Freshman Seminar 21n: Elliptic Curves

William Stein

February 11, 2003

1 Remarks

Your reading for this coming week is about projective spaces, cubic equations, and the elliptic curve group operation.

1.1 Projective Space

The following is a completely general definition of projective space.

Definition 1.1 (Projective Space). Let k be a field and $n \geq 0$ an integer. Then n dimensional projective space is, as a set,

$$\mathbb{P}^n_k = \{(a_1 : a_2 : \cdots : a_{n+1}) \;:\; \text{not all } a_i = 0\;\}/\sim,$$

where $\sim$ is the equivalence relation in which

$$(a_1 : a_2 : \cdots : a_{n+1}) \sim (ca_1 : ca_2 : \cdots : ca_{n+1})$$

for all nonzero $c \in k$. (Think of $(a_1 : a_2 : \cdots : a_{n+1})$ as a ratio.)

When k has a topology, $\mathbb{P}^n_k$ inherits a topology (as a quotient of $k^{n-1} - 0$) which we probably won't worry about much in this course.

1. The projective space of dimension 0 is a single point.
2. The projective line $\mathbb{P}^1_k$ is, as a set,

   $$\{(a_1 : a_2) \;:\; a_1, a_2 \in k\}/\sim \;=\; \{(1 : a) \;:\; a \in k\} \cup \{(0 : 1)\}.$$

   Thus the projective line is the usual line union one extra point $(0, 1)$, which we often think of as being "at infinity".

   (a) The set $\mathbb{P}^1_{\mathbb{R}}$ is the real line along with one extra point at infinity; thus $\mathbb{P}^1_{\mathbb{R}}$ is in bijection with a circle.

   (b) The set $\mathbb{P}^1_{\mathbb{C}}$ is equal to the complex plane $\mathbb{C}$ along with one extra point at infinity. Alternatively, $\mathbb{P}^1_{\mathbb{C}}$ can be thought of as the points on the sphere with the north pole corresponding to the point at infinity.

3. When $n = 2$ we obtain the projective plane:

$$\{(a_1 : a_2 : 1) \ : \ a_1, a_2 \in k\} \cup \{(1 : a : 0) \ : \ a \in k\} \cup \{(0 : 1 : 0)\}.$$

   We can think of $\mathbb{P}^2_k$ as the usual plane along with a copy of $\mathbb{P}^1_k$ "at infinity". The real projective plane $\mathbb{P}^2_{\mathbb{R}}$ looks like a plane union a circle at infinity. The complex projective plane $\mathbb{P}^2_{\mathbb{C}}$ has real dimension 4 so it is harder to describe, but it is where we will primarily work.

4. In general, $\mathbb{P}^n_k$ is usual n-dimension space along with a $\mathbb{P}^{n-1}_k$ "at infinity".

Definition 1.2 (Homogeneous Polynomial). A *homogeneous polynomial* is a polynomial $F(X_1, \ldots, X_n)$ such that $F(cX_1, \ldots, cX_N) = c^d F(X_1, \ldots, X_n)$ for all $c \in k$, where $d = \deg(F)$. Equivalently, each of the monomials in F have the same degree.

Definition 1.3 (Algebraic Variety). An *algebraic variety* in $\mathbb{P}^n_k$ is the set of solutions to a system

$$F_1(X_1, \ldots, X_{n+1}) = \cdots = F_r(X_1, \ldots, X_{n+1}) = 0$$

of homogeneous polynomial equations. The homogeneity condition ensures that this set is well defined.

Definition 1.4 (Algebraic Plane Curve). An *algebraic curve* in $\mathbb{P}^2_k$ is the set of solutions to a single nonconstant homogenous polynomial equation

$$\{(a : b : c) : F_1(a, b, c) = 0\}.$$

1.2 The Group Law

Consider a cubic curve of the form $y^2 = x^3 + ax + b$ and assume that $x^3 + ax + b$ has distinct roots. Then the set

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b\}$$

is the graph of the real points on an elliptic curve. Given two solutions (x_1, y_1) and (x_2, y_2), there is a formula for a third solution (x_3, y_3). It has the marvelous properties that

1. If $x_1, y_1, x_2, y_2 \in \mathbb{Q}$ then $x_3, y_3 \in \mathbb{Q}$.

2. The composition law turns the set $E(\mathbb{R})$ into a *GROUP*.

The composition law is described in the text both algebraically and geometrically, but a complete proof that it has property 2 above is not given. I'm not sure what we'll do about this. My advice is that you would be best served to just believe this on faith at this point. When you learn "algebraic geometry" later in your career, you'll learn a beautiful and conceptually satisfying definition of the group law.

1.3 Skipping Next Monday

We will next meet at 2pm on Tuesday February 18. We will not meet on February 17th, because it is a holiday.

2 Problems from the reading

1. (Jeff) Prove that the line connecting two distinct rational points in the plane is defined by an equation $ax + by + c = 0$ with $a, b, c \in \mathbb{Z}$, then prove that the intersection of any two distinct rational lines in the plane is empty or a single rational point.

