Freshman Seminar 21n: Elliptic Curves

William Stein

February 4, 2003

1 Introduction

Welcome Jeff, Jennifer, Mauro, Alex, and Jenna to the Elliptic Curves Seminar!!

2 Some Math Problems

Try these. If you can't do them, don't worry. That just means we need to slow down the seminar and do more background material. This is fine; we are in now hurry!

1. (Jeff) Does the equation $x^2 + 2y^2 = -17$ have any solutions with $x, y \in \mathbf{Z}$?

2. (Jennifer) Let $p \in \mathbf{Z}$ be a prime. Prove that $\sqrt{p}$ is irrational.

3. (Mauro) Does the equation $x^2 + y^2 + z^2 \equiv 7 \pmod 8$ have any solutions with $x, y, z \in \mathbf{Z}$?

4. (Alex) Fermat's Last Theorem asserts that when $n \geq 3$ then $x^n + y^n = z^n$ has no solutions with $xyz \neq 0$. Is the analogue of this statement true when $n = 2$?

5. (Jenna) Let $G = \{0, 1, 2, 3\}$ be the group of integers under addition modulo 4.

   (a) What is $2 + 3$ in G?

   (b) What is the order of 3 in G?

   (c) Let $H = \{1, 2, 3, 4\}$ be the group of nonzero integers under multiplication modulo 5. Is G isomorphic to H? If not, why not? If so, give an explicit isomorphism.

6. (Jeff) What is the tangent line to the graph of $y^2 = x^3 + 3$ at the point $(1, 2)$? (Hint: Implicit differentiation.)

7. (Jennifer)

   (a) List the elements of a finite field of order 2.

(b) One can prove that there is a finite field k of order 4. Does the cubic equation $x^3 + x + 1 = 0$ have a solution in k?

8. (Mauro)

   (a) Prove that the set of elements of finite order in an abelian group is a subgroup.

   (b) Prove that a group in which every element except the identity has order 2 is abelian.

9. (Alexander) Show by example that the product of elements of finite order in a nonabelian group need not have finite order. (Hint: Consider a construction involving 2×2 matrices.)

10. (Jenna) Describe all groups G which contain no proper subgroup.

3 Reading

Read pages 1–15 of Silverman-Tate. Try each of the following problems, but be able to present a solution to the one with your name next to it:

1. (Jeff) Prove that the line connecting two distinct rational points in the plane is defined by an equation $ax + by + c$ with $a, b, c \in \mathbf{Z}$, 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 $x_n \in \mathbf{Z}/5^n\mathbf{Z}$.

4 Pep Talk

Number Theory is mainly about relations between rational numbers (fractions, which are denoted $\mathbf{Q}$).

Examples:

1. Every positive integer can be written in a unique way (up to order) as a product of primes.
2. The equation $x^2 = 2$ has no solution with $x \in \mathbf{Q}$.
3. The equation $y^2 = x^3 + 2$ has infinitely many solutions (x, y) with $x, y \in \mathbf{Q}$. E.g.,
$$(-1,1), \ldots, \left(\frac{66113}{80656}, \frac{36583777}{22906304}\right), \ldots$$
$$\left(\frac{-64363752249455070879137307239023}{293763056960316465372944069236324}, -\frac{7101756495124011219835271161698654764912754876409}{5034957028437368992912415633092962882910696377832}\right), \ldots$$
(In a few weeks you'll know how I found such big solutions.)

Much of number theory involves *finding integer or rational solutions to polynomial equations.* After all, solutions to such equations *are* relations between numbers.

4.1 Simplest Case: 1 variable

Find solutions to
$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$
with $x \in \mathbf{Q}$. (Here $a_0, a_1, \ldots \in \mathbf{Z}$.)

Rational root theorem: If $x = \frac{b}{c}$ is a solution with $b, c \in \mathbf{Z}$ having no common factor, then $c \mid a_n$ and $b \mid a_0$. So it is easy to determine all solutions in $\mathbf{Q}$ to a polynomial in 1 variable.

(Proof:
$$a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n = 0$$
implies that $c \mid a_n b^n$ so $c \mid a_n$ and $b \mid a_0 c^n$ so $b \mid a_0$.)

