MODELS OF CURVES READING GROUP

ROSS PATERSON

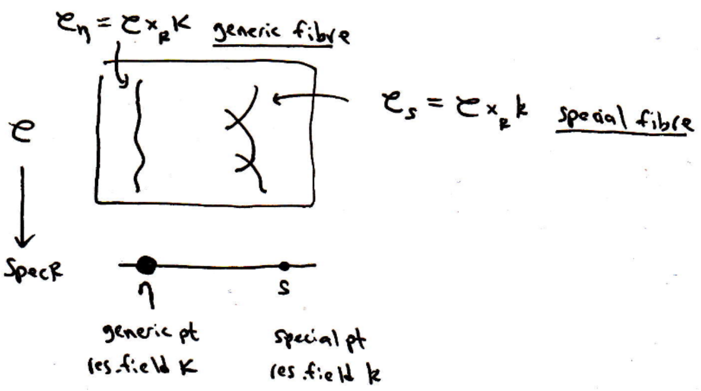
Disclaimer. These notes are notes taken live during sessions of a study group held at the University of Bristol during February–April 2024. The speakers name is listed at the start of each lecture. All errors are the fault of the transcriber, and the notes should therefore be taken with a pinch of salt.

Lecture 1 (Tim): Arithmetic Surfaces

Today we will say a few words about arithmetic surfaces. To begin we take notation:

Notation	Meaning	Examples
R:	a discrete valuation ring (DVR)	$\mathbb{Z}_p$,$\mathbb{F}_p[[T]]$
K:	field of fractions of R	$\mathbb{Q}_p$
k:	residue field of R	$\mathbb{F}_p$
π:	choice of uniformizer	p.

Let $\mathscr{C}/\mathrm{Spec}(R)$ be any scheme, then we have so-called special and generic fibres


$\mathscr{C}_\eta = \mathscr{C} \times_R K$ generic fibre
$\mathscr{C}_s = \mathscr{C} \times_R k$ special fibre
$\mathscr{C}$
Spec R
η
s
generic pt
res field K
special pt
res field k

Definition 1. Let C/K be a non-singular projective geometrically irreducible curve. Then a model of C is a flat proper scheme $\mathscr{C}/\mathrm{Spec}(R)$ of finite type with generic fibre $\mathscr{C}_\eta \cong C$.

How do we actually obtain such a thing?

Example 2. Consider the variety cut out by $C : f = 0 \subseteq \mathbb{P}^2_K$. Scale f to get the coefficients to all be in R and not all divisible by π. Then consider the equation now over R to have

$$\mathscr{C} : f = 0 \subseteq \mathbb{P}^2_R.$$

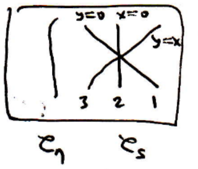
This is a model since the generic fibre is simply C. Moreover the special fibre is the scheme $\mathscr{C}_s : \overline{f} = 0 \subseteq \mathbb{P}^2_k$ given by reducing our equation mod π. Note that flatness is coming from the condition that not all coefficients are divisible by π since if this condition fails then the special fibre is going to be all of $\mathbb{P}^2_k$ and so too large in dimension.

Remark 3 (flat limits). Generally, consider a morphism of schemes $X \to Y$ where X is locally Noetherian and Y is Noetherian and 1-dimensional. Take a closed regular point $y \in Y$ (e.g. $\mathbb{P}^2_R \to \operatorname{Spec}(R) \ni s$). Then a flat scheme $Z \subseteq X \times_Y (Y \backslash \{y\})$ (i.e. $Z \subseteq X \backslash X_y$ where the latter is the gibre over y) (e.g. $C \subseteq \mathbb{P}^2_K$) has a unique flat extension $\tilde{Z}/Y$: namely the closure of Z in X.

Example 4. When $C/K : y^2 = x^3 + ax + b$ for $a, b \in R$ is an elliptic curve, then $\mathscr{C} : y^2 = x^3 + ax + b$ is called a Weierstrass model of C.

The special fibre $\mathscr{C}_s$ of a model $\mathscr{C}$ is a connected (Zariski connectedness), proper, 1-dimensional (flatness) scheme over k.

Example 5. $\mathscr{C} : yx^2(y - x)^3 = \pi \subseteq \mathbb{P}^2_R$ (really $z^6\pi$ but let's not quibble over vagueries about affine models!). Then the special fibre is a union of 3 lines: $y = 0$, $x = 0$ and $y = x$, with multplicities.



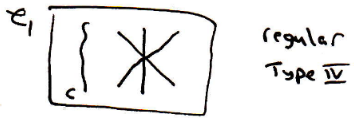
Example 6. Take $K = \mathbb{Q}_p$ with $p \neq 2$. Consider the (projective model of the) curve

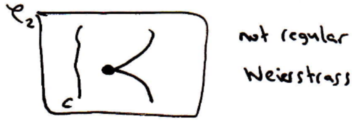
$$C/K : xy(x - y) = 2p.$$

If we look up the classification in Silverman then we see that the Kodaira type of the special fibre is IV. However the transformation

$$X = \frac{2p}{y}, \quad Y = p(1 - (2x/y)),$$

renders this curve isomorphic to $C'/K : Y^2 = X^3 + p^2$. Drawing this out we obtain a different special fibre:
This is not regular.





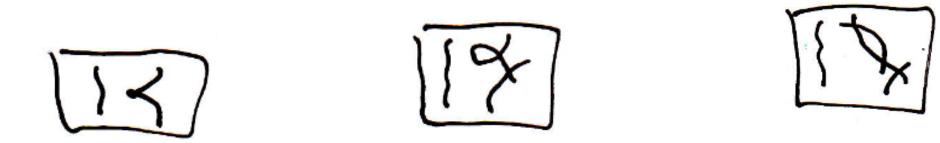
Definition 7. We define certain properties of models.

- $\mathscr{C}$ is a regular model if $\mathscr{C}$ is a regular scheme.
- We say that $\mathscr{C}$ is regular with normal crossings (rnc) if $\mathscr{C}$ is regular and the reduced curve $\mathscr{C}_s^{\text{red}}$ is a normal crossings divisor meaning that the only singularities are ordinary double points.
- We say that $\mathscr{C}$ is snc (strict normal crossings) if it is rnc and has no components which self intersect.

There is a way to associate a graph to each special fibre by defining a vertex for every component and an edge between vertices if they intersect.

Warning: regularity is not a property of the special fibre, but of the model itself!

Facts 8. *We now remark on some important facts.*



(A) Regular model (B) rnc model (C) snc model

The three properties in Definition 7

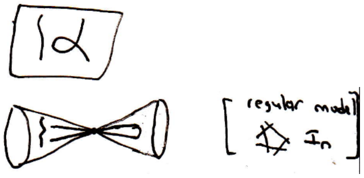
- *It is enough to check regularity at the singular points of the special fibre (including all components of multi[plicity > 1).*
- *Say $f(x, y) = 0 \subseteq \mathbb{A}^2_R$ is singular at $\mathfrak{m} := (x, y, \pi)$ (which corresponds to the point $(x, y) = (0, 0)$ on the special fibre) if and only if* $\dim \mathfrak{m}/\mathfrak{m}^2 = 3$. *This is then equivalent to $f = a + bx + cy + \dots$ with $a \equiv 0 \mod \pi^2$ and $b, c \equiv 0 \mod \pi$*

Example 9. Consider $K = \mathbb{Q}_p$ for $p \neq 2$, and the Weierstrass model

$$\mathscr{C} : y^2 = x^3 + x^2 + p^n.$$

By the second fact above:

- if $n = 1$ then $\mathscr{C}$ is regular, rnc but not snc. In the Kodaira classification this is called type I_1.
- if $n > 1$ then $\mathscr{C}$ is not regular. In the Kodaira classification this is called type I_n.

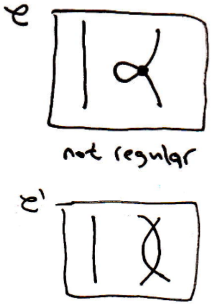


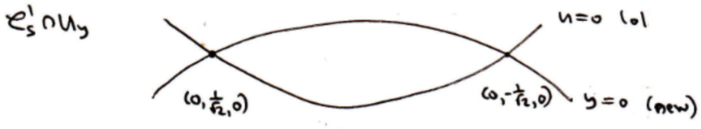
Theorem 10 (Lipman). *Repeatedly normalising (any model $\mathscr{C}$) and blowing up singular points terminates in a regular model $\mathscr{C}' \to \mathscr{C}$. Blowing up further if necessary also gives rnc and snc models.*

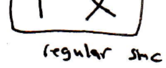
Example 11. $K = \mathbb{Q}_p$, $p \neq 2$. Consider $\mathscr{C} : y^2 = x^3 + 2x^2 + p^2$. This is not regular at the point (x, y, p). Blowing up at this point, we obtain $\mathscr{C}'$ with charts U_∞, U_x, U_y, U_p given by

$$U_y : p = uy,\ x = vy$$

which leads us to the affine model $1 = v^3y + 2v^2 + u^2,\ p = uy \subseteq \mathbb{A}^3_{\mathbb{Z}_p,u,v,y}$. The special fibre has $p = uy = 0$, (see below). This is now a regular model.




$\mathscr{C}'_s \cap U_y$
u=0 (old)
$(0, \frac{1}{\sqrt{2}}, 0)$
$(0, -\frac{1}{\sqrt{2}}, 0)$
y=0 (new)



Remark 12. Some remarks.

