.2.

Remark 3.1. If $\varphi : C_1 \to C_2$ is a non-constant morphism of smooth projective curves, then $g(C_1) \geq g(C_2)$. This is a special case of the Riemann-Hurwitz formula.

Example 3.2 (FLT for $n = 4$).
$$C = \{U^4 + V^4 = W^4\} \subset \mathbb{P}^2$$
has genus 3, and
$$E = \{Y^2Z = X^3 - XZ^2\} \subset \mathbb{P}^2$$
has genus 1. There is a map $\varphi : C \to E$ given by
$$(U : V : W) \mapsto (UW^2 : V^2W : U^3).$$
Any rational point on C maps under φ to a rational point on E. In lecture 1, we showed that the only rational points on E were $\{(0:1:0), (0:0:1), (\pm 1:0:1)\}$. We deduce
$$C(\mathbb{Q}) = \{(\pm 1 : 0 : 1), (0 : \pm 1 : 1)\}$$
This is Fermat's Last Theorem for exponent $n = 4$.

3.1. Orders of vanishing. Let C be an algebraic curve with function field $K(C)$. Let $P \in C$ be a smooth point. Write $\mathrm{ord}_P(f)$ to be the order of vanishing of $f \in K(C)$ at P. This is negative if f has a pole at P, and positive if it has a zero.

$\mathrm{ord}_p : K(C)^* \to \mathbb{Z}$ is a discrete valuation. That is,

- $\mathrm{ord}_p(fg) = \mathrm{ord}_p(f) + \mathrm{ord}_p(g)$, and
- $\mathrm{ord}_p(f+g) \geq \min(\mathrm{ord}_p(f), \mathrm{ord}_p(g))$.

Definition 3.3. $t \in K(C)^*$ is a uniformizer at P if $\mathrm{ord}_p(t) = 1$.

Example 3.4 (Finding uniformizers). (2.4) Let $C = \{g = 0\} \subset \mathbb{A}^2$ where $g \in K[x, y]$ is irreducible. By definition
$$K(C) = \mathrm{Frac}\left(K[x, y]/(g)\right).$$
Write $g = g_0 + g_1(x, y) + g_2(x, y) + \cdots$ where g_i is homogeneous of degree i. Suppose $P = (0, 0)$ is a smooth point on C: that is, $g_0 = 0$ and $g_1(x, y) = \alpha x + \beta y$ has α, β not both zero.

Fact 3.5. *Let $\gamma, \delta \in K$. Then $\gamma x + \delta y$ is a uniformizer iff $\alpha\delta - \beta\gamma \neq 0$.*

That is, you can take any linear combination of x, y in the fraction field, except for the tangent line g_1.

Example 3.6. (2.5) Set
$$C : \{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2.$$

It has projective closure

$$\{Y^2Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2.$$

Let $p = (0:1:0)$ (the unique "point at infinity"). Our aim is to compute $\mathrm{ord}_p(x)$ and $\mathrm{ord}_p(y)$. Put $w = \frac{Z}{Y}$, $t = \frac{X}{Y}$. In this new affine piece, the equation for the curve is

$$w = t(t-w)(t-\lambda w). \tag{3.1}$$

Then p is the point $(t,w) = (0,0)$. By Fact 3.5, either w or t is a uniformizer. But w vanishes to order at least 3, so $\mathrm{ord}_p(t) = 1$. All terms on the right vanish to multiplicity 1, so by the rules of ord_p, $\mathrm{ord}_p(w)$ is exactly 3. So

$$\begin{aligned} \mathrm{ord}_p(x) &= \mathrm{ord}_p \tfrac{t}{w} = -2 \\ \mathrm{ord}_p(y) &= \mathrm{ord}_p \tfrac{1}{w} = -3 \end{aligned}$$

3.2. The degree of a morphism. Let $\varphi : C_1 \to C_2$ be a non-constant morphism of smooth projective algebraic curves. Then there is a ring homomorphism $\varphi^* : K(C_2) \to K(C_1)$ taking $f \mapsto f \circ \varphi$. The kernel of a ring homomorphism is an ideal, and fields don't have ideals, so this is an embedding. That is, you can think of φ as a field extension.

Definition 3.7 (degree, separable). Let $\varphi : C_1 \to C_2$ be as above.

(1) $\deg \varphi = [K(C_1) : \varphi^* K(C_2)]$
(2) φ is *separable* if $K(C_1)/\varphi^* K(C_2)$ is a separable field extension (automatic if $\mathrm{char}\, K = 0$).

Remark 3.8. One can prove:

$$\varphi \text{ is an isomorphism} \iff \deg \varphi = 1.$$

Definition 3.9. Suppose $P \in C_1$ and $Q \in C_2$, where $\varphi(P) = Q$. Let $t \in K(C_2)$ be a uniformizer at Q. Define the ramification index e_φ as

$$e_\varphi(P) = \mathrm{ord}_P(\varphi^* t).$$

This is a positive integer, and one can show it is independent of the choice of t.

(Recall we are working over an algebraically closed field.)

Theorem 3.10. *(2.6) Let $\varphi : C_1 \to C_2$ be a non-constant morphism of smooth projective curves, and $Q \in C_2$. Then*

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi.$$

Moreover, if φ is separable, then $e_\varphi(P) = 1$ for all but finitely many $P \in C_1$.

In particular,

(1) *φ is surjective (there must be points in the fiber for $\deg \varphi$ to be nonzero);*
(2) *$\#\varphi^{-1}(Q) \leq \deg \varphi$ with equality for all but finitely many points $Q \in C_2$.*

3.3. Riemann-Roch space. Let C be a smooth projective curve.

Definition 3.11. A *divisor* on C is a formal sum of points on C, say $D = \sum_{P \in C} n_P P$ with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$.

Definition 3.12.

- D is *effective* (written $D \geq 0$) if $n_P \geq 0$ for all P.
- Define the *degree* as $\deg D = \sum n_P$.
- If $f \in K(C)^*$ we define $\operatorname{div} f = \sum_{P \in C} \operatorname{ord}_P(f) P$.
- The *Riemann-Roch space of D* is the vector space
$$\mathcal{L}(D) = \{f \in K(C)^* \,:\, \operatorname{div} f + D \geq 0\} \cup \{0\}.$$
This is the K-vector space of rationals on C with “poles no worse than specified by D”.

Lecture 4: January 25

Remark 4.1. (2.7) Let C be an algebraic curve. A rational map $\varphi : C \to \mathbb{P}^n$ is given by
$$P \mapsto (f_0(P) : f_1(P) : \cdots : f_n(P))$$
where $f_0, \cdots, f_n \in K(C)$ are not all zero.

Fact 4.2. *If C is smooth, then φ is a morphism.*

Chapter 3: Weierstrass equations

In this section, K is a perfect (but not necessarily algebraically closed) field.

Definition 4.3. An elliptic curve E over K is a smooth projective curve of genus 1, defined over K, with a specified K-rational point 0_E.

Example 4.4. Smooth plane cubics have genus 1 by the degree-genus formula quoted in the last lecture. If p is prime, then
$$C = \{X^3 + pY^3 + p^2 Z^3 = 0\} \subset \mathbb{P}^2$$
is a smooth cubic, but it is not an elliptic curve as C has no $\mathbb{Q}$-rational points (if so then you could scale it so everything is an integer; taking mod p yields a contradiction).

Theorem 4.5. *(3.1) Every elliptic curve E over K is isomorphic to a curve in Weierstrass form, via an isomorphism taking $0_E \mapsto (0 : 1 : 0)$.*

Remark 4.6. In lecture 3, we treated the special case where E is a smooth plane cubic and 0_E is a flex.

Let D be a divisor on E (i.e. D is a formal sum of points on E, by which I mean $\overline{K}$-points, not necessarily rational points). We quote the following theorems:

Fact 4.7.

(1) *Riemann-Roch theorem for genus 1:*

$$\dim \mathcal{L}(D) = \begin{cases} \deg D & \textit{if } \deg D > 0 \\ 0 \textit{ or } 1 & \textit{if } \deg D = 0 \\ 0 & \textit{if } \deg D < 0. \end{cases}$$

(2) *If D is defined over K, i.e. it is fixed by the natural action of $Gal(\overline{K}/K)$, then $\mathcal{L}(D)$ has a basis in $K(E)$.*

Proof of Theorem 3.1. Note $\mathcal{L}(2 \cdot 0_E) \subset \mathcal{L}(3 \cdot 0_E)$ (functions with at worst a double pole $\subset$ functions with at worst a triple pole). Use the fact that these are vector spaces of dimensions 2 and 3, to pick a basis $1, x$ of $\mathcal{L}(2 \cdot 0_E)$ and $1, x, y$ of $\mathcal{L}(3 \cdot 0_E)$. Then the seven elements

$$1, x, y, x^2, xy, x^3, y^2$$

have at worst a pole of order 6; they belong to the 6-dimensional vector space $\mathcal{L}(6 \cdot 0_E)$ so they must satisfy a dependence relation.

We know that x has a double pole, because otherwise it would be in $\mathcal{L}(1 \cdot 0_E)$; similarly y has a pole of order 3. The first five terms above have poles of order, respectively, $0, 2, 3, 4, 5$, but x^3 and y^2 both have poles of order 6. So leaving out x^3 or y^2 gives a basis for $\mathcal{L}(6 \cdot 0_E)$. Thus the coefficients of x^3 and y^2 in the dependence relation are nonzero. Rescaling x and y, we can assume these coefficients are 1, so:

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in K$ (the a_i are in K by the second quoted fact above).

There is a morphism $\varphi : E \to E' \subset \mathbb{P}^2$ given by $P \mapsto (x(P) : y(P) : 1)$. This is a morphism because E is smooth (Fact 4.2).

$$[K(E) : K(x)] = \deg(E \xrightarrow{x} \mathbb{P}^1) = \mathrm{ord}_{0_E}\left(\tfrac{1}{x}\right) = 2$$

(The points mapping to ∞ are the poles, and the only pole is at x; we have to work out multiplicity to get the degree. We get this by pulling back the uniformizer at ∞.) Similarly,

$$[K(E) : K(y)] = \deg(E \xrightarrow{y} \mathbb{P}^1) = \mathrm{ord}_{0_E}\left(\frac{1}{y}\right) = 3$$

Use the tower rule:

$$\begin{tikzcd}
 & K(E) \arrow[d, dash] \arrow[ddl, dash, "2"'] \arrow[ddr, dash, "3"] & \\
 & K(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
K(x) & & K(y)
\end{tikzcd}$$

to show that the degree of the vertical extension is 1, and therefore $K(E) \cong K(x, y)$.

$K(E')$ is generated by things we call x, y modulo the ideal defined by E'. $K(E) = \varphi^* K(E')$ and the degree of this extension is, by definition, the degree of φ. So $\deg \varphi = 1$, so φ is birational. We need to show that φ is an isomorphism.

We need to check that E' is smooth. Check that E' is irreducible. If E' is singular then E and E' are rational. But saying it's rational means saying it has genus zero, which is a contradiction.

So E' is smooth; φ^{-1} is a rational map from a smooth curve into projective space, and so it's an isomorphism (this is a fact you should know). We can rewrite $\varphi : E \to E'$ as $P \mapsto (\frac{x}{y}(P) : 1 : \frac{1}{y}(P))$, and under this $0_E \mapsto (0 : 1 : 0)$ as desired. ○

(Note that two elliptic curves being isomorphic also means their specified points match up in the right way.)

Proposition 4.8. *(3.2) Let E, E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ over K iff the Weierstrass equations are related by a substitution of the form*

$$x = u^2 x' + r$$
$$y = u^3 y' + u^2 s x' + t$$

if E is given in terms of variables x, y, E' is given in terms of x', y', and some $u, r, s, t \in K$ where $u \neq 0$.

Proof.

$$\langle 1, x \rangle = \mathcal{L}(2 \cdot 0_E) = \left\langle 1, x' \right\rangle$$

so $x' = \lambda x + r$ for some $\lambda, r \in K$ for $\lambda \neq 0$. Similarly,

$$\langle 1, x, y \rangle = \mathcal{L}(3 \cdot 0_E) = \left\langle 1, x', y' \right\rangle$$

so $y' = \mu y + \sigma x + t$ for some $\mu, \sigma, t \in K$, where $\mu \neq 0$ (otherwise $y \in span(1, x)$). Looking at the coefficients of x^3 and y^2 we see that $\lambda^3 = \mu^2$. After a tiny manipulation, we see

$$\lambda = u^2, \mu = u^3$$

for some $u \in K^*$, and put $s = \frac{\sigma}{u^2}$. ○

A Weierstrass equation defines an elliptic curve $\iff$ it defines a smooth curve. This is determined by the coefficients $a_1, \cdots, a_6$. But there is a polynomial $\Delta \in \mathbb{Z}[a_1, \cdots, a_6]$ such that the curve is smooth $\iff$ $\Delta(a_1, \cdots, a_6) \neq 0$.

You can complete the square unless $\text{char}(K) = 2$, and get rid of the x^2 term unless $\text{char}(K) = 3$; so in the case when $\text{char}(K) \neq 2, 3$ we can reduce to the case when

$$y^2 = x^3 + ax + b$$

with discriminant $\Delta = -16(4a^3 + 27b^2)$.

Corollary 4.9. *(3.3) Assume* $\text{char}(K) \neq 2, 3$. *Elliptic curves*

$$E : y^2 = x^3 + ax + b$$

$$E' : y^2 = x^3 + a'x + b'$$

are isomorphic over K iff

$$\begin{cases} a' &= u^4 a \\ b' &= u^6 b \end{cases}$$

for some $u \in K^*$.

Proof. E and E' are related by a substitution of the form in Proposition 3.2, but $r = 0$ otherwise we'd introduce an x^2-term, and $t = 0$ otherwise that would mess up the fact we'd completed the square. ○

Lecture 5: January 28

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.

Definition 5.1. The j-invariant of E is

$$j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

Corollary 5.2. *(3.4) $E \cong E' \implies j(E) = j(E')$. The converse holds if $K = \overline{K}$.*

Proof. Let $E' : y^2 = x^3 + a'x + b'$. We saw in the previous lecture that

$$E \cong E' \iff \begin{cases} a' &= u^4 a \\ b' &= u^6 b \end{cases}$$

for some $u \in K^*$. So $(a^3 : b^2) = ((a')^3 : (b')^2)$. The j invariant is just this ratio, after doing a Moebius map. So $(a^3 : b^2) = ((a')^3 : (b')^2) \iff j(E) = j(E')$.

Conversely, solve for a and b given $j(E)$; this involves extracting roots, which is OK over an algebraically closed field. ○

Chapter 4: The group law

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic. Let 0_E be any point. How do you add $P + Q$? By Bezout's theorem, any line meets the cubic E in three points (with multiplicity). Suppose P, Q meet the curve in S. Then the line through 0_E and S meets the curve in a third point R. Define $P \oplus Q = R$.

If $P = Q$, "the line through P and Q" means the tangent line. This way of defining the group law is called the "chord and tangent process".

Theorem 5.3. *(4.1) $(E, \oplus)$ is an abelian group.*

Proof. Commutative: The line PQ is the same as the line QP.

0_E *is the identity:* We need $0_E \oplus P = P$: $0_E P$ meets E in S; $0_E S$ meets E in P.

Inverses: Take the tangent line to 0_E; it meets the curve in S. Let Q be the third point of intersection of E and PS; I claim this is $-P$. Now PQ meets E in S; $S 0_E$ meets E at 0_E.

Associativity: A direct approach turns into a total mess; we need more theory.

Definition 5.4 (Linear equivalence, Picard group $\mathrm{Pic}(E)$). $D_1, D_2 \in \mathrm{Div}(E)$ are *linearly equivalent* if there is some $f \in \overline{K}(E)^*$ such that $\mathrm{div}(f) = D_1 - D_2$.

Define the Picard group

$$\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$$

where $D \sim D'$ if they are linearly equivalent. Also define

$$\mathrm{Div}^0(E) = \{D \in \mathrm{Div}(E) \,:\, \deg D = 0\}$$
$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim .$$

Back to associativity. I will show that φ in the next proposition is an isomorphism of groups (although we can't phrase it that way yet).

Proposition 5.5. *(4.2) Define $\varphi : E \to \mathrm{Pic}^0(E)$ where $\varphi : P \mapsto [P - 0_E]$.*
(1) $\varphi(P \oplus Q) = \varphi(P) + \varphi(Q)$ for all $P, Q \in E$.
(2) φ is a bijection.

Proof. (1) $\ell := PQ$ meets E in S; $m := 0_E S$ meets E again in R.

$$\mathrm{div}(\ell/m) = (P) + (Q) + (S) - (0_E) - (S) - (R) = (P) + (Q) - (0_E) - (P \oplus Q)$$

so

$$(P) + (Q) \sim (0_E) + (P \oplus Q)$$
$$(P) - (0_E) + (Q) - (0_E) \sim (P \oplus Q) - (0_E)$$
$$\varphi(P) + \varphi(Q) = \varphi(P \oplus Q)$$

(2) *Injective:* Suppose $\varphi(P) = \varphi(Q)$ for some $P \neq Q$. That is, $P - 0_E \sim Q - 0_E$ so $P \sim Q$. There exists a rational function f such that $\mathrm{div}(f) = P - Q$ (i.e. this has exactly one zero, at P, and exactly one pole, at Q). Rational functions define a map $E \to \mathbb{P}^1$. This is also a morphism, because E is smooth. Work out the degree by picking a point in $\mathbb{P}^1$ and counting the preimages. There is only one preimage of 0 (f has only zero), so this is a morphism of degree 1. Since these are smooth projective curves, this means that $E \cong \mathbb{P}^1$. But we can't have that: E is a curve of genus 1.

Surjective: Let $[D] \in \mathrm{Pic}^0(E)$. Then $D + (0_E)$ is a divisor of degree 1. Use the Riemann-Roch theorem to say that $\dim \mathcal{L}(D + (0_E)) = 1$. So there is some $f \in \overline{K}(E)^*$ such that $D + (0_E) + \mathrm{div}(f) \geq 0$. D and $\mathrm{div}(f)$ have degree zero (rational functions have the same number of zeroes and poles), and (0_E) has degree 1. So $D + (0_E) + \mathrm{div}(f) = (P)$ for some

$P \in E$.

$$\begin{aligned} D &\sim (P) - (0_E) \\ \varphi(P) &= [D] \end{aligned}$$

○

So φ identifies $(E, \oplus)$ with $(\mathrm{Pic}^0(E), +)$. Therefore φ is associative. ○

Note: in the following, we will use $\ominus$ to denote the inverse in the group law, to distinguish it from negative signs of the affine coordinates.

Formulae for $\oplus$ and $\ominus$. Suppose E is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.1}$$

The point at infinity is where all vertical lines meet.

Calculating $\ominus P_1$: Let $P_1 = (x_1, y_1)$. Since 0_E is a point of inflection, $\ominus P_1$ is the other intersection point of the vertical line through P_1. *(x_1, y_1) is one solution of (5.1); finding the other solution of the form $(x_1, ?)$ amounts to solving a quadratic equation in y. If y_1 is one solution of the quadratic equation $y^2 + Ay + B = 0$ (for $A, B \in K[x]$), then the other solution is $-\frac{B}{A} - y_1$.* That is,

$$\ominus P_1 = (x_1, -(a_1x_1 + a_3) - y_1).$$

Calculating $P_1 \oplus P_2$: Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$; suppose the line P_1P_2 intersects E again at $P' = (x', y')$. A line through infinity is a vertical line: $0_EP'$ meets E again in $P_3 = (x_3, y_3)$, where $x_3 = x'$. Our goal is to obtain an expression for $P_3 = P_1 \oplus P_2$ in terms of the coordinates of P_1 and P_2.

Let $y = \lambda x + \nu$ be the line through the points P_1, P_2, P'. Substitute this into 5.1 to get a cubic in just x with roots x_1, x_2 and x'. *In any cubic $(x - r_1)(x - r_2)(x - r_3)$, the coefficient of x_2 is the sum of the roots; here:*

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x' = x_1 + x_2 + x_3.$$

So $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$. Using the formula for $\ominus$ above, we conclude that

$$\begin{aligned} y_3 &= -(a_1x' + a_3) - (\lambda x' + \nu) \\ &= -(\lambda + a_1)x' - \nu - a_3 \\ &= -(\lambda + a_1)x_3 - \nu - a_3 \qquad \text{because } P_3 = \ominus P'. \end{aligned}$$

It remains to give formulae for λ and ν.

Case 1: $x_1 = x_2$, $P_1 \neq P_2$. In this case, the line P_1P_2 is vertical, and $P_1 \oplus P_2 = 0_E$.

Case 2: $x_1 \neq x_2$. Then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$\nu = y_1 - \lambda x_1 = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}.$$

Case 3: $P_1 = P_2$. The line is the tangent line. . . this is on the handout.

Assume E is defined over K, i.e. $a_1, \cdots, a_6 \in K$.

$$E(K) = \{(x,y) \in K^2 \ : \ x, y \text{ satisfy } 5.1\} \cup \{0_E\}$$

Corollary 5.6. *(4.3) $(E(K), \oplus)$ is an abelian group.*

Proof. It is a subgroup of E.

Identity: 0_E is a K-rational point by definition.

Closure, inverses: See above formulae.

Associative, commutative: Inherited. ○

Lecture 6: January 30

Theorem 6.1. *(4.4) Elliptic curves are group varieties:*

$$[-1] : E \to E, \ \text{where } P \mapsto \ominus P$$
$$\oplus : E \times E \to E, \ \text{where } (P,Q) \mapsto P \oplus Q$$

are morphisms of algebraic varieties.

