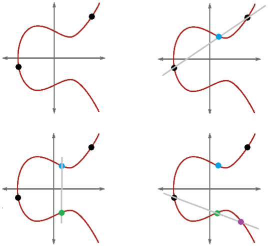
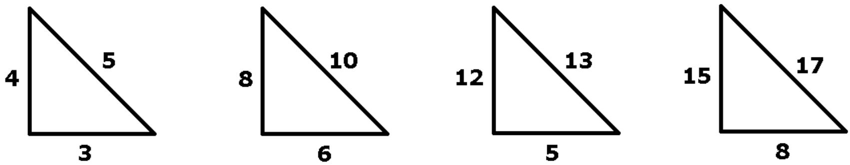
A Million Dollar Question

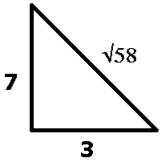
Brian Heinold
Mount St. Mary's University



Right triangles

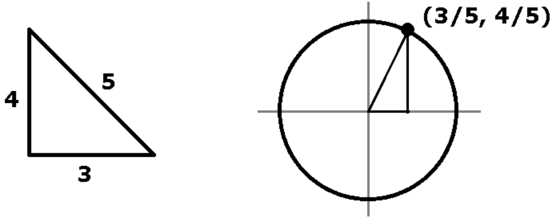


Not so easy to find naïvely...



How to find Pythagorean triples

Pythagorean triples $\Leftrightarrow$ rational points on unit circle

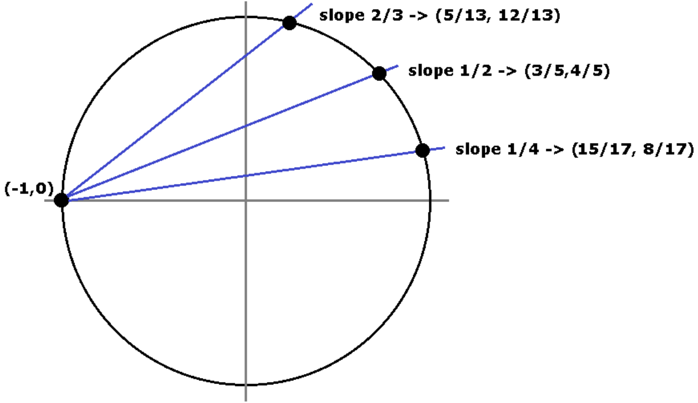


$$a^2 + b^2 = c^2 \leftrightarrow \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

This is in the form of the equation of the unit circle: $x^2 + y^2 = 1$.

How to find Pythagorean triples, cont.

Start with a rational point on the circle and use that to generate all the others.



rational slopes $\Leftrightarrow$ rational points

How to find Pythagorean triples, cont.

The line meets the circle in two points.
We know one is $(-1, 0)$.

Equation of line: $y - 0 = r(x + 1)$
Equation of circle: $x^2 + y^2 = 1$

Plug in: $x^2 + [r(x + 1)]^2 = 1$
Algebra: $(r^2 + 1)x^2 + 2rx + (r^2 - 1) = 0$
Factor: $(x + 1)\left((r^2 + 1)x + (r^2 - 1)\right) = 0$

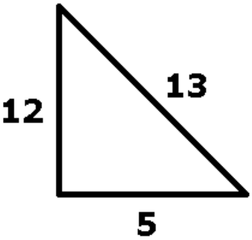
How to find Pythagorean triples, cont.

$$x = \frac{1-r^2}{1+r^2}, \qquad y = \frac{2r}{1+r^2}$$

Try $r = 2/3$:

$x = \frac{5/9}{13/9}$, $y = \frac{4/3}{13/9}$

So $x = 5/13$, $y = 12/13$

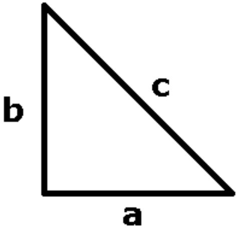


How to find Pythagorean triples, cont.

Formula simplifies to:

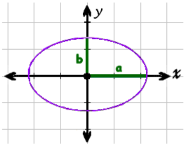
$$a = n^2 - m^2$$
$$b = 2mn$$
$$c = n^2 + m^2$$

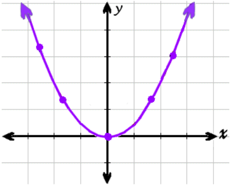
where m, n have no common factors



Other conics

The same process works for finding rational points on ellipses, parabolas, and hyperbolas.