- Regular models do not stay regular in ramified field extensions, e.g. let $\pi = \sqrt[n]{p}$ and $K = \mathbb{Q}_p(\pi)$ and the model
$$y^2 = x^3 + x^2 + p,$$
then this becomes
$$y^2 = x^3 + x^2 + \pi^n.$$
- R_π :=completion of R. Then $\mathscr{C}$ is regular if and only if the base change to R_π is regular. Thus we may as well assume that R is complete, which is nice as over the completion we will often have things like Hensel's lemma at our disposal.
- Can glue regular models to get them over Dedekind domains (e.g. $\mathbb{Z}$).

Lecture 2 (Himanshu Shukla): Properness and implications of regularity

Let K be the field of fractions of a DVR R with maximal ideal m and residue field $k \coloneqq R/m$. Assume that K is complete with respect to the valuation v of R.

1. Motivation

Let $K \coloneqq \mathbb{Q}_p$, $R \coloneqq \mathbb{Z}_p$, $m \coloneqq (p)$, $k \coloneqq \mathbb{F}_p$, and E/K be an elliptic curve given by the Weierstrass model $y^2 = f(x)$, where f is a monic cubic polynomial over R. Let $\overline{E}/k$ be the curve obtained by reducing the coefficients of $f \mod p$ given by $y^2 = \overline{f}$. For a point $P \in E(K)$, let $\overline{P} \in \overline{E}(k)$ be the point obtained by reduction of coordinates $\mod p$. In the terminology of Chapter VII of Silverman's AEC, let $\overline{E}_{ns}(k)$ be the set of non-singular points on $\overline{E}(k)$. Then one has the following proposition.

Proposition 13.

- *$\overline{E}_{ns}(k)$ is a group and $\overline{O} \in \overline{E}_{ns}(k)$.*
- *Let $E^0(K) \coloneqq \{P \in E(K) \mid \overline{P} \in \overline{E}_{ns}(k)\}$. Then $E^0(K)$ is a group and the reduction map $E(K) \to \overline{E}_{ns}(k)$ restricted to $E^0(K)$ is a surjective group homomorphism.*

The surjectivity is due to the Hensel's lemma applied on the polynomial $y^2 - f(\tilde{x}_0)$, where (x_0, y_0) is a point on $\overline{E}_{ns}(k)$ and $\tilde{x}_0 \in R$ is such that $\tilde{x}_0 \equiv x_0 \mod p$. Define $E_1(K)$ to be the kernel of the reduction homomorphism, i.e.

$$E_1(K) \coloneqq \ker\left(E^0(K) \to \overline{E}_{ns}(k)\right),$$

which in the case of Weierstrass model is the set of all points $(x, y) \in E(K)$ such that $v(x), v(y) < 0$, and O. We have the following commutative diagram of pointed sets

$$\begin{tikzcd}
0 \arrow[r] & E_1(K) \arrow[r] \arrow[d, equal] & E^0(K) \arrow[r] \arrow[d, hook] & \overline{E}_{ns}(k) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & E_1(K) \arrow[r] & E(K) \arrow[r] & \overline{E}(k) \arrow[r] & 0
\end{tikzcd},$$

where the top row is also an exact sequence of groups.

We can get a handle on $E^0(K)$ by using the information on $E_1(K)$ and $\overline{E}_{ns}(k)$. We would like to understand $E(K)/E^0(K)$ in order to understand $E(K)$. Now if $\overline{E}(k)$ were to be a group with the reduction map being a homomorphism on $E(K)$, then by snake lemma one gets $E(K)/E^0(K) \hookrightarrow \overline{E}(k)/\overline{E}_{ns}(k)$ and one could have understood $E(K)/E^0(K)$ by studying points $\mod p$. But fortunately/unfortunately $\overline{E}(k)$ is not necessarily a group except if E has good reduction at p.

2. Proper morphisms

We define morphism of schemes to be proper using the valuative criterion of properness due to Chavelley.

Definition 14. Let $f : X \to S$ be a finite type morphism of Noetherian schemes (i.e. X and S can be covered by finitely many $\mathrm{Spec}(A_i)$, with A_i being Noetherian). Then f is said to be *proper* $\iff$ for every DVR R with field of fractions K, given a morphism $s : \mathrm{Spec}(R) \to S$ and a morphism $x : \mathrm{Spec}(K) \to X$ such that the outer square in the following diagram commutes

(1)
$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, "x"] \arrow[d, "\iota"] & X \arrow[d, "f"] \\ \mathrm{Spec}(R) \arrow[r, "s"] \arrow[ur, dashed, "\overline{x}"] & S \end{tikzcd},$$

where ι is the morphism induced by the inclusion $R \to K$. Then there is a unique lift of x to a morphism $\overline{x} : \mathrm{Spec}(R) \to X$ such that everything commutes.

Note that the morphism s makes $\mathrm{Spec}(R)$ an S–scheme and similarly for $\mathrm{Spec}(K)$. If T is another S–scheme then the set of S–morphisms $T \to S \longleftrightarrow$ the set of T-rational points of X. Keeping this in mind, the above diagram says that f is proper $\iff$ if x gives a K rational point on X such that $f(x)$ is gives an R–rational point on S, then there is exactly one way of "*clearing the denominators*" to obtain a R–rational point on X.

Example 15.

- Projective space $\mathbb{P}^n_S$ over S is proper. Hence, for $S = \mathrm{Spec}(R)$ we have $\mathbb{P}^n_R := \mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S$ over $S := \mathrm{Spec}(R)$, and the above definition says that $\mathbb{P}^n_R(K) \longleftrightarrow \mathbb{P}^n_R(R) \longleftrightarrow \mathbb{P}^n_K(K)$, where note that $\mathbb{P}^n_K$ is the generic fibre of $\mathbb{P}^n_R$, which is what one expects from the definition of a projective space.
- If $\mathcal{C}/R$ is an arithmetic surface, then every fibre of $\mathcal{C}$ can be embedded inside projective space, hence we have $\mathcal{C}$ is proper and $\mathcal{C}(R) \longleftrightarrow C(K)$, where C is the generic fibre.

In the case when $\mathcal{C}/R$ is an arithmetic surface with generic fibre C and special fibre $\overline{C}$, then for every point $P \in C(K)$, one can find a representation of P by clearing the denominators as $(\pi^{\alpha_1} a_1 : \ldots : \pi^{\alpha_n} a_n)$, where π is a uniformizer of R such that a_i are units in R and $\alpha_i \geq 0$ with at least one $a_i = 0$. Hence, we have the reduction $\mod \pi$ map $C(K) \to \overline{C}(k)$. In the sense of the diagram (1) it means: given $x : \mathrm{Spec}(K) \to \mathcal{C}$, one has $\overline{x} : \mathrm{Spec}(R) \to \mathcal{C}$. The k–rational point on $\overline{C}(k)$ associated to x corresponds to the composition of morphisms $\mathrm{Spec}(k) \overset{\mu}{\to} \mathrm{Spec}(R) \overset{\overline{x}}{\to} \mathcal{C}$, where μ is the morphism taking the unique point of $\mathrm{Spec}(k)$ to m. Since the composition $f \circ \overline{x} \circ \mu$ has to commute $s \circ \mu$, this gives a morphism $\mathrm{Spec}(k) \to \overline{C}$.

Let $\overline{C}_{ns}$ be the non-singular part of the special fibre, $\mathcal{C}^0$ be the largest non-singular subscheme of $\mathcal{C}$ and $C^0(K)$ be the subset of $C(K)$ that reduce to $\overline{C}_{ns}$. As before, Hensel's lemma implies that the morphism $C^0(K) \to \overline{C}_{ns}(k)$ is surjective. We also have $\mathcal{C}^0(R) \subseteq \mathcal{C}(R) \longleftrightarrow C(K) \supseteq C^0(K)$. Identifying $\mathcal{C}(R)$ with $C(K)$ we have $\mathcal{C}^0(R) \subseteq C^0(K) \subseteq C(K) = \mathcal{C}(R)$. In the next section we would like to see the interaction of some of these sets if $\mathcal{C}$ was regular.

3. Consequences of regular models

We begin with some examples.

Example 16. Recall the regular model for the elliptic curve $E/\mathbb{Q}_p$ given by the Weierstrass model $\mathcal{E}/\mathbb{Z}_p : y^2 = x^3 + x^2 + p$ (Example 9 from Tim's lecture). The special fibre $\overline{C}$ has a singular point $(0, 0)$. If $P := (x, y) \in E(\mathbb{Q}_p)$ is such that

$\overline{P} = (0,0)$, then $p|x$ and $p|y$. Hence $2v(y) = 1$ but $v(y) \geq 1$. Thus we have $E(K) \longleftrightarrow \mathcal{E}(\mathbb{Z}_p) = \mathcal{E}^0(R) = E^0(K)$. Hence $[E(K) : E^0(K)] = 1$.