Proof. (1) By formulae in the last lecture, $[-1] : E \to E$ is a rational map, and hence a morphism (since E is a smooth projective curve).

(2) The formulae from last time show that $\oplus : E \times E \to E$ is a rational map. But the result used in part (1) is specific to curves. This map is regular on $U = \{(P,Q) \in E \times E \ : \ P, Q, P+Q, P-Q \neq 0_E\}$. For $P \in E$, let $\tau_P : E \to E$ sending $X \mapsto P \oplus X$: this is a rational map (from a smooth curve to a projective variety), and hence a morphism.

Factor $\oplus$ as

$$E \times E \xrightarrow{\tau_{-A} \times \tau_{-B}} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{A+B}} E$$

which shows that $\oplus$ is regular on $(\tau_A \times \tau_B)U$, for all $A, B \in E$. So $\oplus$ is regular on $E \times E$. ○

6.1. Statements of results. Let K be any field, and E/K an elliptic curve. Let $E(K)$ be the group of K-rational points on E.

(1) $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, where Λ is a lattice (all integer linear combinations of some $\mathbb{R}$-basis of $\mathbb{C}$)

(2) If $K = \mathbb{R}$, then
$$E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \text{if } \Delta > 0 \\ \mathbb{R}/\mathbb{Z} & \text{if } \Delta < 0 \end{cases}$$

(3) (Hasse's theorem) If $K = \mathbb{F}_q$ (field with q elements), then
$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

(4) Suppose $[K : \mathbb{Q}_p] < \infty$, and $\mathcal{O}_K$ is the ring of integers. Then $E(K)$ has a subgroup of finite index $\cong (\mathcal{O}_K, +)$.

(5) (Mordell-Weil theorem) Suppose $[K : \mathbb{Q}] < \infty$. Then $E(K)$ is a finitely generated abelian group.

(The isomorphisms in (1), (2), and (4) respect the relevant topologies.)

Recall the fact from basic group theory:

Theorem 6.2. *If A is a finitely generated abelian group, then*
$$A \cong (\textit{finite group} \oplus \mathbb{Z}^r).$$
r is called the rank *of A.*

The proof of Mordell-Weil gives an upper bound for the rank of $E(K)$. But, there is no known algorithm (even for $K = \mathbb{Q}$) for computing the rank in all cases.

Remark 6.3 (Brief remark on the case $K = \mathbb{C}$). If $\Lambda = \{a\omega_1 + b\omega_2\}$ (where ω_1, ω_2 is a basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space), there is a correspondence
$$\left\{\begin{matrix} \text{meromorphic functions} \\ \text{on Riemann surface } \mathbb{C}/\Lambda \end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix} \Lambda\text{-invariant meromorphic} \\ \text{functions on } \mathbb{C} \end{matrix}\right\}$$
The set on the left is the function field of $\mathbb{C}/\Lambda$. This function field is generated by $\wp(z)$ and $\wp'(z)$, where $\wp$ is the Weierstrass $\wp$-function.

One shows $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ (an isomorphism of groups and of Riemann surfaces) for some elliptic curve $E/\mathbb{C}$. The other part of the classification of $E(\mathbb{C})$ is the following:

Theorem 6.4 (Uniformization theorem). *Every elliptic curve over $\mathbb{C}$ arises in this way.*

(One proof uses modular forms and the j-invariant.)

Chapter 5: Isogenies

Let E_1, E_2 be elliptic curves.

Definition 6.5 (Isogeny). An *isogeny* is a non-constant morphism $\varphi : E_1 \to E_2$ with $\varphi(0) = 0$.

If there is an isogeny from $E_1 \to E_2$, then we say that E_1 and E_2 are *isogenous.*

Next time we'll prove that these are automatically group homomorphisms, and later we'll prove that this is an equivalence relation (where symmetry is the only non-obvious property).

Over an algebraically closed field, any non-constant morphism of elliptic curves is surjective (see Theorem 2.6).

Definition 6.6. Define

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}.$$

This is an abelian group under

$$(\varphi + \psi)(P) = \varphi(P) \oplus \psi(P).$$

If $E_1 \overset{\varphi}{\to} E_2 \overset{\psi}{\to} E_3$ are isogenies, then $\psi \circ \varphi$ is an isogeny. Why is the composition of non-constant maps, non-constant? Because non-constant is equivalent to surjective. We have a "tower law"

$$\deg(\psi \circ \varphi) = \deg(\psi)\deg(\varphi).$$

Definition 6.7 ($[n]$). For $n \in \mathbb{Z}_{>0}$, define $[n] : E \to E$ to be the map $P \mapsto \underbrace{P \oplus \cdots \oplus P}_{n}$, and if $n < 0$, define $[n] = [-1] \circ [-n]$.

By Theorem 4.4, $[n]$ is a morphism. Why is this non-constant?

Lemma 6.8. *(5.1) Assume* $\mathrm{char}(K) \neq 2$. *Assume the elliptic curve has the form*

$$E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$$

for $e_i \in \overline{K}$. (We know that the e_i are distinct.) Then $E[2] = \{0, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. Let $0 \neq P \in E$, with coordinates $P = (x_P, y_P)$. Then

$$T_P E = \{f'(x_P)(x - x_P) = 2y_P(y - y_P)\}$$

$P \in E[2]$ iff $[2]P = 0$. Use the chord and tangent process: $[2]P = 0$ iff $T_P = \{x = x_p\}$, which happens only if $y_P = 0$. ○

Proposition 6.9. *(5.2) If $0 \neq n \in \mathbb{Z}$ then $[n]$ is an isogeny.*

Proof. We must show that $[n] \neq 0$. Assume $\mathrm{char}(K) \neq 2$.

Case $n = 2$: Lemma 5.1 implies that not every point is a 2-torsion point, so $[2]$ is not the zero map.

Case n is odd: Lemma 5.1 implies that there is a nonzero 2-torsion point T. Then $nT = T \neq 0$, so $[n]$ is not the zero map.

Case n is even: Composition of isogenies is an isogeny: use the fact that $[mn] = [m] \circ [n]$.

If $\mathrm{char}(K) = 2$ then we could replace Lemma 5.1 by an explicit lemma on $E[3]$. ○

If $K = \mathbb{C}$, then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$; the n-torsion of the circle group is $E[n] = (\mathbb{Z}/n\mathbb{Z})^2$. Also, $\deg[n] = n^2$. Later, we'll show that the second statement is true over any field K, and the first holds if $\mathrm{char}(K) \nmid n$.

Definition 6.10 (n-torsion subgroup). The n-torsion subgroup of E is

$$E[n] = \ker([n] : E \to E).$$

Lecture 7: February 1

Theorem 7.1. *(5.3) Let $\varphi : E_1 \to E_2$ be an isogeny. Then $\varphi(P \oplus Q) = \varphi(P) \oplus \varphi(Q)$ for all $P, Q \in E_1$.*

Sketch proof. φ induces a map

$$\varphi_* : \mathrm{Div}^0(E_1) \to \mathrm{Div}^0(E_2) \quad \text{where} \sum_{p \in E_1} n_P P \mapsto \sum_{P \in E_1} n_P \varphi(P).$$

Recall $\varphi^* : K(E_2) \hookrightarrow K(E_1)$ induces a field extension.

Fact 7.2. *If $f \in K(E_1)^*$ then* $\mathrm{div}(N_{K(E_1)/K(E_2)} f) = \varphi_*(\mathrm{div}\, f)$.

So $\mathrm{div}\, f$ gets sent to div(*something*); i.e. φ_* takes principal divisors to principal divisors. Since $\varphi(0_{E_1}) = 0_{E_2}$, the following diagram commutes

$$\begin{tikzcd}
E_1 \arrow[r, "\varphi"] \arrow[d, "\cong"] & E_2 \arrow[d, "\cong"] \\
\mathrm{Pic}^0(E_1) \arrow[r, "\varphi_*"] & \mathrm{Pic}^0(E_2)
\end{tikzcd}$$

where the vertical maps were given by $P \mapsto [P - 0_{E_1}]$. φ_* is a group homomorphism, so φ is a group homomorphism. ○

Example 7.3. We will come up with a 2-isogeny (i.e. an isogeny of degree 2) $E \to E'$ with curves defined:

$$E : y^2 = x(x^2 + ax + b)$$
$$E' : y^2 = x(x^2 + a'x + b')$$

where $a' = -2a, b' = a^2 - 4b$. To make sure there aren't repeated roots, we can assume $2b(a^2 - 4b) \neq 0$. Note that E has a rational 2-torsion point at $(0, 0)$ *(it has a vertical tangent line)*. First rearrange E:

$$x(x^2 + b) = y^2 - ax^2$$

$$\begin{aligned} x^2(x^2-b)^2+4bx^4 = x^2(x^2+b)^2 &= (y^2-ax^2)^2 \\ x^2(x^2-b)^2 &= (y^2-ax^2)^2-4bx^4 \\ &= y^4-2ax^2y^2+(a^2-4b)x^4 \end{aligned}$$

and multiply by y^2/x^6:

$$\left(\frac{y(x^2-b)}{x^2}\right)^2 = \left(\frac{y}{x}\right)^6 + a'\left(\frac{y}{x}\right)^4 + b'\left(\frac{y}{x}\right)^2.$$

Let $\varphi : E \to E'$ be defined by

$$(x,y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2}\right)$$

We need to check that $\varphi(0)=0$. Just count orders of vanishing: remember that x has a double pole, and y has a triple pole. Rewrite the point in projective coordinates:

$$\left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2-b)}{x^2} : 1\right)$$

The orders of vanishing here are -2, -3, 0. Multiply through by the cube of a uniformizer, so the orders are $1,0,3$. That is, this point is the same as $(0:1:0)=0_{E'}$.

What is the degree of φ? We need the following lemma.

Lemma 7.4. (5.4) *Suppose $\varphi : E_1 \to E_2$ is an isogeny. Then there is a morphism $\xi : \mathbb{P}^1 \to \mathbb{P}^1$ making the following diagram commute:*

$$\begin{tikzcd} E_1 \arrow[r, "\varphi"] \arrow[d, "x_1"'] & E_2 \arrow[d, "x_2"] \\ \mathbb{P}^1 \arrow[r, "\xi"] & \mathbb{P}^1 \end{tikzcd}$$

where x_i is the function "take the x-coordinate".

If $\xi(t) = \frac{r(t)}{s(t)}$, for $r,s \in K[t]$ are coprime, then

$$\deg(\varphi) = \deg(\xi) = \max(\deg(r), \deg(s)).$$

Moral: to compute degree, you only need to pay attention to x-coordinates.

Proof. For $i=1,2$, $K(E_i)/K(x_i)$ is a degree 2 extension, with Galois group generated by the map $[-1]^*$ (if char $K \neq 2$, complete the square so it looks like $y^2=f(x)$). By Theorem 5.3, $\varphi \circ [-1] = [-1] \circ \varphi$.

If $f \in K(x_2)$ then

$$[-1]^*(\varphi^* f) = \varphi^*([-1]^* f).$$

f is fixed by pullback by $[-1]$, so $\varphi^* f \in K(x_1)$. Now invoke the tower law:

$$\begin{tikzcd}
 & K(E_1) \arrow[dl, dash, "2"'] \arrow[dd, dash, "\deg\varphi"] \\
K(x_1) \arrow[dd, dash, "\deg\xi"'] & \\
 & K(E_2) \arrow[dl, dash, "2"'] \\
K(x_2) &
\end{tikzcd}$$

There is an inclusion $K(x_2) \hookrightarrow K(x_1)$, where $x_2 \mapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)}$. We will show that the minimal polynomial of x_1 over $K(x_2)$ is

$$f(X) = r(X) - x_2 s(X).$$

It's easy to see that x_1 is a root of f. We need to check it's irreducible. I claim it is irreducible in $K[X, x_2]$: as a polynomial in x_2 it has degree 1; so if it factors, then one factor contains only X. This would imply that r, s have a common factor. Then, by Gauss's lemma, it's irreducible in $K(x_2)[X]$. ○

Now apply this to our example. x gets sent to something $\left(\frac{y}{x}\right)^2$ in terms of both x and y, but recall that (x, y) was a point in E, so $y^2 = x(x^2 + ax + b)$. So

$$\xi(x) = \left(\frac{y}{x}\right)^2 = \frac{x^2 + ax + b}{x}.$$

If $b = 0$, then this would have been singular. So the numerator and denominator are indeed coprime. Then $\deg(\varphi) = \max(\deg x^2 + ax + b, \deg x) = 2$.

Example 7.5. (5.5) Assume $\mathrm{char}(K) \neq 2, 3$, so we can assume an elliptic curve E can be put into Weierstrass form

$$E : y^2 = f(x) = x^3 + ax + b.$$

The $[2]$ map $E \to E$ is given by

$$(x, y) \mapsto \left(\text{slope}^2 - 2x, \cdots\right) = \left(\left(\frac{3x^2 + a}{2y}\right)^2, \cdots\right).$$

In the notation of the lemma, $\xi(x) = \left(\frac{3x^2+a}{2y}\right)^2$. We need to write it as a rational function only in x:

$$\begin{aligned}
\xi(x) &= \frac{(3x^2 + a)^2 - 8x(x^3 + ax + b)}{4(x^3 + ax + b)} \\
&= \frac{x^4 + \cdots}{4(x^3 + ax + b)}
\end{aligned}$$

The maximum degree is 4, but we have to check that these are coprime. Suppose there is some $\theta \in \overline{K}$ that is a root of both numerator and denominator. Since it is a root of the denominator, it is a root of f. Since it is a root of the numerator, it is also a root of f'. This only happens if f has a double root, and that can't happen here because f is nonsingular.

Recall, $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$. Say that 0 has degree 0 by convention.

THEOREM 7.6. *(5.6) The degree map*

$$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form, i.e.

(1) $\deg(n\varphi) = n^2 \cdot \deg \varphi$ *for all* $n \in \mathbb{Z}$*;*
(2) $(\varphi, \psi) \mapsto \deg(\varphi + \psi) - \deg(\varphi) - \deg \psi$ *is* $\mathbb{Z}$*-bilinear;*
(3) *(positive definite)* $\deg \varphi \geq 0$ *with equality iff* $\varphi = 0$*.*

Proof. (3) Trivial: the degree of the morphism is defined as a degree of a field extension; so unless $\varphi = 0$, $\deg \varphi \geq 1$.

T.B.C. ○

LECTURE 8: FEBRUARY 4

Examples class: 2:00 on Friday Feb 8, MR9.

REMARK 8.1. If $\varphi \in \mathrm{Hom}(E_1, E_2)$ then

- $\deg(-\varphi) = \deg([-1] \circ \varphi) = \deg(\varphi)$
- $\deg(2\varphi) = \deg([n] \circ \varphi)^4 \deg \varphi$

LEMMA 8.2 (Parallelogram law). *(5.7) Let* $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$*, then*

$$\deg(\varphi + \psi) + \deg(\varphi - \psi) = 2\deg(\varphi) + 2\deg(\psi).$$

This is a property of all quadratic forms, but we will use it to deduce that deg is a quadratic form.

Proof. We may assume $\varphi, \psi, \varphi + \psi, \varphi - \psi \neq 0$ (check each case, using the remark above and common sense). Assume for simplicity that $\mathrm{char}(K) \neq 2, 3$, so we can write E_2 as

$$E_2 : y^2 = x^3 + ax + b.$$

(The lemma also holds in characteristic 2 and 3.) Write $\varphi : (x, y) \mapsto (\xi_1(x, y), \eta(x, y))$; remember from last lecture that ξ_1 only depends on x. Also write

$$\begin{aligned} \psi : (x, y) &\mapsto (\xi_2(x, y), \eta_2(x, y)) \\ \varphi + \psi : (x, y) &\mapsto (\xi_3(x, y), \eta_3(x, y)) \\ \varphi - \psi : (x, y) &\mapsto (\xi_4(x, y), \eta_4(x, y)) \end{aligned}$$

By the group law on E_2:

$$\xi_3 = \left(\frac{\eta_1 - \eta_2}{\xi_1 - \xi_2}\right)^2 - \xi_1 - \xi_2$$
$$\xi_4 = \left(\frac{\eta_1 + \eta_2}{\xi_1 - \xi_2}\right)^2 - \xi_1 - \xi_2$$

We have $\eta_i^2 = \xi_i^3 + a\xi_i + b$. You could show that

$$\begin{aligned}&(1 : \xi_3 + \xi_4 : \xi_3\xi_4)\\ &\quad= \left((\xi_1 - \xi_2)^2 : 2(\xi_1\xi_2 + a)(\xi_1 + \xi_2) + 4b : \xi_1^2\xi_2^2 - 2a\xi_1\xi_2 - 4b(\xi_1 + \xi_2) + a^2\right)\end{aligned}$$

Put $\xi_i(x) = \frac{r_i(x)}{s_i(x)}$ where $r_i, s_i \in K[x]$ are coprime, and clear denominators:

$$(s_3s_4 : r_3r_4 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : W_1 : W_2)$$
$$W_1 = 2(r_1r_2 + as_1s_2)(r_1s_2 + r_2s_1) + 4bs_1^2s_2^2$$

You can calculate W_2. But you can show that W_0, W_1, W_2 each have degree 2 in r_1 and s_1, and degree 2 in r_2 and s_2.

$$\begin{aligned}\deg(\xi_3) + \deg(\xi_4) &= \max(\deg(r_3), \deg(s_3)) + \max(\deg(r_4), \deg(s_4))\\ &= \max(\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4))\end{aligned}$$

(You have to check each case $r_1 > s_1, r_2 > s_2$, etc.) Claim that s_3s_4, $r_3s_4 + r_4s_3, r_3r_4$ are coprime. We're not going to check that W_0, W_1, W_2 are coprime. But we can say

$$\begin{aligned}\deg(\xi_3) + \deg(\xi_4) &\le \max(\deg(W_0), \deg(W_1), \deg(W_2))\\ &\le 2\max(\deg(r_1), \deg(s_2)) + 2\max(\deg(r_2), \deg(s_2))\end{aligned}$$

So

$$\deg(\varphi + \psi) + \deg(\varphi - \psi) \le 2\deg(\varphi) + 2\deg(\psi)$$

Replacing φ and ψ by $\varphi + \psi$ and $\varphi - \psi$, we get the reverse of the inequality above:

$$\deg(2\varphi) + \deg(2\psi) \le 2\deg(\varphi + \psi) + 2\deg(\varphi - \psi)$$
$$4\deg(\varphi) + 4\deg(\psi) \le 2 \cdot (\deg(\varphi + \psi) + \deg(\varphi - \psi))$$
$$2\deg(\varphi) + 2\deg(\psi) \le \deg(\varphi + \psi) + \deg(\varphi - \psi)$$

○

Lemma 8.3. (5.8) *For all $n \in \mathbb{Z}$,*

$$\deg[n] = n^2.$$

Proof. Induction on n. The base cases $n = 0, 1$ are already known.

Assume we know the lemma in degrees $\le n$. Put $\varphi = [n]$ and $\psi = [1]$ in the previous lemma to get

$$\begin{aligned}\deg([n + 1]) + \deg([n - 1]) &= 2\deg(\varphi) + 2\\ \deg[n + 1] &= 2n^2 + 2 - (n - 2)^2 = (n + 1)^2\end{aligned}$$

This proves the lemma for $n \geq 0$. If n is negative, use the fact that $[n] = [-1][-n]$; but $[-1]$ is an isomorphism (so has degree 1), so $\deg[n] = \deg[-n] = n^2$. ○

Proof of Theorem 5.6. (1) $\deg(n\varphi) = \deg[n] \deg \varphi$, and we just checked that $\deg[n] = n^2$, so this is $n^2 \deg \varphi$ as desired.

(2) Let $\langle \varphi, \psi \rangle = \deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)$. This is symmetric in φ and ψ, so we just need to show linearity in the first argument; that is, we need to show:

$$\langle \varphi_1 + \varphi_2, \varphi_3 \rangle = \langle \varphi_1, \varphi_3 \rangle + \langle \varphi_2, \varphi_3 \rangle$$

In other words, we need to show:

$$\begin{aligned}\deg(\varphi_1 + \varphi_2 + \varphi_3) + \deg(\varphi_1) + \deg(\varphi_2) + \deg(\varphi_3) \\ = \deg(\varphi_1 + \varphi_2) + \deg(\varphi_2 + \varphi_3) + \deg(\varphi_1 + \varphi_3)\end{aligned}$$

This follows from Lemma 5.7 (Exercise). ○

Chapter 6: The invariant differential

Let C be a smooth projective curve over an algebraically closed field K.

Definition 8.4. The space of *Kähler differentials* Ω_C on C is the $K(C)$-vector space generated by symbols df for $f \in K(C)$, subject to the relations

(1) $d(f + g) = df + dg$
(2) (Product rule) $d(fg) = f \cdot dg + g \cdot df$
(3) $da = 0$ for all constants $a \in K$

Fact 8.5. *Since C is a curve, Ω_C is a one-dimensional $K(C)$-vector space.*

Let $\omega \in \Omega_C$ be a nonzero differential, $P \in C$ be a point, and $t \in K(C)$ a uniformizer at P (rational function having a simple pole at P). Anything nonzero in a 1-dimensional vector space forms a basis. So we can write $\omega = f \cdot dt$ for some $f \in K(C)$, and $\mathrm{ord}_P(\omega) = \mathrm{ord}_p(f)$.

Fact 8.6.

(1) *This is independent of the choice of t.*
(2) $\mathrm{ord}_P(\omega) = 0$ *for all but finitely many $P \in C$.*

Definition 8.7.