2. (Jennifer) Find all right triangles with integer side lengths and hypotenuse < 30.

3. (Mauro) For each of the following conics, either find five rational points or prove that there are no rational points:

   (a) $x^2 + y^2 = 6$

   (b) $3x^2 + 5y^2 = 4$

   (c) $3x^2 + 6y^2 = 4$

4. (Alex) Draw a rough graph of the conic $x^2 - y^2 = 1$, then give a formula for all the rational points on this conic.

5. (Jenna) Use induction on n to prove that for every $n \geq 1$, the congruence
$$x^2 + 1 \equiv 0 \pmod{5^n}$$
has a solution $x_n \in \mathbb{Z}/5^n\mathbb{Z}$.

3 New reading and problems

Reading Assignment: *Read pages* **220–232** *of Appendix A and pages* **15–32** *of Chapter I, both that in [Silverman-Tate].*

3.1 Problems for next time.

1. (Jeff) Let $\mathbb{P}^2$ be the set of triples $[a, b, c]$ modulo scalar multiplication, as usual. Define a line in $\mathbb{P}^2$ to be the set of solutions of an equation of the form
$$aX + bY + cZ = 0$$
for some numbers a, b, c not all zero. Prove (from the definition) that any two distinct points in $\mathbb{P}^2$ are contained in a unique line. Then prove that any two distinct lines in $\mathbb{P}^2$ intersect in a unique point.

2. (Jennifer) Let $F(X,Y,Z) \in \mathbb{C}[X,Y,Z]$ be a homogeneous polynomial of degree n. Prove that the partial derivatives of F are homogeneous polynomials of degree $n-1$, and use this to show that

$$X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y} + Z\frac{\partial F}{\partial Z} = nF$$

by differentiating $F(tX,tY,tZ) = t^n$ with respect to t.

3. (Mauro)

   (a) Let C be a curve in $\mathbb{P}^2$ defined by $F(X,Y,Z) = 0$, where F is a homogenous polynomial. Prove that if $P \in \mathbb{P}^2$ satifies the equation

   $$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0, \tag{1}$$

   then P "automatically" satisfies $F(P) = 0$. Thus to find the singular points on C, you just have to find the common solutions to (1); it is not necessary to include $F = 0$.

   (b) Find all singular points on the curve defined by

   $$F(X,Y,Z) = X^7 - Y^2Z^5 = 0.$$

4. (Alex) For each of the given affine curves C_0, find a projective curve C whose affine part is C_0. Then find all of the points at infinity on the projective curve C.

   (a) $3x - 7y + 5 = 0$

   (b) $x^2 + xy - 2y^2 + x - 5y + 7 = 0$

   (c) $x^3 + x^2y - 3xy^2 - 3y^3 + 2x^2 - x + 5 = 0$

5. (Jenna) For each of the following curves C and points P, either find the tangent line to C at P or else verify that C is singular at P.

C	P
$y^2 = x^3 - x$	$(1,0)$
$X^2 + Y^2 = Z^2$	$(3:4:5)$
$x^2 + y^4 + 2xy + 2x + 2y + 1 = 0$	$(-1,0)$
$X^3 + Y^3 + Z^3 = XYZ$	$(1:-1:0)$

6. (Alex) Let C be the cubic curve $u^3 + v^3 = u + v + 1$. In the projective plane, the point $(1 : -1 : 0)$ at infinity lies on this curve. Find rational functoins $x = x(u,v)$ and $y = y(u,v)$ so that x and y satisfy a cubic equation in Weierstrass normal form (i.e., $y^2 = x^3 + ax^2 + bx + c$).

7. (Jeff) Let C be the cubic curve in $\mathbb{P}^2$ given by

$$Y^2 Z = X^3 + aX^2 Z + bXZ^2 + cZ^3.$$

Prove that the point $(0 : 1 : 0)$ on C is nonsingular.

8. (Jenna) Let C_1 and C_2 be the cubics given by the following equations:

$$C_1 : x^3 + 2y^3 - x - 2y = 0, \qquad C_2 : 2x^3 + y^3 - 2x - y = 0.$$

Find the nine points of intersection of C_1 and C_2.

9. (Jennifer) The cubic curve $u^3 + v^3 = \alpha$ (with $\alpha \neq 0$) has a rational point $(1, -1, 0)$ at infinity. Taking this rational point to be $\mathbb{O}$ (the identity element of the group), we can make the points on the curve into a group. Derive a formula for the sum $P_1 + P_2$ of two distinct points $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$.

10. (Mauro) Verify that if u and v satisfy the relation $u^3 + v^3 = 1$, then the quantities

$$x = \frac{12}{u+v} \qquad \text{and} \qquad y = 36\frac{u-v}{u+v}$$

satisfy the relation $y^2 = x^3 - 432$. We thus obtain a birational transformation f from the curve $u^3 + v^3 = 1$ to the curve $y^2 = x^3 - 432$. Each of these cubic curves can have a group law defined on it. Prove that f is an isomorphism of groups, where the zero element for $y^2 = x^3 - 432$ is the point $(0 : 1 : 0)$ and the zero element for $u^3 + v^3 = 1$ is $(1 : -1 : 0)$ (at infinity).

