Mehina 2009 lecture 1 - Curves and elliptic Curves

Yonatan Harpaz

July 25, 2009

1 Curves

2 The Genus

As always in algebraic geometry when study an object, we need to start by understanding its geometry, i.e. its behavior over $\mathbb{C}$ or over $\overline{\mathbb{Q}}$. We will only be interested in smooth projective curves and we know that for such curves the complex points $C(\mathbb{C})$ form a compact manifold of dimension 2. These manifolds will always be orientable, and so are classified by a unique invariant $g \in \mathbb{N}$, called the **genus**, which corresponds to the number of "holes" (the 2-sphere has no holes, the torus has 1, etc). We will refer to it as the genus of the curve C.

We will show how to construct curves of arbitrary genus. For a given $g \in \mathbb{N}$ set $n = 2(g+1)$ and let $a_0, ..., a_n \in \mathbb{C}$ be and define a smooth projective curve C over $\mathbb{C}$ by gluing the two affine curves

$$C_1 : y^2 = \sum_k a_k x^k$$

$$C_2 : w^2 = \sum_k a_k z^{n-k}$$

Let $U_1 \subseteq X_1$ be the open set defined by $x \neq 0$ and $U_2 \subseteq C_2$ the open set defined by $z \neq 0$. Consider the map $U_1 \longrightarrow U_2$ given by

$$z = \frac{1}{x}$$

$$w = \frac{y}{x^{\frac{n}{2}}}$$

Note that this is morphism of algebraic varieties because

$$\left(\frac{y}{x^{\frac{n}{2}}}\right)^2 = \frac{y^2}{x^n} = \frac{\sum_k a_k x^k}{x^n} = \sum_k a_k \left(\frac{1}{x}\right)^{n-k}$$

This map is also invertible. Its inverse is

$$x = \frac{1}{z}$$

$$y = \frac{w}{z^{\frac{n}{2}}}$$

Hence it is an isomorphism. This means we glue C_1 to C_2 along this isomorphism $U_1 \cong U_2$ to obtain a new curve C.

Let us now check when C is smooth. We only need to check each of the affine curves C_1, C_2. Note that both of them are defined by an equation of the form

$$F(x, y) = y^2 - f(x) = 0$$

where f is a polynomial of degree $\leq 2(g+1)$. We claim that such a curve is smooth if and only if f has no double roots. The gradient of F is given by

$$\nabla F = -f'(x)dx + 2ydy$$

Hence $\nabla F = 0$ at the point $(x_0, y_0) \in C$ if and only if $f'(x_0) = 0$ and $y = 0$ (or equivalently $f'(x_0) = 0$ and $f(x_0) = y_0^2 = 0$). This occurs exactly when x_0 is a double root of f.

Now note that if C_2 is smooth then $f = \sum_k a_k x^k$ must has degree at least $n-1$, because other wise $a_{n-1} = a_n = 0$ and then $\sum_k a_k z^{n-k}$ has a double root at $z = 0$. Now it is not hard to verify that if $\sum_k a_k x^k$ is a polynomial of degree at least $n-1$ and has no double roots then $\sum_k a_k z^{n-k}$ satisfies the same condition and C is smooth.

Note also that if f has no double roots then it has no root in the field $\mathbb{C}(x)$ and so $y^2 - f(x)$ is irreducible in $\mathbb{C}[x, y]$. This means that in that case C is also an irreducible variety.

We now want to convince ourselves that C is complete. Note that we have a map $C \longrightarrow \mathbb{P}^1$ given on C_1 and C_2 respectively by

$$\varphi(x, y) = (x : 1)$$

$$\varphi(z, w) = (1 : z)$$

We now that the property of being complete is equivalent to $C(\mathbb{C})$ being compact. Now φ induces a surjective map from $C(\mathbb{C})$ to $\mathbb{P}^1(\mathbb{C})$ (which is compact) and the fiber above every point is finite (its size is either 2 or 1). By some rather simple topological arguments one can prove in that way that $C(\mathbb{C})$ is compact.