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P$$

By the above fact, this is a formal sum that consists of finitely many terms.

Definition 8.8. A *regular differential* ω is one that doesn't have any poles; that is, $\mathrm{div}(\omega) \geq 0$. The space of regular differentials is denoted

$$g(C) = \dim_K \{\omega \in \Omega_C \, : \, \mathrm{div}(\omega) \geq 0\}$$

It turns out that this is a finite-dimensional vector space, and its dimension is called the *genus.*

Fact 8.9.

(1) *(Consequence of Riemann-Roch) If ω is a regular differential, then* $\deg(\mathrm{div}(\omega)) = 2g(C) - 2$

(2) *Suppose $f \in K(C)^*$ and $\mathrm{ord}_P(f) = n \neq 0$. If $\mathrm{char}(K) \nmid n$, then $\mathrm{ord}_P(df) = n - 1$. (Think about f as a power series in t with leading term t^n, and use the standard rules of calculus.)*

Lemma 8.10. *(6.1) Assume* $\mathrm{char}(K) \neq 2$.

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

Then $\omega = \frac{dx}{y}$ is a differential on E with no zeros or poles. In particular, by Fact 8.9(1) we have $g(E) = 1$, and ω is a basis for the 1-dimensional K-vector space of regular differentials on E.

Proof. Let $T_i = (e_i, 0)$. $E[2] = \{0, T_1, T_2, T_3\}$. $\mathrm{div}(y) = (T_1) + (T_2) + (T_3) - 3(0_E)$ (we checked earlier that y has a triple pole at infinity).

If $P = (x_P, y_P) \in E \backslash E[2]$ then $\mathrm{ord}_P(x - x_P) = 1$ and by Fact 8.9, $\mathrm{ord}_p(dx) = 0$. But if P is a 2-torsion point (has a vertical tangent), then $\mathrm{ord}_P(x - e_i) = 2$, and $\mathrm{ord}_p(dx) = 1$. If $P = 0_E$ then $\mathrm{ord}_p(x) = -2$ (we've done this earlier), and $\mathrm{ord}_p(dx) = -3$. So

$$\mathrm{div}(dx) = (T_1) + (T_2) + (T_3) - 3(0_E)$$

and $\mathrm{div}(dx) = \mathrm{div}(y)$, so $\mathrm{div}\,\frac{dx}{y} = 0$. ○

Lecture 9: February 6

Definition 9.1. If $\varphi : C_1 \to C_2$ is a non-constant morphism, then define the map φ^* by:

$$\varphi^* : \Omega_{C_2} \to \Omega_{C_1} \text{ where } f\ dg \mapsto (\varphi^* f) d(\varphi^* g).$$

Lemma 9.2. *(6.2) Let $P \in E$, and let ω be a nonzero regular differential. Define $\tau_P : E \to E$ by $\tau_P : Q \mapsto P \oplus Q$. Then $\tau_P^* \omega = \omega$. We call ω the* invariant differential.

Proof. $\tau_p^*\omega$ is a regular differential on E. So $\tau_p^*\omega = \lambda_p \omega$ for some $\lambda_p \in K^*$ (this is nonzero because we're pulling back by a nonzero differential). The map $E \to \mathbb{P}^1, P \mapsto \lambda_P$ is a morphism of algebraic curves, but not surjective (misses 0 and ∞). But a nonconstant morphism between smooth projective curves is surjective. Therefore, it is constant, so there is some $\lambda \in K^*$ such that $\tau_p^*\omega = \lambda\omega$ for all $p \in E$. Taking $P = 0_E$ shows that $\lambda = 1$. ○

Remark 9.3. In the case $K = \mathbb{C}$, we have an isomorphism $\mathbb{C}/\Lambda \overset{\cong}{\to} E$ given by $z \mapsto (\wp(z), \wp'(z))$. Then the invariant differential is: $\frac{dx}{y} = \frac{\wp'(z)dz}{\wp'(z)} = dz$.

Fact 9.4. *$\Omega_{E\times E}$ is a 2-dimensional vector space over $K(E \times E)$ with basis $pr_1^*\omega$, $pr_2^*\omega$.*

Lemma 9.5. *(6.3) Let $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$, and let ω be the invariant differential on E_2. Then $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.*

Proof. Let $E = E_2$. We have several maps $E \times E \to E$:

$$\begin{aligned} \mu &: (P,Q) \mapsto P \oplus Q \\ pr_1 &: (P,Q) \mapsto P \\ pr_2 &: (P,Q) \mapsto Q \end{aligned}$$

By Fact 9.4

$$\mu^*\omega = f\ pr_1^*\omega + g\ pr_2^*\omega \tag{9.1}$$

for some $f, g \in K(E \times E)$. Let $Q \in E$. Let $i_Q : E \to E \times E$ be the map $P \mapsto (P,Q)$. Apply i_Q^* to (9.4) to get

$$(\mu \circ i_Q)^*\omega = i_Q^* f (pr_1 \circ i_Q)^*\omega + i_Q^* g \underbrace{(pr_2 \circ i_Q)^*}_{\substack{\text{constant map} \\ \text{on } Q}} \omega$$

$$\tau_Q^*\omega = i_Q^* f \omega$$

By Lemma 6.2, $i_Q^* f = 1$ for all $Q \in E$.

So $f(P,Q) = 1$ for all $P, Q \in E$. Similarly, $g(P,Q) = 1$ for all P, Q, and so

$$\mu^*\omega = pr_1^*\omega + pr_2^*\omega$$

We pull back by

$$E_1 \to E \times E \text{ where } P \mapsto (\varphi(P), \psi(P))$$

to get $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$. ○

Lemma 9.6. *(6.4) Let $\varphi : C_1 \to C_2$ be a nonconstant morphism. Then φ is separable iff $\varphi^* : \Omega_{C_2} \to \Omega_{C_1}$ is nonzero.*

Proof. Omitted. ○

Example 9.7. Let $\mathbb{G}_m = \mathbb{A}^1 \backslash \{0\}$ be the multiplicative group. Let $\varphi : \mathbb{G}_m \to \mathbb{G}_m$ be the map $x \mapsto x^n$ for some $n \in \mathbb{Z}$.

$$\varphi^*(dx) = d(x^n) = nx^{n-1}dx$$

As long as $n \nmid \operatorname{char} K$, this is nonzero, and hence φ is separable.

In general, if φ is a separable morphism, then $\#\varphi^{-1}(Q) = \deg(\varphi)$ for all but finitely many points Q. But in this case, φ is a group homomorphism, so every fiber has the same number of elements (size of the kernel). So $\#\ker(\varphi) = \deg(\varphi) = n$.

Theorem 9.8. *(6.5) If $\operatorname{char}(K) \nmid n$ then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.*

Proof. Lemma 6.3 plus an easy induction yields

$$[n]^*\omega = n\omega.$$

We assumed that $\operatorname{char}(K) \nmid n$, and so $[n]$ is separable. So $\#[n]^{-1}Q = \deg[n]$ for all but finitely many $Q \in E$. But $[n]$ is a group homomorphism, so $\#[n]^{-1}Q = \#E[n]$ for all Q. Putting these facts together, $\#E[n] = \deg[n]$. When we checked that deg was a quadratic form, we showed that $\deg[n] = n^2$.

By the structure theorem for finite abelian groups, $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z}$ with $d_1 \mid d_2 \mid \cdots \mid d_t \mid n$. If p is a prime dividing d, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$, but $\#E[p] = p^2$ so $t = 2$, and $d_1 = d_2 = n$. Therefore, $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. ○

Remark 9.9. If $\text{char}(K) = p$ then either $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all r (the *ordinary case*) or $E[p^r] = 0$ for all r (the *supersingular case*).

Theorem 9.10 (Hasse). *(6.6) Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then*

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

Proof. Recall the Galois group $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ of a degree-r extension of $\mathbb{F}_q$ is a cyclic group generated by the Frobenius map $x \mapsto x^q$.

Let E have a Weierstrass equation with coefficients $a_1, \cdots, a_6 \in \mathbb{F}_q$ (so $a_i^q = a_i$ for all i). So x^q and y^q give another solution to the curve. Define the Frobenius endomorphism φ (i.e. an isogeny from E to itself)

$$\varphi : E \to E \text{ where } (x,y) \mapsto (x^q, y^q).$$

This has degree q. Then $E(\mathbb{F}_q) = \{P \in E : \varphi(P) = P\} = \ker(1 - \varphi)$.

Proving Hasse's theorem means working out the size of the kernel.

$$\varphi^*\left(\frac{dx}{y}\right) = \frac{d(x^q)}{y^q} = \frac{qx^{q-1}dx}{y^q}$$

This is zero because we're in characteristic q. By Lemma 6.3,

$$(1-\varphi)^* \tfrac{dx}{y} = \tfrac{dx}{y} - \varphi \tfrac{dx}{y}$$

The second term is zero, and the first term is nonzero. So $1 - \varphi$ is separable. So

$$\#E(\mathbb{F}_q) = \# \ker(1-\varphi) = \deg(1-\varphi).$$

Lecture 10: February 8

Lemma 10.1. *(6.7) Let A be an abelian group, and let $q : A \to \mathbb{Z}$ be a positive definite quadratic form. If $\varphi, \psi \in A$, then*

$$\langle \varphi, \psi \rangle := |q(\varphi + \psi) - q(\varphi) - q(\psi)| \leq 2\sqrt{q(\varphi)q(\psi)}.$$

(Note that $\langle -, - \rangle$ is bilinear by definition.)

(This is basically Cauchy-Schwartz.)

Proof. Assume $\varphi \neq 0$ (otherwise clear). Let $m, n \in \mathbb{Z}$.

$$0 \leq q(m\varphi + n\psi) = \frac{1}{2}\langle m\varphi + n\psi, m\varphi + n\psi \rangle$$

$$\begin{aligned} &= q(\varphi)m^2 + \langle\varphi,\psi\rangle\, mn + q(\psi)n^2 \\ &= q(\varphi)\left(m + \frac{\langle\varphi,\psi\rangle\, n}{2q(\varphi)}\right)^2 + n^2\left(q(\psi) - \frac{\langle\varphi,\psi\rangle^2}{4q(\varphi)}\right) \end{aligned}$$

Take $m = -\langle\varphi,\psi\rangle$ and $n = 2q(\varphi)$ to make the first term $= 0$:

$$0 \leq q(\psi) - \frac{\langle\varphi,\psi\rangle^2}{4q(\varphi)}$$

So $\langle\varphi,\psi\rangle^2 \leq 4q(\varphi)q(\psi)$ and

$$|\langle\varphi,\psi\rangle| \leq 2\sqrt{q(\varphi)q(\psi)}.$$

○

Proof of Theorem 6.6, con't. By Theorem 5.6, $\deg : \mathrm{End}(E) \to \mathbb{Z}$ is a positive definite quadratic form. Apply Lemma 6.7:

$$\left|\underbrace{\deg(1-\varphi)}_{\#E(\mathbb{F}_q)} - \underbrace{\deg(\varphi)}_{q} - \underbrace{\deg(1)}_{1}\right| \leq 2\sqrt{\deg(\varphi)}$$

○

Chapter 7: Formal groups

Let

$$E: \;\; Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

be an elliptic curve. We will work on the affine piece where $Y \neq 0$. Choose new coordinates $t = -\frac{X}{Y}$ and $w = -\frac{Z}{Y}$ (minus signs for consistency with Silverman's book):

$$E: \;\; w = \underbrace{t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3}_{f(t,w)}$$

We will find a power series for $f(t,w)$; that is, an expression

$$w(t) = t^3(1 + A_1t + A_2t^2 + \cdots) \in \mathbb{Z}[a_1, \cdots, a_6][[t]]$$

such that $w(t) = f(t, w(t))$. It turns out that

$$\begin{aligned} A_1 &= a_1 \\ A_2 &= a_1^2 + a_2 \\ A_3 &= a_1^3 + 2a_1a_2 + a_3 \end{aligned}$$

Definition 10.2. Let R be a ring, $I \subset R$ be an ideal. The I-adic topology on R is the topology where the basic open sets have the form $r + I^n$, for $r \in R$ and $n \geq 0$. *(s is close to r if $s \in r + I^N$ for large N; in other words, if the difference $r - s$ is in I^N.)*

Definition 10.3. R is complete w.r.t I if

(1) $\bigcap_{n\geq 0} I^n = \{0\}$, and
(2) every Cauchy sequence converges.

$(x_n)_n$ is a Cauchy sequence in this context if: for every s, there is some N such that $x_n - x_m \in I^s$ for $n, m \geq N$.

Remark 10.4. If $x \in I$, then $\frac{1}{1-x} = 1 + x + x^2 + \cdots$ and so $1 - x \in R^\times$.

Lemma 10.5 (Hensel's lemma). *(7.1) Let R be an integral domain that is complete with respect to the ideal I. Let $F \in R[X]$ and $s \geq 1$. Suppose we are given $a \in R$ such that*

$$F(a) \equiv 0 \pmod{I^s}$$
$$F'(a) \in R^\times.$$

Then there is a unique $b \in R$ such that

$$F(b) = 0$$
$$b \equiv a \pmod{I^s}.$$

Proof. Pick any $\alpha \in R$ such that $\alpha \equiv F'(a) \pmod I$. Replacing $F(X)$ by $\frac{F(X+a)}{\alpha}$, we may assume $a = 0$, $\alpha = 1$. We have $F(0) \equiv 0 \pmod{I^s}$ and $F'(0) \equiv 1 \pmod I$. Define a sequence recursively:

$$x_0 = 0$$
$$x_{n+1} = x_n - F(x_n) \tag{10.1}$$

By an easy induction,

$$x_n \equiv 0 \pmod{I^s} \tag{10.2}$$

for all $n \geq 0$. We need to show that this sequence is Cauchy.

Claim 10.6. $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ *for all $n \geq 0$.*

Proof of claim. By induction on n. If $n = 0$ then we're done.

Suppose $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$.

$$F(X) - F(Y) = (X - Y)(F'(0) + XG(X,Y) + YH(X,Y)) \tag{10.3}$$

for some $G, H \in F[X,Y]$. If $X = x_n$ and $Y = x_{n-1}$, the second bracket is just $1 \pmod I$:

$$F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \pmod{I^{n+s}}$$
$$x_n - F(x_n) \equiv x_{n-1} - F(x_{n-1}) \pmod{I^{n+s}}$$
$$x_{n+q} \equiv x_n \pmod{I^{n+s}}$$

○

So (x_n) is Cauchy. Since R is complete, $x_n \to b$ as $n \to \infty$ for some $b \in R$. Taking limits in (10.1) gives $b = b - F(b)$, and so $F(b) = 0$. Taking limits in (10.2) gives $b \equiv 0 \pmod{I^s}$.

Uniqueness is proved by plugging two supposed solutions into (10.3); I claim that the right bracket is nonzero, which forces $X - Y = 0$. ○

We apply Lemma 7.1 with $R = \mathbb{Z}[a_1, \cdots, a_6][[t]]$ and $I = (t)$. We're looking for a solution to $F(X) = X - f(t,X)$. Set $s = 3$, and use the approximate root $a = 0$. Then

$F(0) = -t^3 \equiv 0 \pmod{t^3}$ and $F'(0) = 1 - a_1 t - a_2 t^3 \in R^\times$. There exists a unique $w \in \mathbb{Z}[a_1, \cdots, a_6][[t]]$ such that $w(t) = f(t, w(t))$ and $w \equiv 0 \pmod{t^3}$.

Remark 10.7. Taking $\alpha = 1$ in the proof, we find $w = \lim_{n\to\infty} w_n$ with $w_0 = 0, w_{n+1} = f(t, w_n)$.

Lemma 10.8. (7.2) *Let R be an integral domain that is complete with respect to the ideal I. Let $a_1, \cdots, a_6 \in R$, and $K = \operatorname{Frac} R$. Then*

$$\widehat{E}(I) = \{(t, w(t)) \in E(K) \,:\, t \in I\}$$

is a subgroup of $E(K)$.

Proof. Taking $t = 0$ gives $0_E \in \widehat{E}(I)$. Let $P_1 = (t_1, w_1)$ and $P_2 = (t_2, w_2)$ be points in $\widehat{E}(I)$. It suffices to show that $-P_1 - P_2 \in \widehat{E}(I)$. Let $P_3 = (t_3, w_3) = -P_1 - P_2$. Let $w = \lambda t + \nu$ be the line through P_1, P_2, P_3. Suppose $t_1, t_2, w_1, w_2 \in I$. We need to show that $t_3, w_3 \in I$. This suffices by uniqueness in Hensel's lemma (there is a unique $w(t) \in I$ that makes this work).

Write

$$w(t) = t^3(1 + A_1 t + A_2 t^2 + \cdots)$$

λ is the slope $\frac{w_2 - w_1}{t_2 - t_1} = \sum_{n=3}^\infty A_{n-3} \frac{t_2^n - t_1^n}{t_2 - t_1}$. Also $\nu = w_1 - \lambda t_1 \in I$ because w_1 and $t_1 \in I$. Finish later.

Lecture 11: February 11

Let R be an integral domain, complete with respect to the ideal I. We have an elliptic curve

$$E : w = f(t, w) = t^3 + a_1 t w + \cdots + a_6 w^3$$

containing points $P_1 = (t_1, w_1)$, $P_2 = (t_2, w_2)$, $P_3 = (t_3, w_3)$ all on the line $w = \lambda t + \nu$. Suppose $t_1, t_2, w_1, w_2 \in I$. We checked that $\lambda, \nu \in I$. Substituting $w = \lambda t + \nu$ into $w = f(t, w)$, we have

$$\lambda t + \nu = t^3 + a_1 t(\lambda t + \nu) + a_2 t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4 t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3$$

$$\begin{aligned} A &:= \text{Coefficient of } t^3 = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3 \in R^\times \\ B &:= \text{Coefficient of } t^2 = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu \in I \end{aligned}$$

$t_3 = -\frac{B}{A} - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. We also could have calculated w_3 by plugging t_3 into the power series; by the uniqueness in Hensel's lemma, this is indeed the same point. That is, $w_3 = w(t_3)$. Thus

$$\widehat{E}(I) = \{(t, w(t)) \in E(K) \,:\, t \in I\}$$

is a subgroup of $E(K)$.

By taking R to be a power series ring in Lemma 7.2,

(1) there is some power series $\iota(t) \in \mathbb{Z}[a_1, \cdots, a_6][[t]]$ such that $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$

(2) there is some $F(t_1,t_2) \in \mathbb{Z}[a_1,\cdots,a_6][[t_1,t_2]]$ such that
$$(t_1,w(t_1)) + (t_2,w(t_2)) = (F(t_1,t_2), w(F(t_1,t_2))).$$

In fact,
$$\iota(X) = -X - a_1X^2 - a_2^2X^3 - (a_1^3 + a_3)X^4 + \cdots$$
and
$$F(X,Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \cdots$$
It follows from the group axioms that

(1) $F(Y,X) = F(X,Y)$
(2) $F(X,0) = X$ and $F(0,Y) = Y$
(3) $F(F(X,Y),Z) = F(X,F(Y,Z))$
(4) $F(X,\iota(X)) = 0$

Definition 11.1. Let R be any ring. A *formal group* over R is a power series $F \in R[[X,Y]]$ satisfying (1) – (3) above.

Motto: formal groups are "a group law without elements".

Exercise 11.2. If F satisfies (1) – (3), then show that there is some power series $\iota(X) = -X + \cdots \in R[[X]]$ such that $F(X,\iota(X)) = 0$.

This is a *1-parameter commutative group*; but we will just call it a formal group because we don't care about any other kinds of formal groups here.

Example 11.3.

(1) $F(X,Y) = X + Y$ is a formal group, which we call $\widehat{\mathbb{G}_a}$.
(2) $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ is the formal group $\widehat{\mathbb{G}_m}$
(3) The formal group $F(X,Y)$ arising from the elliptic curve E is called $\widehat{E}$.

Definition 11.4. Let F,G be formal groups over R.

(1) A morphism $f : F \to G$ is a power series $f \in R[[T]]$ with zero constant term such that $f(F(X,Y)) = G(f(X),f(Y))$.
(2) $F \cong G$ if there are morphisms $f : F \to G$ and $g : G \to F$ satisfying $f \circ g(T) = T$ and $g \circ f(T) = T$.

Theorem 11.5. *(7.3) If $\operatorname{char}(R) = 0$ then every formal group F over R is isomorphic to the additive formal group $\widehat{\mathbb{G}}_a$ over $R \otimes \mathbb{Q}$.*

More precisely,

(1) *there exists a unique power series*
$$\log T = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots$$
with $a_i \in R$ satisfying
$$\log F(X,Y) = \log X + \log Y \tag{11.1}$$
and

(2) *there is a unique power series*

$$\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b^3}{3!}T^3 + \cdots$$

with $b_i \in R$ satisfying

$$\log(\exp T) = T \textit{ and } \exp(\log T) = T.$$

Proof. (1) *Uniqueness of* log*:* For convenience, denote $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$. Suppose we have a series log as above. Let

$$p(T) = \frac{\partial}{\partial T}\log T = 1 + a_2T + a_3T^2 + \cdots .$$

Differentiating (11.1) w.r.t X we get

$$p(F(X,Y))F_1(X,Y) = p(X) + 0$$

Putting $X = 0$,

$$p(Y)F_1(0,Y) = 1$$

so $p(Y) = F_1(0,Y)^{-1}$. So p is uniquely determined by F, and so is log, because log is defined in terms of the coefficients of p.