Also, the number of solutions to $f(x) = 0$ is at most n.

4.2 Two Variables

Consider
$$F(x, y) = 0$$
where $F(x, y)$ is a polynomial in two variables. The graph of $F = 0$ is a plane curve.

Let $\deg(F)$ be the largest degree of any monomial that occurs in F. E.g., $\deg(x^2y^3 + 2y^4) = 5$.

Simplest case: degree 1

$$F(x, y) = ax + by + c = 0.$$

The graph is a line.

Since $\deg(P) = 1$, at least one of $a, b \neq 0$. Without loss, suppose that $a \neq 0$. Then

$$x = -\frac{b}{a}y - \frac{c}{a}.$$

and the solutions to $F = 0$ are exactly the pairs

$$\left\{ \left(-\frac{b}{a}y - \frac{c}{a}, y \right) \ : y \in \mathbf{Q} \right\}.$$

Notice that this is an infinite set of solutions.

Next case: degree 2

$$F(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

with $a, b, c, d, e, f \in \mathbf{Q}$.

The graph of $F = 0$ is a conic. (Ellipse, hyperbola, ...) (A line usually meets the graph in 2 points.)

Such an equation may or may not have solutions unlike the linear case (when $F = 0$ always has a solution).

Fact: $F = 0$ has either no solutions or infinitely many.

Examples

1. $x^2 + y^2 + 1 = 0$ has no solutions with $x, y \in \mathbf{R}$ (the real numbers), hence no solutions $x, y \in \mathbf{Q}$.

2. $x^2 + y^2 - 1 = 0$ (graph is unit circle) has infinitely many solutions. They are

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

   How to find this: Draw the unit circle and a line through $(-1, 0)$ with slope t. This line is $y = t(x + 1)$. Substitute into $x^2 + y^2 - 1$ to find second point of intersection.

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

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

$$x^2 + \frac{2t^2}{t^2 + 1}x + \frac{t^2 - 1}{t^2 + 1} = 0.$$

We know that $x = -1$ is a root, and product of roots is $\frac{t^2-1}{t^2+1}$, so other root is
$$x = \frac{1-t^2}{1+t^2}.$$
Thus
$$y = t(x+1) = \frac{2t}{1+t^2}.$$

Fact: (mostly explained in Silverman-Tate): When $F(x,y)$ has degree 2, the equation $F(x,y) = 0$ has infinitely many solutions (which we can easily parameterize) if and only if it has at least one solution.

Example:
$$x^2 + x^2 = 3$$
has no solution with $x, y \in \mathbf{Q}$.

Proof: $x^2 + y^2 = 3$ has a rational solution if and only if $X^2 + Y^2 = 3Z^2$ has a solution with $X, Y, Z \in \mathbf{Z}$ and $\gcd(X, Y, Z) = 1$ (i.e., there is no prime that simultaneously divides all three of X, Y, Z). Suppose that X, Y, Z is such a solution. Then
$$X^2 + Y^2 \equiv 0 \pmod 3$$
so $X^2 \equiv Y^2 \equiv 0 \pmod 3$ since the squares modulo 3 are $0, 1$. Thus $3 \mid X$ and $3 \mid Y$, so $9 \mid X^2 + Y^2 = 3Z^2$, so $3 \mid Z^2$, hence $3 \mid Z$, which contradicts our assumption that $\gcd(X, Y, Z) = 1$. DONE.

There is a theory that allows one to decide quickly whether or not a quadratic equation $F(X, Y) = 0$ has a solution. I will not discuss it further here, but we can learn more about it in this seminar, if you want.

4.3 Next case: Degree 3

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

This is getting complicated!

Open Problem: Give an algorithm (a "procedure" that on any input terminates in a finite number of steps and outputs "yes" or "no") that decides whether or not $F = 0$ has any rational solutions.

Open Problem: If there is a solution, describe all the solutions?

These are HARD PROBLEMS that are at the core of the frontiers of number theory.

If $F(x,y) = 0$ has a rational solution, then the curve it defines is called an elliptic curve.