4 Motivation: The Congruent Number Problem

Definition 4.1 (Congruent Number). A rational number n is called a *congruent number* if $\pm n$ is the area of a right triangle with rational side lengths. Equivalently, n is congruent if the system of two equations

$$n = ab/2 \qquad \text{and} \qquad a^2 + b^2 = c^2$$

has a solution with $a, b, c \in \mathbb{Q}$.

For example, 6 is the area of the right triangle with side lengths 3, 4, and 5, so 6 is a congruent number. Less obvious is that 5 is also a congruent number; it is the area of the right triangle with side lengths 3/2, 20/3, and 41/6. It is nontrivial to prove that 1, 2, 3, and 4 are not congruent numbers.

Here is a list of the congruent numbers up to 50:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, \ldots$$

Every congruence class modulo 8 except 3 is represented in this list, which suggests that if $n \equiv 3 \pmod 8$ then n is not a congruent number. This is true for $n \leq 218$, but $n = 219$ is a congruent number congruent to 3 mod 8. Something very subtle is going on.

This is another example which hints at the subtlety of congruent numbers. The number 157 is a congruent number, and Don Zagier showed that the *simplest* rational right triangle with area 157 has side lengths

$$a = \frac{6803298487826435051217540}{411340519227716149383203} \quad \text{and} \quad b = \frac{411340519227716149383203}{21666555693714761309610}.$$

This solution would take a long time to find without understanding more about congruent numbers.

Open Problem: Give an algorithm which, given n, outputs whether or not n is a congruent number.

The following proposition establishes a link between elliptic curves and the congruent number problem. This link connects the congruent number problem with the Birch and Swinnerton-Dyer conjecture, which some consider to be the most important open problem in the theory of elliptic curves.

Proposition 4.2. *Let n be a rational number. There is a bijection between*

$$A = \left\{(x, y, z) \in \mathbb{Q}^3 \; : \; \frac{xy}{2} = n, \; x^2 + y^2 = z^2\right\}$$

and

$$B = \left\{(r, s) \in \mathbb{Q}^2 \; : \; s^2 = r^3 - n^2 r, \text{with } s \neq 0\right\}$$

given explicitly by the maps

$$f(x, y, z) = \left(-\frac{ny}{x+z}, \; 2n^2 x + z\right)$$

and

$$g(r, s) = \left(\frac{n^2 - r^2}{s}, \; -\frac{2rn}{s}, \; \frac{n^2 + r^2}{s}\right).$$

Corollary 4.3. *The rational number n is a congruent number if and only if the elliptic curve E_n defined by $y^2 = x^3 - n^2 x$ has a solution with $y \neq 0$.*

Proof. The number n is a congruent number if and only if the set A from Proposition 4.2 is nonempty. By the proposition A is nonempty if and only if B is nonempty, which proves the corollary. □

Example 4.4. Let $n = 5$. Then E_n is defined by $y^2 = x^3 - 25x$, and we find by a brute force search the solution $(-4, -6)$. Then

$$g(-4, -6) = \left(\frac{25 - 16}{-6}, -\frac{-40}{-6}, \frac{25 + 16}{-6}\right) = \left(-\frac{3}{2}, -\frac{20}{3}, -\frac{41}{6}\right).$$

Multiplying through by -1 yields the side lengths of a rational right triangle with area 5.

Theorem 4.5. *Let n be* even *and squarefree, and let E be the elliptic curve*

$$y^2 = x^3 - n^2 x.$$

Then $L(E,1) = 0$ if and only if

$$\#\Big\{(a,b,c) : 4a^2 + b^2 + 8c^2 = \frac{n}{2} : c \text{ is even}\Big\}$$
$$= \#\Big\{(a,b,c) : 4a^2 + b^2 + 8c^2 = \frac{n}{2} : c \text{ is odd}\Big\}.$$

So far I have told you nothing about the meaning of "$L(E,1) = 0$". Suffice for now to know that (a consequence of) the Birch and Swinnerton-Dyer conjecture is the assertion that the set of rational solutions to $y^2 = x^3 - n^2x$ is infinite if and only if "$L(E,1) = 0$". Also, it is easy to prove that this set of solutions is infinite if and only if n is a congruent number.

When $n = 6$, we get

$$\#\emptyset = 2 \cdot \#\emptyset.$$

When $n = 2$, we get

$$\#\{(0,1,0)\} \neq 2 \cdot \#\{(0,1,0)\},$$

so the BSD conjecture predicts that $y^2 = x^3 - 4x$ has no interesting solutions and 2 is not a triangle number.

In fact, this is true. The implication $L(E,1) \neq 0$ implies $y^2 = x^3 - n^2x$ has no interesting solutions was proved by Coates and Wiles (this is the same Wiles who proved Fermat's Last Theorem).

The other implication:

$$L(E,1) = 0 \Longrightarrow y^2 = x^3 - n^2x \text{ has lots of solutions}$$

is a fascinating *open problem.*