Existence of log*:* Let $p(T) = F_1(0,T)^{-1} = 1 + a_2T + a_3T^2 + \cdots$ for some $a_i \in R$. Define log by formally integrating:

$$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots$$

Start with the associativity law:

$$F(F(X,Y),Z) = F(X,F(Y,Z))$$

and take $\frac{d}{dX}$:

$$F_1(X,Y)F_1(F(X,Y),Z) = F_1(X,F(Y,Z))$$

Set $X = 0$:

$$\begin{aligned}F_1(0,Y)F_1(Y,Z) &= F_1(0,F(Y,Z))\\ p(Y)^{-1}F_1(Y,Z) &= p(F(Y,Z))^{-1}\\ P(F(Y,Z))F_1(Y,Z) &= p(Y)\end{aligned}$$

Integrate with respect to Y:

$$\log F(Y,Z) = \log Y + \underbrace{h(Z)}_{\substack{\text{constant from}\\ \text{integrating}}}$$

for some power series h.

But there's symmetry between Y and Z, which forces $h(Z) = \log Z$.

For (2), we use

Lemma 11.6. *(7.4) Let $f(T) = aT + \cdots \in R[[T]]$ with $a \in R^{\times}$. Then there is a unique power series*

$$g(T) = a^{-1}T + \cdots \in R[[T]]$$

such that $f \circ g(T) = T$ and $g \circ f(T) = T$.

Proving the lemma proves the original statement of the theorem. To prove the more specific formulation that says how bad the denominators get in exp, just pick through this proof (exercise).

Proof of Lemma. We construct polynomials $g_n(T) \in R[T]$ such that $f(g_n(T)) = T \pmod{T^{n+1}}$ and $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$. Then let $g(T) = \lim_{n\to\infty} g_n(T)$; this makes sense because R is complete and the second condition on (g_n) ensures that they form a Cauchy sequence (pointwise).

To start the induction, let $g_1(T) = a^{-1}T$.

Now suppose $n \geq 2$ and g_{n-1} exists with the desired properties. Then

$$f(g_{n-1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$$

for some $b \in R$. We put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for some $\lambda \in R$ to be chosen. Then

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}(T)) + \lambda a T^n \pmod{T^{n+1}} \\ &\equiv T + (b + \lambda a)T^n \pmod{T^{n+1}} \end{aligned}$$

so we can choose $\lambda = -\frac{b}{a}$ (we are using the fact that a was a unit). We get

$$g(T) = a^{-1}T + \cdots \in R[[T]]$$

such that

$$f \circ g(T) = T. \tag{11.2}$$

The same construction applied to g gives $h(T) = aT + \cdots \in R[[T]]$ such that

$$g \circ h(T) = T \tag{11.3}$$

$$f(T) \overset{(11.3)}{=} f(g(h(T))) \overset{(11.2)}{=} h(T)$$

○

Theorem 7.3 follows, except for showing the coefficients of $\exp(T)$ which are in $R \otimes \mathbb{Q}$ are of the form $\frac{b_n}{n!}$ with $b_n \in R$ (optional exercise, or see Silverman's book).

Remark 11.7. If $F(X,Y) = (1+X)(1+Y) - 1$, then exp and log are the usual series for $\log(1+T)$ and $\exp(T) - 1$. (The shift of 1 occurs because formal groups require the identity to be called "0".)

Lecture 12: February 13

Examples class: next Friday, 2:30

Construction 12.1. Let $\mathcal{F}$ be a formal group (e.g. $\widehat{\mathbb{G}}_a$, $\widehat{\mathbb{G}}_m$, $\widehat{E}$) given by $F \in R[[X,Y]]$. We want to construct an actual group from this. Suppose R is complete with respect to some ideal I (for example, $R = \mathbb{Z}_p$, $I = p^r\mathbb{Z}_p$ for some $r \geq 1$). If $x, y \in I$ then define a group law

$$x \oplus_{\mathcal{F}} y := F(x,y).$$

These power series converge with respect to the I-adic topology because R is complete. Then $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an abelian group.

For example, $\widehat{\mathbb{G}}_a(I) = (I, +)$ and $\widehat{\mathbb{G}}_m(I) = (1+I, \times)$. In Lemma 7.2 we showed $\widehat{E}(I) \subset E(K)$.

Check that morphisms of formal groups induce group homomorphisms.

Corollary 12.2. *(7.5) Let $\mathcal{F}$ be a formal group over R. Let $n \in \mathbb{Z}$. Suppose $n \in R^*$. Then*

1. *$[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.*
2. *If R is complete w.r.t. an ideal I then $\mathcal{F}(I) \xrightarrow{-\times n} \mathcal{F}(I)$ is an isomorphism.*

In particular, $\mathcal{F}(I)$ has no n-torsion.

Proof. $[1](T)$ is the power series T, and $[n+1](T) = F([n]T, T)$. Induction shows that $[n]T = nT + \cdots \in R[[T]]$. If n is a unit in R, then Lemma 7.4 applies, and shows that $[n]$ has an inverse, which in turn gives an isomorphism of groups. ○

Chapter 8: Elliptic curves over local fields

Let K be a field of characteristic zero. Assume that K is complete w.r.t. some discrete valuation

$$\mathrm{ord}_K : K^* \to \mathbb{Z}.$$

Recall the following constructions from algebraic number theory:

$$\begin{aligned} \text{ring of integers:} \quad & \mathcal{O}_K = \{x \in K \,:\, \mathrm{ord}_K(x) \geq 0\} \cup \{0\} \\ \text{group of units:} \quad & \mathcal{O}_K^* = \{x \in K^* \,:\, \mathrm{ord}_K(x) = 0\} \\ \text{maximal ideal:} \quad & \pi\mathcal{O}_K \text{ where } \mathrm{ord}_K(\pi) = 1 \\ \text{residue field:} \quad & k = \mathcal{O}_K/\pi\mathcal{O}_K \end{aligned}$$

Assume that $\mathrm{char}(k) = p > 0$.

For example, $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$, $\pi\mathcal{O}_K = p\mathbb{Z}_p$, $k = \mathbb{F}_p$.

Remark 12.3. ord is a group homomorphism, and

$$\mathrm{ord}_K(x+y) \geq \min(\mathrm{ord}_K(x), \mathrm{ord}_K(y)).$$

Equality holds when $\operatorname{ord}_K(x) \neq \operatorname{ord}_K(y)$ *and possibly at other times as well.*

Definition 12.4. A Weierstrass equation

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

is *integral* if $a_i \in \mathcal{O}_K$ for all i. It is *minimal* if $\operatorname{ord}_K(\Delta)$ is minimal among all integral Weierstrass equations for E. If you complete the square to make this $y^2 = \mathit{cubic}$, Δ is, up to unit, the discriminant of the cubic.

Remark 12.5.

1. Putting $x = u^2x'$, $y = u^3y'$, we get $a_i = u^ia_i'$. So integral Weierstrass equations exist.
2. If $a_1, \cdots, a_6 \in \mathcal{O}_K$, then $\Delta \in \mathcal{O}_K$. So $\operatorname{ord}_K(\Delta) \in \mathbb{Z}_{\geq 0}$. So minimal Weierstrass equations exist.

Lemma 12.6. *(8.1) Fix an integral Weierstrass equation for E. Suppose $P = (x, y) \in E(K)$ is nonzero. Then one of the following holds:*

1. $x, y \in \mathcal{O}_K$
2. $\operatorname{ord}_K(x) = -2r$, $\operatorname{ord}_K(y) = -3r$ *for some* $r \geq 1$.

Proof. Let $s = \operatorname{ord}_K(x)$ and $t = \operatorname{ord}_K(y)$.

Case $s \geq 0$: If $t < 0$ we get $\operatorname{ord}_K(LHS) = 2t$, and $\operatorname{ord}_K(RHS) \geq 0$, a contradiction. So $t \geq 0$, i.e. $x, y \in \mathcal{O}_K$.

Case $s < 0$: $\operatorname{ord}_K(LHS) \geq \min(2t, s+t, t)$ and $\operatorname{ord}_K(RHS) = 3s$. There are three possible inequalities, and in each case, $t < s < 0$. Now we know that the $2t$ term wins; so $3s = 2t$ which implies $s = -2r, t = -3r$ for some $r \geq 1$. ○

In §7 we put $t = -\frac{x}{y}$ and $w = -\frac{1}{y}$. Let $I = \pi^r\mathcal{O}_K$ for some $r \geq 1$. Then

$$\begin{aligned} \widehat{E}(I) = \widehat{E}(\pi^r\mathcal{O}_K) &= \{(x,y) \in E(K) \,:\, -\tfrac{x}{y}, \tfrac{1}{y} \in \pi^r\mathcal{O}_K\} \\ &= \{(x,y) \in E(K) \,:\, \operatorname{ord} \tfrac{x}{y} \geq r, \operatorname{ord}_K(y) \leq -r\} \\ &\overset{8.1}{=} \{(x,y) \in E(K) \,:\, \operatorname{ord}_K(x) \leq -2r, \operatorname{ord}_K(y) \leq -3r\} \end{aligned}$$

By Lemma 7.2 this is a subgroup of $E(K)$, say $E_r(K)$. We have a series of inclusions

$$\cdots \subset E_2(K) \subset E_1(K) \subset E(K)$$

Proposition 12.7. *(8.2) Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. As defined above, π is the maximal ideal, and the residue field $k = \mathcal{O}_K/\pi\mathcal{O}_K$ has characteristic p. Let $e = \operatorname{ord}_K(p)$. If $r > \frac{e}{p-1}$ then*

$$\log : \mathcal{F}(\pi^r\mathcal{O}_K) \to \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K)$$

is an isomorphism with inverse

$$\exp : \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \to \mathcal{F}(\pi^r\mathcal{O}_K).$$

Proof. The only thing left to check is convergence. Let $x \in \pi^r\mathcal{O}_K$. We must show the series $\log(x)$ and $\exp(x)$ in Theorem 7.3 converge.

Recall: $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$ for $b_i \in \mathcal{O}_K$. Because of the ultrametric law, we just have to check that the terms tend to zero (i.e. tend towards infinite order).

$$\begin{aligned}\mathrm{ord}_K(n!) &= e \cdot \mathrm{ord}_p(n!)\\ &= e\sum_{r=1}^{m}\left[\frac{n}{p^r}\right] && \text{if } p^m \le n < p^{m+1}\\ &\le e\sum_{r=1}^{m}\frac{n}{p^r}\\ &= e\cdot\left(\frac{n}{p-1}\cdot(1-p^{-m})-1\right)\\ &\le \frac{e}{p-1}(n-1)\end{aligned}$$

(you would get $\frac{e}{p-1}$ if the sum went to ∞).

$$\begin{aligned}\mathrm{ord}_K\,\tfrac{b_nx^n}{n!} &\ge 0 + nr - \frac{e}{p-1}(n-1)\\ &= r + (n-1)\underbrace{\left(r - \tfrac{e}{p-1}\right)}_{\substack{>0 \text{ by}\\ \text{hypothesis}}}\end{aligned}$$

This is always $\ge r$ and tends to ∞ as $n \to \infty$. So $\exp(x)$ converges and belongs to $\pi^r\mathcal{O}_K$ (and likewise for log).

So for r sufficiently large,

$$\mathcal{F}(\pi^r\mathcal{O}_K) \cong \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \cong (\pi^r\mathcal{O}_K,+) \cong (\mathcal{O}_K,+).$$

○

Lecture 13: February 15

Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. There is a sequence

$$\cdots \subset \mathcal{F}(\pi^2\mathcal{O}_K) \subset \mathcal{F}(\pi\mathcal{O}_K).$$

We showed in Proposition 8.2 that $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K,+)$ for sufficiently large r.

Lemma 13.1. *(8.3) If $r \ge 1$ then*

$$\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k,+).$$

Proof. From the axioms of a formal group,

$$F(X,Y) = X + Y + XY(\cdots).$$

So if $x, y \in \mathcal{O}_K$,

$$F(\pi^r x, \pi^r y) \equiv \pi^r(x+y) \pmod{\pi^{r+1}}$$

Define a map $\mathcal{F}(\pi^r\mathcal{O}_K) \to (k,+)$ via $\pi^r x \mapsto x \pmod{\pi}$. We checked that this gives a group homomorphism. It is surjective, with kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$. ○

Corollary 13.2. *If $|k| < \infty$, then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

Notation 13.3. The reduction mod π map $\mathcal{O}_K \to \mathcal{O}_K/\pi\mathcal{O}_K = k$ sends $x \mapsto \widetilde{x}$.

Proposition 13.4. *(8.4) The reduction mod π of any two* minimal *Weierstrass equations for E defines isomorphic curves over k.*

Proof. Say the Weierstrass equations are related by $[u; r, s, t]$ for $u \in K^*$, $r, s, t \in K$. Let Δ_1, Δ_2 be the discriminants of the two Weierstrass equations. Then

$$\Delta_1 = u^{12}\Delta_2.$$

Since both equations are minimal, $\mathrm{ord}_K(\Delta_1) = \mathrm{ord}_K(\Delta_2)$. So $\mathrm{ord}_K(u) = 0$ (i.e. u is a unit in $\mathcal{O}_K$). Use the transformation formulae on the formula sheet for the a_i and b_i to give $r, s, t \in \mathcal{O}_K$. (As long as you don't worry about characteristic 2 or 3, you don't have to worry about r, s, t anyway, and this proof is even simpler.)

The Weierstrass equations obtained by reduction are now related by a transformation $[\widetilde{u}; \widetilde{r}, \widetilde{s}, \widetilde{t}]$. ○

Definition 13.5. The reduction $\widetilde{E}/k$ of E/K is the reduction of a minimal Weierstrass equation. E has *good reduction* if $\widetilde{E}$ is non-singular (i.e. $\widetilde{E}$ is an elliptic curve); otherwise call this a *bad reduction*.

Remark 13.6. For an integral Weierstrass equation,

$$\begin{aligned} \mathrm{ord}_K(\Delta) = 0 &\implies \text{minimal + good reduction} \\ 0 < \mathrm{ord}_K(\Delta) < 12 &\implies \text{minimal + bad reduction} \\ \mathrm{ord}_K(\Delta) \geq 12 &\implies \text{if minimal then bad reduction} \end{aligned}$$

There is a well-defined map $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$

$$(x : y : z) \mapsto (\widetilde{x} : \widetilde{y} : \widetilde{z})$$

To avoid ending up with $(0:0:0)$ on the right, you have to choose a representative of $(x : y : z)$ such that $\min(\mathrm{ord}_K(x), \mathrm{ord}_K(y), \mathrm{ord}_K(z)) = 0$ (i.e. at least something is a unit). We restrict to $E(K) \to \widetilde{E}(k)$, sending $p \mapsto \widetilde{p}$.

Lemma 8.1 says $\widehat{E}(\pi\mathcal{O}_K) = E_1(K) = \{P \in E(K) : \widetilde{P} = 0\}$. We want to say that the formal group is the kernel of reduction. This works if reduction is a group homomorphism, which is the case if $\widetilde{E}(k)$ is a group (i.e. it was a good reduction). If it was a bad reduction, we can get rid of the offending singular points: let

$$\widetilde{E}_{ns} = \begin{cases} \widetilde{E} & \text{if good reduction} \\ \widetilde{E} \backslash \{\mathit{singular\ pts.}\} & \text{if bad reduction} \end{cases}$$

The chord and tangent process still defines a group law on $\widetilde{E}_{ns}$. Any line meets a singular point with multiplicity at most 2. In the chord and tangent process, we start with two (smooth) points and try to find the third point of intersection. So there is no danger of running into the singular points this way.

Proposition 13.7. *If E has bad reduction, then*

$$\widetilde{E}_{ns} \cong \mathbb{G}_m \text{ } \mathit{or} \text{ } \mathbb{G}_a$$

(if it's $\mathbb{G}_a$, this can be taken over k, but in the multiplicative case, you might have to add some square roots).

For simplicity assume char $k \neq 2$. Consider an elliptic curve

$$\widetilde{E} : y^2 = f(x) \text{ where } \deg f = 3.$$

The singular points correspond to the repeated roots of f. If there's a double root, then there's a node; if it's a triple root, then there's a cusp.

Case 1: triple root. Assume the triple root is at zero, so the equation is $y^2 = x^3$. Define a map $\mathbb{G}_a \to \widetilde{E}_{ns}$ where $t \mapsto (t^{-2}, t^{-3})$ and $0 \mapsto 0_E$. Let P_1, P_2, P_3 lie on the line $ax + by = 1$. Put $P_i = (x_i, y_i)$.

$$x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$$

This is homogeneous; divide by y_i^3:

$t_i = \frac{x_i}{y_i}$ is a root of $X^3 - aX - b = 0$; so $t_1 + t_2 + t_3 = 0$.

Specialize as necessary to show that inverses work; then read off the fact that this is a group homomorphism.

Case 2: double root. Pick the homomorphism such that the singular points correspond to 0 and ∞ in $\mathbb{G}_m$. The calculation is messier.

Definition 13.8.

$$E_0(K) = \{P \in E(K) \, : \, \widetilde{P} \in \widetilde{E}_{ns}(k)\}$$

(i.e. points that reduce to a smooth point).

Proposition 13.9. *(8.5) $E_0(K) \subset E(K)$ is a subgroup, and reduction mod π gives a surjective group homomorphism $E_0(K) \to \widetilde{E}_{ns}(k)$.*

Proof. Group homomorphism: We need to check that E_0 is closed under the operation $\oplus$. Let $P_1, P_2 \in E_0(K)$. Let $P_3 \in E(K)$ be the point such that $P_1 \oplus P_2 \oplus P_3 = 0_E$: that is, such that P_1, P_2, and P_3 lie on a line $\ell : ax + by + cz = 0$. But then $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3$ lie on *the line $\widetilde{\ell} : \widetilde{a}x + \widetilde{b}y + \widetilde{c}z = 0$. Since ℓ is not degenerate, we could have picked a, b, c with $\min(\text{ord}_K(a), \text{ord}_K(b), \text{ord}_K(c)) = 0$; now $\widetilde{a}, \widetilde{b}, \widetilde{c}$ are not all zero, and $\widetilde{\ell}$ is not the zero line. Since we assumed that $\widetilde{P}_1$ and $\widetilde{P}_2$ were nonsingular, $\widetilde{P}_3$ also has to be nonsingular. Thus, $P_3 \in E_0(K)$.*

Surjective: Let $f(x, y) = y^2 + a_1xy + a_3y - x_3 - \cdots - a_6$ be the usual affine equation for E. Let $\widetilde{P} \in \widetilde{E}_{ns}(k) \backslash \{0\}$ have coordinates $(\widetilde{x}_0, \widetilde{y}_0)$ (for some $x_0, y_0 \in \mathcal{O}_K$). $\widetilde{P}$ is non-singular, so either $\frac{\partial f}{\partial x}(x_0, y_0) \neq 0$ in k or $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0$ in k. Suppose $\frac{\partial f}{\partial x} \not\equiv 0 \pmod{\pi}$. Put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$: $g(x_0) \equiv 0 \pmod{\pi}$ and $g'(x_0) \in \mathcal{O}_K^*$. By Hensel's lemma, there is some $b \in \mathcal{O}_K$ such that $b \equiv x_0 \pmod{\pi}$ and $g(b) = 0$. Then $P = (b, y_0) \in E(K)$ and its reduction mod π is $\widetilde{P}$. ○

Lecture 14: February 18

We had the group of smooth points $E_0(K) \subset E(K)$, which had a kernel we called $E_1(K)$, which is just $\widehat{E}(\pi\mathcal{O}_K)$. We checked that $E_0(K)/E_1(K) \overset{\cong}{\to} \widetilde{E}_{ns}(k)$. We can continue the sequence

$$E_r(K) \subset \cdots \subset E_2(K) \subset E_1(K) \subset E_0(K) \subset E(K)$$

where $E_r(K) = \widehat{E}(\pi^r\mathcal{O}_K)$, and for r sufficiently large, $E_r(K) \cong (\mathcal{O}_K, +)$, and the quotients at each stage are $(k, +)$. We assumed that the residue field k was finite, so we have produced some subgroups of finite index. But, we haven't yet proved that $E_0(K) \subset E(K)$ has finite index.

Lemma 14.1. (8.6)*If $|k| < \infty$, then $\mathbb{P}^n(K)$ is compact (w.r.t the π-adic topology).*

Proof. $\mathcal{O}_K = \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ is profinite (i.e. it's an inverse limit of finite groups). It's a well-known result that profinite groups are compact. $\mathbb{P}^n(K)$ is a union of (finitely many) compact sets of the form

$$V_i = \{(a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) \, : \, a_j \in \mathcal{O}_K\}.$$

○

Lemma 14.2. (8.7) *$E_0(K) \subset E(K)$ has finite index.*

Proof. $E(K) \subset \mathbb{P}^2(K)$ is a closed subset (it's formed by satisfying an equation), hence compact. Our group operations are continuous w.r.t. the topology, i.e. $(E(K), \oplus)$ is a compact topological group. If $\widetilde{E}$ has no singular point, then there's nothing to do. Otherwise, let $(\widetilde{x}_0, \widetilde{y}_0)$ be a singular point (for $x_0, y_0 \in \mathcal{O}_K$). Then

$$E(K) \backslash E_0(K) = \{(x, y) \in E(K) \, : \, \text{ord}_K(x - x_0) \geq 1, \text{ord}_K(y - y_0) \geq 1\}$$

is a closed set.

$E_0(K) \subset E(K)$ is open, and so its cosets are open. These cosets form an open cover of $E(K)$. But $E(K)$ is compact – every open cover has a finite subcover. Cosets don't overlap, so the only way this can happen is for there to have been only finitely many of them to begin with. ○

Definition 14.3. $[E(K) : E_0(K)] < \infty$ is called the *Tamagawa number* $c_K(E)$.

