Elliptic Curves and Galois Representations

Caleb McWhorter

Fall 2014

Definition 0.0.1 (Elliptic Curve)**.** *An elliptic curve is defined by the equation*

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

for some choice of constants A, B. This equation is referred to as the Weierstrass equation for an elliptic curve.

Example 0.0.2 (Packing Problem:)**.** When can one arrange a $y \times y$ square array of spheres into a regular pyramidal array? This amounts to solving

$$y^2 = \sum_{i=1}^{x} i^2 = \frac{x(x+1)(2x+1)}{6} = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$$

for some $x \in \mathbb{Z}^+$, which is an elliptic curve. We know the trivial solutions $x = 0$ and $x = 1$. We can then form a line which hopefully will intersect the curve once more (it does) to find a rational solution. Repeating this process again yields an integer solution of 4900 spheres (which is indeed the only nontrivial integer solution) ▷

Example 0.0.3 (Congruent Number Problem:)**.** Are there right triangles with rational sides having integer area? This problem dates as far back as 900A.D. in Arab manuscripts. A few example of such triangles are: $(3, 4, 5), (8, 15, 17), (4, 15/2, 17/2)$.

▷

1. Chord-Tangent Law
2. j-invarient

Elliptic Curves, Modular Forms, and their L-functions - Lozano-Robledo

1. Elliptic Curve: $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and no repeated roots.
2. Three consecutive integers whose product perfect square?: $y^2 = x(x+1)(x+2)$, no nontrivial solutions.
3. Congruent Number Problem: What integers n are such that there is a right triangle with rational sides and whose area is n. Examples: 6 from (3,4,5), 30 from (5,12,13), 5 from $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$. Problem remains open and has been for over 1000 years. Dates back to Arab manuscripts as far back as 972AD. Fermat showed that no perfect square can be a congruent number.

4. Number $n > 0$ congruent if and only if $y^2 = x^3 - n^2x$ has nonzero rational solutions and there is 1-1 correspondence between such rational points and the congruent numbers. Closet to solution is Tunnell in 1983 which gives necessary conditions which are sufficient given BSD. Several years before Tunnell proved his theorem, Stephens in 1975 showed the weak Birch and SwinnertonDyer conjecture implies any positive integer $n \equiv 5, 6, 7 \mod 8$ is a congruent number. Tunnells achievement was discovering the enumerative criterion for congruent numbers and its relation to the weak Birch and SwinnertonDyer conjecture.

5. Modular Form: Let $\mathbb{C}$ be the complex plane and $\mathbb{H}$ be the upper half plane. A modular form is a function $f : \mathbb{H} \to \mathbb{C}$ with several special properties especially

$$f(z) = f(z+1)$$
$$f\left(\frac{1}{z}\right) = z^k f(z)$$

the integer k is called the *weight* of the modular form.

6. L-function: A function of the form

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n \in \mathbb{C}$ and $s \in \mathbb{C}$. One of the most special examples is $a_n = 1$ for all n which is the Riemann Zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} = \frac{1}{1 - p^{-s}}$$

7. Dirichlet Character ($\mod N$): Homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$. $\chi(n) \in \mathbb{C}$ and $\chi(n)^{\varphi(N)} = 1$ for $(n, N) = 1$ so that $\chi(n)$ must be a root of unity. Extend χ to $\mathbb{Z}$ by letting $a \in \mathbb{Z}$. If $(a, N) = 1$, then $\chi(a) = \chi(a \mod N)$. Otherwise, $\chi(a) = 0$. A Dirichlet L-function s of the form

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where χ is a Dirichlet character. If χ is the trivial Dirichlet character, then we obtain the zeta function $\zeta(s)$.

8. Diophantine Equation: Equation given by polynomial with integer coefficients, i.e.

$$f(x_1, x_2, \cdots, x_r) = 0$$

$f(x_1, x_2, \cdots, x_r) \in \mathbb{Z}[x_1, x_2, \cdots, x_r]$.

9. Hilberts 10th Problem: Devise a process to determine in a finite number of operations whether an equation is solvable in rational integers. 1970, Matiyasevich, Putnam, Robinson no such general algorithm. However, in some cases we can.

    1. Polynomials in one variable: $\frac{p}{q} \in \mathbb{Q}$ solution $f(x) = 0$ then a_n divisible by p and a_0 divisible by q. Gives finite list then check.
    2. Linear equations in two variables: $ax + by = d$ and $ab \neq 0$. Use Euclidean Algorithm to solve then use rational points. Integral solutions if and only if d is divisible by (a, b).

