Abstract. These are the rough ongoing lecture notes for the course 18.782 (Introduction to Arithmetic Geometry) taught at MIT in Fall 2019. The notes will be updated each weekend, following the lectures during the week. Be sure to clear your cache before reloading in order to get the most current version of the notes. If you find any typos/mistakes in the notes, please let me know!

1. Lecture 1

Note: This lecture is intended to be informal and motivational. It discusses several outside concepts (such as Riemann surfaces) which are not strictly needed in the remainder of the course. The lecture also briskly introduces several algebro-geometric concepts in an informal manner, to give intuition; all of these will be reintroduced more slowly and rigorously later in the semester.

1.1. Historical context. A Diophantine equation is a polynomial equation with integral (or rational) coefficients:

$$f(x_1, \ldots, x_n) = 0, \quad f \in \mathbb{Z}[x_1, \ldots, x_n].$$

Diophantus of Alexandria (c. 200-300 AD) wrote a series of texts called *Arithmetica* examining the problem of solving such equations in the integers or the rationals. Given $f$ as above and a commutative ring $R$, let us denote

$$V_f(R) = \{P \in R^n : f(P) = 0\}.$$  

Diophantine analysis is the study of the relationship between Diophantine equations $f = 0$ and the sets $V_f(\mathbb{Z})$ or $V_f(\mathbb{Q})$. Below are some examples of Diophantine equations, which were mentioned by Fermat in his 1650 letter to Carcavi summarizing Fermat’s earlier works:

- For $p$ odd prime, $x^2 + y^2 = p$ is solvable in integers $(x, y) \in \mathbb{Z}^2$ if and only if $p \equiv 1 \mod 4$ (Fermat’s two-square theorem, proved by Euler around 1750).
- For every $k \in \mathbb{Z}_{\geq 1}$, the equation $x^2 + y^2 + z^2 + w^2 = k$ is solvable in integers (Lagrange’s four-square theorem, proved by Lagrange in 1770).
- For every positive nonsquare integer $N$, the equation $x^2 - Ny^2 = 1$ is solvable in integers (Pell’s equation; its solvability goes back to work of Brahmagupta c. 600-700 AD).
- $x^3 + y^3 = z^3$ has no solution in positive integers (the $n = 3$ case of the so-called Fermat’s Last Theorem; this case was proved by Euler in 1770).
- The only integral solutions of $y^2 = x^3 - 2$ are $(x, y) = (\pm 3, 5)$.

(Fermat rarely gave proofs of his claims, and sometimes made incorrect ones.) The study of these and other Diophantine equations (especially involving binary quadratic forms) drove much of the research in number theory in the period following Fermat, and in particular formed the foundations for the development of algebraic number theory.

On the other hand, given an equation $f = 0$ as above, we can view the aggregate of its complex solutions $V_f(\mathbb{C})$ as a geometric object, namely a (complex) algebraic variety. Algebraic geometry is the field devoted to studying the geometric properties of algebraic varieties as well as their interactions with algebraic properties of the defining equations.

Date: September 7, 2019.
Arithmetic geometry is a relatively modern field of mathematics one of whose aims is to build a bridge between the geometric objects \( V_f(\mathbb{C}) \) and the arithmetic objects \( V_f(\mathbb{Z}) \) (or \( V_f(\mathbb{Q}) \)). The fact that there should be a connection between the two aspects of the equation \( f = 0 \) is surprising and adds to the allure of the subject.

Below, we will briefly discuss some of the achievements in the twentieth century, to illustrate the role of geometry in the study of Diophantine equations. Suppose we are given a nonconstant polynomial \( f = f(x,y) \in \mathbb{Q}[x,y] \). Since the set \( V_f(\mathbb{R}) \) of real points on the real affine plane \( \mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2 \) typically, forms a one-dimensional object, we refer to \( V_f \) as an affine plane curve defined over \( \mathbb{Q} \). Let us make the two assumptions about \( f \):

- \( V_f \) is geometrically irreducible, i.e. \( f \) is irreducible as a polynomial in \( \mathbb{C}[x,y] \), and
- \( V_f \) is nonsingular, i.e. \( \nabla f(P) = (\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) \neq 0 \) for every \( P \in V_f(\mathbb{C}) \).

Under these hypotheses, the set of complex points \( V_f(\mathbb{C}) \) admits the structure of a connected Riemann surface (i.e. complex manifold of dimension 1). In the informal discussion that follows, it will be useful for us to consider the “projective curve” \( \overline{V}_f \) obtained by “compactifying” \( V_f \) by adding a finite number of “points at infinity” (we will also assume nonsingularity at these points).