Lemma 8.7 says that this is finite. It turns out that you don't need k to be finite. You can set things up more carefully to get a geometric interpretation of the Tamagawa number (see Silverman's second book).

Fact 14.4. *Either* $c_K(E) = \mathrm{ord}_K(\Delta)$ *or* $c_K(E) \le 4$.

Remark 14.5. If we have good reduction, then $c_K(E) = 1$. But, the converse is false.

If the reduction is the additive group, then $c_K(E) \le 4$. You have *split reduction* if the reduction is the multiplicative group, *and* you don't have to add in any square roots. In this case $c_K(E) = 1$. Otherwise, the reduction is called *nonsplit*, and $c_K(E) = \mathrm{ord}(\Delta)$.

If you're not working with minimal Weierstrass equations, then this doesn't work – you can make E_0 have huge index in $E(K)$.

Theorem 14.6. *(8.8) Let $[K : \mathbb{Q}_p] < \infty$, and let E be an elliptic curve over K. Then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$. In particular $E(K)_{tors}$ is finite (since it injects into $E(K)/E_r(K)$ ← this is because $\mathcal{O}_K \cong E_r(K)$ is torsion-free).*

Fact 14.7. *Let $[L : \mathbb{Q}_p] < \infty$, and L/K be a finite extension. Then $[L : K] = ef$, and you get a diagram*

$$\begin{tikzcd}
K^* \arrow[r, "\mathrm{ord}_K"] \arrow[d, hook] & \mathbb{Z} \arrow[d, "-\times e"] \\
L^* \arrow[r, "\mathrm{ord}_L"] & \mathbb{Z}
\end{tikzcd}$$

where e is the ramification index (take the uniformizer in K^*, and ask for its valuation in L^*). Also, $f = [k_L : k]$, where k and k_L are the residue fields of K and L.

If L/K is Galois, the natural map

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$$

is surjective. The kernel has order e.

Definition 14.8. L/K is *unramified* if $e = 1$.

Fact 14.9. *For each integer $n \ge 1$,*

(1) *k has a unique extension of degree n (unique means unique within some fixed algebraic closure of k);*

(2) *K has a unique unramified extension of degree n, whose residue field is the unique extension of the residue field of K described in (1).*

These are Galois extensions with cyclic Galois group of order n.

Definition 14.10. K^{nr} is the maximal unramified extension of K. Its residue field is $\overline{k}$.

Warning: K^{nr} is not complete (unlike finite extensions).

Proposition 14.11. *(8.9) Suppose E/K has good reduction, and suppose $p \nmid n$ (where p is the characteristic of k). Then*

(1) $E(K^{nr})[n] = E(\overline{K})[n]$ *(every n-torsion point you could imagine is defined over an unramified extension)*
(2) $E(K^{nr}) \overset{-\times n}{\to} E(K^{nr})$ is surjective.

Proof. If L/K is finite and unramified, $E_1(L) \overset{-\times n}{\to} E_1(L)$ is an isomorphism (by Corollary 7.5). In Proposition 8.5, we checked that $E(L) \to \widetilde{E}(k_L)$ is surjective (assuming good reduction).

There is a commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & E_1(K^{nr}) \arrow[r] \arrow[d, "-\times n"] & E(K^{nr}) \arrow[r] \arrow[d, "-\times n"] & \widetilde{E}(\overline{k}) \arrow[r] \arrow[d, "-\times n"] & 0 \\
0 \arrow[r] & E_1(K^{nr}) \arrow[r] & E(K^{nr}) \arrow[r] & \widetilde{E}(\overline{k}) \arrow[r] & 0
\end{tikzcd}$$

The first vertical map is an isomorphism. Now do a diagram chase using the snake lemma to show that $E(K^{nr})[n] \overset{\cong}{\to} \widetilde{E}(\overline{k})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ is an isomorphism and

$$E(K^{nr})/nE(K^{nr}) \cong \widetilde{E}(\overline{k})/n\widetilde{E}(\overline{k}) = 0.$$

But $E(K^{nr})[n] \subset E(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ also by Theorem 6.5. ○

Corollary 14.12. *(8.10) Suppose E/K has good reduction, and $P \nmid n$. If $p \in E(K)$ then $K([n]^{-1}P)/K$ is unramified.*

Note: $[n]^{-1}P = \{Q \in E(\overline{K}) \,:\, nQ = P\}$

$$K(\{P_1, \cdots P_r\}) = K(x_1, \cdots, x_r, y_1, \cdots, y_r) \text{ with } P = (x_i, y_i)$$

Proof. Proposition 8.9(2) shows that there is some $Q \in E(K^{nr})$ such that $nQ = P$. Then $[n]^{-1}P = \{Q + T \,:\, T \in E(\overline{K})[n]\}$. But part (1) of the Proposition shows that all of these points are in $E(K^{nr})$. So $K([n]^{-1}P) \subset K^{nr}$. ○

Chapter 9: The torsion subgroup

We are now working over a field K that is a finite extension of $\mathbb{Q}$. Let E be an elliptic curve over K.

Notation 14.13. For $\mathfrak{P}$ a prime of K (i.e. prime ideal in $\mathcal{O}_K$) we write

$$K_{\mathfrak{P}} = \text{ completion of } K \text{ w.r.t. } \mathfrak{P}\text{-adic valuation.}$$

Definition 14.14. $\mathfrak{P}$ is a prime of good reduction for E/K if $E/K_{\mathfrak{P}}$ has good reduction.

Lemma 14.15. *(9.1) E/K has only finitely many primes of bad reduction.*

Proof. Take a Weierstrass equation for E with $a_1, \cdots, a_6 \in \mathcal{O}_K$. Since E is nonsingular, $0 \neq \Delta \in \mathcal{O}_K$. Factor the discriminant

$$(\Delta) = \mathfrak{P}_1^{\alpha_1} \cdots \mathfrak{P}_r^{\alpha_r}$$

where $\mathfrak{P}_i$ are prime ideals. Let $S = \{\mathfrak{P}_1, \cdots, \mathfrak{P}_r\}$. If $\mathfrak{P} \notin S$, then $\operatorname{ord}_{\mathfrak{P}}(\Delta) = 0$. So $E/k_{\mathfrak{P}}$ has good reduction, and

$$\{ \text{ bad primes for } E \ \} \subset S.$$

○

Lecture 15: February 20

K was a finite extension of $\mathbb{Q}$.

Lemma 15.1. *(9.2) $E(K)_{tors}$ is finite.*

Proof. Take any prime $\mathfrak{P}$, $K \subset K_{\mathfrak{P}}$. Then $E(K)_{tors} \subset E(K_{\mathfrak{P}})_{tors}$, and we checked in Theorem 8.8 that the latter is finite. ○

Lemma 15.2. *(9.3) Let $\mathfrak{P}$ be a prime of good reduction for E/K, with $\mathfrak{P} \nmid n$. Then reduction mod $\mathfrak{P}$ gives an injection*

$$E(K)[n] \hookrightarrow \widetilde{E}(k_{\mathfrak{P}})[n]$$

Proof. $E_1(K_{\mathfrak{P}})$ was the kernel of $E(K_{\mathfrak{P}}) \to \widetilde{E}(k_{\mathfrak{P}})$; this has no n-torsion, since multiplication by n was an isomorphism by Corollary 7.5. ○

Example 15.3.

$$E : y^2 + y = x^3 - x^2$$

Note that $\Delta = -11$. E has good reduction at all $p \neq 11$.

p	2	3	5	7	11	13
$\#\widetilde{E}(\mathbb{F}_p)$	5	5	5	10	-	10

So

$$\#E(\mathbb{Q})_{tors} \mid 5 \cdot 2^a \text{ for some } a \geq 0$$

$$\#E(\mathbb{Q})_{tors} \mid 5 \cdot 3^b \text{ for some } b \geq 0$$

So $\#E(\mathbb{Q})_{tors} \mid 5$. Let $T = (0,0) \in E(\mathbb{Q})$. You can show that $5T = 0$, so $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$.

Example 15.4.

$$E : y^2 + y = x^3 + x^2$$

Now $\Delta = -43$. E has good reduction at all $p \neq 43$

p	2	3	5	7	11	13
$\#\widetilde{E}(\mathbb{F}_p)$	5	6	10	8	9	19

$$\#E(\mathbb{Q})_{tors} \mid 5 \cdot 2^a \text{ for some } a \geq 0$$

$$\#E(\mathbb{Q})_{tors} \mid 9 \cdot 11^b \text{ for some } b \geq 0$$

So $E(\mathbb{Q})_{tors} = \{0\}$.

Take $T = (0,0)$. Since there aren't any torsion points, this has infinite order (and $\operatorname{rank} E(\mathbb{Q}) \geq 1$). So we get a way to find infinitely many solutions to E: just take all the multiples of $(0,0)$.

Example 15.5.

$$E_D : y^2 = x^3 - D^2 x$$

where $D \in \mathbb{Z}$ is square-free. Compute $\Delta = 2^6 D^6$. 2-torsion points consist of roots of the cubic:

$$E_D(\mathbb{Q})_{tors} \supset \{0, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

Let $f(X) = X^3 - D^2X$. If $p \nmid 2D$ then

$$\#\widetilde{E}_D(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \Bigg(\underbrace{\left(\tfrac{f(x)}{p}\right)}_{\substack{Legendre\\symbol}} + 1 \Bigg).$$

The Legendre symbol is multiplicative, so if $p \equiv 3 \pmod 4$ then

$$\left(\frac{f(-x)}{p}\right) = \left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f(x)}{p}\right) = -\left(\frac{f(x)}{p}\right)$$

So the Legendre symbols cancel in pairs, and $\widetilde{E}_D(\mathbb{F}_p) = p + 1$.

Let $m = \#E_D(\mathbb{Q})_{tors}$. We have $4 \mid m \mid p+1$ for all sufficiently large primes p with $p \equiv 3 \pmod 4$ (use the lemma and take p larger than any prime factors of m). I claim that $8 \nmid m$, because otherwise there would be finitely many primes that are 3 mod 8, a contradiction to Dirichlet's theorem on primes in arithmetic progressions. So $m = 4$, and $E_D(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

So

$$\operatorname{rank} E_D(\mathbb{Q}) \geq 1 \iff \begin{array}{c} \exists x, y \in \mathbb{Q} \text{ with} \\ y^2 = x^3 - D^2 x \text{ and } y \neq 0 \end{array} \overset{Lect.1}{\iff} E \text{ is a congruent number}$$

Lemma 15.6 (Torsion points over integral elliptic curves are almost integers). *(9.4) Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation with coefficients $a_1, \cdots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T \in E(\mathbb{Q})_{tors}$, say $T = (x,y)$. Then*

(1) $4x, 8y \in \mathbb{Z}$
(2) *If T is not a 2-torsion point, or $2 \mid a_1$, then $x, y \in \mathbb{Z}$.*

Proof. The Weierstrass equation determines a formal group $\widehat{E}$ over $\mathbb{Z}$. Recall we can use this to construct an actual group

$$\widehat{E}(p^r\mathbb{Z}_p) = \{(x,y) \in E(\mathbb{Q}_p) \,:\, \operatorname{ord}_p(x) \leq -2r, \operatorname{ord}_p(y) \leq -3r\}.$$

By Proposition 8.2,

$$\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +) \text{ if } r > \frac{1}{p-1}$$

(we haven't made any extension of $\mathbb{Q}_p$, so the ramification index here is 1). If $p = 2$, $\widehat{E}(4\mathbb{Z}_2)$ is torsion free; for odd p, $\widehat{E}(p\mathbb{Z}_p)$ is torsion free. So

$$\operatorname{ord}_2(x) \geq -2, \operatorname{ord}_2(y) \geq -3$$
$$\operatorname{ord}_p(x) \geq 0, \operatorname{ord}_p(y) \geq 0 \ \forall p \text{ odd}$$

This proves (1).

For (2), suppose $T \in \widehat{E}(2\mathbb{Z}_2)$.

$$\widehat{E}(2\mathbb{Z}_2)/\widehat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$$

$\widehat{E}(4\mathbb{Z}_2) \cong (\mathbb{Z}_2, +)$ is torsion-free. So $2T = 0$.

$$(x, y) = T = -T = (x, -y - a_1 x - a_3)$$

and equating second coordinates, $2y + a_1 x + a_3 = 0$. But $\operatorname{ord}_2(x) = -2$, $\operatorname{ord}_2(y) = -3$.

$$\underbrace{8y}_{odd} + a_1 \underbrace{(4x)}_{odd} + \underbrace{4a_3}_{even} = 0$$

so a_1 is odd. So if $2T \neq 0$ or a_1 is even, then $T \notin \widehat{E}(2\mathbb{Z}_2)$, and so $x, y \in \mathbb{Z}$. ○

For example, if $y^2 + xy = x^3 + 4x + 1$, then $(-\frac{1}{4}, \frac{1}{8}) \in E(\mathbb{Q})[2]$.

So, over $\mathbb{Q}$ the only annoying prime is 2. A similar thing happens over other number fields, but there might be more annoying primes.

Corollary 15.7 (Lutz-Nagell). *(9.5) Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + ax + b$, for $a, b \in \mathbb{Z}$. Suppose $0 \neq T \in E(\mathbb{Q})_{tors}$, say $T = (x, y)$, then $x, y \in \mathbb{Z}$ and either $y = 0$ (2-torsion point) or $y^2 \mid 4a^3 + 27b^2$.*

Proof. By Lemma 9.4, $x, y \in \mathbb{Z}$. If $2T = 0$, then $y = 0$. Otherwise, $2T$ is not the point at infinity, so it has coordinates (x_2, y_2). Again for the lemma (applied to $2T$), $x_2, y_2 \in \mathbb{Z}$.

$$x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$$

Everything is an integer here, so $y \mid f'(x)$.

Since E is nonsingular, f has no repeated roots – i.e. $f(X)$ and $f'(X)$ are coprime. This means $f(X)$ and $f'(X)^2$ are coprime. Use Euclid's algorithm to produce $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X)^2 = 1$. The coefficients in g, h depend on a, b; a calculation gives

$$(3X^2 + 4a)f'(X)^2 - 27(X^3 + aX - b)f(X) = 4a^3 + 27b^2$$

Since $y \mid f'(x)$ and $y^2 = f(x)$, we get $y^2 \mid (4a^3 + 27b^2)$. ○

Remark 15.8. Mazur showed that if E is an elliptic curve over $\mathbb{Q}$, then the torsion subgroup is one of the following:

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 12, n \neq 11 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4 \end{cases}$$

Lecture 16: February 22

Chapter 10: Kummer Theory

Let K be a field with $\mathrm{char}(K) \nmid n$. Assume $\mu_n \subset K$.

Lemma 16.1. *(10.1) Let $\Delta \subset K^*/(K^*)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$. Then L/K is Galois and*

$$\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_n)$$

where μ_n is the n^{th} roots of unity.

Proof. L/K is Galois since $\mu_n \subset K$ (normality) and $\mathrm{char}(K) \nmid n$ (separability). Define the Kummer pairing

$$\langle -,- \rangle : \mathrm{Gal}(L/K) \times \Delta \to \mu_n \text{ where } (\sigma, x) \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$$

First we need to check that this is well-defined, i.e. that it doesn't depend on the root of x chosen. Suppose $\alpha^n = \beta^n = x$. So $\left(\frac{\alpha}{\beta}\right)^n = 1$, and $\frac{\alpha}{\beta} \in \mu_n$. This is fixed by all $\sigma \in \mathrm{Gal}(L/K)$, so $\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta}$.

Bilinear:

$$\langle \sigma\tau, x \rangle = \frac{\sigma\tau(\sqrt[n]{x})}{\tau(\sqrt[n]{x})} \frac{\tau(\sqrt[n]{x})}{\sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle$$

$$\langle \sigma, xy \rangle = \frac{\sigma(\sqrt[n]{x}\sqrt[n]{y})}{\sqrt[n]{x}\sqrt[n]{y}} \langle \sigma, x \rangle \langle \sigma, y \rangle$$

Non-degenerate: Let $\sigma \in \mathrm{Gal}(L/K)$. If $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$ then $\sigma \sqrt[n]{x} = \sqrt[n]{x}$ for all $x \in \Delta$. But the Galois group fixes K, and now we see it fixes everything used to generate the extension L, so σ fixes every element of L; that is, $\sigma = 1$.

Let $x \in \Delta$. If $\langle \sigma, x \rangle = 1$ for all $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma \sqrt[n]{x} = \sqrt[n]{x}$ for all σ. Elements fixed by all the Galois group are in the base field: so $\sqrt[n]{x} \in K$, and $x \in (K^*)^n$ (the group we'd modded out by at the beginning).

$\langle -,- \rangle$ induces injections

(1) $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Hom}(\Delta, \mu_n)$
(2) $\Delta \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$

The fact that these are injections follows from the non-degeneracy on the right.

By (1), we see that $\mathrm{Gal}\, L/K$ is a finite abelian group of exponent dividing n (use the fact that $\mathrm{Hom}(A, \mu_n)$ is the dual of A^* and so has the same order as A). Also by looking at orders, (1) and (2) above give:

$$|\mathrm{Gal}(L/K)| \overset{(1)}{\leq} |\Delta| \overset{(2)}{\leq} |\mathrm{Gal}(L/K)|\,.$$

Therefore, (1) and (2) are isomorphisms. ○

Proposition 16.2. *(10.2) There is a bijection*

$$\left\{\begin{matrix}\textit{finite subgroups}\\ \Delta \subset K^*/(K^*)^n\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\textit{finite abelian extensions } L/K\\ \textit{of exponent dividing } n\end{matrix}\right\}$$

where $\Delta \mapsto K(\sqrt[n]{\Delta})$ *and, in the reverse direction,* $L \mapsto (K^* \cap (L^*)^n)/(K^*)^n$.

Proof. Let L/K be a finite abelian extension of exponent dividing n. Let

$$\Delta = (K^* \cap (L^*)^n)/(K^*)^n.$$

Then $K(\sqrt[n]{\Delta}) \subset L$. We need to show that these are isomorphic.

Let $G = \mathrm{Gal}(L/K)$. The Kummer pairing gives an injection

$$\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$$

Claim 16.3. *This map is surjective.*

Proof. Let $\chi : G \to \mu_n$ be a group homomorphism. Think of the elements of G as maps $L \to L$, so they are an L-vector space.

Fact 16.4. *Distinct automorphisms are linearly independent.*

There exists $a \in L$ such that

$$\sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$$

(or else this linear combination would be the zero automorphism). Let y be the LHS above. Let $\sigma \in G$.

$$\begin{aligned}\sigma(y) &= \sum_{\tau\in G} \chi(\tau)^{-1}\sigma\tau(a)\\ &= \sum_{\tau\in G} \chi(\sigma^{-1}\tau)^{-1}\tau(a) = \underbrace{\chi(\sigma)}_{\in\mu_n} y.\end{aligned}$$

But $\chi(\sigma)$ is a n^{th} root of unity, so

$$\sigma(y^n) = y^n \ \forall \sigma \in G.$$

Set $x = y^n \in K^*$, and note that $x \in K^* \cap (L^*)^n = \Delta$. So $\chi : \sigma \mapsto \frac{\sigma(y)}{y} = \chi(\sigma)$, which shows $x \in \Delta$ is the required preimage of χ under the map $\Delta \to \mathrm{Hom}(G, \mu_n)$.

End of proof of Claim.

Now $\Delta \to \mathrm{Hom}(G, \mu_n)$ is an isomorphism. So $|\Delta| = |\mathrm{Hom}(G, \mu_n)| = |G|$. We have

$$[K(\sqrt[n]{\Delta}) : K] = |\,\mathrm{Gal}(K(\sqrt[n]{\Delta})/K) \overset{10.1}{=} |\Delta|$$

$$[L:K] = |\operatorname{Gal}(L/K)| = |G|$$

and these are equal because we just proved $\Delta \to \operatorname{Hom}(G, \mu_n)$ is an isomorphism (and hence $|\Delta| = |G|$). Since $K(\sqrt[n]{\Delta}) \subset L$, this gives $L = K(\sqrt[n]{\Delta})$ as desired.

It remains to show that the composition in the other direction is the identity. Let $\Delta \subset K^*/(K^*)^n$ be a finite subgroup; set $L := K(\sqrt[n]{\Delta})$ and $\Delta' = \frac{K^* \cap (L^*)^n}{(K^*)^n}$. We need to show that $\Delta = \Delta'$.

It is clear that $\Delta \subset \Delta'$. But

$$L = K(\sqrt[n]{\Delta}) \subset K(\sqrt[n]{\Delta'}) \subset L$$

By Lemma 10.1, $|\Delta| = |\Delta'|$, and since we already have one inclusion, they are equal. ○

Proposition 16.5. *(10.3) Let K be a number field containing all n^{th} roots of unity. Let S be a finite set of primes of K. There are only finitely many extensions L/K such that*

(1) L/K is abelian of exponent dividing n, and
(2) L/K is unramified at all primes outside S.

Proof. By Proposition 10.2, $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subset K^*/(K^*)^n$.

Let $\mathfrak{P}$ be a prime of K. We can factor $\mathfrak{P}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$ for some prime ideals P_i in $\mathcal{O}_L$.

