Modern Math Workshop 2013

Undergraduate Mini-Course #2:

A Survey of Diophantine Equations

Edray Herber Goins

Department of Mathematics
Purdue University

October 2, 2013

PURDUE UNIVERSITY

Abstract

There are many beautiful identities involving positive integers. For example, Pythagoras knew $3^2 + 4^2 = 5^2$ while Plato knew $3^3 + 4^3 + 5^3 = 6^3$. Euler discovered $59^4 + 158^4 = 133^4 + 134^4$, and even a famous story involving G. H. Hardy and Srinivasa Ramanujan involves $1^3 + 12^3 = 9^3 + 10^3$. But how does one find such identities?

Around the third century, the Greek mathematician Diophantus of Alexandria introduced a systematic study of integer solutions to polynomial equations. In this session, we'll focus on various types of so-called Diophantine Equations, discussing such topics as the Postage Stamp Problem, Pythagorean Triples, Pell's Equations, Elliptic Curves, the ABC Conjecture and Fermat's Last Theorem.

Modern Math Workshop

Undergraduate Mini-Course #2: Part I

1:00 PM – 2:25 PM

SACNAS National Convention

Room 210B

Henry B. Gonzalez Convention Center

What is the

Modern Math Worksop 2013?

Hosting Mathematics Institutions

1. AIM: American Institute of Mathematics
2. IAS: Institute for Advanced Study
3. ICERM: Institute for Computational and Experimental Research in Math
4. IMA: Institute for Mathematics and its Applications
5. IPAM: Institute for Pure and Applied Mathematics
6. MBI: Mathematical Biosciences Institute
7. MSRI: Mathematical Sciences Research Institute
8. NIMBioS: National Institute for Mathematical and Biological Synthesis
9. SAMSI: Statistical and Applied Mathematical Sciences Institute

Research Experiences for Undergraduate Faculty (June 4 – 8, 2012)

`http://aimath.org/ARCC/workshops/reuf4.html`

Mathematical Sciences Research Institute Undergraduate Program

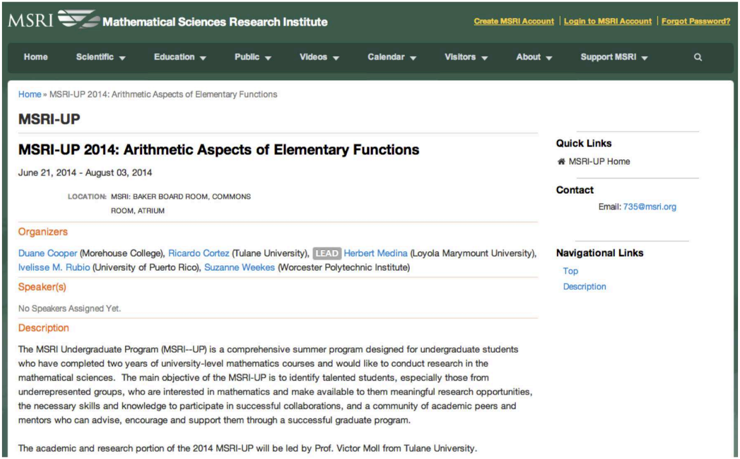
MSRI-UP 2010: Elliptic Curves and Applications

http://www.msri.org/web/msri/pages/137

Mathematical Sciences Research Institute Undergraduate Program

MSRI-UP 2010: Elliptic Curves and Applications

http://www.msri.org/web/msri/pages/137



MSRI Mathematical Sciences Research Institute

Create MSRI Account | Login to MSRI Account | Forgot Password?

Home | Scientific | Education | Public | Videos | Calendar | Visitors | About | Support MSRI

Home » MSRI-UP 2014: Arithmetic Aspects of Elementary Functions

MSRI-UP

MSRI-UP 2014: Arithmetic Aspects of Elementary Functions

June 21, 2014 - August 03, 2014

LOCATION: MSRI: BAKER BOARD ROOM, COMMONS ROOM, ATRIUM

Organizers

Duane Cooper (Morehouse College), Ricardo Cortez (Tulane University), LEAD Herbert Medina (Loyola Marymount University), Ivelisse M. Rubio (University of Puerto Rico), Suzanne Weekes (Worcester Polytechnic Institute)

Speaker(s)

No Speakers Assigned Yet.

