1 EC

1.1 Fermat's method of infinite descent

- Defn: rational triangles, primitive triangles
- **Prop: parametrisation for primitive triangles: every primitive triangle is of the form...**
- **Defn: congruent number**
- Lemma: equivalent condition of being a congruent number
- **Thm:** 1 **is not a congruent number**
- Lemma: infinite descent polynomial version
- Baby defn of elliptic curves
- Example: what is $E(\mathbb{Q})$ where $E : y^2 = x^3 - x$?
- Cor: if E/K is an EC, then $E(K(t)) = E(K)$. Why does this imply elliptic curves are not rational?

1.2 Remarks on Algebraic curves

- Def: Rational plane curve, rational parametrisation
- Prop: if $K = \bar{K}$ then C is rational $\iff g(C) = 0$, C is EC $\iff g(C) = 1$ (Don't know proof)
- Def: $\mathrm{ord}_P(C)$
- Fact: $\mathrm{ord}_P : K(C)^* \to \mathbb{Z}$ is a discrete valuation
- Def: Uniformizer of $\mathrm{ord}_P(t)$
- Example: consider the curve $\{y^2 = x(x-1)(x-\lambda)\}$. Consider homogenizing it, and compute ord_P at each point.

Concepts related to divisors

- Defn: divisor, degree of a divisor, effective divisor, principle divisor
- Defn: $\mathrm{div}(f)$ where $f \in K(C)^*$.
- **Defn: Riemann Roch space**
- **Thm: Riemann- Roch thm**, no proof

Differentforms of curves

- **Prop: Change curves to legendre form. Don't know its proof.**
- Defn: weierstrass equation and legendre form
- Defn: degree of a morphism, separable morphism
- Thm: formula relating $e_\phi(P)$ to $\deg(\phi)$.Three properties of nonconstant morphism.
-
-

1.3 Wierstrass equations

- Prop: What equations give point of inflection?
- **Defn: elliptic curve**: the real definition
- **Thm: every elliptic curve is isomorphic over K to a curve in weierstrass form, sending O_E to $(0:1:0)$.** Unfamiliar.
- Prop: Isomorphic ECs only differ in W-form by change of variable. Unfamiliar.
- Cor: When char $K \neq 2, 3$, then isomorphisms of EC is of a certain form. Unfamiliar.
- **Def: J=invariant**
- Cor: relationship between J invariant and ECs
- **Thm: Method to derive $\ominus P$ and $P \oplus Q$ and $2P, 3P, 4P$ on the fly when $P = (0, 0)$.**

1.4 Group Law

- **Thm: $E(K)$ is an abelian group. 1. identity, 2. inverse, 3. associativity**
- Defn: Linearly equivalent divisors, $\text{Pic}(E), \text{Pic}^0(E)$
- Defn: $\psi : E \to \text{Pic}^0(E)$
- Prop: **Two properties of ψ** which helps to finish proving group law.
- Silverman 3.1, helps with above theorem:
  If C is a smooth curve and $f \in \overline{K}(C)^*$ then
  - $\text{div}(f) = 0 \iff f \in \overline{K}^*$
  - $\deg(\text{div}(f)) = 0$. i.e. principle divisors always have degree 0.
- Thm: Elliptic curves are group varieties
- Thm and concepts: Weierstrass p theorem
- Thm: statement of results: $K = \mathbb{C}, \mathbb{R}$, local field, number field, finite field.

1.5 Isogenies

- **Def: Isogeny, isogenous,** $\hom(E_1, E_2)$
- Remark: structure of $\hom(E_1, E_2)$. $\deg(\phi_1\phi_2) = \deg(\phi_1)\deg(\phi_2)$
- **Def: the $[n]$ map, $n-$torsion group, $E[n]$**
- Remark: if we have $K = \mathbb{C}$, what is $\deg[n]$? what is $E[n]$
- Lemma: If char $K \neq 2$, $y^2 = (x - e_1)(x - e_2)(x - e_3)$, what is $E[2]$?
- **Prop: $[n]$ is an isogeny**
- Cor: $\hom(E_1, E_2)$ is a torsion- free $\mathbb{Z}-$module
- **Thm: $\phi : E_1 \to E_2$ is an isogeny, then $\phi(P + Q) = \phi(P) + \phi(Q)$, $\forall P, Q \in E$**

