NOTES ON THE ARITHMETIC OF ALGEBRAIC CURVES

PETE L. CLARK

1. What's Nice About Algebraic Curves

In this course we are going to study algebraic curves – i.e., one-dimensional algebraic varieties – and how they vary in one-parameter families.

In fact curves are by far the most intensively studied class of algebraic varieties (and this is true pretty much across the board, from complex algebraic geometers to arithmetic geometers).[1] Let us begin by recalling some nice properties that curves have and most higher-dimensional varieties lack.

1. Topological classification: Here let us work, for simplicity, over the complex numbers (although with suitable technology, one can establish quite similar results in positive characteristic). Any smooth, projective connected algebraic variety over $\mathbb{C}$ determines a complex manifold, whose complex dimension is equal to the algebraic dimension of the variety and therefore whose dimension as a real manifold is equal to twice that. Therefore a complex algebraic curve gives rise to a compact topological surface, whereas a complex surface gives rise to a compact topological 4-manifold. But the jump in topological complexity between 2-dimensional manifolds and 4-dimensional manifolds is extreme. Every (orientable, as all $\mathbb{C}$-manifolds are) compact surface is homeomorphic to a g-holed torus (a 0-holed torus being a sphere). Thus there is a single topological invariant, the **genus** g. Moreover the topology of a genus g surface is well-understood: in particular its fundamental group is known to be

$$\Pi(g) = \langle a_1, b_1, \ldots, a_g, b_g \mid [a_1, b_1] \cdots [a_g, b_g] = 1\rangle.$$

On the other hand, *every* finitely presented group is the fundamental group of some compact topological 4-manifold. Being the fundamental group of an algebraic complex manifold brings some additional restrictions: for instance, Hodge theory implies that its abelianization is of the form $\mathbb{Z}^{2n} \oplus T$ where T is a finite abelian group – i.e., its first Betti number must be even. In fact it can be shown that a finitely presented group is the fundamental group of an algebraic surface iff it is the fundamental group of any smooth algebraic variety (iff it is the fundamental group of a compact Kähler manifold). Exactly what class of groups this might be is a fascinating open problem: indeed there is a book called **Fundamental Groups of Compact Kähler Manifolds** (which does not come close to solving the problem, but presents lots of interesting results).

This observation has important geometric consequences: when one studies families of algebraic varieties – roughly speaking, **moduli spaces** – in order to for the

[1]Probably second place goes to abelian varieties, in part because of their close relationship with curves.

family to form a connected variety, one needs to fix all the discrete invariants of the family. In fact, in any connected family of smooth varieties, the members of the family must all be homeomorphic to each other.[2] Thus it is natural to study $\mathcal{M}_g$, the family of all (isomorphism classes of) nice algebraic curves of fixed genus $g \in \mathbb{N}$. If we wanted to study the family of all algebraic curves, it would be $\coprod_{g=0}^{\infty} \mathcal{M}_g$, i.e., an infinite disjoint union of connected components. Such a thing exists as a scheme (the category of schemes is closed under all disjoint unions) but it is non-Noetherian and not of finite type, so certainly is not itself an algebraic variety. For all of these reasons we are very far from understanding the moduli spaces of higher-dimensional varieties in general.

2. Desingularization via normalization: let V be a variety over a field k which is geometrically integral (i.e., when viewed as a scheme over the algebraic closure of k it is reduced and irreducible) but not necessarily regular: i.e., not all local rings are regular.[3] In fact, suppose that it is not regular: it "has singularities." One of the most important problems in all of algebraic geometry (again, across the various flavors and subdisciplines) is to **resolve the singularities** of V. By definition, this means finding a nonsingular variety $\tilde{V}$ together with a proper birational morphism $f : \tilde{V} \to V$ which is an isomorphism on the preimage of the nonsingular points.