Description

The MSRI Undergraduate Program (MSRI--UP) is a comprehensive summer program designed for undergraduate students who have completed two years of university-level mathematics courses and would like to conduct research in the mathematical sciences. The main objective of the MSRI-UP is to identify talented students, especially those from underrepresented groups, who are interested in mathematics and make available to them meaningful research opportunities, the necessary skills and knowledge to participate in successful collaborations, and a community of academic peers and mentors who can advise, encourage and support them through a successful graduate program.

The academic and research portion of the 2014 MSRI-UP will be led by Prof. Victor Moll from Tulane University.

Quick Links

MSRI-UP Home

Contact

Email: 735@msri.org

Navigational Links

Top

Description

Mathematical Sciences Research Institute Undergraduate Program

MSRI-UP 2014: Arithmetic Aspects of Elementary Functions

`http://www.msri.org/msri_ups/735`

Goals of the Modern Math Workshop

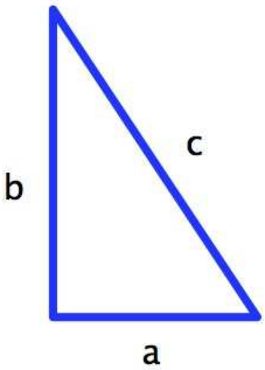
- As part of the Mathematical Sciences Collaborative Diversity Initiatives, nine mathematics institutes will host their annual pre-conference event, the 2013 Modern Math Workshop.
- The Modern Math Workshop is intended to re-invigorate the focus of mathematics students and faculty at minority-serving institutions and the research careers of minority mathematicians.
- On Day 1 (October 2), two minicourses geared towards an undergraduate audience will run concurrently during the Modern Math Workshop. Undergraduate applicants will select their minicouse of choice when they register.
- On both Days 1 and 2 (October 2 – 3), a series of eight talks geared towards early career researchers will be given on exciting and current research topics associated with the hosting institutes' upcoming programs. Each of the hosting institutes selected these speakers to represent them at the Modern Math Workshop.

Outline of Talk

1. Part I: 1:00 PM – 2:25 PM
   - Pythagorean Triples
   - Pell's Equation
   - Fermat's Last Theorem and Beal's Conjecture
   - Pythagorean Quadruples
   - The *ABC* Conjecture
2. Break: 2:30 PM – 2:40 PM
3. Part II: 2:45 PM – 3:40 PM
   - Elliptic Integrals
   - Elliptic Curves
   - Heron Triangles
   - The *ABC* Conjecture

Some Motivating Questions

Pythagorean Triples



Motivating Question

What are some positive integers a, b, and c such that $a^2 + b^2 = c^2$?

Pythagorean Triples

$$3^2 + 4^2 = 5^2 \qquad 8^2 + 15^2 = 17^2 \qquad 10^2 + 24^2 = 26^2$$
$$6^2 + 8^2 = 10^2 \qquad 12^2 + 16^2 = 20^2 \qquad 20^2 + 21^2 = 29^2$$
$$5^2 + 12^2 = 13^2 \qquad 7^2 + 24^2 = 25^2 \qquad 16^2 + 30^2 = 34^2$$

Motivating Questions

Consider the equation $a^2 + b^2 = c^2$.