Example 17. Recall that the elliptic curve $E/\mathbb{Q}_p$ given by the Weierstrass model $\mathcal{E}/\mathbb{Z}_p : y^2 = x^3 + 2x^2 + p^2$ is not regular (Example 11 from Tim's lecture). However there is a regular model given by

$$\mathcal{E}'/\mathbb{Z}_p : \begin{cases} 1 = yv^3 + 2v^2 + u^2, \\ p = uy \end{cases},$$

with isomorphism between generic fibres given by $x \mapsto uy$, $y \mapsto y$, $p = uy$. Note that the above equations are for the intersection of the affine model of $\mathcal{E}'$ with the chart U_y as before. If we work with $\mathcal{E}$, then we see that if $x \in \mathbb{Z}_p$ is such that $v(x) > 1$, then up to even powers of p, we have $f(x) = 1 + O(p^2)$ which is a square. Therefore, for every x such that $v(x) > 1$, one obtains points $P \in E(\mathbb{Z}_p)$ such that $\overline{P} = (0,0)$. Similarly one can show that for each $r \geq 1$, and x such that $v(x) = -2r$, one can obtain points reducing to $\overline{O}$. This implies that there are "many" points reducing to both $\overline{E}_{ns}(\mathbb{F}_p)$ and $(0,0)$. Clearly, we have $\mathcal{E}^0(\mathbb{Z}_p) \subsetneq \mathcal{E}(\mathbb{Z}_p)$.

We now consider the regular model $\mathcal{E}'$, we get that the two non-singular points $(0, \pm 1/\sqrt{2}, 0) \in \overline{E}_{ns}(\mathbb{F}_p)$ do not lift to $\mathcal{C}(\mathbb{Z}_p)$, because otherwise $p|u$ and $p|y$ and $p = p^2 a$, where $(u, v, y) \in E'(\mathbb{Z}_p)$ is a lift of $(0, \pm 1/\sqrt{2}, 0)$ and $a \in \mathbb{Z}_p^\times$. Other than the points $(0, \pm 1/\sqrt{2}, 0)$ every other point on $\overline{E'}(\mathbb{F}_p)$ is smooth and by Hensel's lemma lifts to a point of $\mathcal{E}'(\mathbb{Z}_p)$. Therefore, $\mathcal{E}'(\mathbb{Z}_p) = \mathcal{E}'^0(\mathbb{Z}_p) = E'(\mathbb{Q}_p) = E'^0(\mathbb{Q}_p)$.

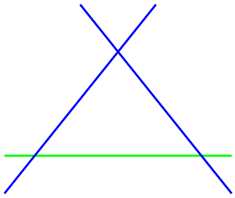
Any point in $\mathcal{E}'(\mathbb{Z}_p)$, with $y \equiv 0 \mod p$ and $u \not\equiv 0 \mod p$ implies that $1 = 2v^2 + u^2 \mod p$ and hence $x = vy \equiv 0 \mod p$, i.e. P corresponds to a point on $\mathcal{E}(\mathbb{Z}_p)$ mapping to $(0,0)$ on $\overline{E}$. Furthermore, the set of points on $\overline{E'}(\mathbb{F}_p)$ with $u = 0$ and $y \neq 0$ corresponds to the set of points on $\overline{E}_{ns}(\mathbb{F}_p)$. Now since $E' \simeq E$, we have $E'(\mathbb{Q}_p) \simeq E(\mathbb{Q}_p)$, but $E^0(\mathbb{Q}_p)$ corresponds to only one of the two components of $\overline{E'}_{ns}(\mathbb{F}_p)$. Hence $[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)] = 2$.

The above two examples suggest that in order to study the quotient $E(K)/E^0(K)$, one can study study some regular model $\mathcal{E}'$ of E where $\mathcal{E}'(R) = \mathcal{E}'^0(R)$, $E(K) \simeq E'(K)$ and study the components of the special fibre $\overline{E'}$ which correspond to $E^0(K)$. However, this model should be "minimal" (provide ref. (Gergely's talk)) in some way so that we do not add more components than we need. Recall that, one can always create regular models from the non-regular models by blowing up (Theorem 10 from Tim's lecture). The following theorem allows us to do the same.

Theorem 18. *(provide ref. (Silverman 2, Chapter 4)) Let $\mathcal{C}/R$ be proper and be a regular model of C/K and $P \in \mathcal{C}(R)$. Then $\overline{P} \in \overline{C}_{ns}(k)$, and hence $\mathcal{C}^0(R) = \mathcal{C}(R) = C(K)$.*

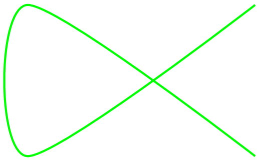
Question 19. *Let $\mathcal{C}/R$ be proper such that $\mathcal{C}^0(R) = \mathcal{C}(R)$. Then is $\mathcal{C}$ a regular model?*

Answer (Sam Frengley)**.** No. Consider a regular model $\mathcal{C}/R$ of C/K which looks as follows in the special fibre



,

where the blue components are swapped by the Galois. $\mathcal{C}(R)$ reduces to the set of non-singular k–rational points on the green component. Blowing down the blue-components gives us a non-regular model $\mathcal{C}'/R$ of C/K such that special fibre $\overline{C'}$ looks like



The singular point in $\overline{C'}$ does not lift to $\mathcal{C}'(R)$, since it is coming from blowing down the blue components, hence $\mathcal{C}'(R) = \mathcal{C}'^0(R)$ but $\mathcal{C}$ is not-regular.

Lecture 3 (Sam): Intersection Theory

References: Silverman (*Advanced Topics in the Arithmetic of Elliptic Curves*) Chapters III-IV.

Algebraic Surfaces

Throughout, K is a field.

Definition 20. An algebraic surface over K is a smooth projective geometrically integral variety S/K of dimension 2. Moreover,

- A Prime divisor on S is an integral $D \subseteq S$ of codimension 1;
- $\mathrm{Div}(S) :=$ free abelian group on prime divisors.

Fix an algebraic surface S/K.

Theorem 21. *There is a unique pairing*

$$\mathrm{Div}(S) \times \mathrm{Div}(S) \to \mathbb{Z}$$
$$(C, D) \mapsto C \cdot D.$$

called the intersection pairing and satisfying the following.

(i) If C, D are non-singular and meet transversely ($\forall P \in C \cap D$, the maximal ideal of $\mathcal{O}_{S,P}$ is $\langle f, g\rangle$ for f, g local equations for C, D), then $C \cdot D = \# C \cap D$;
(ii) It is symmetric: $C \cdot D = D \cdot C$;
(iii) It is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$;
(iv) It is invariant under linear equivalence: if $C_1 \sim C_2$ then $C_1 \cdot D = C_2 \cdot D$ (recall: $C_1 \sim C_2$ if and only if $C_1 - C_2 = \mathrm{Div}(f)$ for some function $f \in K(S)$).

Remark 22. Really, this is a pairing for $\mathrm{Cl}(S) \cong \mathrm{CaCl}(S) \cong \mathrm{Pic}(S)$.

Example 23. If we look at $S := \mathbb{P}^2$, then $\mathrm{Pic}(S) = \langle \mathcal{O}(1) \rangle \cong \mathbb{Z}$ is generated by the twisted sheaf $\mathcal{O}(1)$. Identifying $\mathcal{O}(1)$ with $1 \in \mathbb{Z}$ then the intersection pairing is given by multiplication in $\mathbb{Z}$. For curves $C, D \subseteq S$ of degrees c, d we get $C \cdot D = cd$.

Question 24. *How do we compute this in general?*

Proposition 25. *If $C, D \in \mathrm{Div}(S)$ are effective divisors with no common component then*

$$C \cdot D = \sum_{P \in C \cap D} (C \cdot D)_P,$$

where $(C \cdot D)_P = \dim_K \mathcal{O}_{S,p} / \langle f, g \rangle$ where $\langle f, g \rangle$ are local equations for C, D.

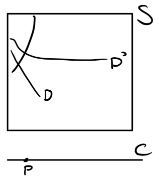
Definition 26. We say that S is fibred over a(n irreducible) curve C/K if there is a surjective morphism

$$\pi : S \to C.$$

For $D \subseteq S$, the image $\pi(D) = \{P\}$ is a (closed) point (call this vertical) or all of C (call this horizontal).

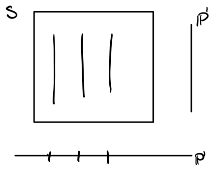
Proposition 27. *Consider a fibration $\pi : S \to C$ a vertical divisor D. Then*

- *(a)* $D^2 \leq 0$*;*
- *(b)* $D^2 = 0$ *if and only if* $\exists \alpha \in \mathbb{Q}^\times$ *and* $\delta \in \mathrm{Div}(C)$ *such that* $D = \alpha \pi^*(\delta)$*.*



Let's now look at an explicit example.

Example 28. Consider $S = \mathbb{P}^1 \times \mathbb{P}^2$, so that $\mathrm{Pic}(S) = \langle \mathcal{O}(1,0), \mathcal{O}(0,1) \rangle \cong \mathbb{Z}^2$. Then the intersection product is $\mathcal{O}(a,b) \cdot \mathcal{O}(c,d) = ad + bc$, $\mathcal{O}(a,b)^2 = 2ab$.



Arithmetic Surfaces

- Let R be a DVR, with maximal ideal $\mathfrak{m}$ and let $K = \mathrm{Frac}(R)$ be the fraction field and $k = R/\mathfrak{m}$ be the residue field.
- Let $\mathscr{C}/R$ be an arithmetic surface: so we have a morphism $\mathscr{C} \to \mathrm{Spec}(R)$ which is flat, proper etc., and of relative dimension 1, and denote by $C = \mathscr{C}_\eta$ the generic fibre.
- Assume that $\mathscr{C}$ is normal
- Assume that $\Gamma \subset \mathscr{C}$ is a prime divisor, again we have horizontal and vertical divisor. In this setting we note that prime horizontal divisors are given by $C(\overline{K})/\mathrm{Gal}(\overline{K}/K)$ (when $\mathscr{C}$ is regular), and prime vertical are components of the special fibre $\mathscr{C}_s$.
- $\mathrm{Div}_s(\mathscr{C})$ is the free abelian group on the prime vertical divisors.