Some history on this problem: resolution of singularities for complex algebraic surfaces was done in the early twentieth century by various people and with various degrees of rigor. The first algebraic proof – valid, in particular, for all fields of characteristic 0 – is due to Zariski (1939). Later (1944), Zariski extended his work to threefolds in characteristic 0. The case of surfaces of arbitrary positive characteristic was done by Abyhankar in 1956; later (1966) Abhyankar resolved singularities of threefolds in characteristic $p > 5$. Resolution of singularities for all dimensions in characteristic 0 was done by Hironaka in 1964, for which he received the Fields Medal. (Finally, resolution of singularities of **arithmetic surfaces** was done by a variety of people in the sixties and seventies – we will cover this result later in the course.) The other cases in positive characteristic remain open!

For curves, however desingularization is comparatively trivial. Indeed there are two possibilities: upon embedding a curve in a nonsingular surface, one can resolve singularities by repeatedly **blowing up**: this is often preferred computationally. More intrinsically though, for any integral scheme S we can consider its **normalization** $S^n \to S$. This is just geometric language for taking the integral closure. Recall the following algebraic fact:

Theorem 1. *Let R be a local Noetherian domain of dimension one. The following are equivalent:*
a) R is normal, i.e., integrally closed in its fraction field.
b) R is nonsingular, i.e., if $\mathfrak{m}$ is the maximal ideal, then the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over the field $R/\mathfrak{m}$ is 1.
c) R is a discrete valuation ring (DVR).

[2]This is an important and nontrivial fact that, for some reason, seems not to get mentioned explicitly in most texts.

[3]We will review all this terminology in more detail later, so don't worry (yet) if you are hazy on the exact meanings of these terms.

Geometrically, this means that a normal algebraic variety is "nonsingular in codimension one": its singular locus consists of subvarities of codimension two or more. But aha – for algebraic curves, codimension two or more means empty! Thus desingularization is equivalent to normalization in dimension one.

Example: Take the standard affine curve with a cusp singularity: $A = k[x, y]/(y^2 - x^3)$. A little bit of thought shows that this k-algebra is isomorphic to $k[t^2, t^3]$ and that its integral closure is just $k[t]$. The map $\mathbb{A}^1 = \operatorname{Spec} k[t] \to \operatorname{Spec} A$ is an isomorphism on all local rings except the origin.

Remark: It turns out that the desingularization of surfaces (including arithmetic surfaces) proceeds as follows: first normalize, giving a normal two-dimesional scheme, so that its singular locus consists of finitely many isolated points. Then repeatedly blow up each of these singular points until all its preimages become nonsingular. So in practice this is not much harder than the one-dimensional case. But we will still have to prove that this is the case!

In contrast, a normal 3-fold may be singular along entire curves, and blowing up need not rectify this. I confess to not personally knowing what to do, although others (even others close by) certainly do.

3. Birational models

Another problem, somehow complementary to the desingularization problem, is the problem of regular models. Let $V_{/k}$ be a geometrically integral variety, with function field $K = k(V)$. A **regular model** for V is a complete regular variety W which is birationally equivalent to V: i.e., $k(V) \cong k(W)$. In other words, we have rational maps between V and W each inducing the identity on the function fields. In any equivalence class of rational maps $f : X \to Y$ there is a unique map which is defined on a largest possible dense open subset U of X. The complement $X \setminus U$ is called the **indeterminacy locus** of f. We have the following basic result:

Theorem 2. *Let $f : X \to Y$ be a rational map from a regular variety X to a complete variety Y. Then the indeterminacy locus of f has codimension at least* 2.

For curves this implies the following:

Theorem 3. *(Liu, Prop. 7.13) Let $X_{/k}$ be an integral curve. Then there is, up to isomorphism, a unique projective regular curve $C_{/k}$ with $k(C) \cong k(X)$.*

Because of this theorem one can reduce the study of algebraic curves to the study of one-variable (i.e., transcendence degree 1) function fields. Moreover, one can give a curve by a singular equation and refer, harmlessly and unambiguously, to the corresponding associated complete regular curve. For instance, hyperelliptic curves are generally given in this way. Of course this does not hold for higher dimensional varieties: given any regular model, one can blow up as many times as one likes to get a nonisomorphic model.