1. What are **some** integer solutions (a, b, c)?
2. What are **all** integer solutions (a, b, c)?

Proposition

For any Pythagorean Triple (a, b, c), there exist integers m and n such that

$$a : b : c = 2\,m\,n \;:\; m^2 - n^2 \;:\; m^2 + n^2.$$

Proof: Define the integers m and n by the relation

$$\frac{m}{n} = \frac{a}{c-b} \quad \Longrightarrow \quad \begin{matrix} a = \dfrac{m}{n}(c-b) \\ a^2 = c^2 - b^2 \end{matrix} \quad \Longrightarrow \quad \begin{matrix} \dfrac{a}{c} = \dfrac{2\,m\,n}{m^2+n^2} \\ \dfrac{b}{c} = \dfrac{m^2-n^2}{m^2+n^2} \end{matrix}$$

$$3^2 + 4^2 = 5^2 \qquad 8^2 + 15^2 = 17^2 \qquad 10^2 + 24^2 = 26^2$$

$$6^2 + 8^2 = 10^2 \qquad 12^2 + 16^2 = 20^2 \qquad 20^2 + 21^2 = 29^2$$

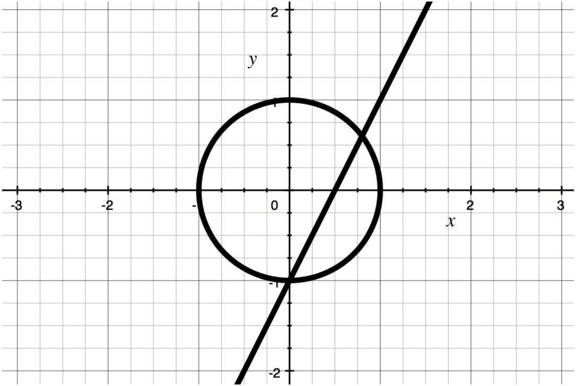
$$5^2 + 12^2 = 13^2 \qquad 7^2 + 24^2 = 25^2 \qquad 16^2 + 30^2 = 34^2$$

a	b	c	m/n
3	4	5	3
6	8	10	3
5	12	13	5

a	b	c	m/n
8	15	17	4
12	16	20	3
7	24	25	7

a	b	c	m/n
10	24	26	5
20	21	29	5/2
16	30	34	4

Geometric Interpretation



$$x = \frac{a}{c} = \frac{2\,m\,n}{m^2 + n^2} \qquad y = \frac{b}{c} = \frac{m^2 - n^2}{m^2 + n^2} \quad \Longrightarrow \quad \frac{m}{n} = \frac{y+1}{x} \quad \Longrightarrow \quad y = (m/n)\,x - 1, \quad x^2 + y^2 = 1$$

General Algorithm

Consider a quadratic equation

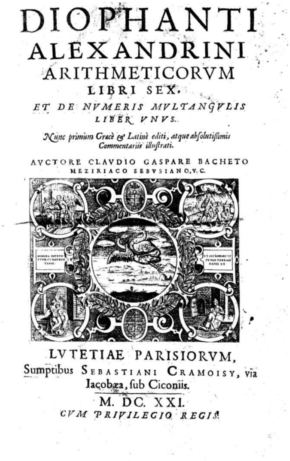
$$A\,a^2 + B\,a\,b + C\,b^2 + D\,a\,c + E\,b\,c + F\,c^2 = 0$$

with fixed integer coefficients A, B, C, D, E, and F. We can express this as a matrix product

$$\frac{1}{2}\begin{bmatrix} a \\ b \\ c \end{bmatrix}^T \begin{bmatrix} 2\,A & B & D \\ B & 2\,C & E \\ D & E & 2\,F \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = 0.$$

Motivating Questions

1. What are **some** integer solutions (a, b, c)?
2. What are **all** integer solutions (a, b, c)?



Cover of the 1621 translation of Diophantus' Arithmetica

http://en.wikipedia.org/wiki/Diophantus

General Algorithm

$$A\,a^2 + B\,a\,b + C\,b^2 + D\,a\,c + E\,b\,c + F\,c^2 = 0$$

- Step #1: Find a solution (a_0, b_0, c_0) with say $c_0 \neq 0$.
- Step #2: Substitute

$$x = \frac{a}{c} \qquad y = \frac{b}{c} \qquad \frac{m}{n} = \frac{b\,c_0 - b_0\,c}{a\,c_0 - a_0\,c} \qquad \Longrightarrow \qquad \begin{aligned} y &= (m/n)\,(x - x_0) + y_0 \\ A\,x^2 + B\,x\,y + C\,y^2 + D\,x + E\,y + F &= 0 \end{aligned}$$