Definition 29. Let $\Gamma_1 \neq \Gamma_2 \in \mathrm{Div}(\mathscr{C})$, and $x \in \mathscr{C}_s$ be a closed point.

- A uniformiser for Γ_i at a point x is an element $f_i \in \mathcal{O}_{\mathscr{C},x}$ such that

  $$\mathrm{ord}_{\Gamma_i}(f_i) = 1; \quad \mathrm{ord}_{\Gamma'}(f_i) = 0$$

  for every prime divisor $\Gamma' \neq \Gamma$ with $x \in \Gamma'$.

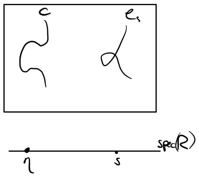


FIGURE 2. An arithmetic surface

- The local intersection multiplicity is
$$(\Gamma_1 \cdot \Gamma_2)_x = \dim_k \mathcal{O}_{\mathscr{C},x} / \langle f_1, f_2 \rangle$$

Theorem 30. *Let $\mathscr{C}/R$ be regular and proper. Then there is a unique bilinear pairing*
$$\begin{aligned} \mathrm{Div}(\mathscr{C}) \times \mathrm{Div}_s(\mathscr{C}) &\to \mathbb{Z} \\ (D, F) &\mapsto D \cdot F \end{aligned}$$
such that

(1) *If $D \in \mathrm{Div}(\mathscr{C})$, $F \in \mathrm{Div}_s(\mathscr{C})$ distinct and irreducible then*
$$D \cdot F = \sum_{x \in D \cap F} (D \cdot F)_x.$$
(2) *For $D_1, D_2 \in \mathrm{Div}(\mathscr{C})$, if $D_1 \sim D_2$ and $F \in \mathrm{Div}_s(\mathscr{C})$ then $D_1 \cdot F = D_2 \cdot F$.*
(3) *$F_1, F_2 \in \mathrm{Div}_s(\mathscr{C})$ then $F_1 \cdot F_2 = F_2 \cdot F_1$*

Example 31. Let $R = \mathbb{Z}_p$, $\mathscr{C} : y^2 = x^3 + x^2 + p^2$, and $D : x = 0$ (closure of the point $(0, p) \in C(\mathbb{Q}_p)$) and $F = \mathscr{C}_p$ be the special fibre. Then (were this regular, which it is not), we get
$$(D{\cdot}F) = (D{\cdot}F)_{\overline{(0,0)}} = \dim_{\mathbb{F}_p} \left(\mathbb{Z}_p[x,y]/(y^2 - x^3 - x^2 - p^2, x, p)\right) = \dim_{\mathbb{F}_p} \mathbb{F}_p[y]/y^2 = 2.$$

Proposition 32. *If $\mathscr{C}/R$ is regular then*

(a) *$\mathscr{C}_s$ is connected;*
(b) *For $F \in \mathrm{Div}_s(\mathscr{C})$ with $F^2 \leq 0$, the following are equivalent*
   (i) *$F^2 = 0$;*
   (ii) *$F \cdot F' = 0$ for all $F' \in \mathrm{Div}_s(\mathscr{C})$;*
   (iii) *$F = \alpha \mathscr{C}_s$ for some $\alpha \in \mathbb{Q}$.*

ADJUNCTION FORMULA

Definition 33. The arithmetic genus of a proper irreducible curve F/k is $P_a(F) = \dim H^1(F, \mathcal{O}_F)$ (this can be extended to connected support).

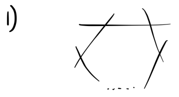
Remark 34. We have:

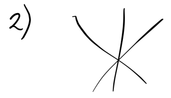
- $P_a(F) = g(F)$ (geometric genus) if F is non-singular;
- for a nodal curve, $P_a(F) = g(F) + \#$nodes;
- P_a is constant in flat families;

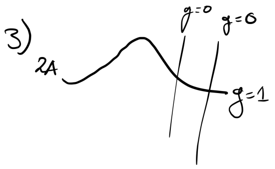
Proposition 35. (1) *For a canonical divisor $K_{\mathscr{C}}$ on $\mathscr{C}$, we have*
$$2P_a(F) - 2 = F \cdot (F + K_{\mathscr{C}}) \quad \forall F \in \mathrm{Div}_s(\mathscr{C}).$$
(2) *If $\mathscr{C}$ is regular then we have $P_a(\mathscr{C}_s) = P_a(C) = g(C)$.*

(3) *For $F \in \mathrm{Div}_s(\mathscr{C})$ irreducible, we have $P_a(F) \geq 0$, with equality if and only if $F \cong \mathbb{P}^1_k$*

Example 36. Consider the following types.





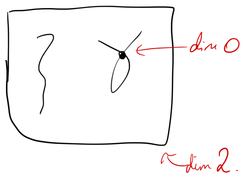


In cases 1) and 2) (known as I_n and IV reduction) we can deduce that the genus of our generic fibre must have been $g(C) = 1$. In the final case, 3), we can determine that the generic fibre has genus $g(C) = 2$.

Lecture 4 (Gergely): Minimal Models

Today we will discuss the existence of minimal models. Tim already mentioned this existence, but we will now give some details. We maintain the notation (R, K, k etc.) from last time.

Normalisation



Let X be a scheme. If X is normal (plus some mild conditions) then the singular locus of X has codimension at least 2. For an affine integral scheme $\mathrm{Spec}(A)$, we have the associated integral closure (in its field of fractions) $A' \supseteq A$. We can use these to construct the normalisation X' of X, essentially by integrally closing an affine cover.

Lipman's existence theorem. Let $\mathscr{C}$ be a model of a curve C/K over R. Then there exists $\mathscr{C}(1), \mathscr{C}(2), \ldots$ models of C/K

$$\mathscr{C} \leftarrow \mathscr{C}(1) \leftarrow \mathscr{C}(2) \leftarrow \ldots$$

where $\mathscr{C}(i+1)$ is the normalisation of the blow-up of a singular point $P \in \mathscr{C}(i)$.

Definition 37. A modification of a model $\mathscr{C}$ is a birational morphism which is an isomorphism away from some singular point $P \in \mathscr{C}$. It is a blow-up if the preimage $f^{-1}(P)$ has arithmetic genus 0.

Theorem 38 (Lipman's existence theorem)**.** *After finitely many steps, we arrive at a regular scheme. I.e., there exists n such that $\mathscr{C}(n)$ is regular.*

We will not discuss the proof in depth, and instead discuss minimality.

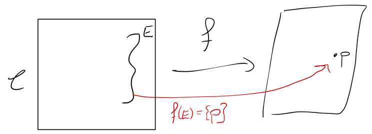
Definition 39. A relatively minimal regular model $\mathscr{C}$ of C/K is one which satisfies:

(1) it is regular
(2) if $f : \mathscr{C} \to \mathscr{C}'$ is a birational and proper morphism then f must be an isomorphism.

We say there is a minimal regular model if all relatively minimal regular models are isomorphic.

Lemma 40. *$\mathscr{C}$ is minimal if and only if every birational map $Y \to \mathscr{C}$ is a morphism.*

Let $\mathscr{C}$ be regular. Then we try to "blow-down" $\mathscr{C}$ until we get some minimal regular model.



Note that a blow-down is a morphim which is an isomorphism outside of a fixed component (which is the one we are blowing down)!

Definition 41. Let E be a divisor of $\mathscr{C}$. Then E is called exceptional if one can blow-down along E, with $f(E) = Q$ a point such that $\dim \mathcal{O}_Q = 2$.

Theorem 42 (Castelnuovo's criterion)**.** *Let $\mathscr{C}$ be a regular model of C/K. Let E be a prime divisor on $\mathscr{C}$. Then E is exceptional if and only if all of the following:*

- *$E \subseteq \mathscr{C}_s$ is contained in the special fibre (in particular it is vertical).*
- *The arithmetic genus of E is 0.*
- *$E^2 = -1$ (under the intersection pairing from last time).*

Observe:

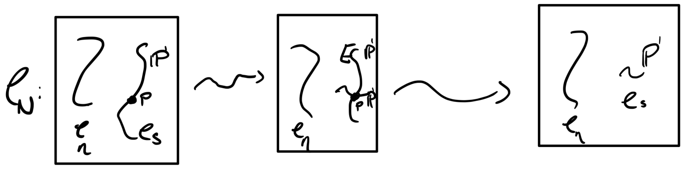
(1) Blowing down $f : \mathscr{C} \to \mathscr{C}'$ removes one exceptional divisor;
(2) there are only finitely many exceptional divisors (follows from noetherian plus being contained in the special fibre).