3. Conics: Legendre gives method to do this for conics via a stereographic projection (once found one of them, look to find one using $\mod p$ for all p including ∞). Typically, only need be done for finitely many. This is for rational points. Integral points are more difficult to find, e.g. Pell's equation $x^2 - Dy^2 = 1$.
4. Cubic equations: No algorithm to yield all rational solutions. There are conjectural algorithms.
5. Higher degree: Degree ≥ 4 have genus ≥ 2 except some of degree 4 have genus 1. Mordell conjectured curve $\mathcal{C}$ of genus ≥ 2 can have only finitely many rational solutions and proved by Faltings 1983.

10. Elliptic Curve (over $\mathbb{Q}$): Smooth cubic projective curve E defined over $\mathbb{Q}$ with at least one rational point $\mathcal{O} \in E(\mathbb{Q})$, called the origin or the identity.

11. Siegel's Theorem, 1929: Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, then E has only a finite number of integral points. (Follows from Roth theorem on Diophantine approximation). Alan Baker found the number of such

$$\max(|x|, |y|) < \exp((10^6 \cdot \max(|A|, |B|))^{10^6})$$

12. Mordell-Weil (conjectured Poincaré in 1908, proved Mordell in 1922, generalized in thesis by Weil in 1928): $E(\mathbb{Q})$ is a finitely generated abelian group. Hence, $E(\mathbb{Q})$ is sometimes called the Mordell-Weil group of E.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{torsion}}$$

13. Proof of Mordell-Weil: Weak Mordell-Weil theorem (that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite for $m \geq 2$), height functions on abelian groups, and the descent theorem.

14. Conjecture: Let $N \geq 0$ be natural. Then there exists an elliptic curve E defined over $\mathbb{Q}$ with rank $r \geq N$. Largest known rank is 28 discovered by Elkies in 2006 with trivial torsion.

15. What groups can occur as the torsion subgroup? Conjecture by Ogg proved by Mazur: Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q})_{\text{torsion}}$ is isomorphic to

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, 3, \cdots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z}, & \text{with } 1 \leq M \leq 4 \end{cases}$$

each one of these cases can occur (and each infinitely many). Examples:

Curve	Torsion	Generators
$y^2 = x^3 - 2$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(2,0)}{(0,0)}$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(3,6)}{(0,0)}$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(-3,18)}{(2,-2)}$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\binom{(30,-90)}{(-40,400)}$

Figure 1: A table of elliptic curves of given torsion subgroup.

So if P is a point of order at least 13, then it must have infinite order then $E(\mathbb{Q})$ contains an infinite amount of distinct rational points. Not helpful in computation.

16. Nagell-Lutz: Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation

$$y^2 = x^3 + Ax + B \text{ for } A, B \in \mathbb{Z}$$

then every torsion point $P \neq \mathcal{O}$ of E satisfies:

1. The coordinates of P are integers.
2. If P is a point of order $n \geq 3$, then $4A^3 + 27B^2$ is divisible by $y(P)^2$.
3. If P is of order 2, then $y(P) = 0$ and $x(P)^3 + Ax(P) + B = 0$.

17. Reduction pg 37???

18.

Rational Points on Elliptic Curves

1. The curve $y^2 = x^3 - 2$ has infinitely many rational solutions but only finitely many integral solutions.

2. The questions we ask given $f(x, y) = 0$:

   1. Are there any solutions in integers?
   2. Are there any solutions in rational numbers?
   3. Are there infinitely many solutions in integers?
   4. Are there infinitely many solutions in rational numbers?

   Only the third has been fully answered and there are good partial answers for the last. For polynomials in more variables, there are only partial answers to any. The work of Davis, Matijasevič, and Robinson shows that in general it is not possible to answer the first.

3. Rational points on conics $ax^2 + bxy + cy^2 + dx + ey + f = 0$): If there exists a rational point $\mathcal{O}$, find a appropriate nonintersecting rational line and project onto it. We get a 1-1 correspondence between the rational points on the conic (strictly speaking, we do miss a point where the line on the conic is parallel to the projected line but in the projective plane this is taken care of).

4. Rational Parametrization of the Circle: Project line $y = t(1 + x)$ onto circle (connecting (-1,0) to point $(0, t)$ where $t \in \mathbb{Q}$). Solving yields

$$x = \cos\theta = \frac{1 - t^2}{1 + t^2} \qquad y = \sin\theta = \frac{2t}{1 + t^2}$$

5. Are there rational solutions to $x^2 + y^2 = 3$? Write $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. Clear denominators and obtain $X^2 + Y^2 = 3Z^2$. Check $\mod 3$ and find $1 \equiv X^2 + Y^2 \not\equiv 0 \mod 3$, so there are none.

6. Bezout's Theorem: Let C_1 and C_2 be projective curves with no common components. Then

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \deg C_1 \deg C_2$$

where the sums is taken over all points of $C_1 \cap C_2$ having complex coordinates. In particular, if C_1 and C_2 are smooth curves with only transversal intersections, then $\#(C_1 \cap C_2) = \deg C_1 \deg C_2$. In all cases,

$$\#(C_1 \cap C_2) \leq \deg C_1 \deg C_2$$

7. The choice of origin for the chord-tangent law. The map

$$P \mapsto P + (\mathcal{O}' - \mathcal{O})$$

is an isomorphism.