Another approach is to embed C as a closed subvariety of some complete variety. Recall the weighted projective space $\mathbb{P}\left(1, \frac{n}{2}, 1\right)$ from Tomer's lecture. You saw that this is a complete variety of dimension 2. The equation

$$y^2 = \sum_k a_k x^k z^{n-k}$$

is well defined on $\mathbb{P}\left(1, \frac{n}{2}, 1\right)$ with projective coordinates $x : y : z$ where x and z have weight 1 and y has weight $\frac{n}{2}$. Its solution set is a closed (and hence projective) subvariety. Call it X.

Now note that X can be covered by two affine open sets given by $x \neq 0$ and $z \neq 0$ respectively (the point $(1 : 0 : 0) \in \mathbb{P}\left(1, \frac{n}{2}, 1\right)$ is not on X). These two affine subsets are then isomorphic to C_1 and C_2 respectively, and one easily checks that the gluing map is the same. Hence $X \cong C$ and C is complete.

We now wish to calculate the genus of C. Let $\widetilde{f}(x, z) = \sum_k a_k x^k z^{n-k}$ and think of C as embedded in $\mathbb{P}\left(1, \frac{n}{2}, 1\right)$ as the solution set to the equation

$$y^2 = \widetilde{f}(x, z)$$

The map $\varphi : C \longrightarrow \mathbb{P}^1$ can be written as

$$\varphi(x : y : z) = (x : z)$$

This map is well defined because the point $(1 : 0 : 0) \in \mathbb{P}\left(1, \frac{n}{2}, 1\right)$ is not on C. Now the fiber over a point $(x : z) \in \mathbb{P}^1(\mathbb{C})$ consists of the points $(x : y : z)$ where $y = \pm\sqrt{(f(x, z))}$. There are exactly $n = 2(g + 1)$ different points $(x_1 : z_1), ..., (x_n : z_n) \in \mathbb{P}^1(\mathbb{C})$ for which $\widetilde{f}(x_i, z_i) = 0$ (these are called **ramification** points). Over these points there is a unique point in C, and over any other point there are two points in C.

Now let $I_i \subseteq \mathbb{P}^1(\mathbb{C})$ be a line segment connecting $(x_{2i} : z_{2i})$ and $(x_{2i+1} : z_{2i+1})$ and suppose that the I_i's don't intersect each other. Let $U \subseteq \mathbb{P}^1(\mathbb{C})$ be the complement of the union of the I_i's. Assume for simplicity that U is contained in the affine set $x \neq 0$ and so we identify $U(\mathbb{C})$ with an open subset of the complex plane via the coordinate $u = \frac{x}{z}$. Let $f(u) = \widetilde{f}(u, 1)$. Then $f(u) \neq 0$ for every $u \in U(\mathbb{C})$ and in fact every loop in U circles an even number of roots of f.

From the theory of complex functions we know that in that case we can choose the square root $\sqrt{f(u)}$ continuously on all of U. This means that $\varphi^{-1}(U) = U_1 \cap U_2$ is a disjoint union of two sets, such that each $U_i(\mathbb{C})$ is homeomorphic to $U(\mathbb{C})$. Note that $U(\mathbb{C})$ is homeomorphic to the sphere with $g + 1$ closed discs removed. The subsets $U_1(\mathbb{C}), U_2(\mathbb{C}) \subseteq C(\mathbb{C})$ have a common boundary which is $\cup_i \varphi^{-1}(I_i)$ and is homeomorphic to a disjoin union of $g + 1$ circles. We then see that gluing two spheres with $g+1$ discs removed along their boundary which is a union of circles gives a 2 dimensional manifold of genus g.