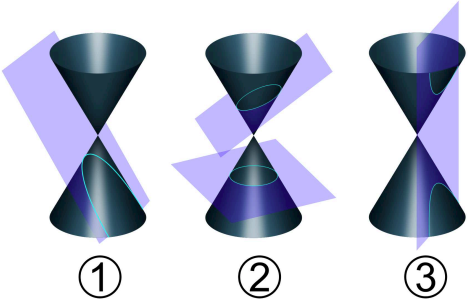
- Step #3: Create a Taylor Series around (x_0, y_0):

$$x = x_0 - \frac{(2\,A\,x_0 + B\,y_0 + D)\,n^2 + (B\,x_0 + 2\,C\,y_0 + E)\,m\,n}{A\,n^2 + B\,m\,n + C\,m^2}$$

$$y = y_0 - \frac{(2\,A\,x_0 + B\,y_0 + D)\,m\,n + (B\,x_0 + 2\,C\,y_0 + E)\,m^2}{A\,n^2 + B\,m\,n + C\,m^2}$$

Conic Sections

$$A x^2 + B x y + C y^2 + D x + E y + F = 0$$



1. $B^2 - 4 A C = 0$: Lines and Parabolas
2. $B^2 - 4 A C < 0$: Circles and Ellipses
3. $B^2 - 4 A C > 0$: Hyperbolas

Conic Sections

Proposition

Given one rational point (x_0, y_0) on the conic section

$$A\,x^2 + B\,x\,y + C\,y^2 + D\,x + E\,y + F = 0$$

then every rational point (x, y) is in the form

$$x = x_0 - \frac{(2\,A\,x_0 + B\,y_0 + D)\,n^2 + (B\,x_0 + 2\,C\,y_0 + E)\,m\,n}{A\,n^2 + B\,m\,n + C\,m^2}$$

$$y = y_0 - \frac{(2\,A\,x_0 + B\,y_0 + D)\,m\,n + (B\,x_0 + 2\,C\,y_0 + E)\,m^2}{A\,n^2 + B\,m\,n + C\,m^2}$$

for some integers m and n.

Corollary

If there is one rational solution (x_0, y_0), then there are infinitely many rational solutions (x, y).

Examples

- The circle $x^2 + y^2 = 1$ has a rational point $(x_0, y_0) = (0, -1)$, so all rational points are in the form
$$(x, y) = \left(\frac{2\,m\,n}{m^2 + n^2}, \ \frac{m^2 - n^2}{m^2 + n^2} \right).$$

- For any integer d, the curve $x^2 - d\,y^2 = 1$ has a rational point $(x_0, y_0) = (1, 0)$, so all rational points are in the form
$$(x, y) = \left(\frac{d\,m^2 + n^2}{d\,m^2 - n^2}, \ \frac{2\,m\,n}{d\,m^2 - n^2} \right).$$

Pell's Equation

Motivating Questions

Fix an integer d that is not a square, and consider the equation $x^2 - d\,y^2 = 1$.

- What are all **rational** solutions (x, y)?
- What are all **integral** solutions (x, y)?

- 1657: Pierre de Fermat
- 1658: William Brouncker, John Wallis
- 1659: Johann Rahn, John Pell
- 1766: Leonhard Euler
- 1771: Joseph-Louis Lagrange

- 628 AD: Brahmagupta
- 1150 AD: Bhaskaracharya

Example

For $d = 2$, we have the equation $x^2 - 2\,y^2 = 1$.

