Elliptic Curves

Martin Leslie

Congruent numbers

- We call a positive integer n a *congruent number* if there exists a right angled triangle with sides of rational length and area n.
- For example the 3-4-5 triangle has area 6 so 6 is a congruent number. What about 5?
- We require $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $n = ab/2$. Make the change of variables $x = \frac{n(a+c)}{b}$ and $y = \frac{2n^2(a+c)}{b^2}$. We can easily check that

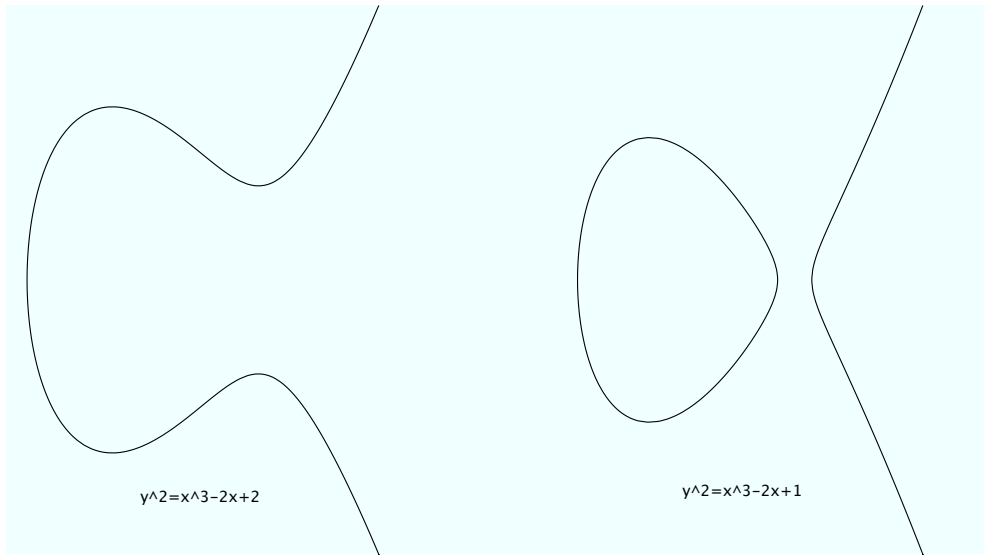
$$y^2 = x^3 - n^2 x.$$

Congruent numbers

- If we find a point (x, y) on $y^2 = x^3 - n^2x$ then we can again check that $a = \frac{x^2-n^2}{y}$, $b = \frac{2nx}{y}$ and $c = \frac{x^2+n^2}{y}$
- So, if we can find a rational point (x, y) on this curve with $y \neq 0$ then we can find a, b, c rational. So a positive integer n is a congruent number iff there exists a rational point on this curve with $y \neq 0$.
- Actually, $y^2 = x^3 - nx$ is an elliptic curve.

Elliptic Curves

- An elliptic curve, defined over the rationals, is the set of (possibly complex) points on a curve $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$ together with a 'point at infinity', $\mathcal{O}$.
- We also require the curve to be non-singular – to have no cusps or self intersections. This is equivalent to requiring that $x^3 + ax + b$ has no repeated roots or that $4a^3 + 27b^2 \neq 0$.