One can also argue via the notion of Euler characteristic. It turns out that if we triangulate a 2 dimensional manifold using V vertices, E edges and F faces then the quantity $F - E + V$ is independent of the triangulation, and is called the Euler characteristic. In particular for a 2 dimensional manifold of genus g this quantity is

$$F - E + V = 2 - 2g$$

and in particular for a sphere its always 2 (e.g. the tetrahedron with $F = 4, E = 6, V = 4$) and for a torus it is 0. Now triangulate the sphere $\mathbb{P}^1(\mathbb{C})$ in such a way that all the ramification points are vertices. Let F, E, V be the amounts of

faces, edges and vertices in this triangulation. The triangulate $C(\mathbb{C})$ in such a way that φ maps vertices to vertices, edges to edges and faces to faces. We then see that we have use exactly $2F$ faces, $2E$ edges and $2V - n$ vertices (because a ramification point has only one pre-image in $C(\mathbb{C})$ and a non-ramification point has 2). We then get

$$2 - 2g = 2F - 2E + 2V - n = 4 - n$$

or

$$g = \frac{n}{2} - 1$$

which means that by choosing $n = 2(g + 1)$ we are ensuring that the resulting curve has genus g.

The genus is the most fundamental invariant of curves. However, it is not a complete invariant, i.e. there can be many non-isomorphic curves (even over an algebraically closed field) with the same genus. Tomorrow we will talk about genus 1 curves and we will see examples.

In genus 0, though, all curves are isomorphic (over any algebraically closed field) to $\mathbb{P}^1$. They may be, however, curves which are isomorphic to $\mathbb{P}^1$ over, say, $\overline{\mathbb{Q}}$, but not over $\mathbb{Q}$. For example, the two projective curves $C_1, C_2 \subseteq \mathbb{P}^2$ given by the equations

$$C_1 : x^2 + y^2 + z^2 = 0$$
$$C_2 : x^2 + y^2 - z^2 = 0$$

are isomorphic over $\overline{\mathbb{Q}}$ by the isomorphism

$$z \mapsto iz$$

but not over $\mathbb{Q}$ (the first has no rational points and the second has, for example, the point $(0 : 1 : 1)$). The sharp reader will notice that the same argument shows that in fact they are not isomorphic over $\mathbb{R}$.

It turns out (and we will explain more about why that is after the Galois cohomology lecture) that a curve defined over $\mathbb{Q}$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if it has a rational point. This means that on curves of genus 0 we have the following behavior: It either has no rational points, or infinitely many (in which case finding an explicit isomorphism to $\mathbb{P}^1$ will give a nice parametrization of all the rational points).

This is of course not true for higher genus. The behavior of rational points on genus 1 curves is very rich and interesting, as will see in the next section. For now let us just say that a curve of genus 1 may have no rational points, may have finitely many or may have infinitely many rational points. Further more, due a special structure of genus 1 curves, we can in some case obtain something similar to a "parametrization" of the rational points.

For genus ≥ 2 we have a (hard) theorem of Faltings which states that such curves have only finitely many rational points. Hence we see that the genus has a fundamental connection to the behavior of rational points. This is part of a fundamental deep theme in arithmetic algebraic geometry: the geometry has a deep influence on the arithmetic behavior.

3 Elliptic Curves

3.1 The Group Operation

Yesterday we've discussed curves and learned of the important invariant called the **genus**. In this talk we will discuss the genus 1 case, which have a particularly rich theory. Our approach will start with looking at the geometry of the curve, i.e. looking at it over $\overline{\mathbb{Q}}$ or over $\mathbb{C}$.

Over $\mathbb{C}$ we see that the points form a torus. The torus has a very interesting property: one can put a group structure on it so that the group operations are continuous. Such an object is called a topological group. One is then tempted to ask whether this can be done in the setting of algebraic geometry as well, and the (surprising) answer is: Yes!