If $x \in K^*$ represents an element of Δ, then

$$n \cdot \operatorname{ord}_{P_i}(\sqrt[n]{x}) = \operatorname{ord}_{P_i}(x) = e_i \operatorname{ord}_{\mathfrak{P}}(x).$$

If $\mathfrak{P} \notin S$ then $\mathfrak{P}$ is unramified, so all the $e_i = 1$. So from the equation above we see that $\operatorname{ord}_{\mathfrak{P}}(x) \equiv 0 \pmod{n}$. So $\Delta \subset K(S, n)$ where

$$K(S, n) = \{x \in K^*/(K^*)^n : \operatorname{ord}_{\mathfrak{P}}(x) \equiv 0 \pmod{n}\ \forall \mathfrak{P} \notin S\}.$$

For example, $\mathbb{Q}(\{3, 17\}, 2) = \langle -1, 3, 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We have reduced this proposition to the following lemma:

Lemma 16.6. *(10.4) $K(S, n)$ is finite.*

Proof. We need the following two facts from algebraic number theory:

(1) The class group is finite
(2) Dirichlet's Unit theorem ($\mathcal{O}_K^*$ is finitely generated)

Let I_K be the group of fractional ideals in K. The class group is the cokernel of the map $K^* \to I_K$, where $x \mapsto (x)$. So we have an exact sequence

$$0 \to \mathcal{O}_K^* \to K^* \to I_K \to Cl_K \to 0$$

Let $P_K = i(K^*)$ be the group of principal fractional ideals. We can break up the above short exact sequence into two new ones:

$$0 \to \mathcal{O}_K^* \to K^* \to P_K \to 0$$

$$0 \to P_K \to I_K \to Cl_K \to 0$$

which gives two diagrams

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^* \arrow[r] \arrow[d, "n"] & K^* \arrow[r] \arrow[d, "n"] & P_K \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & \mathcal{O}_K^* \arrow[r] & K^* \arrow[r] & P_K \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & P_K \arrow[r] \arrow[d, "n"] & I_K \arrow[r] \arrow[d, "n"] & Cl_K \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & P_K \arrow[r] & I_K \arrow[r] & Cl_K \arrow[r] & 0
\end{tikzcd}$$

Applying the snake lemma,

$$0 \to {\mathcal{O}_K}^*/(\mathcal{O}_K^*)^n \to K^*/(K^*)^n \to P_k/P_K^n \to 0 \tag{16.1}$$

If $Cl_K[n]$ is the kernel of the multiplication-by-n map, we get

$$0 \to Cl_K[n] \to P_K/P_K^n \to I_K/I_K^n \to Cl_K/Cl_K^n \to 0 \tag{16.2}$$

By definition, the image of $K(S,n)$ in I_K/I_K^n is finite.

Using (16.2) and the fact that Cl_K is finite, we see that the image of $K(S,n)$ in P_K/P_K^n is finite.

Using (16.1) and the fact that $\mathcal{O}_K^*$ is finitely-generated, we see that $K(S,n)$ is finite. ○

Lecture 17: February 25

Chapter 11: Mordell-Weil

Let K be a number field, E an elliptic curve over K. Let $n \geq 2$.

Theorem 17.1 (Weak Mordell-Weil). *(11.1)*

$$|E(K)/nE(K)| < \infty$$

We will use this to prove the full Mordell-Weil theorem. It suffices to use $n = 2$, but considering general n gives more information about the rank.

Lemma 17.2. *(11.2) Assume $E[n] \subset E(K)$. Let*

$$S = \{\text{ primes of bad reduction for } E \} \cup \{\text{primes dividing } n\}$$

Let $L = K([n]^{-1}P)$ for some $P \in E(K)$. (This is a finite extension: you can use the group law to solve for the points Q such that $nQ = P$.) Then:

(1) *L/K is abelian of exponent dividing n*
(2) *L/K is unramified at all $\mathfrak{P} \nmid S$*

Proof. (1) Let $Q \in E$ with $nQ = P$. All other points in L are gotten by adding an n-torsion point; since we're assuming all the n-torsion points are defined over Q, $L = K(Q)$. Let M/K be a Galois closure of L/K. For $\sigma \in \mathrm{Gal}(M/K)$, $\sigma(Q) - Q \in E[n] \subset E(K)$, and so $\sigma(Q) \in E(L)$. Thus, $\sigma(L) = L$ for all $\sigma \in \mathrm{Gal}(M/K)$, and so L/K is Galois.

Define $f : \mathrm{Gal}(L/K) \to E[n]$ where $\sigma \mapsto \sigma Q - Q$.

f injective: Suppose $f(\sigma) = 0$. Then $\sigma Q = Q$. σ pointwise fixes L, so $\sigma = 1$.

f is a group homomorphism:

$$\begin{aligned} f(\sigma\tau) &= \sigma\tau Q - Q \\ &= \sigma(\tau Q - Q) + \sigma Q - Q \\ &= \sigma f(\tau) + f(\sigma) \\ &= f(\tau) + f(\sigma) \end{aligned}$$

where the last line is because $f(*)$ is an n-torsion point, which is in $E(K)$ and hence fixed by the Galois group.

So $f : \mathrm{Gal}(L/K) \hookrightarrow E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. So L/K is abelian of exponent dividing n.

(2) See Corollary 8.10. ○

Remark 17.3. If $E[n] \subset E(K)$ and L/K is a finite Galois extension, then, analogously to the Kummer pairing, we get an injective group homomorphism

$$\frac{E(K) \cap nE(L)}{nE(K)} \to \mathrm{Hom}(\mathrm{Gal}(L/K), E[n]) \text{ where } P \mapsto (\sigma \mapsto \sigma Q_P - Q_P)$$

where Q_P is a point such that $nQ_P = P$.

Lemma 17.4. *(11.3) If L/K is a finite Galois extension, then the natural map*

$$E(K)\Big/nE(K) \xrightarrow{\alpha} E(L)\Big/nE(L)$$

has finite kernel.

Proof. There is a surjective group homomorphism

$$\frac{E(L) \cap [n]^{-1}E(K)}{E(K)} \xrightarrow{-\times n} \frac{E(K) \cap nE(L)}{nE(K)} = \ker(\alpha)$$

Let X be a set, and A an abelian group,

$$Map(X, A) = \{maps : X \to A\}$$

is a group under pointwise operations. There is an injective group homomorphism

$$\begin{aligned} \frac{E(L) \cap [n]^{-1}E(K)}{E(K)} &\hookrightarrow Map(\mathrm{Gal}(L/K), E[n]) \\ Q &\mapsto (\sigma \mapsto \sigma Q - Q) \end{aligned}$$

(If $\sigma Q = Q$ for all $\sigma \in \mathrm{Gal}(L/K)$ then $Q \in E(K)$.) $\mathrm{Gal}(L/K)$ and $E[n]$ are finite, so the space of maps between them is finite. ○

Proof of Theorem 11.1. By Lemma 11.3, we may extend the field K such that

(1) $\mu_n \subset K$
(2) $E[n] \subset E(K)$

(It turns out that (2) $\implies$ (1), by the *Weil pairing*, to be discussed later.)

Let L be the composite of all field extensions of the form $K([n]^{-1}P)$ for $P \in E(K)$. By Lemma 11.2 and Proposition 10.3, there are only finitely many such extensions. So $[L : K] < \infty$.

The map

$$\frac{E(K)}{nE(K)} \to \frac{E(L)}{nE(L)}$$

is the zero map. By Lemma 11.3, $\frac{E(K)}{nE(K)}$ is finite. ○

Remark 17.5. If $K = \mathbb{R}, \mathbb{C}$ or $[K : \mathbb{Q}_p] < \infty$, then we know

$$\frac{E(K)}{nE(K)} < \infty$$

but $E(K)$ is *not* finitely generated (it's uncountable).

Fact 17.6. *If K is a number field, there is a quadratic form (called the* canonical height*)*

$$\widehat{h} : E(K) \to \mathbb{R}_{\geq 0}$$

with the property that for any $B \in \mathbb{R}$,

$$\{P \in E(K) \, : \, \widehat{h}(P) \leq B\} \text{ is finite.} \tag{17.1}$$

Theorem 17.7 (Mordell-Weil). *(11.4) Let K be a number field, and E an elliptic curve over K. Then $E(K)$ is a finitely-generated abelian group.*

Proof. Fix an integer $n \geq 2$. By the Weak Mordell-Weil Theorem, $E(K)/nE(K)$ has finite order. Pick coset representatives $P_1, \cdots, P_r$. Let

$$\Sigma = \{P \in E(K) \, : \, \widehat{h}(P) \leq \max_{1 \leq i \leq r} \widehat{h}(P_i)\}.$$

Claim 17.8. *Σ generates $E(K)$.*

Proof of claim. If not, by (17.1), we can pick $P \in E(K) \backslash \langle \Sigma \rangle$ of minimal height. Then $P = P_i + nQ$; Q is not in the subgroup generated by Σ, because if it was, then P would also be generated by Σ since P_i is. Because P was minimal, $\widehat{h}(P) \leq \widehat{h}(Q)$.

$$\begin{aligned} 4\widehat{h}(P) &\leq 4\widehat{h}(Q) \\ &\leq n^2 \widehat{h}(Q) = \widehat{h}(nQ) \end{aligned}$$

$$
\begin{aligned}
&= \widehat{h}(P - P_i) \\
&\le \widehat{h}(P - P_i) + \widehat{h}(P + P_i) \\
&= 2\widehat{h}(P) + 2\widehat{h}(P_i) \text{ by the Parallelogram Law} \\
\widehat{h}(P) &\le \widehat{h}(P_i)
\end{aligned}
$$

This shows that $P \in \Sigma$, a contradiction. ○

Σ is finite by (17.1). ○

LEMMA 17.9. *(11.5) Let $P \in E(K)$. Then*

$$P \in E(K)_{tors} \iff \widehat{h}(P) = 0$$

Proof. ($\implies$) $nP = 0$ so $n^2\widehat{h}(P) = \widehat{h}(nP) = 0$ (since $\widehat{h}$ is a quadratic form). So $\widehat{h}(P) = 0$.

($\impliedby$) If $\widehat{h}(P) = 0$ then $\widehat{h}(nP) = 0$ for all $n \in \mathbb{Z}$.

$$\{nP \,:\, n \in \mathbb{Z}\}$$

is finite by (17.1), so $P \in E(K)_{tors}$. ○

This gives another proof that $E(K)_{tors}$ is finite.

LECTURE 18: FEBRUARY 27

CHAPTER 12: HEIGHTS

For simplicity let $K = \mathbb{Q}$.

DEFINITION 18.1. Write $P \in \mathbb{P}^n(\mathbb{Q})$ as $P = (a_0 : \cdots : a_n)$; we may assume that $a_i \in \mathbb{Z}$ with $\gcd(a_0, \cdots, a_n) = 1$. Then define

$$H(P) := \max_{0 \le i \le n} |a_i|\,.$$

LEMMA 18.2. *(12.1) Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be homogeneous polynomials of degree d, with no common root in $\mathbb{P}^1(\overline{\mathbb{Q}})$ (i.e. they have no common factor, even over $\overline{\mathbb{Q}}$). Let $F : \mathbb{P}^1 \to \mathbb{P}^1$ be the map $(x_1 : x_2) \mapsto (f_1(x_1, x_2) : f_2(x_1, x_2))$.*

Then there exist $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d \quad \forall P \in \mathbb{P}^1(\mathbb{Q}).$$

Proof. Without loss of generality assume $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$.

Upper bound: Write $P = (a : b)$ where $a, b \in \mathbb{Z}$ are coprime. Then

$$H(F(P)) \le \max(|f_1(a, b)|, |f_2(a, b)|)$$

$$\leq c_2 \max(|a|^d, |b|^d)$$

where $c_2 = \max_{i=1,2}$(sum of absolute values of coefficients of f_i). (Remember that a, b, and all coefficients are integers.) Then $H(F(P)) \leq c_2 H(P)^d$.

Lower bound: We claim that there are some homogeneous polynomials $g_{ij} \in \mathbb{Z}[X_1, X_2]$ of degree $d-1$ and some integer $\kappa > 0$ such that

$$\sum_{j=1}^{2} g_{ij} f_j = \kappa X_i^{2d-1} \tag{18.1}$$

Indeed, running Euclid's algorithm on $f_1(X,1)$ and $f_2(X,1)$ yields polynomials $r, s \in \mathbb{Q}[X]$ with degrees $< d$ such that

$$r(X) f_1(X,1) + s(X) f_2(X,1) = 1.$$

Homogenize and clear denominators to get an equation of the form (18.1), with $i = 2$. Similarly, one can obtain an analogous expression for $i = 1$.

Write $P = (a_1 : a_2)$ where a_1, a_2 are coprime integers. By equation (18.1),

$$\sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = \kappa a_i^{2d-1}.$$

Therefore, $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(\kappa a_1^{2d-1}, \kappa a_2^{2d-1})$. Since a_1, a_2 were coprime, this is κ.

But also

$$\begin{aligned} |\kappa a_i^{2d-1}| &\leq \underbrace{\max_{j=1,2} |f_j(a_1, a_2)|}_{\leq \kappa H(F(P))} \underbrace{\sum_{j=1}^{2} |g_{ij}(a_1, a_2)|}_{\leq \gamma_i H(P)^{d-1}} \\ |a_i|^{2d-1} &\leq \gamma_i H(F(P)) H(P)^{d-1} \\ H(P)^{2d-1} &\leq \max(\gamma_1, \gamma_2) H(F(P)) H(P)^{d-1} \\ \underbrace{\frac{1}{\max(\gamma_1, \gamma_2)}}_{c_1} H(P)^d &\leq H(F(P)) \end{aligned}$$

○

Notation 18.3. For $x \in \mathbb{Q}$, define $H(x) = H(x : 1)$ (i.e. write $x = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ coprime, and define $H(x) = \max(|a|, |b|)$).

Let E be an elliptic curve over $\mathbb{Q}$, which we can write as $y^2 = x^3 + ax + b$.

Definition 18.4. Define the height of a rational point:

$$H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$$

$$P \mapsto \begin{cases} H(x) & \text{if } P = (x, y) \\ 1 & \text{if } P = 0_E \end{cases}$$

and define the logarithmic height:

$$\begin{aligned} h : E(\mathbb{Q}) &\to \mathbb{R}_{\geq 0} \\ P &\mapsto \log(H(P)) \end{aligned}$$

Lemma 18.5. *(12.2) Let E, E' be elliptic curves over $\mathbb{Q}$; let $\varphi : E \to E'$ be an isogeny defined over $\mathbb{Q}$. Then there is some constant c such that*

$$|h(\varphi(P)) - (\deg\varphi)h(P)| < c$$

for all $P \in E(\mathbb{Q})$.

Note that c depends on E, E', and φ but not on P.

Recall Lemma 5.4 says that $\deg(\varphi) = \deg(\xi)$ where ξ is the map

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "x"] & E' \arrow[d, "x"] \\ \mathbb{P}^1 \arrow[r, "\xi"] & \mathbb{P}^1 \end{tikzcd}$$

Suppose $d = \deg(\varphi)$. By Lemma 12.1, we can find $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \leq H(\varphi(P)) \leq c_2 H(P)^d.$$

Taking logs gives

$$|h(\varphi(P)) - dh(P)| \leq \underbrace{\log(\max(\frac{1}{c_1}, c_2))}_{c}.$$

Example 18.6. Let $\varphi = [2] : E \to E$. Then there is some $c > 0$ such that

$$|h(2P) - 4h(P)| < c$$

for all $P \in E(\mathbb{Q})$.

Definition 18.7. The canonical height is

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$$

Convergence: Let $m \geq n$.

$$\begin{aligned} \left|\frac{1}{4^m}h(2^mP) - \frac{1}{4^n}h(2^nP)\right| &\leq \sum_{r=n}^{m-1} \left|\frac{1}{4^{r+1}}h(2^{r+1}P) - \frac{1}{4^r}h(2^rP)\right| \\ &= \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} \left|h(2^{r+1}P - 4h(2^rP))\right| \qquad \text{triangle ineq.} \\ &= c\sum_{r=n}^{m-1} \frac{1}{4^{r+1}} \leq \frac{c}{4^{n+1}}\left(\frac{1}{1-\frac{1}{4}}\right) = \frac{c}{3\cdot 4^n} \end{aligned}$$

This tends to 0 as $n \to \infty$, so the sequence is Cauchy.

Lemma 18.8. *(12.3) $|h(P) - \widehat{h}(P)|$ is bounded for $P \in E(\mathbb{Q})$.*

Proof. Put $n = 0$ in the above calculation to get

$$\left| \frac{1}{4^m} h(2^m P) - h(P) \right| < \frac{3}{c}.$$

Take $\lim_{m\to\infty}$. ○

Lemma 18.9. *(12.4) Let $\varphi : E \to E'$ be an isogeny defined over $\mathbb{Q}$. Then*

$$\widehat{h}(\varphi(P)) = (\deg \varphi)\widehat{h}(P)$$

for all $P \in E(\mathbb{Q})$.

Proof. By Lemma 12.2, there is some constant c with

$$|h(\varphi(P)) - (\deg \varphi) h(P)| < c$$

for all $P \in E(\mathbb{Q})$. Replace P by $2^n P$ and divide by 4^n:

$$\left| \frac{1}{4^n} h(2^n \varphi(P)) - \frac{1}{4^n} (\deg \varphi) h(2^n P) \right| < \frac{c}{4^n}.$$

Take the limit $n \to \infty$. ○

Remark 18.10. Lemma 12.4 also shows that $\widehat{h}$ does not depend on the choice of Weierstrass equation.

Lemma 18.11. *(12.5)*

$$\#\{P \in E(\mathbb{Q}) \,:\, \widehat{h}(P) \le B\} < \infty.$$

Proof. By Lemma 12.3, bounding $\widehat{h}$ also bounds h; this bounds the numerator and the denominator, so there are only finitely many choices for x. Given x, we have ≤ 2 choices for y. ○

We need to show that $\widehat{h}$ is a quadratic form.

Lecture 19: March 1

Examples class: Friday March 8, 2:30 PM

Recall the naive height was $h(P) = \log H(P)$, where $H : (x, y) \mapsto \max(|r|, |s|)$ where $x = \frac{r}{s}$ and r, s are coprime integers. The canonical height was $\widehat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$.

By Lemma 12.4, $\widehat{h}(nP) = n^2 \widehat{h}(P)$.

Lemma 19.1. *(12.6) Let E be an elliptic curve over $\mathbb{Q}$. Then there is some constant c such that*

$$H(P+Q)H(P-Q) \le c \cdot H(P)^2 H(Q)^2$$

for all $P, Q \in E(\mathbb{Q})$ such that $P, Q, P-Q, P+Q \neq 0_E$.

Proof. Write $P = (\xi_1, \eta_1)$, $Q = (\xi_2, \eta_2)$, $P+Q = (\xi_3, \eta_3)$, $P-Q = (\xi_4, \eta_4)$. Write $\xi_i = \frac{r_i}{s_i}$ for coprime r_i, s_i. See the proof of Lemma 5.7.

$$(s_3s_4 : r_3r_4 + r_4s_3 : r_3r_4) = (W_0 : W_1 : W_2)$$

where $W_0 = (r_1s_2 - r_2s_1)^2$. W_0, W_1, W_2 each have degree 2 in r_1, s_1 and have degree 2 in r_2, s_2.

$$\begin{aligned} H(P+Q)H(P-Q) &= \max(|r_3|, |s_3|)\max(|r_4|, |s_4|) \\ &\le 2\max(|r_3r_4|, |r_3s_4 + r_4s_3|, |s_3s_4|) \\ &\le 2\max(|W_0|, |W_1|, |W_2|) \\ &\le c \cdot H(P)^2 H(Q)^2 \end{aligned}$$

There are a bunch of cases to check to prove the first inequality, depending on what $\max(|r_3|, |s_3|)$, etc., is. ○

Theorem 19.2. *(12.7) $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\ge 0}$ is a quadratic form.*

Proof. Take logs in Lemma 12.6 to obtain

$$h(P+Q) + h(P-Q) \le 2h(P) + 2h(Q) + c'$$

if $P, Q, P+Q, P-Q \neq 0$. But if $P - Q = 0$, then this still holds, because $|h(2P) - 4h(P)|$ is bounded.

Replace P and Q by 2^nP and 2^nQ and divide by 4^n. Take the limit to get

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) \le 2\widehat{h}(P) + 2\widehat{h}(Q)$$

Replacing P and Q by $P+Q$ and $P-Q$, and using the fact that $\widehat{h}(2P) = 4\widehat{h}(P)$ we get the reverse inequality.

$\widehat{h}$ satisfies the parallelogram law, and hence (by Example sheet 2), $\widehat{h}$ is a quadratic form. ○

Remark 19.3. The theory extends to arbitrary number fields. But, you need to modify the definition of height since $\mathcal{O}_K$ need not be a UFD. For $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(K)$, define $H(P) = \prod_v \max_{0 \le i \le n} |x_i|_v$ where the product is taken over places of the number field. This is well-defined, since $\prod_v |\lambda|_v = 1$ for all $\lambda \in K^*$ (so multiplying all the x_i by λ doesn't affect $H(P)$).

Chapter 13: Dual isogenies and the Weil pairing

Let K be a perfect field (every finite extension is separable, hence has a Galois closure). Fields of characteristic 0, and finite fields, are all perfect.