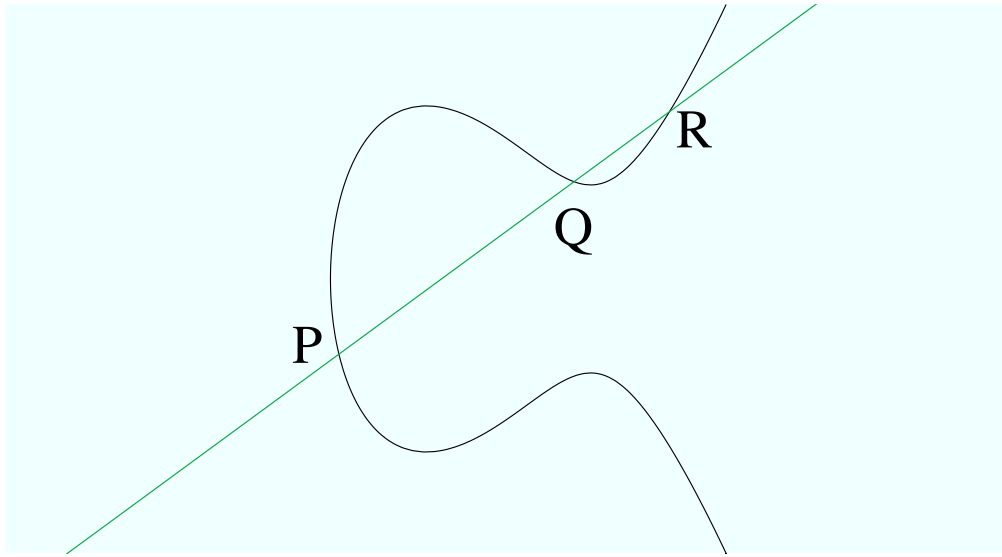


A (slightly) better definition

- We can define an elliptic curve to be a nonsingular projective plane curve given by $Y^2Z = X^3 + aXZ^2 + bZ^3$.
- The hyperplane at infinity is $Z = 0$. But if $Z = 0$ then $X^3 = 0$ so a point is of the form $(0 : Y : 0) = (0 : 1 : 0)$. So there is only one point at infinity, $\mathcal{O} = (0 : 1 : 0)$.
- If $Z \neq 0$ then we can divide out by it and $(X/Z : Y/Z : 1)$ is a point on $(Y/Z)^2 = (X/Z)^3 + a(X/Z) + b$.

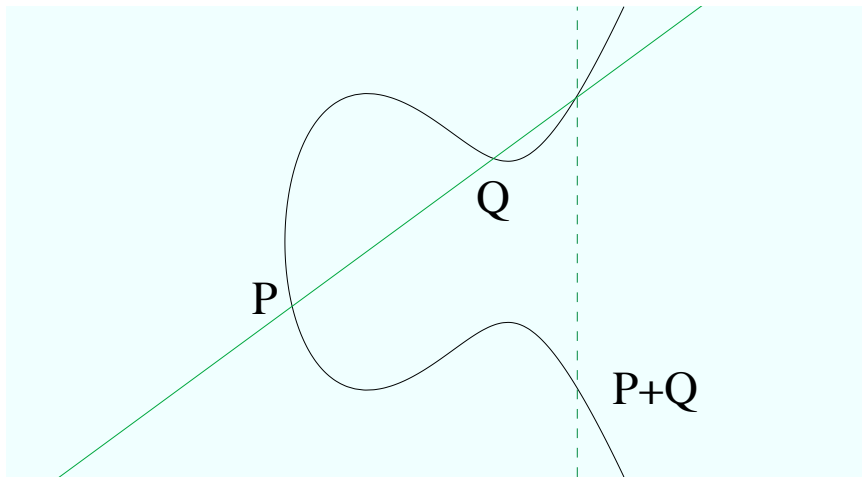
Finding rational points

- Given two rational points on an elliptic curve, how could we find another one?
- A line between two rational points should intersect a cubic curve in another point and this point will be rational.
- So does this give us a group?



The Group Law

- Given two points on an elliptic curve draw the line from P to Q until you hit the curve again.
- Next draw a line from the point at infinity to this point. The point $P + Q$ is where this line intersects the elliptic curve again.



Equations for group law

- Notice that $P + \mathcal{O} = P$ and that $(x, y) + (x, -y) = \mathcal{O}$.
- If we're not in one of these cases then we're adding $P_1 = (x_1, y_1)$ to $P_2 = (x_2, y_2)$ to get $P + Q = (x_3, y_3)$ and we have two more cases:
  - $x_1 \neq x_2$: We can find the equation of the line between P_1 and P_2 to be $y = \lambda x + \nu$ with $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$.
  - $x_1 = x_2$. We must have $y_1 = y_2$ so the line between P_1 and P_2 is the tangent line $y = \lambda x + \nu$ with $\lambda = \frac{3x_1^2 + a}{2y_1}$ and $\nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1}$.
- Then in both cases $x_3 = -\lambda^2 - x_1 - x_2$ and $y_3 = \lambda x_3 + \nu$.