There is one minor caveat for curves over an imperfect field k: we know that normal = regular, but that need not imply **smooth**. Indeed smoothness is the more geometric property: a variety $X_{/k}$ is smooth iff its basechange to $X_{/\overline{k}}$ is smooth. Looking at the above theorem, we see that birational modification has nothing to do with this: the function field $k(X)$ of a nonsmooth integral curve has an intrinsic pathology which we will discuss later.

4. Structure of (geometrically) irreducible subvarieties

Given an algebraic variety $V_{/k}$, one often wants to know about all of its irreducible subvarieties. In general, they have complicated geometry. However, the only (geometrically) irreducible subvarieties of an algebraic curve are the points and the curve itself: much easier! (So, for instance, the Hodge conjecture holds trivially for complex algebraic curves.) On any (nice) variety V, the zero-dimensional subvarieties – 0-cycles – and codimension one subvarieties – divisors – are especially important. Indeed, one can associate to V one abelian variety, the **Albanese abelian variety** by taking 0-cycles of degree 0 modulo a certain equivalence relation, and another abelian vareity, the **Picard variety**, by taking divisors of degree 0 modulo a(n obviously different) equivalence relation. It turns out that the Albanese and Picard varieties are naturally **dual** in the sense of abelian varieties, but they need not be isomorphic. However for a curve we tautologically have Albanese = Picard, and thus either one is self-dual. Instead of Albanese or Picard one often says **Jacobian variety**.

Ironically, the passage from curves to arithmetic surfaces involves "giving back" all of these nice properties: we will have (i) in general a complicated topology (as regards, e.g. the combinatorial structure of singular fibers), (ii) work to do to show that our desingularization recipe always works, (iii) more than one "canonical" regular model, and (iv) a more complicated construction of the Picard variety.

2. Course outline

This course is devoted to the arithmetic algebraic geometry of algebraic curves. It consists of the following parts:

Part 0: A general review of varieties over an arbitrary field k, together with some basic scheme theory.

Part 1: A study of nice (= smooth, projective, geometrically connected) curves over an arbitrary field k.

Especially, we wish to examine what differences a non-algebraically closed field brings. The greater part of the theory goes through verbatim or with easy modifications: especially, theory of divisors and line bundles, Riemann-Roch theorem. A few sample differences:

(i) Over an imperfect field, one must distinguish between normal curves and smooth curves.
(ii) Every curve over an infinite field embeds in $\mathbb{P}^3$. Over every finite field k there exists a sequence of curves C_n with $\#C_n(\mathbb{F}_q) \rightarrow \infty$; clearly only finitely many of these curves can be embedded in any fixed $\mathbb{P}^N$!
(iii) Additional features may arise when $C(k) = \emptyset$, in particular:
(iiia) A smooth conic need not be isomorphic (or birational) to $\mathbb{P}^1$;
(iiib) A genus one curve need not be an elliptic curve, and need not be embeddable

into $\mathbb{P}^2$ via a cubic equation.
(iiic) A rational divisor class on C need not contain any rational divisor.

Part 3: Families of curves.

In algebraic geometry it is inevitable that we study not just individual algebraic varieties, but algebraic families of algebraic varieties. Indeed, the fact a morphism $f : V \to B$ of algebraic varieties can also be viewed as a family of varieties over the base B is probably the single most ubiquitous trick in the subject. The key property on f that one imposes in order to get some continuity on the fibers – i.e., in order for the fibers to resemble each other in some way – is **flatness**. For a flat map (over a connected base) the dimensions of the fibers are constant. In particular, let V be any projective n-dimensional variety, let $f : V \to \mathbb{P}^1$ be a nonconstant rational function on f; then we can view V as a parameterized family of $n-1$-dimensional varieties over $\mathbb{P}^1$. If desired, we can repeat this process on the fibers. So in some sense the basic case to understand (although, to be sure, one might want to understand other cases, if possible) is of a map $f : S \to C$ from a surface to a curve. This can be viewed as a family of curves over a curve: a **fibered surface**.