8. Note on Chord-Tangent law: If line tangent at P, then third point is also P. If you have an inflection point, then the point must also be P.

9. The chord-tangent law is invariant under birational transformations.

10. Elliptic Curve: Comes from calculating arc length of ellipse. At end you get $y = \sqrt{f(x)}$ so that $y^2 = f(x)$.

11. Singular Cubics are fairly trivial to analyze as far as finding rational points - though Mordell's Theorem does not hold for them.

Elliptic Curves - Washington

1. Square array of sphere to be arranged into pyramid. Want

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

Defines elliptic curve $\frac{1}{3}x^2 + \frac{1}{2}x^2 + \frac{1}{6}x$. Know solutions $(0,0)$ and $(1,1)$, connect to form line $y = x$ and make substitution and obtain $x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$. Know roots $x = 0$ and $x = 1$, apply the rational roots test and get $0 + 1 + x = \frac{3}{2}$ so that $x = y = \frac{1}{2}$. Continue this process to obtain 4900 spheres (70×70 array and a 24 sphere high pyramid).

2. $a^4 + b^4 = c^4$ has no integer solutions where $abc \neq 0$. Suppose $a \neq 0$. Let

$$x = \frac{b^2 + c^2}{a^2} \quad , \quad y = 4\frac{b(b^2 + c^2)}{a^2}$$

Then we have $y^2 = x^3 - 4x$, an elliptic curve. The cubic Fermat equation can be changed to elliptic curve $y^2 = x^3 - 432$.

3. Elliptic Curve, E: Equation of form $y^2 = x^3 + Ax + B$, where A and B are constants. This is called the Weierstrass equation for an elliptic curve. The field K will be specified. If L is a field with $L \supseteq K$ then

$$E(L) = \{\infty\} \cup \{(x,y) \in L \times L \mid y^2 = x^3 + Ax + B\}$$

Not possible to graph (meaningfully) over most fields. Note we do not allow multiple roots. That is, $4A^3 + 27B^2 \neq 0$. Why?

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2)$$

so that the roots must be distinct. Given

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where a_i are constants, note that in fields of not characteristic 2, we complete the square and obtain

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

with $y_1 = y + a_1x/2 + a_3/2$ and constants a_2', a_4', a_6'. Then if the field is not characteristic 3, $x_1 = x + a_2'/3$ and obtain the Weierstrass equation for an elliptic curve. Need to treat characteristic 2 fields differently. However, "most", but not all, elliptic curves over fields characteristic 3 still have form $y^2 = x^3 + Ax + B$. The general case is $y^2 = x^3 + Cx^2 + Ax + B$.

4. LEFT OFF ON PAGE 14.

Introduction to Elliptic Curves and Modular Forms - Kobliz

1. Theorem (Tunnell): Let n be an odd squarefree natural number. Then

   (a) n is congruent.

   (b) The number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.

   (a) implies (b) and if the BSD holds, then (b) implies (a).

2. Example how complex congruent numbers can be: 157 has a hypotenuse with 50 digits in its numerator.

3. The congruent number problem: Let (x, y) be a point with rational coordinates on the curve $y^2 = x^3 - n^2x$. Suppose that x satisfies the two conditions: (i) it is the square of a rational number and (ii) its denominator is even Then there exists a right triangle with rational sides and area n which corresponds to x under the correspondence (X, Y, Z) with $X < Y < Z$ and

   $$X, Y, Z \mapsto x = (Z/2)^2$$
   $$x \to X = \sqrt{x+n} - \sqrt{x-n}, Y = \sqrt{x+n} + \sqrt{x-n}, Z = 2\sqrt{x}$$

   In particular, n is a congruent number if and only if there exists x such that $x + n$ and $x - n$ are squares of rational numbers. Hence, congruent numbers correspond to points $P = (x, y)$ which are "twice" a rational $P' = (x', y')$. That is, $P + P' = (x, y)$, where $+$ is the addition on an elliptic curve.

4. Elliptic Curve: $C : y^2 = f(x)$ over a field K with characteristic not 2. That is, $f(x) \in K[x]$. In general, $x_0, y_0 \in K'$ coordinates on curve C defined by $F(x, y) = 0$. C is smooth at (x_0, y_0) if $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are not both zero at (x_0, y_0). If char $K \neq 2$, this is the case $F(x, y) = y^2 - f(x)$ has nonzero partials, which are $2y_0$ and $-f'(x_0)$. As char $K \neq 2$, then these are both zero only if $y = 0$ and $f'(x_0)$ is zero which means only if there is a multiple root. Thus, C is smooth if $f(x)$ has distinct roots in K.