Then \( \overline{V}_f(\mathbb{C}) \) is a closed Riemann surface, which is topologically characterized by its genus \( g \) or number of “doughnut holes” on the surface. We have the following basic trichotomy, in differential geometric terms:

- \((g = 0)\. \overline{V}_f(\mathbb{C}) \) is topologically a sphere. It can be given a complete Riemannian metric of constant positive curvature, so as to be “positively curved.” Its Euler characteristic is positive: \( \chi > 0 \).
- \((g = 1)\. \overline{V}_f(\mathbb{C}) \) is topologically a torus. It can be given a complete Riemannian metric of constant zero curvature, so as to be “flat” (like the world as imagined by Pacman.) Its Euler characteristic is zero: \( \chi = 0 \).
- \((g \geq 2)\. \overline{V}_f(\mathbb{C}) \) can be given a complete Riemannian metric of constant negative curvature, so as to be “negatively curved” (like on the surface of a saddle.) Its Euler characteristic is negative: \( \chi < 0 \).

Suppose now that \( \overline{V}_f(\mathbb{Q}) \) is nonempty. (This is a highly nontrivial assumption!) We then have the following trichotomy in the behavior of \( \overline{V}_f(\mathbb{Q}) \).

- \((g = 0)\. \overline{V}_f(\mathbb{Q}) \) is infinite.
- \((g = 1)\. \overline{V}_f(\mathbb{Q}) \) has the structure of an abelian group; and this group is in fact finitely generated. This latter statement was conjectured by Poincaré in 1901; it was proved by Mordell in 1921, with generalization by Weil in 1928.
- \((g \geq 2)\. \overline{V}_f(\mathbb{Q}) \) is finite. This was conjectured by Mordell in 1923, and proved by Faltings in 1983, which led to his 1986 Fields medal.

Thus, the trichotomy of curvature in geometry reverberates in arithmetic!

1.2. Rational points on conics. Let us consider the problem of finding rational solutions to Diophantine equations of degree 2 in two variables (i.e. equations of conics). Our analysis will serve to illustrate the utility of geometric intuition in solving Diophantine problems.

Example 1. Let us determine \( V_f(\mathbb{Q}) \) where

\[
(1) \quad f(x, y) = x^2 + y^2 - 1.
\]

Note that the set \( V_f(\mathbb{R}) \) of real solutions to equation (1) forms a unit circle in the real affine plane \( \mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2 \). The rational solutions correspond to the points on the unit circle with rational \( x \)- and \( y \)-coordinates.
To determine $V_f(\mathbb{Q})$, first note that $(-1,0)$ lies in $V_f(\mathbb{Q})$. If $(x,y)$ is any other rational point in $V_f(\mathbb{Q})$, then the line joining $(-1,0)$ to $(x,y)$ has rational slope. Conversely, a line of rational slope $t \in \mathbb{Q}$ through $(-1,0)$ intersects $V_f$ at exactly at one other point $(x_t,y_t)$, and this point is rational. Indeed, note that $(x_t,y_t)$ solves simultaneously the equations

$$x^2 + y^2 = 1 \quad \text{and} \quad y = t(x+1).$$

Substitution give us

$$x^2 + t^2(x+1)^2 = 1 \implies (x+1)((1 + t^2)x - (1 - t^2)) = 0.$$

If $x = -1$ then $y = 0$, which is excluded. If $x \neq 0$, we see that

$$(x_t, y_t) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

Therefore, we have

$$V_f(\mathbb{Q}) = \left\{\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) : t \in \mathbb{Q}\right\} \cup \{(-1,0)\}.$$

Note that we may informally view $(-1,0)$ as the point obtained by letting the parameter $t$ “tend to infinity;” indeed, note that

$$\lim_{|t| \to \infty} \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) = (-1,0).$$

To give a cleaner presentation of $V_f(\mathbb{Q})$, it will be useful to work with projective curves, which are introduced below.

Fix a base field $k$ (say $\mathbb{Q}$). The projective $n$-space $\mathbb{P}^n$ over $k$ is defined by setting, for each field extension $L/k$,

$$\mathbb{P}^n(L) = \frac{L^{n+1} \setminus \{(0, \ldots, 0)\}}{\sim}$$

where the equivalence relation $\sim$ on $L^{n+1} \setminus \{(0, \ldots, 0)\}$ is given by

$$(a_0, \ldots, a_n) \sim (b_1, \ldots, b_n)$$

if and only if $(a_0, \ldots, a_n) = (\lambda \cdot b_1, \ldots, \lambda \cdot b_n)$ for some $\lambda \in L^\times$. Note that $\mathbb{P}^n(L)$ may be viewed as the space of lines through the origin (more precisely, one-dimensional vector subspaces) in the vector space $L^{n+1}$ over $L$. Given $a_0, \ldots, a_n \in L$ not all zero, we shall denote the class of $(a_0, \ldots, a_n)$ in $\mathbb{P}^n(L)$ by $(a_0 : \cdots : a_n)$.