Theorem 43. *Consider a sequence of blow-downs*

$$\mathscr{C} \to \mathscr{C}_1 \to \mathscr{C}_2 \to \mathscr{C}_3 \to \cdots \to \mathscr{C}_N$$

such that $\mathscr{C}_N$ has no exceptional divisors. Then:

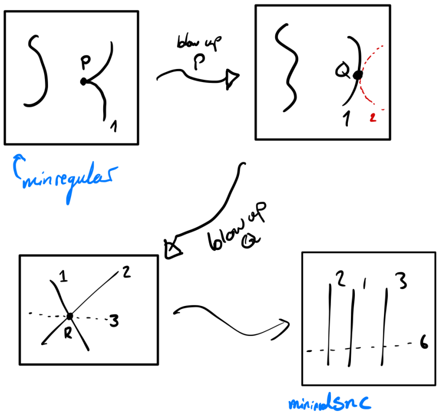
- *if $(\mathscr{C}_N)_s$ has arithmetic genus at least 1 then $\mathscr{C}_N$ is a minimal regular model;*
- *otherwise $\mathscr{C}_N$ it is relatively minimal.*



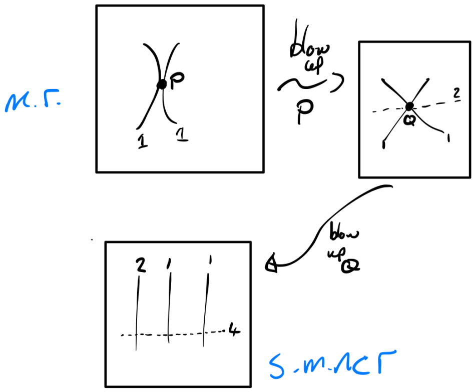
Note that given an exceptional divisor $E \subseteq \mathscr{C}$ and a blow-down $f : \mathscr{C} \to \mathscr{C}'$ along E with $f(E) = P$

(1) $\mathscr{C}', P$ determine E;
(2) $\mathscr{C}, E$ determine $\mathscr{C}'$.

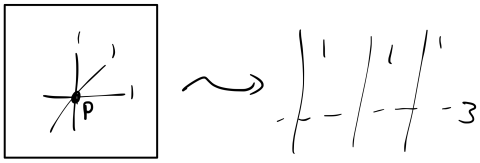
Example 44. Type II elliptic curves over $\mathbb{Q}_p$ are given by $y^2 = X^3 - p$



Example 45. Type III are given by $y^2 = x^3 - px$



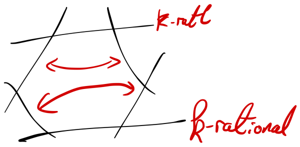
Example 46. Type IV $y^2 = x^3 - p^2$



Galois action on the special fibre

Consider the action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$ on the special fibre $\mathscr{C}_s$. For a minimal regular model of C/K.

Example 47. For example consider an I_6 type elliptic curve. Then Galois can act in a few ways, for instance:



In fact, one can show using this picture that for I_n elliptic curves then there are either 2 or 1 Galois invariant components depending on $n \mod 2$.

Say $\mathscr{C}_s = \sum_{i=1}^{N} r_i C_i = \pi_*(s)$ where s is the special point on $\operatorname{Spec}(R)$ and $\pi : \mathscr{C} \to \operatorname{Spec}(R)$ is the structure morphism. Then

1. $\mathscr{C}_s$ is connected;
2. $r_i > 0$;
3. $C_i \cdot C_j \geq 0$ for all $i \neq j$;

Definition 48. The type of a model is defined to be the collection

$$(N, (C_i \cdot C_j)_{i,j}, (C_i \cdot K)_i, r_i),$$

where K is in the canonical class.

Theorem 49. *For each genus g, there are only finitely many families of types of minimal regular models.*

Theorem 50 (Winters)**.** *Let $k = k^{\text{al}}$ be an algebraically closed field of characteristic 0. Let $\mathscr{C}_s^{\text{red}} = Z_1 + \cdots + Z_n$ be a locally planar reduced curve over k, and let $m_i \geq 1$ be such that $m_i \mid \sum_{j \neq i} m_j (Z_i \cdot Z_j)$. Then there exists a regular model $\mathscr{C}$ such that $\mathscr{C}_s = \sum_{i=1}^{n} m_i Z_i$.*

Lecture 5 (Holly): The Birch and Swinnerton-Dyer Formula

Statement

Notation 51. Today we adopt the following notation.

- K is a number field
- E/K is an elliptic curve
- $|\cdot|_v$ is a normalised absolute value on K_v, the completion of K at a place v
- q_v is the cardinality of the residue field at a finite place v.

Conjecture 52. *Assuming that $Ш_E$ is finite, and that $L(E, s)$ has analytic continuation, then the leading term is*

$$\frac{\# Ш_E \operatorname{Reg}_E C_E}{\# E(K)_{\text{tors}}^2 \sqrt{|\Delta_K|}},$$

where Δ_K is the discriminant of K, Reg_E is the regulator.

Today we will focus on the term C_E which is constructed of local data.

Definition 53. Fix a regular differential $\omega \neq 0$ on E/K. Then

$$C_E := \prod_{v \nmid \infty} c_{E/K_v} \left| \frac{\omega}{\omega_v^\circ} \right|_v \cdot \prod_{\substack{v \mid \infty \\ K_v \cong \mathbb{R}}} \int_{E(K_v)} |\omega| \cdot \prod_{\substack{v \mid \infty \\ K_v \cong \mathbb{C}}} \int_{E(K_v)} |\omega \wedge \overline{\omega}| = \prod_v C_{E/K_v}.$$

Here

- $c_{E/K_v} = [E(K_v) : E_0(K_v)]$ is the Tamagawa number of E at $v \nmid \infty$
- ω_v° is the Néron differential for E at $v \nmid \infty$.

If $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is a minimal Weierstrass equation over K_v then $\omega_v^\circ = \frac{dx}{2y+a_1x+a_3}$.

Example 54. For $E/\mathbb{Q} : y^2 = x^3 + 17^{12}$, the discriminant is $\Delta_E = -2^3 3^3 17^{24}$, so the equation is minimal over $\mathbb{Q}_p$ for $p \neq 17$ and hence $\omega_p^\circ = \pm\frac{dx}{2y}$ for $p \neq 17$.

For $p = 17$ we need the substitution $y = 17^6Y$, $x = 17^4X$ to get $E : Y^2 = X^3 + 1$ which has discriminant $\Delta = -2^3 3^3$ so this model is minimal over $\mathbb{Q}_17$ and hence $\omega_{17}^\circ = \frac{dX}{2Y} = 17^2\frac{dx}{2y}$.

Remark 55. If $E/\mathbb{Q}$ then there is a global minimal model, and so we can do take a global minimal differential ω to obtain

$$C_E = \prod_p c_{E/\mathbb{Q}_p} \int_{E(\mathbb{R})} |\omega| .$$

Remark 56. Each C_{E/K_v} depends on ω, but note that this can only differ by a scalar and if $\alpha \in K^\times$ then

$$C_{E/K_v}(\alpha\omega) = |\alpha|_v \, C_{E/K_v}(\omega),$$

so by the product rule the total expression C_E does not depend on this choice.

Lemma 57 (Tate)**.** *Let $v \nmid \infty$. Then*

$$c_{E/K_v} \left|\frac{\omega}{\omega_v^\circ}\right|_v = L_v(E, q_v^{-1})^{-1} \int_{E(K_v)} |\omega| .$$

Tamagawa Numbers

Notation 58. Take the following notation

- $\mathcal{K}$ is a non-archimedean local field
- $\mathcal{O}_\mathcal{K}$ is the ring of integers
- k is the residue field and has cardinality q
- $A/\mathcal{K}$ is an abelian variety, $C/\mathcal{K}$ is a smooth proper geometrically connected curve over $\mathcal{K}$.

Definition 59. Let $\mathcal{A}/\mathcal{K}$ be a Néron model for A/K. Let $\Phi_A := \mathcal{A}_s/\mathcal{A}_s^\circ$ be the special fibre of $\mathcal{A}$ modulo the connected component of the identity $\mathcal{A}_s^\circ$. We call this the Néron component group. Then

$$c_{A/\mathcal{K}} = \#\Phi_A(k) = \#\Phi_A(\overline{k})^{\mathrm{Gal}(\overline{k}/k)}$$

Remark 60. Néron models always exist.

Theorem 61 (Raynaud)**.** *Let $\mathcal{C}/\mathcal{O}_\mathcal{K}$ be a (minimal?) regular model for the curve $C/\mathcal{K}$. Let $I = \{T_1, \dots, T_n\}$ be the irreducible components of $\mathcal{C}_s$ over $\overline{k}$. Write m_i for the multiplicity of T_i. Define, extending linearly, maps*

$$\begin{aligned} \alpha &: \mathbb{Z}^I \to \mathbb{Z}^I & \beta &: \mathbb{Z}^I \to \mathbb{Z} \\ T_i &\mapsto \sum_{j=1}^n (T_i \cdot T_j)T_j; & T_i &\mapsto m_i. \end{aligned}$$

Then if $A = \mathrm{Jac}(C)$ *is the Jacobian, then*

$$\Phi_A(\overline{k}) \cong \ker(\beta)/\mathrm{im}(\alpha),$$

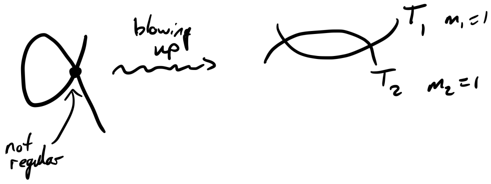
in particular, $C_{A/\mathcal{K}} = \#\left(\ker(\beta)/\mathrm{im}(\alpha)\right)^{\mathrm{Gal}(\overline{k}/k)}$

Remark 62. Note that $\mathrm{im}(\alpha) \subseteq \ker(\beta)$ since for fixed i we have an identity

$$\sum_{j=1}^{n} m_j (T_i \cdot T_j)$$

since this is the intersection of T_i with the whole special fibre.