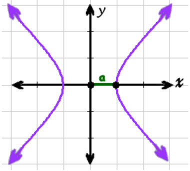


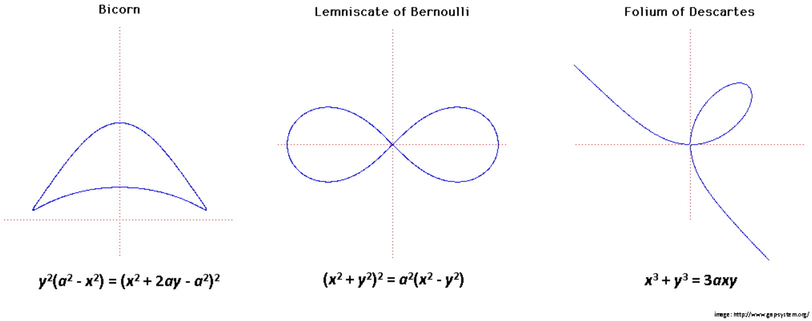
image: http://mathforum.org/cgraph/history/glossary.htm

These are all degree 2 curves:

parabola: $y = ax^2 + bx + c$
ellipse/hyperbola: $a(x - x_0)^2 \pm b(y - y_0)^2 = 1$

Higher degree curves

What about higher degree curves?



Possibilities for curves

Possibilities:

1. Infinitely many rational points ($x^2 + y^2 = 1$)
2. No rational points ($x^2 + y^2 = 3$)
3. Finitely many rational points ($x^4 + y^4 = 2$)

Possibilities by degree:

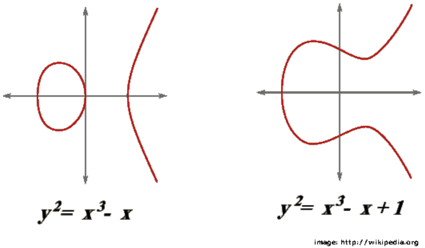
- Degree 1 or 2: None or infinite many
- Degree 3: None, finite #, or infinitely many
- Degree ≥ 4: None or finite # (deep theorem)

Elliptic curves

The most interesting case is degree 3.
Degree 3 curves can be algebraically transformed into the following form:

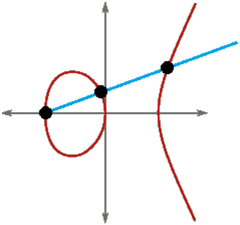
$$y^2 = x^3 + ax + b$$

If the curve has no cusps or self-intersections, it is called an **elliptic curve**.



Old approach fails

Pythagorean triple approach fails.

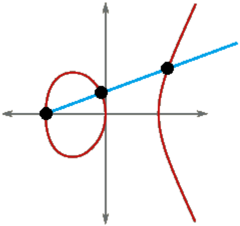


Line meets curve in three points.

When we substitute line equation in and factor, we could get something like $(x+1)(x^2-3)$.

Or does it?

But it can be modified to work.

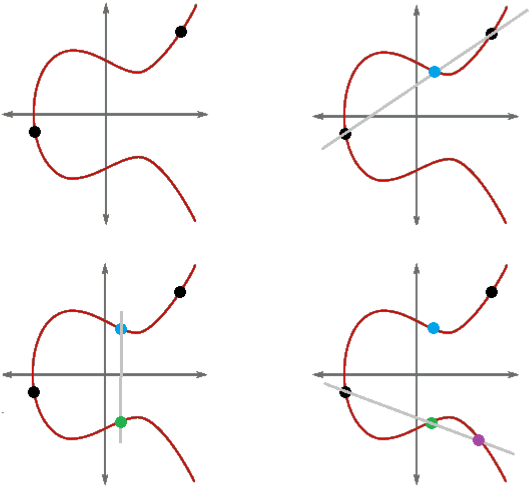


Suppose you start with two rational points.

When we substitute line equation in and factor, we get something like $(x - p_1)(x - p_2)(x - p_3)$ and since p_1 and p_2 are rational, then so is p_3.

Chord and tangent procedure

We can repeatedly apply this idea to generate more rational points.



How many points do you need?

- You will always get all the rational points using this method.
- But you may need to start with more than one or two points in order to generate all of them.
- The number of points you need is called the *rank*.
- Note: a rank 0 curve has only finitely many rational points.
- By Mordell's Theorem (1923), the rank is finite.