Proposition 19.4. *(13.1) Let $\Phi \subset E(\overline{K})$ be a finite, $\mathrm{Gal}(\overline{K}/K)$-stable subgroup. Then there exists an elliptic curve E'/K and a separable isogeny $\varphi : E \to E'$ defined over K with kernel Φ such that every isogeny $\psi : E \to E''$ with $\Phi \subset \ker\psi$ factors uniquely via φ.*

$$\begin{tikzcd}
E \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & E'' \\
& E' \arrow[ur, dashed, "\exists!"'] &
\end{tikzcd}$$

Proof. Omitted. The basic idea is to form $E' = E/\Phi$ with function field $K(E)^{\Phi}$. ($P \in \Phi$ acts on the function field via τ_P^*, where $\tau_P : E \to E$ is translation by P.) ○

To define the dual isogeny I think you need a stronger statement:

Proposition 19.5. *Let $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be nonconstant isogenies, and assume that φ is separable. If $\ker\varphi \subset \ker\psi$ then there is a unique isogeny $\lambda : E_2 \to E_3$ satisfying $\psi = \lambda \circ \varphi$.*

$$\begin{tikzcd}
E_1 \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & E_3 \\
& E_2 \arrow[ur, dashed, "\exists!"'] &
\end{tikzcd}$$

Proof. See Silverman, III.4.11. ○

Proposition/ Definition 19.6. (13.2) $\varphi : E \to E'$ is an isogeny of degree n. Then there exists a unique isogeny $\widehat{\varphi} : E' \to E$, called the *dual isogeny*, such that $\widehat{\varphi} \circ \varphi = [n]$.

Proof. Case 1: φ is separable. $|\ker\varphi| = \deg\varphi = n$; so everything in the kernel has degree dividing n, and is hence contained in $\ker[n]$. Then apply Proposition 19.5 with $\psi = [n]$.

Case 2: φ inseparable. Omitted. Read Silverman.

But we can check uniqueness. Suppose ψ_1 and ψ_2 are candidates: $\psi_1 \circ \varphi = \psi_2 \circ \varphi$. So $(\psi_1 - \psi_2) \circ \varphi = 0$. Taking degrees shows that $\varphi_1 = \varphi_2$. ○

Remark 19.7.
(1) $\deg[n] = n^2$, so $\deg\varphi = \deg\widehat{\varphi}$. In particular, $\widehat{[n]} = [n]$.
(2) $\varphi\widehat{\varphi}\varphi = \varphi \circ [n]_E = [n]_{E'} \circ \varphi$ *(second equality because φ is a homomorphism)*, which shows that $\varphi\widehat{\varphi} = [n]_{E'}$. In particular, $\widehat{\widehat{\varphi}} = \varphi$.
(3) If $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$ it can be shown that $\widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}$. Proving this gives another way to show that $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form.
(4) "Being isogenous" is an equivalence relation.

Definition 19.8. Define

$$\mathrm{sum} : \mathrm{Div}\, E \to E$$

$$\underbrace{\sum n_p \cdot P}_{\text{formal sum}} \mapsto \underbrace{\sum n_p P}_{\text{add using group law}}$$

Recall there is an isomorphism $\varphi : E \overset{\cong}{\to} \mathrm{Pic}^0(E)$ given by $P \mapsto [P-0]$. Since $\varphi(P \oplus Q) = \varphi(P)+\varphi(Q)$ (5.5), the composition $\mathrm{Div}^0 E \xrightarrow{sum} E \xrightarrow{\varphi} \mathrm{Pic}^0(E)$ takes $P-Q \mapsto P \oplus (-Q) \mapsto \varphi(P \oplus (-Q)) = \varphi(P) - \varphi(Q) = [P-0] - [Q-0] = [P-Q]$. In general, $D \mapsto [D]$. This immediately proves:

Lemma 19.9. *(13.3) Let $D \in \mathrm{Div}^0(E)$. Then $D \sim 0$ iff $\mathrm{sum}(D) = 0_E$.*

Lecture 20: March 4

If $\varphi : E \to E'$ is an isogeny, then there is an induced map $\varphi^* : \mathrm{Div}\, E' \to \mathrm{Div}\, E$, where $\varphi^* P = \sum_{\varphi(Q)=P} Q$.

Let $\varphi : E \to E'$ be an isogeny of degree n, and let $\widehat{\varphi} : E' \to E$ be the dual isogeny. Assume $\mathrm{char}\, K \nmid n$. We will define the Weil pairing

$$E[\varphi] \times E'[\widehat{\varphi}] \to \mu_n$$

(where $E[\varphi] := \ker \varphi$). Let $T \in E'[\widehat{\varphi}]$. Then $T \in \ker \varphi\widehat{\varphi} = \ker[n]$ so $nT = 0$. Apply Lemma 13.3 to $n \cdot T - n \cdot 0$ to obtain some $f \in \overline{K}(E')^*$ such that $\mathrm{div}\, f = n \cdot T - n \cdot 0$.

Pick $T_0 \in E(\overline{K})$ with $\varphi(T_0) = T$. Then

$$\varphi^*(T) - \varphi^*(0_{E'}) = \sum_{P \in E[\varphi]} (P \oplus T_0) - \sum_{P \in E[\varphi]} (P)$$

has sum $nT_0 = \widehat{\varphi}\varphi T_0 = \widehat{\varphi} T = 0$. So there exists $g \in \overline{K}(E)^*$ such that $\mathrm{div}(g) = \varphi^*(T) - \varphi^*(0)$.

Now

$$\begin{aligned}\mathrm{div}\, \varphi^* f = \varphi^* \mathrm{div}\, f &= n(\varphi^* T - \varphi^* 0) \\ &= n\, \mathrm{div}\, g = \mathrm{div}\, g^n\end{aligned}$$

so $\varphi^* f = cg^n$ for some constant $c \in \overline{K}^*$ (two functions that have the same divisor are the same up to multiplication by nonzero constant). Rescale f, so we can assume $c = 1$. Now

$$\varphi^* f = g^n.$$

If $S \in E[\varphi]$ then

$$\begin{aligned}\mathrm{div}\, \tau_S^* g &= \tau_S^* \mathrm{div}\, g \\ &= \tau_S^* \big(\sum_{P \in E[\varphi]} (T_0 \oplus P) + \sum_{P \in E[\varphi]} P\big) \\ &= \sum \tau_S^*(T_0 \oplus P) - \sum \tau_S^* P\end{aligned}$$

$$\begin{aligned}&= \sum T_0 \oplus P \ominus S - \sum P \ominus S \\ &= \sum T_0 \oplus P - \sum P = \operatorname{div} g\end{aligned}$$

since $S \in E[\varphi]$ (and so $-S \in E[\varphi]$) so adding $-S$ just permutes the P's. This implies $\tau_S^* g = \zeta g$ for some $\zeta \in \overline{K}^*$. Equivalently,

$$\zeta = \frac{g(X \oplus S)}{g(X)}$$

is independent of the choice of $X \in E(\overline{K})$. Now

$$\zeta^n = \frac{g(X \oplus S)^n}{g(X)^n} = \frac{f \circ \varphi(X \oplus S)}{f \circ \varphi(X)} = \frac{f \circ \varphi(X)}{f \circ \varphi(X)} = 1.$$

So $\zeta \in \mu_n$.

Define $e_\varphi(S, T) = \frac{g(X+S)}{g(X)}$.

Proposition 20.1. *e_φ is bilinear and nondegenerate.*

Proof. Linearity in the first argument:

$$\begin{aligned}e_\varphi(S_1 + S_2, T) &= \frac{g(X + S_1 + S_2)}{g(X + S_2)} \cdot \frac{g(X + S_2)}{g(X)} \\ &= e_\varphi(S_1, T) \cdot e_\varphi(S_2, T)\end{aligned}$$

Linearity in the second argument: Let $T_1, T_2 \in E'[\widehat{\varphi}]$. Find f_1, f_2 such that $\operatorname{div}(f_i) = n(T_i) - n(0)$ and $\varphi^* f_i = g_i^n$ for $i = 1, 2$.

There exists $h \in \overline{K}(E')^*$ such that

$$\operatorname{div} h = (T_1) + (T_2) - (T_1 \oplus T_2) - (0)$$

Now put $f = \frac{f_1 f_2}{h^n}$, $g = \frac{g_1 g_2}{\varphi^* h}$. Then

$$\operatorname{div} f = n(T_1 + T_2) - n(0)$$

and

$$\varphi^* f = \frac{(\varphi^* f_1)(\varphi^* f_2)}{(\varphi^* h)^n} = \frac{g_1^n g_2^n}{\varphi^*(h)^n} = g^n.$$

So

$$\begin{aligned}e_\varphi(S, T_1 + T_2) &= \frac{g(X + S)}{g(X)} \\ &= \frac{g_1(X + S)}{g_1(X)} \cdot \frac{g_2(X + S)}{g_2(X)} \cdot \underbrace{\frac{h(\varphi(X))}{h(\varphi(X + S))}}_{1} \\ &= e_\varphi(S, T_1) e_\varphi(S, T_2)\end{aligned}$$

e_φ nondegenerate: Fix $T \in E'[\widehat{\varphi}]$. Suppose $e_\varphi(S, T) = 1$ for all $S \in E[\varphi]$. Then, by definition of ζ, $\tau_S^* g = g$ for all $S \in E[\varphi]$.

We have a field extension $\overline{K}(E)/\varphi^*\overline{K}(E')$; this is a Galois extension with group $E[\varphi]$. Since g is fixed by everything in the Galois group, we have $g \in \varphi^*\overline{K}(E')$; that is, $g = \varphi^* h$ for some $h \in \overline{K}(E')$.

We had $\varphi^* f = g^n = (\varphi^* h)^n$, which shows $f = h^n$. So $\operatorname{div} h = (T) - (0)$; principal divisors have degree zero and sum to zero, and that can only happen if $T = 0$.

We've shown that there is an inclusion $E'[\widehat{\varphi}] \hookrightarrow \operatorname{Hom}(E[\varphi], \mu_n)$. Since $n = \deg \varphi = \deg \widehat{\varphi}$, this is an isomorphism. Non-degeneracy on the right follows by group theory. ○

Lemma 20.2. *(13.5) If E, E', φ are defined over K, then the Weil pairing is Galois-equivariant. That is,*

$$e_\varphi(\sigma S, \sigma T) = \sigma(e_\varphi(S, T))$$

for all $S \in E[\varphi]$, $T \in E'[\widehat{\varphi}]$, $\sigma \in \operatorname{Gal}(\overline{K}/K)$.

Proof. $\operatorname{div} f = n(T) - n(0)$ and $\operatorname{div}(\sigma(f)) = n(\sigma T) - n(0)$ (σ fixes zero). From the definition, $\varphi^* f = g^n$, so $\varphi^*(\sigma f) = (\sigma g)^n$.

$$\begin{aligned} e_\varphi(\sigma S, \sigma T) &= \frac{(\sigma g)(\sigma X + \sigma S)}{(\sigma g)(\sigma X)} \\ &= \sigma\left(\frac{g(X+S)}{g(X)}\right) = \sigma(e_\varphi(S, T)) \end{aligned}$$

○

Taking $\varphi = [n] : E \to E$, we have $\widehat{\varphi} = [n]$, and the Weil pairing is a map $e_n : E[n] \times E[n] \to \mu_{n^2}$. But by the previous two lemmas, the image is actually in μ_n (everything is killed by multiplication by n).

Corollary 20.3. *If $E[n](K) = E[n](\overline{K})$ then $\mu_n \subset K$.*

Proof. Let S, T be a basis for $E[n](\overline{K}) \cong (\mathbb{Z}/n\mathbb{Z})^2$. By the non-degeneracy of e_n, $e_n(S, T) = \zeta_n$ is a primitive n^{th} root of unity. For $\sigma \in \operatorname{Gal}(\overline{K}/K)$,

$$\begin{aligned} \sigma(\zeta_n) &= \sigma(e_n(S, T)) \\ &= e_n(\sigma S, \sigma T) \\ &= e_n(S, T) = \zeta_n \end{aligned}$$

and so $\zeta_n \in K$. ○

Example 20.4. There is no elliptic curve E over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Proposition 20.5 (Properties of the Weil Pairing).

(1) *(Alternating) $e_n(T, T) = 1$ for all $T \in E[n]$ (and that implies $e_n(S, T) = e_n(T, S)^{-1}$).*

(2) *Dual isogenies are adjoints with respect to e_n: that is, if $\varphi : E \to E'$ and $\widehat{\varphi} : E' \to E$, then $e_n(\varphi S, T) = e_n(S, \widehat{\varphi} T)$ for all $S \in E[n]$, $T \in E'[n]$.*

(3) *(Compatibility) $e_{mn}(S, T) = e_m(nS, T)$ for all $S \in E[mn]$, $T \in E[m]$.*

Proposition 20.6. *(13.7) An endomorphism φ of E induces an endomorphism $\varphi_n \in \operatorname{End} E[n] \cong \operatorname{Mat}_2(\mathbb{Z}/n\mathbb{Z})$.*

Then $\deg\varphi \equiv \det\varphi_n \pmod{n}$.

Proof. Let S, T be a basis for $E[n]$. We can write $\varphi(S) = aS + cT$, $\varphi(T) = bS + dT$, so φ_n is the matrix $\varphi_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (for $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$). Since the Weil pairing is non-degenerate, $e_n(S, T) = \zeta_n$ is a primitive n^{th} root of unity.

$$\begin{aligned} \zeta_n^{\deg\varphi} &= e_n((\deg\varphi)S, T) \\ &= e_n(\widehat{\varphi}\varphi S, T) \\ &= e_n(\varphi S, \varphi T) && \text{adjoint property} \\ &= e_n(aS + cT, bS + dT) \\ &= e_n(S, T)^{ad-bc} = \zeta_n^{ad-bc} \end{aligned}$$

ζ_n is a primitive n^{th} root of unity, and

$$\deg\varphi \equiv ad - bc \equiv \det\varphi_n \pmod{n}.$$

○

Lecture 21: March 6

Let ℓ be prime. The Tate module $T_\ell(E)$ is the inverse limit of the following sequence

$$\cdots \to E[\ell^3] \overset{\times\ell}{\to} E[\ell^2] \overset{-\times\ell}{\to} E[\ell].$$

Then $T_\ell(E) \cong \mathbb{Z}_\ell^2$. The morphism of *End* modules in Proposition 13.7 induces a morphism

$$\begin{aligned} \operatorname{End}(E) &\to \operatorname{End}(T_\ell(E)) \cong \operatorname{Mat}_2(\mathbb{Z}_\ell) \\ \varphi &\mapsto \varphi_\ell \end{aligned}$$

where $\deg\varphi = \det\varphi_\ell$.

Chapter 14: Galois cohomology

Let G be a group, and A a G-module: an abelian group with G acting on A via a group homomorphism. (Note that a G-module is the same thing as a $\mathbb{Z}[G]$-module, where $\mathbb{Z}[G]$ is the group ring.)

Definition 21.1. $H^0(G, A) = A^G = \{a \in A : \sigma(a) = a \ \forall\sigma \in G\}$

The set of "cochains" is $C^1(G, A) = \{\mathit{maps}\ G \to A\}$; this is an abelian group.

The set of cocycles is $Z^1(G, A) = \{(a_\sigma)_{\sigma\in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma \ \forall\sigma, \tau \in G\}$.

Inside this is the set of coboundaries: $B^1(G,A) = \{(\sigma b - b)_{\sigma\in G} : b \in A\}$.

Define

$$H^1(G,A) = \frac{Z^1(G,A)}{B^1(G,A)}.$$

For example, if the action of G on A is trivial, $H^1(G,A)$ is the set of group homomorphisms $G \to A$.

Theorem 21.2. *A short exact sequence of G-modules*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

gives rise to a long exact sequence

$$0 \to A^G \xrightarrow{f} B^G \xrightarrow{g} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{f_*} H^1(G,B) \xrightarrow{g_*} H^1(G,C).$$

Proof. Omitted (a long list of things to check).

Comment – definition of δ: Let $c \in C^G$. Since g is surjective, there is $b \in B$ such that $g(b) = c$. Then $g(\sigma b - b) = \sigma c - c = 0$ for all $\sigma \in G$. Since $\sigma b - b$ is in the kernel of g, it is in the image of f: $\sigma b - b = f(a_\sigma)$ for some $a_\sigma \in A$. You can check that $(a_\sigma)_{\sigma\in G} \in Z^1(G,A)$.

We define $\delta(c)$ to be the class of $(a_\sigma)_{\sigma\in G}$ in $H^1(G,A)$. You still need to check a lot of things, including the fact that $\delta(c)$ is well-defined (what happens if you choose a different preimage b?). ○

Theorem 21.3. *(14.2) Let A be a G-module, and $H \lhd G$ a normal subgroup. There is an* inflation-restriction exact sequence*:*

$$0 \to H^1(G/H, A^H) \xrightarrow{inf} H^1(G,A) \xrightarrow{res} H^1(H,A)$$

Proof. Lots more checking. ○

Let K be a perfect field. $\mathrm{Gal}(\overline{K}/K)$ is a topological group with basis of open subgroups $\mathrm{Gal}(\overline{K}/L)$ for $[L:K] < \infty$. If $G = \mathrm{Gal}(\overline{K}/K)$ we modify the definition of $H^1(G,A)$ by insisting:

(1) the stabilizer of each $a \in A$ is open in G;
(2) all cochains $G \to A$ are continuous when A is given the discrete topology.

Then $H^1(\mathrm{Gal}(\overline{K}/K), A) = \varinjlim_L H^1(\mathrm{Gal}(L,K), A^{\mathrm{Gal}(\overline{K}/L)})$ where the direct limit is taken over all *finite* Galois extensions L/K, with respect to the inflation maps.

Theorem 21.4 (Hilbert's Theorem 90). *(14.3) Let L/K be a finite Galois extension. Then $H^1(\mathrm{Gal}(L/K), L^*) = 0$.*
Given a cycle (a_σ), $\sum_\tau a_\tau^{-1}\tau$ is not the zero operator (linear independence of τ's). So find nonzero $x = \sum_\tau a_\tau^{-1}\tau(y)$ and compute $\sigma(x)$ to show it's a boundary.

Proof. Let $G = \mathrm{Gal}(L/K)$, and let $(a_\sigma) \in Z^1(G, L^*)$. Use the fact that distinct automorphisms are linearly independent. Then there is some $y \in L$ such that $x := \sum_{\tau\in G} a_\tau^{-1}\tau(y) \neq 0$. Then

$$\begin{aligned}\sigma(x) &= \sum_{\tau\in G}\sigma(a_\tau)^{-1}\sigma\tau(y)\\ &= a_\sigma\sum_{\tau\in G}a_{\sigma\tau}^{-1}\sigma\tau(y) && \text{defn. cocycle}\\ &= a_\sigma x.\end{aligned}$$

So $a_\sigma = \frac{\sigma(x)}{x}$, and our original cocycle (a_σ) was a coboundary. Thus H^1 is trivial. ○

COROLLARY 21.5. $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$.

APPLICATION 21.6. Assume char $K \nmid n$. There is an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to \mu_n \to \overline{K}^* \xrightarrow{x\mapsto x^n} \overline{K}^* \to 0.$$

This gives a long exact sequence

$$\cdots \to K^* \to K^* \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \to \underbrace{H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*)}_{\substack{0\\ \text{by } 14.3}} \to \cdots$$

Therefore, $H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n$.

If $\mu_n \subset K$ (as we assumed in the Kummer theory section), *then* $\mathrm{Gal}(\overline{K}/K)$ *acts trivially on* μ_n*, so [continuous] cycles are just [continuous] group homomorphisms and there are no nontrivial coboundaries. Thus we can write the previous isomorphism as*

$$\mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n.$$

Continuous homomorphisms here are the ones that factor through some finite Galois extension. Note that the finite subgroups of $\mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n)$ are of the form $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ where L/K is a finite abelian extension of exponent dividing n. (This recovers Proposition 10.2.)

NOTATION 21.7. To reduce annoyance, write $H^1(K, -)$ to mean $H^1(\mathrm{Gal}(\overline{K}/K), -)$.

Let $\varphi : E \to E'$ be an isogeny of elliptic curves over K. This induces an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to E[\varphi] \to E \to E' \to 0.$$

The long exact sequence is

$$\cdots \to E(K) \xrightarrow{\varphi} E'(K) \xrightarrow{\delta} H^1(K, E[\varphi]) \to H^1(K, E) \xrightarrow{\varphi_*} H^1(K, E')$$

which we can rearrange into a short exact sequence

$$0 \to E'/\varphi E(K) \to H^1(K, E[\varphi]) \to H^1(K, E)[\varphi_*] \to 0$$

(where $X[f]$ means "kernel of f in X" as before).

Now take a number field K. Let

$$M_K = \{\text{places of } K\} = \{\text{finte places}\} \cup \{\text{infinite places}\}$$

where finite places correspond to primes $\mathfrak{P} \subset \mathcal{O}_K$, and the infinite places correspond to real, and complex conjugate pairs, of embeddings $K \hookrightarrow \mathbb{C}$.

For $v \in M_K$, let K_v be the completion w.r.t. the v-adic topology. Now fix an embedding $\overline{K} \subset \overline{K}_v$; then $\mathrm{Gal}(\overline{K}_v/K_v) \subset \mathrm{Gal}(\overline{K}/K)$. We have

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\varphi E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\varphi]) \arrow[r] \arrow[d, "res_v"] \arrow[dr, dotted] & H^1(K, E)[\varphi_*] \arrow[r] \arrow[d, "res_v"] & 0 \\
0 \arrow[r] & E'(K_v)/\varphi E(K_v) \arrow[r, "\delta_v"] & H^1(K_v, E[\varphi]) \arrow[r] & H^1(K_v, E)[\varphi_*] \arrow[r] & 0
\end{tikzcd}$$

Lecture 22: March 8

We consider the kernel of the dotted arrow in the diagram at the end of the last lecture.