- Remark: compare and contrast the above with $\hom(E_1, E_2)$ being an abelian group.
- **Thm:** $\deg([n]) = n^2$. Following helps to prove this
  - Lemma: There exists a morphism $\xi : \mathbb{P}^1 \to \mathbb{P}^1$ that makes a diagram commute. Other edges are the x_1, x_2 map that extracts the $x-$coordinate. What can you say about degrees?
  - **Remark: above lemma tell us how to compute deg of an isog** Unfamiliar.
  - Lemma: $\deg([2]) = 4$
  - Defn: quadratic form
  - Lemma: quadratic form $\iff$ parallelogram law
  - Lemma: rewrite x_3, x_4 in terms of w_0, w_1, w_2.
  - **Thm: degree is a quadratic form**.Unfamiliar with the proof, too much calculations
  - in 2003,2007 exams, tested the proof that deg map is a quad form
- Example: isogeny that is not $[n]$, showed up in the last section on cyclic isogeny as well
-

1.6 Invariant differential

- **Defn: Ω_C, the space of differentials, as a vector space spanned by df**
- Def: order of vanishing
- Facts: Ω_C is a 1-diml vector space and that if $ord_p(f) = n \neq 0$ then $ord_p(df) = n - 1$
- for any f, $ord_p(f) = 0$ for all but finitely many p
- **Def:** $div(w)$
- Defn: genus
- Lemma: If char$K \neq 2$, and $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$, e_i distinct. Then $w = dx/y$ is a differential on E with no zeros or poles. $g(E) = 1$ and the v.s. of regular differentials is 1diml spanned by ω.
- **Lemma: motivation and definition of the invariant differential**
- Lemma: given $\phi, \psi \in Hom(E_1, E_2)$ ω an invariant differential on E_2, then $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$ Unfamiliar with proof.
- **Lemma: ϕ is separable iff $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is nonzero.**
- **Thm: If** char $K \nmid n, E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

1.7 Elliptic curves over finite fields

- Lemma: a AM-GM-like (sign flipped) inequality for positive definitive quadratic forms
- **Def: The frobenius endomorphism. What is its degree?**
- Prop: ϕ is separable, but $1 - \phi$ is not
- **Thm: Hasse's theorem**
- Defn: zeta function

- Defn: Inner product and trace
- Lemma: A formula that links $\text{tr}(\phi)$ with $\deg(\phi)$.
- Defn: Zeta function for curves
- **Lemma: zeta function for elliptic curve can be expressed as a rational function.**
- Remark: prove Riemann hypothesis for elliptic curves, doesn't seem too important so come back later

1.8 Formal groups

This is in preparation for EC in local fields

- **The following ideas motivate the group law**
- Defn: I-adic topology
- Defn: cauchy sequence in the $I-$adic topology
- Def: Ring complete with I-adic topology
- Remark: $1 - x \in R^*$ if $x \in I$
- Lemma: Hensel's lemma, formal groups version
- **Remark: Approximating E with power series**. The whole thought process. That is, get a power series $w(t)$ that solves $F(x) = x - f(t, x)$ which solves the weierstrass equation
- **Defn: the set $\hat{E}(I) = \{(t, w) \in E(K), t, w \in I\}$. Also can be written as $\hat{E}(I) = \{(t, w(t)) \in E(K), t \in I\}$ as the solution is unique by Hensel**
- **Thm: the set $\hat{E}(I)$ is a subgroup of $E(K)$.**
- **Defn: formal group**
- Defn: morphism and isomorphism of formal groups
- **Thm: is Char $R = 0$, then every formal group F over R is isomorphic to $\hat{\mathbb{G}_\alpha}$ over $R \otimes \mathbb{Q}$** In the proof, define log and exp as these morphisms or isomorphisms. Log: Show uniqueness and existence. Proof shaky
- Defn: $[n]$ in terms of formal grous. $[n]T = F((n-1)T, T)$.
- Cor: $[n]$ gives you $F \to F$ an isomorphism of groups so $F(I)$ has no $[n]$ torsion.
-