**Example 2.** As a set,

$$\mathbb{P}^1(L) = \{[1 : a] : a \in L\} \cup \{[0 : 1]\} = L \sqcup \{\infty\}.$$

For example, $\mathbb{P}^1(\mathbb{C})$ is the Riemann sphere giving a one-point compactification of the complex plane $\mathbb{C}$. In general, we have

$$\mathbb{P}^n(L) = \{[1 : a_1 : \cdots : a_n] : a_i \in L\} \sqcup \{[0 : a_1 : \cdots : a_n] : a_i \in L\}$$

$$= \mathbb{A}^n(L) \sqcup \mathbb{P}^{n-1}(L).$$

Thus, $\mathbb{P}^n$ may be viewed as a “compactification” of the affine space $\mathbb{A}^n$ obtained by adding $\mathbb{P}^{n-1}$ “at infinity.”

For a homogeneous polynomial $F(X_0, X_1, X_2) \in \mathbb{Q}[X_0, X_1, X_2]$ of degree $d \geq 1$ and field extension $L/\mathbb{Q}$, the zero set

$$V_F(L) = \{(a_0 : a_1 : a_2) \in \mathbb{P}^2(L) : F(a_0, a_1, a_2) = 0\}$$

is well-defined, since $F(\lambda X_0, \lambda X_1, \lambda X_2) = \lambda^d F(X_0, X_1, X_2)$ for every $\lambda \in L^\times$. We refer to $V_F$ as a projective curve defined over $\mathbb{Q}$. 

3
Example 3. Let \( f(x, y) = x^2 + y^2 - 1 \) as in Example 1. The zero set \( V_F(\mathbb{C}) \) in \( \mathbb{P}^2(\mathbb{C}) \) of the homogenization
\[
F(X_0, X_1, X_2) = X_0^2 f(\frac{X_1}{X_0}, \frac{X_2}{X_0}) = X_1^2 + X_2^2 - X_0^2
\]
is given by the union of two sets
\[
\{(1 : a_1 : a_2) \in \mathbb{P}^2(\mathbb{C}) : F(1, a_1, a_2) = f(a_1, a_2) = 0\} = V_f(\mathbb{C})
\]
and
\[
\{(0 : a_1 : a_2) \in \mathbb{P}^2(\mathbb{C}) : F(0, a_1, a_2) = a_1^2 + a_2^2 = 0\} = \{(0 : 1 : i), (0 : 1 : -i)\}.
\]
Thus, we have
\[
V_F(\mathbb{C}) = V_f(\mathbb{C}) \sqcup \{(0 : 1 : i), (0 : 1 : -i)\}
\]
and we may view \((0 : 1 : i)\) and \((0 : 1 : -i)\) as points “at infinity” of \( V_f \) in \( \mathbb{P}^2 \). Note that we have a well-defined map
\[
\mathbb{P}^1(\mathbb{C}) \to V_f(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})
\]
given by
\[
(t_0 : t_1) \mapsto (\frac{t_0^2}{t_0^2 + t_1^2} : \frac{t_1^2}{t_0^2 + t_1^2} : 2t_0t_1),
\]
which in fact establishes a bijection between (the complex points and) rational points of \( \mathbb{P}^1 \) and \( V_f \). Note that the restriction of the map above to the affine line \( \mathbb{A}^1 = \{(1 : t)\} \subset \mathbb{P}^1 \) can be written
\[
t = (1 : t) \mapsto (1 + t^2 : 1 - t^2 : 2t) = \left(1 : \frac{1 - t^2}{1 + t^2} : \frac{2t}{1 + t^2}\right) = \left(1 - \frac{t^2}{1 + t^2} : \frac{2t}{1 + t^2}\right)
\]
which agrees with the rational parametrization given in Example 1. We will later revisit this example and show that the map given above is an isomorphism of algebraic curves over \( \mathbb{Q} \), so we may write
\[
\mathbb{P}^1 \cong V_f.
\]

It is easy to see that, although our discussion was limited to a particular conic section \( x^2 + y^2 = 1 \), the same argument can be used a to give a rational parametrization of rational points for an arbitrary nondegenerate conic section, provided that it has at least one rational point to begin with. This leads to the following result:

Theorem 4. Let \( C \) be a geometrically irreducible (smooth) projective curve of degree 2 in \( \mathbb{P}^2 \) defined over \( \mathbb{Q} \). Then the following are equivalent:

1. \( C(\mathbb{Q}) \) is nonempty.
2. \( C \cong \mathbb{P}^1 \) over \( \mathbb{Q} \).

This naturally leads us to the problem of finding necessary and sufficient conditions for a curve \( C \) as above to have a rational point. This will be solved by the Hasse-Minkowski theorem, which will be covered in later lectures.