3. Three Examples

Example 1: Consider the following fibered surface:

$$E_t : y^2 + (-t^2 + t + 1)xy + (-t^3 + t^2)y = x^3 + (-t^3 + t^2)x^2.$$

This gives an (affine) surface in $\mathbb{A}^3$. Moreover, the fiber over (almost!) any t is an elliptic curve. This is an example of an **elliptic surface**. In fact, for every elliptic curve E_t, the rational point $(x, y) = (0, 0)$ is a 7-torsion point, and E_t is indeed the universal family of elliptic curves endowed with a 7-torsion point. Thus, if you want to prove a statement about any elliptic curve over any field with a rational 7-torsion point, you can work with this one surface.

In working with algebraic curves, one is most interested in the (roughly...) universal family, i.e., a family which includes every possible curve up to isomorphism. For each fixed genus, this is given by a family over the moduli space $\mathcal{M}_g$, which is an irreducible variety of dimension $3g - 3$, except when $g = 0$ and $\mathcal{M}_0$ is just a single point, or $g = 1$ and $\mathcal{M}_1 = \mathbb{A}^1_j$ is the affine line.

Note that the affine line is *not* a projective variety. One way to look at it is that the j-invariant is a rational function, and like any nonconstant rational function it must have poles. A cubic equation with $j = \infty$ is singular: equivalently, its discriminant is 0 so it fails to have distinct roots. This happens all the time: for instance, on the above elliptic surface we have[4]

$$\Delta(t) = t^{17} - 15t^{16} + 82t^{15} - 237t^{14} + 413t^{13} - 455t^{12} + 315t^{11} - 127t^{10} + 22t^9 + 2t^8 - t^7$$

so e.g. the fiber $t = 0$ is singular: we get $E_0 : y^2 + xy = x^3$. Notice that this is a nodal singularity.

[4]According to MAGMA...

Geometric digression: an elliptic curve is given by a double cover of $\mathbb{P}^1$ which is branched over 4 points. Because the automorphism group of $\mathbb{P}^1$ (the Riemann sphere, if you like) is triply transitive, we can send the first three points to $0, 1, \infty$ (or whatever your three favorite points on $\mathbb{P}^1$ may be!) but then we have used up our automorphisms and the remaining point must be some element of $\mathbb{P}^1$ different from these three. But over a compact space we would have to be able to take a limit as the fourth point appoached any of the first three, so we must have singular fibers.

So far our discussion has been entirely geometric. But the miracle is that the notion of "family of curves over a smooth, one-dimensional base" is flexible to include also arithmetic families. For instance, let $E_{/Q}$ be any elliptic curve. It can, like any projective variety, be given by a system of equations with coefficients in $\mathbb{Z}$. Then, for any prime p, via the homomorphism $\mathbb{Z} \rightarrow \mathbb{F}_p$, we can view E as a variety over $\mathbb{F}_p$. A moment's thought shows that this is innocuous at leas almost always: in other words, the induced curve over $\mathbb{F}_p$ will have nonzero discriminant except for finitely many primes p (the ones dividing the numerator or denoninator of $\Delta(E) \in \mathbb{Q} \setminus 0$) and away from these primes will define an elliptic curve over $\mathbb{F}_p$. Moreover, any Weierstrass equations will differ by a change of variables which is invertible over $\mathbb{Z}_p$ for all but finitely many p, and that means that except for finitely many fibers, the curve we get does not depend upon the integral equation we have chosen. On the other hand, there may certainly be some bad fibers.