Definition 22.1. Define the φ-Selmer group to be

$$S^{(\varphi)}(E/K) = \ker\Big(H^1(K, E[\varphi]) \to \textstyle\prod_{v \in M_K} H^1(K_v, E)\Big).$$

This is the kernel of the diagonal map above, and (because the rows are exact), this can be rewritten

$$\{x \in H^1(K, E[\varphi]) \,:\, res_v(x) \in \mathrm{im}(\delta_v)\ \forall v\}.$$

Define the Tate-Shafarevich group to be

$$Ш(E/K) = \ker(H^1(K, E) \to \prod_{v \in M_K} H^1(K_v, E)).$$

We get a short exact sequence

$$0 \to E'(K)/\varphi E(K) \to S^{(\varphi)}(E/K) \to Ш(E/K)[\varphi_*] \to 0$$

and if we take $\varphi = [n] : E \to E$, this is

$$0 \to E(K)/nE(K) \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0. \tag{22.1}$$

We saw that computing ranks of elliptic curves is equivalent to computing $E(K)/nE(K)$, and it turns out that there is a finite and efficient algorithm for computing $S^{(n)}(E/K)$; so you can get an upper bound for the rank, but the problem is Ш.

Conjecture 22.2. $Ш(E/K)$ is finite.

If this is true, then it turns out that the rank of $E(K)$ is effectively computable.

Definition 22.3. For a finite set $S \subset M_K$ of places containing all the infinite places we define

$$H^1(K, A; S) = \ker\big(H^1(K, A) \to \textstyle\prod_{v \notin S} H^1(K_v^{nr}, A)\big)$$

where K_v^{nr} is the maximal unramified extension of K_v.

Remark 22.4. $\mathrm{Gal}(\overline{K}_v/K_v)$ is the decomposition group; it is defined only up to conjugacy, due to the choice involved in embedding it in $\mathrm{Gal}(\overline{K}/K)$. Inside this we have the inertia group $\mathrm{Gal}(\overline{K}_v/K_v^{nr})$.

The proof of weak Mordell-Weil can be rephrased in the following steps:

(1) Show $S^{(n)}(E/K) \subset H^1(K, E[n]; S)$ where
$$S = \{ \text{ primes of bad reduction for } E\} \cup \{v \mid n\} \cup \{\text{infinite places}\}.$$
(2) Show $H^1(K, E[n]; S)$ is finite.
(3) Conclude from (22.1) that $|E(K)/nE(K)| < \infty$.

Proof of (1). Let $v \notin S$. There is a commutative diagram with exact rows

$$\begin{tikzcd}
\cdots \arrow[r] & E(K_v) \arrow[r, "\times n"] \arrow[d, hook] & E(K_v) \arrow[r, "\delta_v"] \arrow[d, hook] & H^1(K_v, E[n]) \arrow[r] \arrow[d, "res"] & \cdots \\
\cdots \arrow[r] & E(K_v^{nr}) \arrow[r, "\times n"] & E(K_v^{nr}) \arrow[r, "\alpha"] & H^1(K_v^{nr}, E[n]) \arrow[r] & \cdots
\end{tikzcd}$$

The multiplication by n map on the bottom row is surjective by Proposition 8.9 (and the choice of S). So $\alpha = 0$. Do a diagram chase to show that $\mathrm{im}(\delta_v) \subset \ker(res)$. ○

Proof of (2). By inflation-restriction, we can replace K by a finite Galois extension. So without loss of generality $\mu_n \subset K$ and $E[n] \subset E(K)$. Then $E[n] \cong \mu_n \times \mu_n$ as $\mathrm{Gal}(\overline{K}/K)$-modules. So
$$H^1(K, E[n]; S) \cong H^1(K, \mu_n; S)^2.$$
By Application 21.6 of Hilbert's Theorem 90,
$$H^1(K, \mu_n) \cong K^*/(K^*)^n$$
and the image of $H^1(K, \mu_n; S) \subset H^1(K, \mu_n)$ is contained in $K(S, n)$, hence finite.

○

Chapter 15: Descent by cyclic isogeny

Let E, E' be elliptic curves over a number field K. Let $\varphi : E \to E'$ be an isogeny of degree n. Suppose $E'[\widehat{\varphi}] = \mathbb{Z}/n\mathbb{Z}$ is generated by $T \in E'(K)$. Then
$$\begin{aligned} E[\varphi] &\to \mu_n \\ S &\mapsto e_\varphi(S, T) \end{aligned}$$
is an isomorphism as $\mathrm{Gal}(\overline{K}/K)$-modules. We have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules
$$0 \to \mu_n \to E \xrightarrow{\varphi} E' \to 0$$
which gives rise to a long exact sequence
$$\cdots \to E(K) \xrightarrow{\varphi} E'(K) \xrightarrow{\delta} H^1(K, \mu_n) \to H^1(K, E)$$

By Application 21.6 of Hilbert's Theorem 90, $H^1(K,\mu_n) \cong K^*/(K^*)^n$. Let's study the map $\alpha : E'(K) \to K^*/(K^*)^n$, defined to be the composite of δ with the isomorphism in Application 21.6.

Theorem 22.5. *(15.1) Let $f \in K(E')$ and $g \in K(E)$ with $\operatorname{div} f = n(T) - n(0)$, and $\varphi^* f = g^n$. (We can pick f, g defined over K because $T \in E'(K)$.) Then $\alpha(P) = f(P) \pmod{(K^*)^n}$ for all $P \in E'(K) \backslash \{0, T\}$.*

Proof. Let $Q \in E(\overline{K})$ with $\varphi(Q) = P$ (since φ was surjective). Then $\delta(P)$ is represented by the cocycle $\sigma \mapsto \sigma Q - Q \in E[\varphi] \cong \mu_n$. By the definition of the Weil pairing,

$$e_\varphi(\sigma Q - Q, T) = \frac{g(\sigma Q - Q + X)}{g(X)}$$

for any $X \in E[\overline{K}]$ (excluding the zeroes and poles of g). Take $X = Q$:

$$= \frac{g(\sigma Q)}{g(Q)} = \frac{\sigma(g(Q))}{g(Q)}$$
$$= \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}}$$

since $\varphi(Q) = P$ and $\varphi^* f = g^n$

We had an isomorphism

$$K^*/(K^*)^n \overset{\cong}{\to} H^1(K,\mu_n)$$
$$x \mapsto \left(\frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}}\right)_\sigma .$$

Therefore, $\alpha(P) = f(P) \pmod{(K^*)^n}$. ○

Lecture 23: March 11

Descent by 2-isogeny. Consider

$$E : y^2 = x^3 + ax^2 + bx$$
$$E' : y^2 = x^3 + a'x^2 + b'x$$

where $a' = -2a, b' = a^2 - 4b$. You can check that the following 2-isogenies are dual:

$$\varphi : E \to E', \qquad (x,y) \mapsto \left(\left(\tfrac{y}{x}\right)^2, \tfrac{y(x^2-b)}{x^2}\right)$$
$$\widehat{\varphi} : E' \to E, \qquad (x,y) \mapsto \left(\left(\tfrac{y}{2x}\right)^2, \tfrac{y(x^2-b')}{8x^2}\right).$$

Let $T = (0,0) \in E(K)$ and $T' = (0,0) \in E'(K)$. We have $E[\varphi] = \{0, T\}$ and $E[\widehat{\varphi}] = \{0, T'\}$.

Proposition 23.1. *(15.2) There is a group homomorphism*

$$\begin{aligned} \alpha : E'(K) &\to K^*/(K^*)^2 \\ (x,y) &\mapsto \begin{cases} x \pmod{(K^*)^2} & \text{if } x \neq 0 \\ b' \pmod{(K^*)^2} & \text{if } x = 0 \end{cases} \end{aligned}$$

with kernel $\varphi(E(K))$.

Proof. Either apply Theorem 15.1 with $f = x \in K(E')$ and $g = \frac{y}{x} \in K(E)$, or use direct calculation (see problem sheet). ○

We'd like to study the following maps

$$\begin{aligned} \alpha_E &: E(K)/\widehat{\varphi}E'(K) \hookrightarrow K^*/(K^*)^2 \\ \alpha_{E'} &: E'(K)/\varphi E(K) \hookrightarrow K^*/(K^*)^2 \end{aligned}$$

Lemma 23.2. *(15.3)*

$$2^{\operatorname{rank} E(K)} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4}$$

Proof. Since $\widehat{\varphi}\varphi = [2]_E$ and $\varphi\widehat{\varphi} = [2]_{E'}$ there is an exact sequence

$$0 \to \underbrace{E(K)[\varphi]}_{\mathbb{Z}/2\mathbb{Z}} \to E(K)[2] \xrightarrow{\varphi} \underbrace{E'(K)[\widehat{\varphi}]}_{\mathbb{Z}/2\mathbb{Z}}$$

$$\to \underbrace{E'(K)/\varphi E(K)}_{\operatorname{im}\alpha_{E'}} \xrightarrow{\widehat{\varphi}} E(K)/2E(K) \to \underbrace{E(K)/\widehat{\varphi}E'(K)}_{\operatorname{im}\alpha_E} \to 0$$

Then

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{|\mathbb{Z}/2\mathbb{Z}| \cdot |\mathbb{Z}/2\mathbb{Z}|}$$

By the Mordell-Weil theorem, $E(K) \cong \Delta \times \mathbb{Z}^r$ where Δ is finite and $r \geq 0$. Then

$$E(K)/2E(K) \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r.$$

But also

$$E(K)[2] \cong \Delta[2].$$

Since Δ is finite, $\Delta/2\Delta$ and $\Delta[2]$ have the same order. Taking orders and dividing, we have

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r$$

○

Lemma 23.3. *(15.4) Assume K is a number field, and $a, b \in \mathcal{O}_K$. Then $\operatorname{im}\alpha_E \subset K(S,2)$ where $S = \{$primes dividing $b\}$.*

Proof. We must show that if $x, y \in K$ with $y^2 = x(x^2 + ax + b)$ and $\mathfrak{P}$ a prime of K with $\operatorname{ord}_{\mathfrak{P}}(b) = 0$, then $\operatorname{ord}_{\mathfrak{P}}(x)$ is even.

Case 1: $\operatorname{ord}_{\mathfrak{P}}(x) < 0$. By Lemma 8.1, $\operatorname{ord}_{\mathfrak{P}}(x) = -2r$ and $\operatorname{ord}_{\mathfrak{P}}(y) = -3r$ for some $r \geq 1$. In particular, $\operatorname{ord}_{\mathfrak{P}}(x)$ is even, so we're done.

Case 2: $\operatorname{ord}_{\mathfrak{P}}(x) = 0$. Done.

Case 3: $\operatorname{ord}_{\mathfrak{P}}(x) > 0$. Then $\operatorname{ord}_{\mathfrak{P}}(x^2+ax+b) = 0$. Then $\operatorname{ord}_{\mathfrak{P}}(x) = \operatorname{ord}_{\mathfrak{P}}(y^2) = 2\operatorname{ord}_{\mathfrak{P}}(y)$. ○

Lemma 23.4. *(15.5) If $b_1 b_2 = b$ then $b_1(K^*)^2 \in \operatorname{im}\alpha_E$ iff*

$$w^2 = b_1u^4 + au^2v^2 + b_2v^4 \tag{23.1}$$

is soluble for $u, v, w \in K$ not all zero.

Proof. If $b_1 \in (K^*)^2$ or $b_2 \in (K^*)^2$ then both conditions are satisfied *(in this case $b_1 = b$ up to squares, and b is in the image of E since $\alpha_E(T) = b \pmod{(K^*)^2}$)*. So we may assume $b_1 \notin (K^*)^2$, $b_2 \notin (K^*)^2$. Then

$$\begin{aligned} b_1(K^*)^2 \in \operatorname{im}\alpha_E &\iff \exists (x,y) \in E(K) \text{ s.t. } x = b_1t^2 \text{ for some } t \in K^* \\ &\implies y^2 = b_1t^2((b_1t^2)^2 + ab_1t^2 + b) \\ &\implies \left(\frac{y}{b_1t}\right)^2 = b_1t^4 + at^2 + b_2 \end{aligned}$$

So (23.1) has solution $u = t, v = 1, w = \frac{y}{b_1t}$.

Conversely, if (u, v, w) is a solution to (23.1), then $uv \neq 0$ and

$$(b_1\left(\frac{u}{v}\right)^2, b_1\left(\frac{uw}{v^3}\right)) \in E(K)$$

is a rational point whose x-coordinate is b_1 (up to the square of something). ○

Now take $K = \mathbb{Q}$.

Example 23.5. Recall the elliptic curve from the first lecture:

$$E : y^2 = x^3 - x.$$

We showed that this has no solution, i.e. $\operatorname{rank} E(\mathbb{Q}) = 0$. Let's do this with different methods. Here $a = 0$ and $b = -1$ and

$$\operatorname{im}\alpha_E \subset \langle -1 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

But $-1 \in \operatorname{im}\alpha_E$, so $\operatorname{im}\alpha_E = \langle -1 \rangle$. Consider

$$E' : y^2 = x^3 + 4x.$$

Now $b = 4$, and $\operatorname{im}\alpha_{E'} \subset \langle -1, 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. The subgroup $\langle -1, 2 \rangle$ has three nontrivial elements $b_1 = -1, 2, -2$. To check if these are in $\operatorname{im}\alpha_{E'}$, we need to check if solutions exist for the following:

$$w^2 = -y^4 - 4v^4 \text{ insoluble over } \mathbb{R}$$

$$w^2 = 2u^4 + 2v^4 \text{ solution } u = v = 1, w = 2$$

$$w^2 = -2u^4 - 2v^4 \text{ insoluble over } \mathbb{R}$$

So $\operatorname{im}\alpha_{E'} = \langle 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$, and hence $E(\mathbb{Q}) = 0$ (as we discovered in the first lecture).

Example 23.6. Let p be a prime with $p \equiv 5 \pmod 8$. Consider $E : y^2 = x^3 + px$. To check if $b_1 = -1$ is in the image, check that $w^2 = -u^4 - pv^4$ is insoluble over $\mathbb{R}$. So $\operatorname{im}\alpha_E = \langle p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Now consider

$$E' : y^2 = x^3 - 4px.$$

Then $\operatorname{im}\alpha_{E'} \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Note $\alpha_{E'}(T') = (-p) \cdot (\mathbb{Q}^*)^2$. We have to check if $b_1 = 2, -2, p$ are in the image; that is, we have to find solutions for

$$w^2 = 2u^4 - 2pv^4 \tag{23.2}$$

$$w^2 = -2u^4 + 2pv^4 \tag{23.3}$$

$$w^2 = pu^4 - 4pv^4 \tag{23.4}$$

Suppose (23.2) is soluble; without loss of generality $u, v, w \in \mathbb{Z}$ and $\gcd(u, v) = 1$. IF $p \mid u$ then $p \mid w$ and $p \mid v$, which contradicts u, v being coprime. So $w^2 \equiv 2u^4 \not\equiv 0 \pmod p$. That is, $\left(\frac{2}{p}\right) = +1$ which contradicts the assumption that $p \equiv 5 \pmod 8$.

Likewise, (23.3) is insoluble since $\left(\frac{-2}{p}\right) = -1$. So, $\operatorname{im}\alpha_{E'} \subset \langle p, -1 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We don't know if the group has size 2 or 4, but we can say

$$\operatorname{rank} E(\mathbb{Q}) = \begin{cases} 0 & \text{if (23.4) is not soluble} \\ 1 & \text{otherwise} \end{cases}$$

Since $p \equiv 1 \pmod 4$ (we were assuming $p \equiv 5 \pmod 8$), then -1 is a square; hence it is a square in $\mathbb{Q}_p^*$, so -1 is a solution to (23.1) over $\mathbb{Q}_p$.

(23.4) is soluble over $\mathbb{Q}_2$ since $p - 4 \in (\mathbb{Q}_2^*)^2$, and is soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.

Conjecture: $\operatorname{rank} E(\mathbb{Q}) = 1$ for all $p \equiv 5 \pmod 8$. (This has been proven, under the assumption that Ш is finite.)

p	u	v	w
5	1	1	1
13	1	1	3
29	1	1	5
27	5	3	151
53	1	1	7

Lecture 24: March 13

Given an elliptic curve $E : y^2 = x^3 + ax^2 + bx$, we were looking for the image of $\alpha_E : E(\mathbb{Q})/\widehat{\varphi}E'(\mathbb{Q}) \hookrightarrow K^*/(K^*)^2$.

By Lemma 15.5, the Selmer group can be written

$$S^{(\widehat{\varphi})}(E'/\mathbb{Q}) = \{b_1(\mathbb{Q}^*)^2 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \,:\, (23.1) \text{ has solutions over } \mathbb{R} \text{ and all } \mathbb{Q}_p\}.$$

Fact 24.1. *If $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b(a^2-4b)$, then (23.1) is soluble over $\mathbb{Q}_p$. So you only have to check the primes dividing $2bb'$, where $b' = a^2-4b$.*

Example 24.2. Let $E : y^2 = x^3 + 17x$. Then $\operatorname{im}(\alpha_E) = \langle 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$$E' : y^2 = x^3 - 4 \cdot 17x$$

$\operatorname{im}(\alpha_{E'}) \subset \langle -1, 2, 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ We know that -17 is in the image, as is the identity. Let's check $b_1 = 2$. This corresponds to

$$w^2 = 2u^4 - 2 \cdot 17v^4$$

Replace w by $2w$ and divide through by 2:

$$C : 2w^2 = u^4 - 17v^4 \tag{24.1}$$

It turns out that (23.1) is a double cover of $\mathbb{P}^1$, ramified at 4 points. For a field K,

$$C(K) = \{(u,v,w) \in K^3 \backslash \{0\} \text{ satisfying } (24.1)\}/\sim$$

where $(u,v,w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for $\lambda \in K^*$.

$C(\mathbb{Q}_2) \neq \emptyset$ since $17 \in (\mathbb{Q}_2^*)^4$ (anything that is 1 mod 16 is a 4^{th} power by Hensel's lemma).

$C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in (\mathbb{Q}_{17}^*)^2$ (again by Hensel's lemma).

$C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$.

So $C(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$.

Suppose $(u,v,w) \in C(\mathbb{Q})$. Without loss of generality $u,v,w \in \mathbb{Z}$ and $\gcd(u,v) = 1$. If $17 \mid w$ then $17 \mid u$, and so $17 \mid v$, contradicting the assumption that u, v are coprime. So if $p \mid w$ then $p \neq 17$ and 17 is a fourth power. We will just use the fact that 17 is a square (i.e. $\left(\frac{17}{p}\right) = 1$).

$$\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right) = 1$$

and $\left(\frac{-1}{17}\right) = 1$. w is a product of things, each of which are squares mod 17, so w is a square mod 17. Look at equation C mod 17:

$$2w^2 \equiv u^4 \pmod 17$$

So 2 is a fourth power mod 17. But $(\mathbb{F}_{17}^*)^4 = \{\pm 1, \pm 4\}$. This is a contradiction. So $C(\mathbb{Q}) = \emptyset$.

We say that the *Hasse principle* holds whenever $C(\mathbb{Q}_v) \neq 0 \; \forall v$ implies $C(\mathbb{Q}) = \emptyset$. So the above example illustrates a failure of the Hasse principle.

Recall the short exact sequence

$$0 \to E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \to S^{(\varphi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\varphi] \to 0$$

C represents a nonzero element in $Ш(E/\mathbb{Q})$.

Birch-Swinnerton-Dyer Conjecture. Let $E/\mathbb{Q}$ be an elliptic curve.

Definition 24.3.

$$L_p(E,s) = \begin{cases} (1-a_p p^{-s} + p^{1-2s})^{-1} & \text{if } p \text{ has good reduction} \\ (1-p^{-s})^{-1} & \text{if split multiplicative reduction} \\ (1+p^{-s})^{-1} * \text{ if non-split} & \\ 1 & \text{if additive reduction} \end{cases}$$

where a_p is defined by $\#\widetilde{E}(\mathbb{F}_p) = 1 + p - a_p$. Define

$$L(E,s) = \prod_p L_p(E,s).$$

By Hasse's theorem, $|a_p| \le 2\sqrt{p}$. This allows you to check convergence: $L(E,s)$ converges if $\mathrm{Re}(s) > \frac{3}{2}$.

Theorem 24.4 (Wiles, Breuil, Conrad, Diamond, Taylor). *$L(E,s)$ is the L-function of a weight 2 modular form, and has an analytic continuation to all of $\mathbb{C}$ (and a functional equation relating $L(E,s)$ to $L(E,2-s)$).*

Conjecture 24.5 (Weak BSD).

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\, E(\mathbb{Q})$$

We call $\mathrm{ord}_{s=1} L(E,s)$ the *analytic rank*.

Conjecture 24.6 (Strong BSD).

$$\lim_{s\to 1} \frac{1}{(s-1)^r} L(E,s) = \frac{\Omega_E \,\mathrm{Reg}(E(\mathbb{Q}))|Ш(E/\mathbb{Q})| \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}$$

where:

- $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is the Tamagawa number
- $r = \mathrm{rank}\, E(\mathbb{Q})$
- $\mathrm{Reg}(E(\mathbb{Q})) = \det(\langle P_i, P_j\rangle)_{i,j=1,\cdots,r}$, where $\langle P, Q\rangle = \widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)$
- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{|2y+a_1x+a_3|}$ where a_i are coefficients of a globally minimal Weierstrass equation (minimal at all primes)

The best result to date is

Theorem 24.7 (Kolyragin). *If $\mathrm{ord}_{s=1} L(E,s) = 0$ or 1 then Weak BSD holds, and $Ш(E/\mathbb{Q})$ is finite. Moreover, there is an algorithm for checking Strong BSD.*