First of all note that a group has a special point, called the unit. The torus as a topological space doesn't have any special point, and nor does an algebraic genus 1 curve. In fact, for every point on the torus there exists a group structure such that this point is the unit. Hence we expect that the construction of the group structure will involve an (arbitrary) choice of a point to be the unit. We call a curve of genus 1 with a choice of point on in an **elliptic curve**.

Now in the previous lecture we saw that an affine curve of the form

$$y^2 = x^3 + Cx^2 + Ax + B$$

can be completed to a smooth projective genus 1 curves. One possible way to do this is to take the projective curve $E \subseteq \mathbb{P}^2$ given by the homogenous equation

$$zy^2 = x^3 + Cx^2z + Axz^2 + Bz^3$$

when $z \neq 0$ we get our affine curve and there is a unique point on E with $z = 0$ - the point $(0 : 1 : 0)$, which we will call ∞. We will denote by $U = E - \setminus\{\infty\}$ the original affine curve. Note that by preforming the coordinate change $x \mapsto x + \frac{C}{3}$ one can make the coefficient of x^2 to be 0, so from no on we will assume that $C = 0$.

Let us try to construct algebraically a group structure on E in which ∞ is the unit. We need to find a way to take 2 points in $E(\overline{\mathbb{Q}}$ and calculate from them a third point. But note that out curve is given by a cubic equation in $\mathbb{P}^2$. Hence by Bezout's theorem, if we take a line between two points, it will intersect the our curve in one additional point (note that a line cannot be equal to E so Bezout will be true). Note that this additional point might be equal to one of the starting points. This is the case is called intersection with multiplicity.

This gives us indeed a binary operation on $E(\overline{\mathbb{Q}})$. Could this be our group structure? Our first guess should be no, because this operation does not depend on the point we have chosen to be the unit. To give a more definite no, since we wish to have ∞ as a unit element if this was our group structure we should expect the line passing through ∞ and P to have multiplicity at P (i.e. would not meet E at any other point). But this is not true in general. Let $P = (a : b : 1)$ and take the line $x = az$. This line intersects E at the points $\infty, (a : b : 1)$ and $(a : -b : 1)$. In general $(a : b : 1) \neq (a : -b : 1)$.

Hence we see that this cannot be our group structure. Hence we do a small modification: we declare that this binary operation takes two points to the inverse of their sum. This implies in particular that when we pass a line from ∞ to P, the third intersection point is the inverse of P. By the above considerations this means that the inverse of the point $(a : b : 1)$ is $(a : -b : 1)$. Now the group operation on two points is calculated as follows: first we pass a line between them, get the third intersection point and take its inverse by inverting its y coordinate.

We claim that this operation gives an algebraic map $E \times E \longrightarrow E$. We will construct this map on the affine subset $U \times U$ and leave it as an exercise to complete the description. Given two points $(a : b : 1), (d : e : 1)$ we will find a line l of the form

$$y = Mx + N$$

that passes between them. We get the equations

$$Ma + N = b$$

$$Md + N = e$$

and solve them to get

$$M = \frac{b-e}{a-d}$$

$$N = b - \frac{a(b-e)}{a-d} = \frac{b(a-d) - a(b-e)}{a-d} = \frac{ae - bd}{a-d}$$

We now want to find a third point on l which meets E. To do that we will substitute it in the equation for E and get

$$(Mx + N)^2 - x^3 - Ax - B = 0$$

$$M^2x^2 + 2MNx + N^2 - x^3 - Ax - B = 0$$

$$x^3 - M^2x^2 + (A - 2MN)x + B - N^2 = 0$$

This is a monic polynomial in x and so its trace, which is $-M^2$, is minus the some of its roots. Since it has two roots - a and d - that we know of we find that the third root must by

$$x = M^2 - a - d = \left(\frac{b-e}{a-d}\right)^2 - (a + d)$$

The corresponding y is then

$$y = Mx + N = M^3 - M(a + d) + N = \left(\frac{b-e}{a-d}\right)^3 - \frac{b-e}{a-d}(a + d) + \frac{ae - bd}{a-d}$$