There are infinitely many rational solutions:

$$\begin{aligned} y &= (m/n)\,(x-1) \\ x^2 - 2\,y^2 &= 1 \end{aligned} \qquad \Longrightarrow \qquad (x, y) = \left(\frac{2\,m^2 + n^2}{2\,m^2 - n^2},\ \frac{2\,m\,n}{2\,m^2 - n^2} \right).$$

We can find a few integral solutions:

$$\begin{aligned} (x_0, y_0) &= (1, 0) \\ (x_1, y_1) &= (3, 2) \\ (x_2, y_2) &= (17, 12) \\ (x_3, y_3) &= (99, 70) \\ (x_4, y_4) &= (577, 408) \end{aligned} \qquad \Longrightarrow \qquad x_n + y_n\sqrt{2} = \left(3 + 2\sqrt{2}\right)^n.$$

Proposition

Fix an integer d that is not a square, and consider the equation $x^2 - d\,y^2 = 1$.

- There are infinitely many rational solutions (x, y).
- There are infinitely many integral solutions if and only if d is positive.

Approach: Using the relation $x^2 - d\,y^2 = \left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right)$, we consider the ring

$$\mathbb{Z}[\sqrt{d}] = \left\{ x + y\sqrt{d} \,\middle|\, x,\, y \in \mathbb{Z} \right\}.$$

We denote the norm of $a = x + y\sqrt{d}$ as $\mathbb{N}\,a = x^2 - d\,y^2$ as it has the property $\mathbb{N}\,(a \cdot b) = \mathbb{N}\,a \cdot \mathbb{N}\,b$. If $\delta = x_1 + y_1\sqrt{d}$ has $\mathbb{N}\,\delta = 1$, then so do the numbers

$$x_n + y_n\sqrt{d} = \delta^n = \left(x_1 + y_1\sqrt{d}\right)^n.$$

Group Structure of Pell's Equation

Proposition

Fix an integer d that is not a square, and consider the equation $x^2 - d\,y^2 = 1$.

- We have a one-to-one correspondence

$$\begin{array}{ccc} \left\{ (x,y) \in \mathbb{Z} \times \mathbb{Z} \,\middle|\, x^2 - d\,y^2 = 1 \right\} & \longrightarrow & G = \left\{ a \in \mathbb{Z}[\sqrt{d}] \,\middle|\, \mathbb{N}\,a = 1 \right\}, \\ (x,y) & \mapsto & a = x + y\sqrt{d}. \end{array}$$

- The collection of integer solutions (x, y) to $x^2 - d\,y^2 = 1$ forms a commutative group. The group law is

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1\,x_2 + d\,y_1\,y_2,\ x_1\,y_2 + x_2\,y_1)$$

  with identity $(1, 0)$ and inverse $[-1](x, y) = (x, -y)$.
- Assuming G has an element $\delta' > 1$, there is a unique positive real number $\delta = x_1 + y_1\sqrt{d}$ such that $a = \pm\delta^n$. That is, $G \simeq Z_2 \times \mathbb{Z}$ is generated by -1 and δ.

Proof: Choose $a = x + y\sqrt{d} \in G$. Consider the identities

$$\begin{aligned} a &= x + y\sqrt{d}, & -a &= -x - y\sqrt{d}, \\ a^{-1} &= x - y\sqrt{d}, & -a^{-1} &= -x + y\sqrt{d}. \end{aligned}$$

Without loss of generality, assume $a \geq 1$. Let $\delta > 1$ be that least such element in G. Choose the positive integer n such that $\delta^n \leq a < \delta^{n+1}$, and denote $b = a/\delta^n \in G$. By the minimality of δ we must have $b = 1$. □

Corollary

Assume that we can find at least one solution (x_1, y_1) with $x_1 > 1$. Then there are infinitely many integer solutions to $x^2 - d\,y^2 = 1$.

Proof: Assuming $\delta = x_1 + y_1\sqrt{d} > 1$ exists, write $x_n + y_n\sqrt{d} = \delta^n$. Then

$$(x_n, y_n) = \left(\frac{\delta^n + \delta^{-n}}{2}, \frac{\delta^n - \delta^{-n}}{2\sqrt{d}} \right) \implies \frac{x_n}{y_n} = \sqrt{d}\,\frac{\delta^{2n} + 1}{\delta^{2n} - 1} \to \sqrt{d}.$$

Motivating Question

How do we construct $\delta = x_1 + y_1\sqrt{d}$?