- Under this definition of the group law the (possibly complex) points on the elliptic curve form an abelian group (with identity $\mathcal{O}$) that we will denote E.
- There is a subgroup made up of the points on the elliptic curve that have rational coordinates, denoted $E(\mathbb{Q})$.
- As we are doing number theory we are interested in finding this group.

Why We Study Elliptic Curves

- Applications:
  - Elliptic curve cryptography.
  - Elliptic curve integer factorisation.
  - Proving Fermat's Last Theorem.
- Elliptic curves are smooth projective curves of genus one with a specified basepoint. Curves of genus zero are conics and are well understood – if they have one rational point then they have infinitely many.
- Curves of genus greater than one have only finitely many rational points by a deep theorem of Falting. Thus elliptic curves are an interesting boundary case that have provided much of the motivation for modern algebraic geometry and arithmetic geometry.

The Mordell–Weil Theorem

Theorem (Mordell 1922)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.*

- By the fundamental theorem of finitely generated abelian groups this means that

$$E(\mathbb{Q}) \cong E_{\mathrm{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r.$$

The Torsion subgroup

- We can find the points of finite order using the following

  Theorem (Nagell 1935, Lutz 1937)**.** *Let E be an elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$. Then a non-identity torsion point (x, y) has $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$.*

- More surprisingly, there are only a finite number of possibilities for the torsion subgroup.

  Theorem (Mazur 1978)**.** *The isomorphism type of $E_{\mathrm{tors}}(\mathbb{Q})$ is one of*

  - $\mathbb{Z}/n\mathbb{Z}$ *for* $n = 1, 2, \ldots, 8, 9, 10, 12$*, or*
  - $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *for* $n = 2, 4, 6, 8$*.*

Finding the rank

- There is no known effective method to find r, the rank.
- Since we are looking for rational points you might think we can just search for them. However relatively simple curves can have very complicated points.
- For example the curve $y^2 = x^3 + 877x$ has rank one and the x–coordinate of a generator is given by

$$\left(\frac{6127760831879473681 01}{788415358606390021 0} \right)^2 .$$

Rank

- It is conjectured that there are curves of arbitrarily high rank (although most elliptic curves are of very small rank).
- As of 2006 the curve of highest known rank is of rank at least 28. It is given by

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x+$$
$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9.$$

The Congruent number problem

- We have the following solution (if we can find ranks effectively) to our congruent number problem

  Theorem. *A positive integer n is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2x$ has rank greater than zero.*

- The congruent numbers less than 100 are

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41,$$
$$45, 46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79,$$
$$80, 84, 85, 86, 87, 88, 92, 93, 94, 95, 96$$

- Tunnel (1983) gave an effective procedure for determining if n is a congruent number assuming the Birch–Swinnerton-Dyer conjecture.

Calculating the rank

- Programs like mwrank/Pari/Sage/Magma can calculate ranks quite well practically but there is no algorithm that always works.
- Going back to our motivating problem consider the question of the congruent number problem for $n = 5$. We'll solve it using Sage.

Birch–Swinnerton-Dyer conjecture

- The Clay Institute is offering one million dollars for a proof of the Birch–Swinnerton-Dyer conjecture. Associated to an elliptic curve E is an L–series $L_E(s)$. The BSD conjecture is that
  - $L_E(s)$ has a zero at $s = 1$ of order equal to the rank of $E(\mathbb{Q})$; and
  - $$\lim_{s \to 1} \frac{L_E(s)}{(s-1)^r} = \frac{\Omega R |Ш| \prod_{p|\Delta} c_p}{|E_{\text{tors}}(\mathbb{Q})|^2}.$$

Ellipses and Elliptic Integrals

- Why are they called elliptic curves?
- Start with an ellipse parameterized by $x = a\cos\theta$ and $y = b\sin\theta$. Then the arc length from $\theta = 0$ to ϕ is

$$\begin{aligned}\int_0^\phi \sqrt{(dx/d\theta)^2 + (dy/d\theta)^2} &= \int_0^\phi \sqrt{a^2\sin^2\theta + b^2\cos^2\theta} \\ &= \int_0^\phi \sqrt{b^2 - (b^2 - a^2)\sin^2\theta} \\ &= b\int_0^\phi \sqrt{1 - (1 - a^2/b^2)\sin^2\theta}\end{aligned}$$

- So define the elliptic integral of the second kind by $E(\phi, k) = \int_0^\phi \sqrt{1 - k^2\sin^2\theta}\, d\theta$.