The point is that we really do want to know about these bad fibers as precisely as we can: much of the important information about the curve is contained in them. For instance:

Example 2: Take $d = -1$ in the family above, getting

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

By design, the point $(0, 0)$ is a rational 7-torsion point on E. Now let us reduce E modulo 2. Apparently we get a homomorphism

$$E(\mathbb{Q}) = E(\mathbb{Z}) \xrightarrow{r} \tilde{E}(\mathbb{Z}/2\mathbb{Z}).$$

By some relatively elementary general theory (namely, of formal groups over discrete valuation fields: [Silverman, §IV.6] the kernel of this reduction map has only 2-power torsion. In particular, an odd-order torsion element, like P, must map injectively into $\tilde{E}$.

But now we recall the following beautiful and useful theorem due to André Weil:

Theorem 4. *(Riemann Hypothesis for Curves Over Finite Fields) Let C be a smooth, projective, geometrically connected curve of genus g over a finite field $\mathbb{F}_q$. Then we have the following inequality on the number $\#C(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on C:*

$$|\#C(\mathbb{F}_q) - (q + 1)| \leq \lfloor 2g\sqrt{q} \rfloor.$$

Remark: For instance, a nice proof of this using geometry of surfaces can be found as an exercise in Chapter V of Hartshorne.

Applying $g = 1$, $q = 2$, we get we get $\mathbb{E}(\mathbb{F}_2) \leq 5$ for any elliptic curve over $\mathbb{F}_2$.

But this means something has gone terribly wrong: there is no 7-torsion point here!

The problem is that the Weierstrass equation becomes singular modulo 2: indeed we have $\Delta(E) = -1664$, which is zero modulo 2. Thus it is wrong to speak of the "reduced elliptic curve" $\tilde{E}$.

This is as much as one may be told in a first course on elliptic curves. But there is much more going on here. First of all, the argument correctly shows that any elliptic curve over $\mathbb{Q}$ with a rational 7-torsion point cannot have good reduction at $p = 2$. (A nice exercise is to see this directly from the universal equation given above.) Notice what kind of statement this is: the standard slogan in this field is "geometry influences arithmetic", which is most certainly true. But here we have arithmetic influencing geometry: a $\mathbb{Q}$-rational 7-torsion point influences the geometry of the special fiber at $p = 2$.

But slogans are cheap: **where did the 7-torsion point go**? In other words, is there some honest geometric object $\tilde{E}_{/\mathbb{F}_2}$ which renders true the exact sequence[5]

$$0 \to \mathcal{K} \to E(\mathbb{Q}_2) \xrightarrow{r} \tilde{E}(\mathbb{F}_2) \to 0$$

Yes, there is. For any elliptic curve $E_{/\mathbb{Q}}$, there is a smooth group scheme $\tilde{E}_{/\mathbb{Z}}$, the **Néron model**, which is characterized by the following universal mapping property: if $X_{\mathbb{Z}}$ is any smooth scheme, then

$$\mathrm{Mor}_{\mathbb{Q}}(X_{/\mathbb{Q}}, E_{/\mathbb{Q}}) = \mathrm{Mor}_{\mathbb{Z}}(X_{/\mathbb{Z}}, \tilde{E}_{/\mathbb{Z}}).$$

In other words, every morphism on the generic fibers extends uniquely to a morphism over all of $\mathbb{Z}$. In other words, the Néron model is precisely the right adjoint to the functor from the category of smooth $\mathbb{Z}$-schemes to the category of $\mathbb{Q}$-schemes. In particular, it follows that $\tilde{E}(\mathbb{Z}_p) = \tilde{E}(\mathbb{Q}_p)$, so the reduction map in question is precisely the reduction map $\tilde{E}(\mathbb{Z}_p) \to \tilde{E}(\mathbb{F}_p)$. In this case, $\tilde{E}_{/\mathbb{F}_2} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{G}_m$: in other words, the special fiber is a disconnected group with 7 different components, and the 7-torsion points will cycle through the components.

