

Notes on Diophantine Geometry

Zachary Miner

January 24, 2008

Rational Points on Curves of Genus Zero

Given a system of equations:

$$X : \begin{cases} f_1 = 0 \\ \vdots \\ f_m = 0 \end{cases}.$$

with $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, we would like to determine if X is a curve - and once we have done that, determine its genus. One way to do this is to find a point off the curve and project from there. You lose information on the geometry of X (in particular the genus) but keep the dimension of X .

Let X be an irreducible algebraic set, i.e., (f_1, \dots, f_m) is a prime ideal. Next, let $R = K[x_1, \dots, x_n]/(f_1, \dots, f_m)$ and let $K(X)$ denote the field of fractions of R . Then the dimension of X is just the transcendence degree of $K(X)$ over K :

$$\text{Tr deg}_K K(X) = \dim X.$$

X is a curve if $\dim X = 1$, that is, if some x_i is not in \overline{K} , and all other x_j are algebraic over $K(x_i)$.

We say that X, Y , irreducible algebraic sets, are birationally isomorphic if their function fields $K(X), K(Y)$ are isomorphic as field extensions of K .

Example 1. If $n = 2$ and $m = 1$, $f(x_1, x_2) = 0$, then this is a curve.

Now, we consider the genus $g(X)$ of an irreducible curve X . Over a subfield of \mathbb{C} , the genus can be obtained from the topology of $X(\mathbb{C})$. An algebraic definition of genus is the dimension of the space of regular 1-forms

on a smooth projective model. If X is a plane curve of degree d , then we have the following formula for the genus:

$$g(X) = \frac{1}{2}(d-1)(d-2) - \sum_{p \text{ singular}} \delta_p,$$

where, if the singularity is an ordinary singularity with m branches, then $\delta_p = \frac{1}{2}m(m-1)$. (So, δ_p depends on the singularity. There is an algorithm for computing it in general, but you won't find it in these notes.)

Background. Singular points are, for example, points $(x, y) \in \mathbb{C}^2$ with

$$f(x, y) = \frac{\partial f}{\partial x}(x, y) = \frac{\partial f}{\partial y}(x, y) = 0.$$

Example 2. For smooth (projective) plane curves of degree d , the genus is $\frac{1}{2}(d-1)(d-2)$.

We may recall from last time, before notes existed, that we separated the genus into three cases: $g = 0$, $g = 1$, and $g > 1$. The degree formula for these separate cases then says:

$$\begin{aligned} g = 0 &\iff d = 1, 2 \\ g = 1 &\iff d = 3 \\ g > 1 &\iff d \geq 4. \end{aligned}$$

Definition. An irreducible curve X is *parametrizable* (also, *rational*) over K if there exist $\varphi_1, \dots, \varphi_n \in K(t)$ (not all constant) such that for all $j = 1, \dots, m$ we have $f_j(\varphi_1, \dots, \varphi_n) = 0$.

Theorem 1. *A curve is parametrizable over K if and only if it has genus zero and a smooth point with coordinates in K .*

Proof. (\Rightarrow) If X is parametrizable then $K(X)$ embeds in $K(t)$. This is seen by considering the map $\alpha : K[x_1, \dots, x_n] \rightarrow K(t)$ which sends $x_i \mapsto \varphi_i(t)$. Then $f_i \in \ker \alpha$, so that α induces a map $R = K[x_1, \dots, x_n]/(f_1, \dots, f_m) \rightarrow K(t)$. Thus, by Luroth's theorem, $K(X)$ is purely transcendental over K . X is therefore birationally isomorphic to a line, and so has genus zero and many smooth points in K .

(\Leftarrow) A sketch of the proof in this direction: Use $g(X) = 0$ together with the smooth point P and the Riemann-Roch space $L(P)$ of functions whose

only pole is a simple pole at P to get that $\dim L(P) = 2$. Then, we find a non-constant $f \in L(P)$, where $f : X \rightarrow \mathbb{P}^1$ has only one (simple) pole, so it has degree 1, making it a birational isomorphism. Thus, $f^{-1} : \mathbb{P}^1 \rightarrow X$ is a parametrization. \square

Example 3. Consider the curve $X : x^2 + y^2 = 1$. Then X has a point at $P = (1, 0)$. By the degree formula for the genus, $g(X) = 0$. We will give a parametrization of X working geometrically: Any line through P intersects the curve in exactly one other point (unless it is tangent at P). The equation of a line through $(1, 0)$ is given by $y = t(x - 1)$. Substituting this into X for y and solving for x gives: $x = \frac{t^2 - 1}{t^2 + 1}$. Then, $y = t(x - 1) = \frac{-2t}{t^2 + 1}$. This is our parametrization.

Assume K is perfect (e.g. has characteristic zero). By the genus formula and the fact that the genus is non negative, a cubic has at most one singularity. If a curve has a singular point in a field bigger than K , then its conjugates are also singular points so the curve must have other singular points. Therefore, we may conclude that an absolutely irreducible cubic with a singular point automatically has its singular point with coordinates in the ground field. The method used in the last example to find a parametrization works in this instance, too. You take the pencil of lines through the singular point, and because it is singular, this will give you a parametrization, hence lots of points. That is we get the following:

Corollary 2. *A singular cubic always has lots of points over the ground field.*

Example 4. Consider $X : y^2 = x^3 + x^2$. Then X has a singular point at the origin $P = (0, 0)$. The equation of a line through $(0, 0)$ is given by $y = tx$. Then, we get $x = t^2 - 1$, and so $y = t(t^2 - 1)$.

Example 5. But, $x^2 + y^2 = -1$ has *no* solutions over \mathbb{R} . So, a smooth curve of degree 2 and genus 0, may have no points over \mathbb{Q} or even \mathbb{R} . However, it does have points over \mathbb{C} .

Example 6. Another example is $x^2 + y^2 = 0$. But, this curve is reducible:
 $X = \{x = iy\} \cup \{x = -iy\}$.

Theorem 3. *Every curve of genus zero over K is birationally isomorphic to a conic.*

Proof. We will not give a proof, just remark that the proof uses the negative of the canonical divisor, which gives us a divisor of degree two on the curve. \square

Theorem 4. (Legendre) *If $a, b, c \in \mathbb{Z}$ not all zero, then $ax^2 + by^2 + cz^2 = 0$ has a solution $(x, y, z) \in \mathbb{Z}^3 \setminus \{0, 0, 0\}$, if and only if there is a solution to $ax^2 + by^2 + cz^2 \equiv 0 \pmod{m}$ with $(x, y, z) \in (\mathbb{Z}/m)^3 \setminus \{0, 0, 0\}$ for all $m \geq 2$.*

This was the original statement of Legendre, but the way to restate it which allows for generalizations is:

Theorem 5. *An absolutely irreducible conic X over \mathbb{Q} has a point with coordinates in \mathbb{Q} if and only if X has points with coordinates in \mathbb{Q}_p , the field of p -adic numbers, for all primes p (and \mathbb{R}).*

Proof. See next week's notes. \square