Determining the rank is tough

- There is no known algorithm to determine the rank of any elliptic curve, or even determine if the rank is nonzero.
- To get some insight into the problem, instead look at the curves modulo a prime p
- Example: $y^2 = x^2 + 2x + 3 \pmod{11}$
- One solution is $(5, 4)$ because LHS is $4^2 \equiv 5 \pmod{11}$ and the RHS is $5^2 + 2 \cdot 5 + 3 = 38 \equiv 5 \pmod{11}$.
- A computer search can find all the solutions.

The Birch Swinnerton-Dyer Conjecture

In the early 1960s Brian Birch and Peter Swinnerton-Dyer did computer searches for rational solutions.

They conjectured that the number of solutions, N_p, satisfies

$$\prod_{p \leq x} \frac{N_p}{p} \approx C\,(\log x)^r$$

as $x \to \infty$, where r is the rank of the curve, and C is a constant.

More formally

Their conjecture is often phrased using higher mathematics:

Then we can define the incomplete L-series of C (incomplete because we omit the Euler factors for primes $p|2\Delta$) by

$$L(C,s) := \prod_{p\nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

We view this as a function of the complex variable s and this Euler product is then known to converge for $\mathrm{Re}(s) > 3/2$. A conjecture going back to Hasse (see the commentary on 1952(d) in [26]) predicted that $L(C,s)$ should have a holomorphic continuation as a function of s to the whole complex plane. This has now been proved ([25], [24], [1]). We can now state the millenium prize problem:

Conjecture (Birch and Swinnerton-Dyer). *The Taylor expansion of $L(C,s)$ at $s=1$ has the form*

$$L(C,s) = c(s-1)^r + \textit{higher order terms}$$

with $c \neq 0$ and $r = \mathrm{rank}(C(\mathbb{Q}))$.

In particular this conjecture asserts that $L(C,1) = 0 \Leftrightarrow C(\mathbb{Q})$ is infinite.

Above: A part of Andrew Wiles's description from http://www.claymath.org

Even more formally

Let E be an elliptic curve over $\mathbb{Q}$, and let $L(E,s)$ be the L-series attached to E .

Conjecture 1 (Birch and Swinnerton-Dyer)

1. $L(E,s)$ has a zero at $s=1$ of order equal to the rank of $E(\mathbb{Q})$.
2. Let $R = \mathbf{rank}(E(\mathbb{Q}))$. Then the residue of $L(E,s)$ at $s=1$, i.e. $\lim_{s\to 1}(s-1)^{-R}L(E,s)$ has a concrete expression involving the following invariants of E : the real period, the Tate-Shafarevich group, the elliptic regulator and the Neron model of E .

J. Tate said about this conjecture: ``*This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group (Sha) which is not known to be finite!*'' The precise statement of the conjecture asserts that:

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^R} = \frac{|\,\mathrm{Sha}\,|\cdot\Omega\cdot\mathrm{Reg}(E/\mathbb{Q})\cdot\prod_p c_p}{|E_{\mathrm{tors}}(\mathbb{Q})|^2}$$

where

- R is the rank of $E/\mathbb{Q}$.
- Ω is either the real period or twice the real period of a minimal model for E , depending on whether $E(\mathbb{R})$ is connected or not.
- $|\,\mathrm{Sha}\,|$ is the order of the Tate-Shafarevich group of $E/\mathbb{Q}$.
- $\mathrm{Reg}(E/\mathbb{Q})$ is the elliptic regulator of $E(\mathbb{Q})$.
- $|E_{\mathrm{tors}}(\mathbb{Q})|$ is the number of torsion points on $E/\mathbb{Q}$ (including the point at infinity $\mathcal{O}$).
- c_p is an elementary local factor, equal to the cardinality of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ is the set of points in $E(\mathbb{Q}_p)$ whose reduction modulo p is non-singular in $E(\mathbb{F}_p)$. Notice that if p is a prime of good reduction for $E/\mathbb{Q}$ then $c_p = 1$, so only $c_p \neq 1$ only for finitely many primes p . The number c_p is usually called the Tamagawa number of E at p .

From PlanetMath.org

Progress

There have been a few partial results. Among them are:

- Average rank is less than 1
- At least 10% of elliptic curves have rank 1
- At least 80% have rank 0 or 1
- The conjecture is true for a nonzero proportion of curves

If true, the conjecture would give a way to determine the rank of an elliptic curve.

Uses of elliptic curves

Elliptic curves are important for

- Cryptography
- Digital signatures
- Factoring large numbers
- Determining if a number is prime
- Proof of Fermat's Last Theorem