This can be deduced directly from the general theory we will explore in this course. In fact, the minimal Weierstrass model has all the data we need to construct the Néron model. The fact that $\Delta(E) = -2^7 \cdot 13$ will tell us that the singular point of the Weierstrass model is not a regular point of the arithmetic surface; to desingularize it we need to blow up six times: therefore the special fiber of a regular model is given by joining 7 rational curves in a cyclic manner. From here, it turns out that we can get the Néron model (as a scheme) just by removing all the singular points – after all the Néron model is supposed to be smooth! – and then we get exactly 7 copies of $\mathbb{P}^1$ minus two points, which is what we claimed above.

Arguments like this can be used to systematically bound torsion points on abelian varieties defined over p-adic fields with certain "reduction properties": see [P.L. Clark and X. Xarles].

[5]The group $\mathcal{K}$ is the group of $\mathbb{Z}_2$-rational points on the associated formal group of E; all you need to do know is either take my word for it that such groups have no odd-order torsion or look it up in Silverman, *loc. cit.*.

Finally, here is an example which is numerically simpler but has some subly important implications.

Example 3: Start with your favorite field k and your favorite elliptic curve over that field, say:

$$E : y^2 = x^3 + ax + b, \ a, b \in k.$$

Now consider the rational function field $K = k(t)$ and regard E as an elliptic curve over k. Moreover, let us make the change of variables $(x, y) = (t^{-2}X, t^{-3}Y)$, getting

$$E : t^{-6}Y^2 = t^{-6}X^3 + t^{-2}aX + b.$$

Multiplying through by t^6 we get

$$E : Y^2 = X^3 + t^4aX + t^6.$$

As an elliptic curve over $k(t)$, this is certainly isomorphic to the curve we started with. On the other hand, we can now view E as being defined over $R = k[t]$ and therefore as a family of elliptic curves over the affine line $\mathbb{A}^1_{/k} = \operatorname{Spec} k[t]$. Now at any point $\mathfrak{p} \in \mathbb{A}^1$ other than 0 (i.e., at any prime ideal other than (t)), we haven't changed anything: in particular, reducing modulo $\mathfrak{p}$ we get an elliptic curve over $k(\mathfrak{p}$ which is the same elliptic curve that we started with. (Or, alternately, the change of variables we made is invertible over the local ring $R_{\mathfrak{p}}$.) However, if we reduce modulo t something has changed: we get the singular curve $Y^2 = X^3$.

Okay, so what? From this apparently trivial computation we can deduce two consequences:

First, the moduli space of elliptic curves is not compact[6]. Why? Because the point of a moduli space $\mathcal{M}$ for a class of geometric objects if that if you have a family $E \to X$ of such objects, then there is an algebraic **classifying map** $X \to \mathcal{M}$: you just send $x \in X$ to the isomorphism class of the fiber E_x in $\mathcal{M}$. So here we get a map $c : \mathring{A}^1 \setminus 0 \to \mathcal{M}_1$, the moduli space of elliptic curves. In particular c is a rationally defined map with domain the regular curve $\mathbb{P}^1$, so as we have seen, if $\mathcal{M}_1$ were complete then c would extend to all of c, in particular to the fiber $t = 0$, but the fiber over 0 is not an elliptic curve. So $\mathcal{M}_1$ is not compact.

That's not really a shocker, since if you know about elliptic curves you know that $\mathcal{M}_1$ is also isomorphic to the affine line $\mathbb{A}^1$, the classifying map being given by the j-invariant. When $t = 0$, $j(E_t) = \infty$: again, so what?