Elliptic Integrals and Elliptic Functions

- Then define the elliptic integral of the first kind by

$$F(\phi, k) = \int_0^\phi \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}}.$$

- Now, fixing k, we can find the inverse to the function $u = F(\phi, k)$ which allows us to define Jacobi's elliptic functions by $\operatorname{sn} u = \sin \phi$, $\operatorname{cn} u = \cos \phi$ and $\operatorname{dn} u = \sqrt{1 - k^2 \sin^2 \phi}$.
- These are elliptic functions: they have a period on the real axis and somehow one on the imaginary axis too.

Elliptic Functions and Elliptic Curves

- We have $\mathrm{sn}^2 + \mathrm{cn}^2 = 1$ and $\mathrm{dn}^2 + k^2\,\mathrm{sn}^2 = 1$.
- On the intersection of these two surfaces in $\mathbb{CP}^3$ we have $\mathrm{dn}^2 = 1 - k^2\,\mathrm{sn}^2 = 1 - k^2(1 - \mathrm{cn}^2)^2$.
- If we let $y = \mathrm{dn}$ and $x = \mathrm{cn}$ we have $y^2 = \mathrm{quartic\ in}\ x$ which is an elliptic curve (with a change of coordinates).
- In fact every elliptic curve is parameterized by elliptic functions (usually we use Weierstrass $\wp$ functions).
- So elliptic curves are so named because they are parameterized by elliptic functions, which are the inverses of elliptic integrals, which are used to find the arc length of ellipses.

Cryptography

- Private Key cryptography is like giving a key to your friend in person and later sending them a locked box.
- Public key cryptography is like sending out padlocks to everyone in the world and you just keep the key.
- But to do this you need some kind of problem that is hard to answer, easy to verify an answer. Number theory has provided two such problems: factoring and discrete logs.

ElGamal for Elliptic Curves

- (setup) Choose an elliptic curve E over $\mathbb{F}_q$, together with a point P on the curve. This generates a cyclic subgroup G of order n. Each user picks an integer $l \in \{0, 1, \ldots, n-1\}$ (the private key) and makes public lP (the public key). Suppose that $m \in G$ is a message and that user A wants to send m to user B.
- A generates a random integer $k \in \{0, 1, \ldots, n-1\}$ and computes kP.
- A looks up B's public key lP and computes $m + k(lP)$.
- A sends to B the pair $(kP, m + klP)$.
- B computes $(m + klP) - l(kP) = m$ and recovers the message

Attacks?

- An eavesdropper knows E, P, lP, kP, $m + klP$. How could they find m?
- If they could find l given P and lP then they could recover the message. This is the *discrete logarithm problem for elliptic curves*. Maybe they could do it some other way but no-one has ever thought of one.
- So elliptic cryptosystems are (believed to be) secure because the elliptic curve discrete log problem is (believed to be) hard.
- The best algorithms for discrete log on a well chosen $G \leq E$ are general purpose algorithms that run in order of $\sqrt{(n)}$ time.

Elliptic Curve Cryptography

- We have efficient algorithms for adding points together so we can work with elliptic curves over $\mathbb{F}_q$ with q several hundred decimal digits long. This makes discrete log algorithms infeasible.
- Elliptic curve cryptography is faster than finite field cryptography once we take into account the smaller key sizes required.
- Elliptic curve key agreement and digital signature algorithms are part of NSA's Suite B cryptography used for securing secrets up to the level of 'Top Secret'.

The End

- Any questions?