Now recall that in order to get our group operation we know need to take the inverse of this point, i.e. multiply y by -1. Hence we get that our group operation can be written as a rational function

$$(x, y) = \left(\left(\frac{b-e}{a-d}\right)^2 - (a + d), -\left(\frac{b-e}{a-d}\right)^3 + \frac{(b-e)(a+d)}{a-d} - \frac{ae - bd}{a-d}\right)$$

Isn't this a problem? This is a rational function, and not a polynomial. In particular it seems to be undefined when $a = d$. The problem might be connected to the fact that we can't define the group operation only on the affine subset $U \subseteq E$ given by $z \neq 0$, because the addition of two points might be ∞. Hence we make a first attempt to solve this by writing the point (x, y) in projective coordinates $(x : y : z)$ as

$$x = (a-d)(b-e)^2 - (a-d)^3(a+d)$$
$$y = -(b-e)^3 + (a-d)^2(b-e)(a+d) - (a-d)^2(ae-bd)$$
$$z = (a-d)^3$$

It seems that we have cheated no one: now when $a = d$ and $e = b$ all three terms vanish and we don't get a well defined point. In order to solve this problem we need to define this function differently when we approach the $a = d, e = b$ area. To do that we write M and N differently using the curve equations:

$$M = \frac{b-e}{a-d} = \frac{b^2-e^2}{(b+e)(a-d)} = \frac{a^3-d^3+A(a-d)}{(b+e)(a-d)} = \frac{a^2+ad+d^2+A}{b+e}$$

$$N = \frac{ae-bd}{a-d} = \frac{(b+e)(ae-bd)}{(b+e)(a-d)} = \frac{ae^2-db^2+eb(a-d)}{(b+e)(a-d)} =$$
$$\frac{ad^3+Aad+aB-da^3-Aad-Bd+eb(a-d)}{(b+e)(a-d)} = \frac{B-ad(d+a)+eb}{b+e}$$

We then get

$$x = \left(\frac{a^2+ad+d^2+A}{b+e}\right)^2 - (a+d)$$
$$y = -\left(\frac{a^2+ad+d^2+A}{b+e}\right)^3 + \frac{(a^2+ad+d^2+A)(a+d)}{b+e} - \frac{B-ad(d+a)+eb}{b+e}$$

and so an alternative expression for our function is

$$x = (b+e)(a^2+ad+d^2+A)^2 - (b+e)^3(a+d)$$
$$y = -(a^2+ad+d^2+A)^3+(b+e)^2(a^2+ad+d^2+A)(a+d)-(b+e)^2(B-ad(d+a)+eb)$$
$$z = (b+e)^3$$

Now all three coordinates vanish exactly when $e+b = 0$ and $a^2+ad+d^2+A = 0$. Note that this can't coincide with the case $a = d, e = b$ because then $e = b = 0$ and $3a^2+A$. But if $b = 0$ then $a^3+Aa+B = 0$ so a is a root of both x^3+Ax+B and its derivative $3x^2 + A$ which can't be because $x^3 + Ax + B$ doesn't have double roots.

Note that we still need to show that this map extends to a morphism defined on all of $E \times E$ (and not just the product of the affine sets $U \times U$).

Example: Consider the elliptic curve

$$y^2 = x^3 - 11$$

The solution $P = (3, 4)$ is simple and easy to find. We can use it to form solutions which are more complicated by adding the point with itself. Since we are adding two identical points we will use the alternative formula for M, N:

$$M = \frac{a^2 + ad + d^2 + A}{b + e} = \frac{27}{8}$$

$$N = \frac{B - ad(d + a) + eb}{b + e} = \frac{-11 - 54 + 16}{8} = \frac{-49}{8}$$

Hence the point $P + P$ has coordinates

$$x = M^2 - a - d = \frac{27^2}{64} - 6 = \frac{345}{64}$$

$$y = -(Mx + N) = -\frac{27}{8}\frac{345}{64} + \frac{49}{8} = \frac{-6179}{512}$$

And indeed

$$\frac{345^3}{64^3} - 11 = \frac{38180041}{64^3} = \frac{(-6179)^2}{512^2}$$

So we have a solution which is quite more complicated than the one we've started with.