Well, it's rarely profitable to study global geometry on an incomplete space. Inevitably we want a **compactification** of the moduli space. Often these compactifications are gained by broadening the moduli problem to include certain "degenerate forms" of the objects of the original moduli space. If you didn't know any better, you might think that there would be *some* compactification $\overline{\mathcal{M}}$ of the moduli space of elliptic curves that included the cuspidal curve of arithmetic genus one. But actually our computation has shown that this is impossible! Why? By a compactification, we mean a complete variety $\overline{\mathcal{M}}$ containing $\mathcal{M}^1$ as a dense subvariety. Since $\mathcal{M}^1 = \mathbb{A}^1$ is irreducible, so would its compactification have to be irreducible, and

[6]Strictly speaking I mean "not complete", but I wish to use the more suggestively topological terminology

a fortiori, connected. But our moduli map is **constant** on all of $\mathbb{A}^1 \setminus 0$: it takes every fiber to $j(E) \in k$. So being continuous with respect to the Zariski topology, c would have to get mapped to the same nonsingular elliptic curve, and hence not to the cuspidal curve. In other words, a cuspidal cubic is not a suitable candidate for a "generalized elliptic curve."

If you think about it, the most natural compactification of $\mathcal{M}^1 = \mathbb{A}^1$ is evidently just the projective line $\mathbb{P}^1$: indeed it is the only possible **normal** compactification. Thus we are looking for exactly one isomorphism class of "generalized elliptic curves", so – by a process of elimination if nothing else – the obvious guess is that the point $j = \infty$ on the moduli space should correspond to the isomorphism class of the nodal cubic $y^2 = x^3 - x^2$. Remarkably, this example gives exactly the right intuition as to how to compactify the moduli space $\mathcal{M}_g$ of smooth curves of genus g: what kind of singular curves should we admit?

Remark: Notice that by claiming that such a compactification exists as a moduli space, we are making the following claim: if $\mathcal{E} \to \mathbb{A}^1$ is surface fibered over the affine line such that all smooth fibers have the same j-invariant, then all of the singular fibers (if any) must be cusps and not nodes. Challenge for those familiar with elliptic curves: prove this!

4. Where we're going: results on arithmetic surfaces

A **Dedekind scheme** will be a scheme which is integral, Noetherian, normal and of dimension at most one. Notice that an affine Dedekind scheme is precisely a Dedekind domain, so this notion is just a globalization. The other important case of a Dedekind scheme is a curve over a field k which is not necessarily projective but otherwise nice. Notice that any Dedekind scheme has a field of fractions $K = K(S)$.

If S is a one-dimensional Dedekind scheme, an **arithmetic surface over S**, denoted $\pi : \mathcal{C} \to S$, is an integral, normal projective, flat S-scheme of dimension 2. (In fact, as essentially came up in class already, flatness of π here is equivalent to its surjectivity.) Note that Q. Liu requires an arithmetic surface to be **regular** (as, in fact, I have done in my own papers), but in fact "nature" often gives us singular arithmetic surfaces:

Example: Let R be a Dedekind domain, and $E_{/K(R)}$ be an elliptic curve. Then there exists a Weierstrass equation

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

with $a_1, \ldots, a_6 \in R$. Regarding E as an equation with R-coefficients gives us a subscheme $\mathcal{W}$ of $\mathbb{P}^2_{/R}$ hence (by composition) a morphism $\pi : \mathcal{W} \to \operatorname{Spec} R$. Then indeed $\mathcal{W}$ is an arithmetic surface in our sense (see Proposition 9.4.26 of Liu). In particular, it is normal but – as we have already seen – not necessarily regular.

If $\pi : \mathcal{C} \to S$ is an arithmetic surface, we say that it is a **model** of the curve $C_{/K(S)}$. In particular, unless there is specific indication to the contrary, models are necessarily normal and projective, though not necessarily regular.

We are now grappling with the subtleties of higher-dimensional algebraic geometry: in particular, there will be many different models of a given curve $C_{/K(S)}$. Here are some basic questions:

Question 1: Can we always find a model $\mathcal{C} \to S$ which is **smooth** – i.e., for which **all** fibers are smooth curves?