1.9 Elliptic curves over local fields

- **Defn: Minimal weierstrass equation**
- Question why does minimal weierstrass equation exist?
- Lemma: in weierstrass equation, $(x, y) \neq 0_E$, either $x, y \in \mathcal{O}_K$ or $v(x) = -2s, v(y) = -3s$ for some $s > 1$.
- **Defn:** $\hat{E}(\pi^r \mathcal{O}_K)$
- The filtration $E_i(K)$ and the filtration $F(\pi^r \mathcal{O}_K)$ for a formal group

- **Prop: Let F be a formal group over $\mathcal{O}_K$. Then if $e = v(p)$ and $r > \frac{e}{p-1}$**

$$\log : F(\pi^r \mathcal{O}_K) \to \hat{\mathbb{G}}_\alpha(\pi^r \mathcal{O}_K)$$

  is an isomorphism. exp also gives you an isomorphism other way around.

- **Prop: if $r \geq 1$, then**

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

- Cor: If $|k| < \infty$, then $F(\pi \mathcal{O}_K)$ contains a subgroup of finite index and is iso to $\mathcal{O}_K, +$.

- Prop: given an elliptic curve, then given two minimal weierstrass equations for E, the reduction modulo π defines isomorphic curves.

- **Defn: reduction, good reduction, bad reduction**

- When $V(\Delta)$ is what, it has a good reduction? When it has a bad reduction? When it may not be minimal?

- **Defn: Kernel of reduction: $E_1(K) = \hat{E}(\pi \mathcal{O}_K) = \{p \in E(k) : \tilde{p} = 0\}$, where $\tilde{}$ just means reduction modulo π. Precisely the points that maps to PoI in the reduced equation.**

- **Def: $\tilde{E}_{ns}$**

- When two singular situations corresponds to G_a and G_m?

- **Defn: $E_0(K)$: points on $E(K)$ who reduces to a nonsingular point**

- Prop: $E_0(K)$ is a subgroup of $E(K)$ and reduction mod π is surjective group hom: $E_0(K) \to \tilde{E_{ns}}(k)$.

- **Thm: If $[K : \mathbb{Q}_p] < \infty$, then $E(K)$ contains a subgroup $E_r(K)$ of finite index with $E_r(K) \simeq (\mathcal{O}_K, +)$**

- Remark: some definition in local fields: ramified, unramified, ramification index, residue field degree, max unram extension

- Thm: Suppose $[K : \mathbb{Q}_p] < \infty$, E/K an EC with good reduction, $p \nmid n$, if $P \in E(K)$, then $K([n]^{-1}P)/K$ is unramified.

- **Remark: make a diagram with two SES.**

$$0 \to E_1(K_m) \to E(K_m) \to \tilde{E}(k_m) \to 0$$

  and take UR, and take $[n]$ map, and snake lemma, show it is unramified.

- Defn: Tawagama number

- **Recall definitions: $E_r(K), E_0(K), \tilde{E_{ns}}, E_1(K)$**

- **Lem: If $|k| < \infty$ then $E_0(K) \subset E(K)$ has finite index**

1.10 Elliptic curves over number fields

- Setting: $[K : \mathbb{Q}]$ a number field
- **Defn: prime of good reduction**. Given E/K, what does it mean when it has good reduction?
- Lemma: E/K only have finitely many primes of bad reduction
- Defn: $E(K)_{tor}$
- Lemma: $E(K)_{tor}$ is finite.
- Lemma: $E(K)[n] \hookrightarrow \tilde{E}(k_p)[n]$ if p is a prime of good reduction and $p \nmid n$. Idea: torsion wont disappear, so it suffices to look at the torsion in modulo p.
- **Remark:** $\#\tilde{E}_D(\mathbb{F}_p) = p + 1$ when p is 3 mod 4.
- **Thm: Consider $E_D : y^2 = x^3 - D^2 x$ again. Show that rank $E_D(\mathbb{Q}) \geq 1 \iff D$ is a congruent number.**
- $E(\mathbb{Q})_{tor}$ have almost integer coordinates. That is, if a point (x, y) is a torsion, then $4x, 8y \in \mathbb{Z}$.
- **Thm: Lutz- Nagell**. Proof some stupid calculation hope wont get tested.
- Remark: Mazur only 15 possibilities for $E(\mathbb{Q})_{tor}$