Note that we have defined the group operation only for curves which are given in the form

$$y^2 = x^3 + Ax + B$$

called the Weierstrass form. It can be shown that every curve of genus 1 which has a point over a field k is isomorphic over k to a curve of this form. Hence every elliptic curve over k (which by definition has a point over k) can be written in this form.

It is good to note that this form is not unique. For example for any A, B and $u \neq 0$ the curves

$$y^2 = x^3 + Ax + B$$

$$y^2 = x^3 + u^4 Ax + u^6 B$$

are isomorphic by the isomorphism $x \mapsto u^2 x, y \mapsto u^3 u$. The group operation we have defined will not change if we change the Weierstrass form to an isomorphic one.

3.2 Torsion Points

A fundamental principle in algebraic geometry is that if a geometric property of the variety over $\mathbb{C}$ can be expressed in algebraic terms then it is true over any algebraically closed field of characteristic 0 (and most of the time over any characteristic).

A nice example of this principle is given by subgroup of torsion points. Note that on the torus we have that the subgroup of all elements of order n is isomorphic to $\mathbb{Z}/n \times \mathbb{Z}/n$. Since the group operation is given by polynomial functions

we can express the property of being of order n algebraically as solutions to polynomial equations.

If we will analyze the number of solutions these polynomials have (by carefully examining their degrees) we'll get n^2 (because this is what we get over $\mathbb{C}$) and so this number will be true over any characteristic 0 field (the group structure can also be found in that way). If we go to positive characteristic we'll get the same answer as long as n is prime to p.

3.3 The Mordell-Weil Group

Since the group operation is defined over $\mathbb{Q}$ we see that when we add two rational points we get another rational point. Hence the set of rational points on an elliptic curve forms an abelian group, called the Mordell-Weil group. The following is a classic result :

Theorem 3.1. *(Mordell-Weil) The Mordell-Weil group of rational points on an elliptic curve is finitely generated.*

A finitely generated group is always isomorphic to $F \otimes \mathbb{Z}^r$ for some finite group F and number r, called the rank. It turns out that the torsion part of the Mordell-Weil group is quite well understood: it has very few possibilities and its size cannot exceed 22. It can also be effectively determined (using a computer) for any given elliptic curve.

On the other hand, the rank is much less understood. It is not even known if elliptic curves can have arbitrarily large rank (the record is something like 24...). You will see in the Galois cohomology lectures a method to bound the rank of a given elliptic curve. Note that if one can find r then in principal one can search for points until r independent points are found and then use them to give a parametrization of all the points on the curve.

In particular the example above has rank 2. The Mordell-Weil group is generated freely by the points $(3, 4), (9/4, 5/8)$.

A famous conjecture regarding the rank of the Mordell-Weil group is the Birch-Swinnerton-Dyer conjecture which relates the rank to the vanishing order of some analytic function (called the L-function) which can be computed from the curve (and in particular from the number of points on the curve over finite fields). The proof of this conjecture is worth $1,000,000$ dollars.

3.4 Abelian Varieties

One may ask for generalizations of the concept of elliptic curves. One possible direction is to find other complete varieties which admit group structures. It can be shown that in such case the group operation will have to be abelian, and in fact the complex points of such a creature will be higher dimensional tori. These are called **abelian varieties** and you will here more about them in the Picard group lecture.

It turns out to be really hard to give explicit equations which define abelian varieties. The only examples which can described explicitly are those which are products of elliptic curves or product of elliptic curves mod a finite subgroup.