Answer: No. We saw that any elliptic curve $E_{/\mathbb{Q}}$ admitting a rational 7-torsion point must have bad reduction at 2.

So let's try a weaker question:

Question 2: Can we always find a model $\mathcal{C} \to S$ which is **regular**, i.e., for which the two-dimensional scheme $\mathcal{C}$ itself is nonsingular at every point?

Note that in the geometric case – i.e., S is a curve over a field – this amounts to resolution of singularities for surfaces (in arbitrary characteristic). This is true, but nontrivial. Similarly, Question 2 has a positive answer: this is a very important result called **arithmetic resolution of singularities**.

As a side remark, recall that resolution of singularities for varieties of dimension at least three over an algebraically closed field of positive characteristic remains open in general: this is one of the most important open problems in algebraic geometry. It follows from this that we do not know whether one can find regular models for higher dimensional families over a Dedekind scheme, although to my knowledge it is widely believed that this should be the case.

Question 3: Among all regular models of $C_{/K(S)}$, are there any canonical ones?

Answer: yes. First there is (in positive genus) a unique **minimal regular model**, exactly as in the case of "geometric" surfaces. This has many nice properties. But in fact there are other "canonical" ones: there is one which is called the **canonical model** (in the sense of being constructed out of differentials); and there is another called the **SNC-model**.

Question 4: What can we say about the singularities of the minimal regular model of an arithmetic surface of genus g?

Answer: Not much – this is very difficult in general. The complete classification in the case of elliptic curves was worked out by Kodaira and Néron: we will see it. In genus 2 it was done by Ueno. So far as I know it has not been completed for any higher genus: it has the flavor of a combinatorial exercise of (at least) exponentially increasing complexity.

Question 5: Is there anything we can do about this?

Answer: yes!

Theorem 5. *(Deligne-Mumford) Let $C_{/K(S)}$ be any nice curve of genus $g \geq 1$.*
a) There exists a finite base extension L/K such that the minimal regular model of C over the integral closure T of S in L is semistable: i.e., all fibers are reduced and with only ordinary double point singularities.
b) If $g \geq 2$, then over the same extension the canonical model is a ***stable curve****.*

In other words, after making a finite base extension, the only singularities we need to worry about are the most generic and innocent of all: ordinary double point singularities. In fact, among semistable curves of genus g, the more singularities there are, the easier it is to analyze the behavior compared to nonsingular curves of the same genus. The limiting case is that of a **totally degenerate** semistable curve of arithmetic genus g, i.e., a bunch of rational curves glued together at ordinary double points. A sneaky trick is to reduce questions about smooth curves to totally degenerate semistable curves: I have engaged in this myself.

This theorem is important in both algebraic and arithmetic geometry, for different reasons. In algebraic geometry, making a finite base extension is often harmless, since it is often enough to think of families of curves locally in the true analytic sense: i.e., a family of curves over a small disk in the complex plane. In arithmetic geometry one is very interested in understanding the extension $L/K(S)$ needed to obtain semistable reduction (under suitable hypotheses this extension is essentially unique). In particular it has an interpretation in terms of the Galois representation on torsion points of the Jacobian abelian variety $J(C)$. In fact, there is a similar semistable reduction theorem for abelian varieties (first proved by Grothendieck), and the two theorems are equivalent – a curve has semistable reduction iff its Jacobian does, and either theorem can be deduced from the other. Indeed Deligne-Rapoport's proof goes by way of reduction (so to speak!) to Grothendieck's theorem. Nowadays there are proofs which go the other way, in particular one due to Artin-Winters. This approach gives critical information on the geometry of the Néron model of a Jacobian abelian variety $J(C)$ in terms of the minimal regular model of C, and we aspire to give at least some description of this beautiful theory at the end of our course.