Example 63. Consider $E : y^2 = x^3 + 2x^2 + p^2$ over $\mathbb{Q}_p$ for an odd prime p. Then you obtain a nodal cubic whose singular point is not regular. This is an elliptic curve of type II.

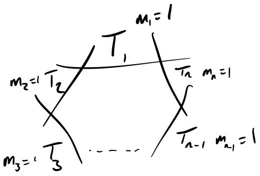


We get $\ker(\beta) = \langle T_1 - T_2 \rangle_{\mathbb{Z}}$, and

$$\alpha(T_1) = (T_1 \cdot T_1)T_1 + (T_1 \cdot T_2)T_2 = -2T_1 + 2T_2 = -2(T_1 - T_2) = -\alpha(T_2),$$

so $\Phi_A \cong \mathbb{Z}/2\mathbb{Z}$. Note that Galois swaps T_1 and T_2 or acts trivially, and in both cases we have trivial action on Φ_A.

Example 64. For $n \geq 3$ consider an elliptic curve with reduction type I_n.



Then $\ker(\beta) = \langle T_i - T_{i+1} \ : \ i \in \{1, \ldots, n-1\} \rangle_{\mathbb{Z}}$. Write $M = ((T_i \cdot T_j))_{1 \leq i,j \leq n}$, then

$$\alpha : a \mapsto a \cdot M,$$

the image of α is thus spanned by the columns of M. Computing this we get

$$M = \begin{pmatrix} -2 & 1 & 0 & \ldots & 0 & 1 \\ 1 & -2 & 1 & \ldots & 0 & 0 \\ 0 & 1 & -2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & \ldots & 1 & -2 \end{pmatrix}.$$

Then we just get $\mathrm{im}(\alpha) = \langle T_1 - 2T_2 + T_3, \ \ldots, \ T_{n-2} - 2T_{n-1} + T_n, n(T_{n-1} - T_n) \rangle_{\mathbb{Z}}$, and $\Phi_A \cong \mathbb{Z}/n\mathbb{Z}$.

If Galois acts trivially then $c = n$, and else Galois acts nontrivially and we see the only options depend on parity of n:

- If n is odd then we get $c = 1$;

- If n is even then we get $c = 2$;

Lecture 6 (Ross): Minimal rnc Models I

Notation 65. Today we adopt the following notation.

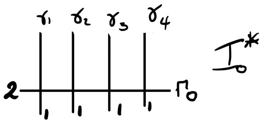
- R is a DVR
- $K = \mathrm{Frac}(R)$ is the fraction field
- k is the residue field
- C/K is a curve of genus $g > 0$ with rnc model $\mathscr{C}/R$.

Dual Graphs

For each of the finitely many components of the special fibre $\Gamma \subseteq \mathscr{C}_s$, we write

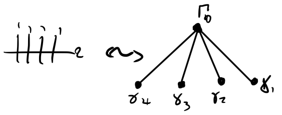
- g_Γ for the geometric genus;
- $g^a_\Gamma = g_\Gamma + \#\{\text{loops}\}$ for the arithmetic genus;
- m_Γ for the multiplicity of Γ, so that as a divisor on $\mathscr{C}$ we have $\mathscr{C}_s = \sum_\Gamma m_\Gamma \Gamma$.

Example 66 (I_0^*)**.** Consider an elliptic curve with I_0^* reduction, for example $py^2 = x(x-1)(x+1)$. Then in this case all of the components are smooth $\mathbb{P}^1$s, hence $g_\Gamma = 0$

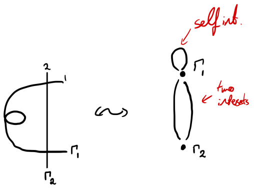


Definition 67. The dual graph of $\mathscr{C}_s$ is the graph with vertices given by the irreducible components of $\mathscr{C}_s$ and edges for each ordinary double point.

Example 68 (I_0^*)**.** We have the dual graph of the I_0^* reduction type:



Example 69. Here is a more exotic reduction and its dual graph:



Self Intersection Formula

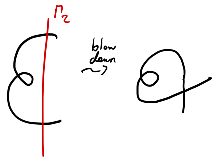
Lemma 70. *Let $\Gamma \subset \mathscr{C}_s$ be an irreducible component, and let $\Gamma_1, \ldots, \Gamma_r$ be the end point of all edges which are not loops out of Γ in the dual graph. Then*

$$\Gamma \cdot \Gamma = -\frac{m_{\Gamma_1}\Gamma_1 \cdot \Gamma + \cdots + m_{\Gamma_r}\Gamma_r \cdot \Gamma}{m_\Gamma},$$

and moreover $\Gamma \cdot \Gamma = 0$ if and only if $\Gamma = \mathscr{C}_s$ is the full special fibre.

Example 71 (I_0^*)**.** Continuing Example 68 we can now compute $\Gamma_0 \cdot \Gamma_0 = -2$ and $\gamma_i \cdot \gamma_i = -2$. In particular we have a minimal model since there are no -1 curves to blow down.

Example 72. Continuing Example 69 we can now compute $\Gamma_1 \cdot \Gamma_1 = -4$ (note that there are two edges!) and $\Gamma_2 \cdot \Gamma_2 = -1$. Looking at Γ_2 we see that in fact it is a smooth $\mathbb{P}^1$ which can be blown down and so the minimal model can be obtained as:



Proof of Lemma 70. We apply results Proposition 32 to obtain that $0 = \Gamma \cdot \mathscr{C}_s = \sum_\gamma m_\gamma (\Gamma \cdot \gamma)$, so that when we rearrange

$$\begin{aligned} m_\Gamma(\Gamma \cdot \Gamma) &= -\sum_{\gamma \neq \gamma} m_\gamma(\Gamma \cdot \gamma) \\ &= -\sum_{i=1}^{r} m_{\Gamma_i}, \end{aligned}$$

as required. The second claim is simply Proposition 32(b)(iii). □

Principal Components

Let Γ and $\Gamma_1, \ldots, \Gamma_r$ be as above.

Definition 73. Γ is principal if

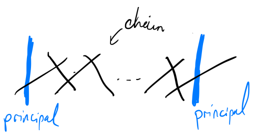
(1) Arithmetic genus $g^a_\Gamma > 0$ (i.e. $g_\Gamma > 0$ or there are loops);
(2) $r \geq 3$.

Thus Γ is non-principal if it has geometric genus 0 and at most two edges and no loops connected to it in the dual graph

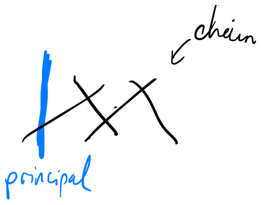
Remark 74. The only reduction in genus > 0 with no principal components is I_n and its multiples.

Note that non-principal components form chains of smooth $\mathbb{P}^1$s, and that these come in two flavours:

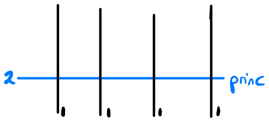
Links:



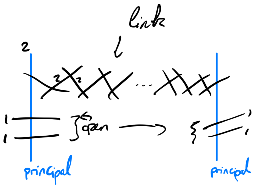
Chains:



Example 75. Continuing with the example of I_0^* reduction, we have 4 chains attached to one principal component:



Example 76. Consider I_n^* reduction, then we have a link and 4 chains:



Our goal for the rest of this talk and the next talk will be to classify minimal rnc models, which we break into two problems:

- Classify all possible principal components (next time)
- Classify all possible chains (today)

Chains

Suppose we have a link chain, so that the dual graph has a line:

$$\Gamma_0 \text{ —— } \Gamma_1 \text{ —— } \dots \text{ —— } \Gamma_r \text{ —— } \Gamma_{r+1}.$$

For brevity, let us further write $d_i = m_{\Gamma_i}$ for the multiplicity of Γ_i in $\mathscr{C}_s$.

Hence by Lemma 70, for the components in our link (i.e. for $i \in \{1, \dots, r\}$) we have

$$\Gamma_i \cdot \Gamma_i = -\frac{d_{i-1} + d_{i+1}}{d_i} \in \mathbb{Z}_{\leq 0}. \tag{2}$$

Moreover $\mathscr{C}$ is minimal rnc if and only if $\Gamma \cdot \Gamma < -1$ for every non-principal component Γ in $\mathscr{C}_s$, so we obtain minimality by reducing chains.

Using the theorem of Winters (Theorem 50) we see that it is enough to check what sequences $(d_i)_i$ are possible combinatorially, since we can then construct a geometric realisation. The correct definition for the sequences allowed by geometry is the following.

Definition 77. $d_0, \dots, d_{r+1} \in \mathbb{Z}_{\geq 1}$ is a link sequence if for all $i \in \{1, \dots, r\}$ we have

$$\frac{d_{i-1} + d_{i+1}}{d_i} \in \mathbb{Z}_{>1}.$$

Example 78. In the case of I_n^* in Example 76 we get the sequence $2, 2, \dots, 2$. But there are plenty more (non-constant) sequences we can have, for example:

- 6,5,4,3,2,1;
- 8,3,1,1,1,3,8.

Remark 79. Note the following properties of a link sequence:

- $d_{i-1} \equiv -d_{i+1} \mod d_i$, so in particular $\gcd(d_{i-1}, d_i) = \gcd(d_i, d_{i+1})$. Hence we obtain
$$\gcd(d_0, d_1) = \gcd(d_1, d_2) = \dots = \gcd(d_r, d_{r+1}).$$
In particular these are all equal to $\gcd(d_0, \dots, d_{r+1})$. Hence since our link is always a multiple of one with $\gcd = 1$, we can reduce to that case.
- Since $d_{i-1} + d_{i+1} \geq 2d_i$, there are no local maxima, so every sequence either monotonically decreases, monotonically increases, or decreases then increases with one minimal in the middle.