Continued Fractions

Given a real number x, define the following sequence

$$x_0 = x, \qquad x_{k+1} = \frac{1}{x_k - \lfloor x_k \rfloor} \qquad \text{for} \qquad k = 0,\, 1,\, 2,\, \ldots.$$

Denote $a_k = \lfloor x_k \rfloor$ as integers. We have the expression

$$x = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \frac{1}{x_2}} = \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}.$$

Denote the nth convergent as the rational number

$$\{a_0; a_1, a_2, \ldots, a_{n-1}\} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + a_{n-1}}}} = \frac{p_n}{q_n}.$$

Example

Consider $x = \sqrt{2}$. Recall that we define

$$x_0 = x, \qquad x_{k+1} = \frac{1}{x_k - \lfloor x_k \rfloor}, \qquad \text{and} \qquad a_k = \lfloor x_k \rfloor.$$

We find the specific numbers

$$x_0 = \sqrt{2}, \qquad x_1 = \frac{1}{\sqrt{2}-1} = 1 + \sqrt{2}, \qquad x_2 = \frac{1}{(1+\sqrt{2}) - 2} = 1 + \sqrt{2}.$$

Then $a_0 = 1$ while $a_1 = a_2 = \cdots = 2$. We have the expression

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}.$$

The Fundamental Solution

Theorem (Joseph-Louis Lagrange, 1771)

Fix a positive integer d which is not a square.

- $\sqrt{d} = \{a_0; \overline{a_1, \dots, a_{h-1}, 2\,a_0}\}$, where the overline denotes that h terms repeat indefinitely.
- If we consider the hth convergent, say $\{a_0;\, a_1, \dots, a_{h-1}\} = p_h/q_h$, then

$$p_h^2 - d\,q_h^2 = (-1)^h.$$

- Every integral solution (x, y) to $x^2 - d\,y^2 = 1$ can be expressed as $x + y\sqrt{d} = \pm\delta^n$, where

$$\delta = \begin{cases} p_h + q_h\sqrt{d} & \text{if } h \text{ is even,} \\ p_{2h} + q_{2h}\sqrt{d} = \left(p_h + q_h\sqrt{d}\right)^2 & \text{if } h \text{ is odd.} \end{cases}$$

Example

Consider $d = 2$. The continued fraction is

$$\sqrt{2} = \{1; \overline{2}\}$$

which has $h = 1$.

Consider the convergent

$$\frac{p_1}{q_1} = \{1\} = \frac{1}{1} \qquad \Longrightarrow \qquad p_{11}^2 - 2\, q_{11}^2 = -1.$$

On the other hand,

$$\frac{p_2}{q_2} = \{1; 2\} = 1 + \frac{1}{2} = \frac{3}{2}.$$

The fundamental solution is $\delta = 3 + 2\sqrt{2} = \left(1 + \sqrt{2}\right)^2$, so every integral solution (x, y) to $x^2 - 2\,y^2 = 1$ satisfies

$$x + y\sqrt{2} = \pm\left(3 + 2\sqrt{2}\right)^n.$$

Example

Consider $d = 61$. The continued fraction is

$$\sqrt{61} = \{7; \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}\}$$

which has $h = 11$.
Consider the convergent

$$\frac{p_{11}}{q_{11}} = \{7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1\} = \frac{29718}{3805} \qquad \Longrightarrow \qquad p_{11}^2 - 61\, q_{11}^2 = -1.$$

On the other hand,

$$\frac{p_{22}}{q_{22}} = \{7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1\} = \frac{1766319049}{226153980}.$$

The fundamental solution is
$\delta = 1766319049 + 226153980\sqrt{61} = \left(29718 + 3805\sqrt{61}\right)^2$, so every integral solution (x, y) to $x^2 - 61\, y^2 = 1$ satisfies

$$x + y\sqrt{61} = \pm\left(1766319049 + 226153980\sqrt{61}\right)^n.$$

Can we generalize?