1.11 Kummer Theory

- **Lemma: given $\Delta \subseteq K^*/((K^*)^n$, be a finite group. Then $L = K(\sqrt[n]{\Delta})$ is galois and there exists**
$$\text{Gal}(L/K) \simeq \hom(\Delta, \mu_n)$$
- Defn: Kummer pairing: well defined, bilinear, nondegen in both arguments
- **Thm: The kummer theory bijection**

  There is a bijection between the following:

  1. Finite subgroups $\Delta \subseteq K^*/(K^*)^n$
  2. Finite abelian extensions of L/K of exponent dividing n

$$\Delta \mapsto K(\sqrt[n]{\Delta})$$
$$\frac{(L^*)^n \cap K^*}{(K^*)^n} \hookleftarrow L$$

- **There are only finitely many extensions L/K that satisfies certain properties:**
  - K a number field, $\mu_n \subseteq K$
  - S a finite set of primes of K
  - Then, there are only finitely many extensions such that
    * finite abelian of exponents dividing n
    * unramified at all primes $p \notin S$
- Defn: $K(S, n)$
- Lemma: $K(S, n)$ is finite. This lemma proves previous theorem, but doubt testable

1.12 Elliptic curves over number fields II

- Lemma: $E(K)/nE(K) \to E(L)/nE(L)$ has finite kernel
- Lem: Let $E(K)$ be an EC over a number field. If $P \in E(K)$ then $K([n]^{-1}P)/K$ is Galois. If $E[n] \subseteq E(K)$ then the galois group is abelian of exponent dividing n.
- **Thm: Weak Mordell- Weil theorem**
- **Thm: Mordell- Weil theorem**
- Remark: Existence of the canonical height

1.13 Heights

- Defn: Height $H : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{Z}$
- Lem: Lipschitz-like condition for heights of $F : \mathbb{P}^1 \to \mathbb{P}^1$.
- Defn: Height $H : \mathbb{Q} \to \mathbb{Z}$. Height: $H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$. Little height: $h : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$
- Lemma: $|h(\phi(P)) - \deg(\phi)h(P)|$ is bounded.
- **Defn: canonical height**
- Lemma: $|h(P) - \hat{h}(P)|$ is bounded for all $P \in E(\mathbb{Q})$.
- **Cor:** $\hat{h}$ satisfies the condition that for any $B > 0, \ldots$
- Prop: $\hat{\phi}(P) = \deg(\phi)\hat{h}(P)$
- Thm: quadratic form

1.14 Dual Isogenies and Weil Pairing

1.14.1 Dual Isogenies

- Thm 14.1 The universal-property-like theorem for EC
- Prop 14.2 **The unique existence of the dual isogeny**. As well as some properties
- Defn. Sum of divisors
- Lem 14.3 Dual isogenies distribute with the sum
- Equation relating degree to trace and that $\phi + \hat{\phi} = tr(\phi)$
- Think of dual isogenies as add to trace, multiply to degree.
- Lem 14.4 A divisor is principle $\iff$ (some conditions with sum)
- **Definition of Weil Pairing**
- **Prop 14.5 The Weil pairing is nondegenerate and bilinear**

1.15 Galois Cohomology

- **Defn: group cohomology:** $H^0(G, A) = A^G$**,** $C^1(G, A), Z^1(G, A), B^1(G, A), H^1(G, A)$
- Theorem: SES into LES (snake lemma in Galois cohomology)
- inflation restriction, really wish to skip
- **Hilbert 90:** $H^1(\mathrm{Gal}(L/K), L^*) = 0$
- Some stuff are skipped.
- **Defn: Construction of Selmer group**
- **Defn: Tate shafarech group**
- **The SES that relates the Selmer group to the Tate shafavech group**
- Thm: $S^{(n)}(E/K)$ is finite. big proof, so skipped
-

1.16 Descent by Cyclic Isogeny

- Two key lemmas in computing rank of $y^2 = x(x^2 + ax + b)$
- **Method: Be able to compute the rank of the elliptic curve over $\mathbb{Q}$, with techniques and things to watch out**
- Strong and weak BSD conjecture