Definition 80. The depth of a link sequence $(d_i)_{i=0}^{r+1}$ with $\gcd(d_0, \dots, d_{r+1}) = g$ is

$$\#\{i \ : \ d_i = g\} - 1.$$

Example 81. The depths of some sequences are:

- $6, 5, 4, 3, 2, 1$ is 0;
- $8, 3, 1, 1, 1, 3, 8$ is 2;
- the link chain in I_n^* is n.

Definition 82. Define

$$i(d, m) := \min \{x \in \mathbb{Z}_{>0} \ : \ dx \equiv \gcd(d, m) \mod m\}.$$

We now have the main classification theorem for (link) chains.

Theorem 83 (Hirzebruch–Jung, Obus–Wewers, Dokchitser)**.** *Fix $d_0, d_r + 1$ and the classes of $d_1 \mod d_0$ and $d_r \mod d_{r+1}$. Then for any link chain $(d_0, \dots, d_{r+1})$ satisfying these of depth n, we have*

(1) $\gcd(d_0, d_1) = \gcd(d_r, d_{r+1})$*;*
(2) $n + \frac{i(d_1, d_0)}{d_0} + \frac{i(d_r, d_{r+1})}{d_{r+1}} > 0.$

Conversely, under such conditions a chain exists and is unique.

Remark 84. For open chains you can set d_{r+1} and obtain analogous results (without a depth parameter) classifying (uniquely!) open chains.

Lecture 7 (Sam F): L-Functions

We'll talk about L-functions. You've probably seen one before, for example the Riemann zeta function:

$$\zeta(s) := \sum_{n \geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1};$$

or an $L-$function associated to a Dirichlet character:

$$L(\chi, s) := \sum_{n \geq 1} \chi(n) n^{-s};$$

or the L-function assoiated to an elliptic curve $E/\mathbb{Q}$:

$$L(E, s) := \prod_p L_p(E, p^{-s})^{-1} \approx \prod_p (1 - a_p p^{-s} + p \cdot p^{-2s})^{-1},$$

where really
(3)

$$L_p(E, T) := \begin{cases} 1 - a_p T + pT^2 & \text{if good reduction} \\ 1 - T & \text{if multiplicative reduction with trivial Frobenius action on tangent lines at the s} \\ 1 + T & \text{if multiplicative reduction with Frobenius action swapping tangent lines at the s} \\ 1 & \text{if additive reduction} \end{cases}$$

Morally: L-functions should come from Galois representations. Now to set some notation.

Notation 85. Let $\ell \neq p$ be primes, $X/\mathbb{Q}_p$ be a 'nice' variety, and shorten

$$H^i(X) := H^i_{\text{ét}}(X, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Let $G_p := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, let $I_p \leq G_p$ be the inertia subgroup, and choose a(n arithmetic) Frobenius element $\mathrm{Frob}_p \in G_p$. For a $\mathbb{Q}_\ell$-vector space V (with G_p-action) we write

$$V^\vee := \mathrm{Hom}_{\mathbb{Q}_\ell}(V, \mathbb{Q}_\ell),$$

where we act on a homomorphism f by $\sigma \in G_p$ via

$$\sigma \cdot f(x) := f(\sigma^{-1}x)$$

How do we define an associated L-function? As follows.

Definition 86. With notation as above, we write:

$$L_p(H^i(X), T) := \det\left(1 - \mathrm{Frob}_p^{-1} T \mid H^i(X)^{I_p}\right).$$

Remark 87. Note that the action of Frobenius is well defined and independent of the choice of Frobenius element when we are looking at $H^i(X)^{I_p}$, since any two Frobenii differ by an element of I_p.

Example 88. If $X = \mathrm{Spec}(\mathbb{Q}_p)$ then $H^0(X) \cong \mathbb{Q}_\ell$ with trivial G_p-action. In particular, $H^0(X)^{I_p} = H^0(X)$, and Frobenius also acts trivially so we get

$$L_p(H^i(\mathrm{Spec}(\mathbb{Q}_p), T) = 1 - T,$$

which is the correct factor for $\zeta(s)$ when $T = p^{-s}$!

Elliptic Curves

Let $E/\mathbb{Q}_p$ be an elliptic curve. Then recall the Tate module

$$T_\ell(E) := \lim_{\leftarrow} E[\ell^n],$$

and write $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Recall also the following, which we take as a fact:

Fact: $H^1_{\text{ét}}(E, \mathbb{Z}_p) \cong T_\ell(E)^\vee$, and so $H^1(E) \cong V_\ell(E)^\vee$.

Good Reduction.

Theorem 89 (Néron–Ogg–Shafarevich)**.** *E has good reduction if and only if $E[\ell^n]$ is unramified for all n (and $\ell \neq p$). This is also is equivalent to $T_\ell(E)$ being unramified, or equivalently $V_\ell(E)$ being unramified.*

Note that this means that when we have good reduction for $E/\mathbb{Q}_p$ we get $H^1(E)^{I_p} = H^1(E)$. Moreover then the characteristic polynomial of Frobenius on $T_\ell(E)$ is $T^2 - a_pT + p$ and so since $H^1(E)$ is dual to it, the characteristic polynomial of Frobenius inverse is the same (and as presented in (3)).

Multiplicative Reduction. Here we have a nodal cusp on the reduction. There is then the theory of Tate curves.

Theorem 90 (Tate)**.** *If $E/\mathbb{Q}_p$ has split multiplicative reduction then there exists an element $q \in {\mathbb{Q}_p}^\times$ with $|q| < 1$ such that*

$$E(\overline{\mathbb{Q}_p}) \cong \overline{\mathbb{Q}_p}^\times / q^{\mathbb{Z}},$$

as G_p-modules.

In particular, when there is split multiplicative reduction, we have

$$E[\ell^n] \cong \mu_\ell^n \times \left\langle q^{1/\ell^n} \right\rangle .$$

In particular, if $K = \mathbb{Q}_p(\mu_{\ell^n})$ then $K(q^{1/n})/K$ is totally ramified, and $K/\mathbb{Q}_p$ is unramified. Moreover any Galois element acts by

$$\sigma : q^{1/n} \mapsto \zeta q^{1/n}$$

for some $\zeta \in \mu_{\ell^n}$, and so lifts to an element in I_p.

Fix $(\zeta, 1)$ and $(1, q^{1/\ell^n})$ as a basis for $E[\ell^n]$. Looking at how such a σ acts,

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

on the Tate module $V_\ell(E)$. In particular, σ acts on $H^1(E) = T_\ell(E)^\vee$ as the transpose inverse and so as $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$.

This allows us to conclude that $(T_\ell(E)^\vee)^{I_p} \cong \mathbb{Q}_\ell$ is 1-dimensional since $K/\mathbb{Q}_\ell$ was unramified and so we have characterised all Inertia action above. We then have action by Frobenius which fixes q^{1/ℓ^n} and maps $\zeta \mapsto \zeta^p$. Hence

$$\mathrm{Frob}_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \text{ on } T_\ell(E).$$

Hence the action by the inverse transpose (i.e. the action on $H^1(E)$) is then $\begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ and since we are only interested in the inertia invariants (the right hand column) we end up with trivial Frobenius action and so

$$L_p(H^1(E), T) = 1 - T.$$

Remark 91. In the non-split case one tensors this whole thing with the unramified quadratic character χ to obtain $1 + T$ at the end.

Why Tate curves? Why should we have had this weird isomorphism of Tate? Well, we'd like to generalise the situation over $\mathbb{C}$ where

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda,$$

except $\overline{\mathbb{Q}_p}/\Lambda$ is not so nice when Λ is a lattice. If we instead exponentiate, so $E(\mathbb{C}) \cong \mathbb{C}^\times/q^\Lambda$, where $q = e^{2\pi z}$, then everything works the same for $\mathbb{C}$ and now it is nice for $\mathbb{Q}_p$. It turns out that the conditions needed to make all the power series etc converge is in fact multiplicative reduction!

Models of Curves

Let $\mathcal{E}/\mathbb{Z}_p$ be the Néron model for E. We get the following.

Theorem 92.

$$H^1_{\acute{e}t}(E, \mathbb{Q}_\ell)^{I_p} \cong H^1_{\acute{e}t}(\mathcal{E}_{\mathbb{F}_p}, \mathbb{Q}_\ell)^{I_p}$$

Remark 93. For a nice curve C, we get $H^1(C) \cong H^1(\mathrm{Jac}(C))$.

Sketch proof. $\mathcal{E}[\ell^n]$ is quasi-finite over $\mathbb{Z}_p$, and is isomorphic to some finite $\mathcal{F} \sqcup$stuff with empty special fibre. $E[\ell^n]^{I_p} \cong \mathcal{E}[\ell^n](\overline{\mathbb{Q}_p})^{I_p} \cong \mathcal{F}(\overline{\mathbb{Q}_p}) \cong \mathcal{F}(\overline{\mathbb{F}_p}) = \mathcal{E}(\overline{\mathbb{F}_p})$ (so when one dualises one reaches the trivial module!). □

Lemma 94. *In the multiplicative reduction case,*

$$L_p(H^1(E),T) = \begin{cases} 1-T & \textit{if} \\ 1+T & \textit{if} \end{cases}$$

Proof. The special fibre of $\mathcal{E}$ is $\mathbb{G}_m \times \mathbb{Z}/n$.

$$\lim_{\leftarrow} \mathcal{E}_{\mathbb{F}_p}[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \lim_{\leftarrow} \mu_{\ell^n} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

with Galois action. □

Lecture 8 (Matt): Galois Representations

Notation 95.

- K non archimedean local field;
- $\mathcal{O}_K$ the valuation ring;
- k the residue field of characteristic $p \neq \ell$;
- I_K the inertia in G_K the absolute Galois group;
- Frob is the geometric Frobenius;
- C/K a nice curve with model $\mathscr{C}/\mathcal{O}_K$;
- For a G_K representation ρ, we write $L(\rho,T) = \det(1 - \mathrm{Frob}T|\rho^{I_K})$;
- $L(C,T) = L(H^1(C),T)$ where $H^1(C) := H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_\ell)$.

Our aim today is to use models to construct Euler factors and recover information about $H^1(C)$.

Theorem 96. *Let ρ be an Artin representation of G_K, i.e. one which factors through a finite extension. Then*

(1) If ρ is unramified then $L(\rho,T)$ determines ρ;

(2) If $\mathcal{F} = \{F/K : \mathrm{Res}_{G_F}\rho \text{ is unramified}\}$, then $\{L(\mathrm{Res}_{G_F}\rho, T)\}_{F\in\mathcal{F}}$ determines ρ.

Corollary 97. *One can recover $H^1(C)$ from understanding Euler factors for fields where C is semistable.*

In fact if $K/\mathbb{Q}_p$ then one can take a finite set $\mathcal{F}$ only depending on the genus $g(C)$.

Example 98.

(1) $\rho = \chi_{\text{cyc}}^k$, $k \in \mathbb{C}$ where χ_{cyc} is unramified, $\chi_{\text{cyc}}(\text{Frob}) = q$. Then

$$L(\rho,T) = 1 - q^k T.$$

(2) Let χ be the quadratic character of $\mathrm{Gal}(\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p)$, then the restriction map induces an isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p(\sqrt{u},\sqrt{p})/\mathbb{Q}_p(\sqrt{up})) \cong \mathrm{Gal}(\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p).$$

But moving a character χ on the right to one $\tilde{\chi}$ on the left, we have an unramified character so can compute $\tilde{\chi} = \mathrm{Res}_{\mathbb{Q}(\sqrt{up})}$ from $L(\tilde{\chi},T)$.

(3) $E : y^2 = x^3 + 7^4/\mathbb{Q}_7$. Note that E does not have good reduction but it does over $F = \mathbb{Q}_7(\sqrt[3]{7})$. Hence by Néron–Ogg–Shafarevich the Galois action factors through $\mathrm{Gal}(\mathbb{Q}_7^{\text{nr}}(\sqrt[3]{7})/\mathbb{Q}_7) \cong C_3$. Fix $\zeta_3 \equiv 2 \mod 7$ in $\mathbb{Q}_7$ and let $\iota : \sqrt[3]{7} \mapsto \zeta_3\sqrt[3]{7}$. So

$$\rho_E(\iota) = \begin{pmatrix} \frac{-1+\sqrt{-3}}{2} & 0 \\ 0 & \frac{-1-\sqrt{-3}}{2} \end{pmatrix},$$

since this is an order 3 matrix with trivial determinant by the Weil pairing (where we are diagonalising). Moreover $\rho(\mathrm{Frob}) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ The point count over $F = \mathbb{Q}_7(\sqrt[3]{7}) : y^2 = x^3 + 1$ which has 12 $\mathbb{F}_7$ points so $\{\alpha, \beta\} = \{-2 \pm \sqrt{-3}\}$.

Let $F' = \mathbb{Q}_7(\sqrt[3]{14})$, then it is an exercise to show that $\mathrm{Frob}_F\iota$ is a Frobenius element for F'. Now over F' we have $E \cong y^2 = x^3 + 2^{-4}$ and $\#E_{F'}(\mathbb{F}_7) = 3$. Hence the eigenvalues are $\frac{1}{2}(5 \pm \sqrt{-3})$. Hence $\alpha = -2 - \sqrt{-3}$ and $\beta = -2 + \sqrt{-3}$.

Exercise 99. Have some exercises!

(1) Redo the last example with $p = 5$.
(2) Describe $H^1(C)$ for $C : y^2 = x^p - p/\mathbb{Q}_p$ (warning, hard!)

Now let's look at recovering the Euler factor from $\mathscr{C}$. Similar to last time, we have the following.

Theorem 100. *Suppose $\mathscr{C}/\mathcal{O}_K$ is a proper regular model. Then as $G_k \cong G_K/I_K$-modules we have*

$$H^1_{\acute{e}t}(C) \cong H^1_{\acute{e}t}(\mathscr{C}_{\bar{k}}) \cong H^1_{\acute{e}t}(\mathscr{C}^{\mathrm{red}}_{\bar{k}}).$$

where the first isomorphism holds with $\mathbb{Z}_\ell$-coefficients for most ℓ, and the second is true for $\mathbb{Z}_\ell$-coefficients for all ℓ.

Theorem 101. *Let $X/\mathbb{F}_q$ be a separated variety, then*

$$Z(X,T) := \exp\left(\sum_{n \geq 1} \frac{|X(\mathbb{F}_{q^n})|}{n} T^n\right) = \prod_i \det\left(1 - \mathrm{Frob}T | H^i_c(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}},$$

where the subscript c refers to compactly supported cohomology.

Corollary 102. *Let $\mathscr{C}/\mathcal{O}_K$ be a proper regular model. Then*

$$Z(\mathscr{C}^{\mathrm{red}}_{(k)}, T) = \frac{P_1(T)}{P_0(T)P_2(T)},$$

where $P_i(T) := \left(1 - \mathrm{Frob}T | H^i_{\acute{e}t}(\mathscr{C}^{\mathrm{red}}_{\bar{k}})\right)$. Moreover, $P_0(T) = 1 - T$ and $H^2_{\acute{e}t}(\mathscr{C}^{\mathrm{red}}_{\bar{k}}) \cong \mathbb{Q}_\ell(1)[\text{irreducible components}]$ as a G_k-module.

We want $L(C,T) = P_1(T)$. Recall that $\log(1 - T) = -\sum_{n \geq 1} \frac{T^n}{n}$.

Example 103. Consider type II elliptic curves. Note that Frobenius acts trivially as components have different multiplicities. We now compute directly:

$$H^2_{\mathrm{\acute{e}t}}(\mathscr{C}) = \mathbb{Q}_\ell(1)^{\oplus 3},$$

so $P_2(T) = (1-qT)^3$. Let us now compute $P_1(T)$: our point counts are $\mathscr{C}_k(\mathbb{F}_{q^m}) = 3(q^m+1) - 2 = 3q^m + 1$, and now looking at the zeta function

$$\begin{aligned} Z(\mathscr{C}^{\mathrm{red}}_{\overline{k}}, T) &= \exp\left(\sum_{n\geq 1} \frac{3p^m+1}{m} T^m\right) \\ &= \exp\left(3\sum_{n\geq 1} \frac{q^m}{m} T^m + \sum_{n\geq 1} \frac{1}{m} T^m\right) \\ &= \exp\left(-3\log(1-qT) - \log(1-T)\right) \\ &= \frac{1}{(1-T)(1-qT)^3}. \end{aligned}$$

Hence $L(C,T) = Z(\mathscr{C}^{\mathrm{red}}_{\overline{k}}, T)P_0(T)P_2(T) = 1$.

Example 104. Consider type I_n for n even where Frobenius acts nontrivially as C_2 flipping the graph.

Note that we can easily count points to obtain

$$\mathscr{C}_k(\mathbb{F}_{q^m}) = \begin{cases} 2(q^m+1) & \text{if } m \text{ is odd;} \\ nq^m & \text{if } m \text{ is even.} \end{cases}$$

Hence

$$\begin{aligned} Z(\mathscr{C}^{\mathrm{red}}_{\overline{k}}, T) &= \exp\left(\sum_{m \text{ even}} \frac{(n-2)q^m - 2}{m} T^m + \sum_{m\geq 1} \frac{2q^m+2}{m} T^m\right) \\ &= \exp\left(\sum_{s\geq 1} \frac{(n-2)q^{2s} - 2}{2s} T^{2s} + \sum_{m\geq 1} \frac{2q^m+2}{m} T^m\right) \end{aligned}$$

Considering each factor separately:

$$\begin{aligned} \exp\left(\sum_{s\geq 1} \frac{(n-2)q^{2s} - 2}{2s} T^{2s}\right) &= \exp\left(\sum_{s\geq 1} \frac{\frac{n-2}{2}q^{2s}q^{2s}}{s} T^{2s} + \sum_{s\geq 1} \frac{1}{s} T^{2s}\right) \\ &= \frac{1-T^2}{(1-q^2T^2)^{(n-2)/2}}. \end{aligned}$$

Hence $Z(\mathscr{C}^{\mathrm{red}}, T) = \frac{1-T^2}{(1-q^2T^2)^{(n-2)/2}(1-T)^2(1-qT)^2} = \frac{1+T}{1-q^2T^2}^{(n-2)/2}(1-T)(1-qT)^2$. In particular we know

$$P_2(T) = (1-qT)^2(1-q^2T^2)^{(n-2)/2},$$

where the first factor comes from 2 rational $\mathbb{P}^1$s and the latter from the non-rational ones. Hence $L(C,T) = 1+T$.