Fermat's Last Theorem and Generalizations

Let m, n, and k be positive integers. We generalize $a^2 + b^2 = c^2$ to the equation

$$a^m + b^n = c^k.$$

Theorem (Pierre de Fermat, 1637; Andrew Wiles, 1994)

When $m = n = k \geq 3$, the only integral solutions (a, b, c) to $a^n + b^n = c^n$ must satisfy $a\,b\,c = 0$.

Conjecture (Andrew Beal, Robert Tijdeman, Don Bernard Zagier)

When m, n, $k \geq 3$ the integral solutions (a, b, c) have a factor in common, that is, $\gcd(a, b, c) \geq 2$.

$$10^2 + (-7)^3 = (-3)^5 \qquad 3^3 + 6^3 = 3^5$$

$$13^2 + 7^3 = 2^9 \qquad 162^3 + 27^4 = 3^{14}$$

$$3^2 + (-2)^3 = 1^k \qquad 7^6 + 7^7 = 98^3$$

Beal's Conjecture / Tijdeman-Zagier Conjecture.

Fix integers $m, n, k \geq 3$. The only integers a, b, and c such that $a^m + b^n = c^k$ either satisfy $a\,b\,c = 0$ or $gcd(a, b, c) \geq 2$.

Initially, Beal offered \$5,000 to anyone who could prove this conjecture, but this prize was recently increased to \$1,000,000. Just last week, actress Danica McKellar and mathematician Jordan Ellenberg appeared on the Today Show to discuss this conjecture!

We have some remaining cases though: what if at least one of m, n, and k is either 1 or 2? The Conjecture is definitely false. For example, $10^2 + (-7)^3 = (-3)^5$ for

http://dessindenfants.wordpress.com

Pythagorean Quadruples

We say that (a, b, c, d) is a Pythagorean quadruple if a, b, c, and d are nonzero integers such that $a^2 + b^2 + c^2 = d^2$.

$$
\begin{array}{ccccccc}
 & & & & 1^2+2^2+2^2 & = & 3^2 \\
 & & & & 2^2+3^2+6^2 & = & 7^2 \\
 & & 1^2+4^2+8^2 & = & 4^2+4^2+7^2 & = & 9^2 \\
 & & 2^2+6^2+9^2 & = & 6^2+6^2+7^2 & = & 11^2 \\
 & & & & 3^2+4^2+12^2 & = & 13^2 \\
 & & 2^2+5^2+14^2 & = & 2^2+10^2+11^2 & = & 15^2 \\
 & & 1^2+12^2+12^2 & = & 8^2+9^2+12^2 & = & 17^2 \\
1^2+6^2+18^2 & = & 6^2+6^2+17^2 & = & 6^2+10^2+15^2 & = & 19^2
\end{array}
$$

Motivating Questions

- What are **some** integer solutions (a, b, c, d)?
- What are **all** integer solutions (a, b, c, d)?

Pythagorean Quadruples

Theorem

If (a, b, c, d) is a tuple of integers such that $a^2 + b^2 + c^2 = d^2$, then there exist integers m, n, and p such that

$$a : b : c : d = 2\,m\,n \;:\; 2\,m\,p \;:\; m^2 - n^2 - p^2 \;:\; m^2 + n^2 + p^2.$$

Proof: The proof is similar to that for the triples. First assume that (a, b, c, d) is a Pythagorean quadruple. Let m, n, and p be integers such that

$$\frac{a + i\,b}{d + c} = \frac{n + i\,p}{m} \qquad \text{and} \qquad a^2 + b^2 + c^2 = d^2.$$

We find that

$$\frac{a}{d} = \frac{2\,m\,n}{m^2 + n^2 + p^2}, \qquad \frac{b}{d} = \frac{2\,m\,p}{m^2 + n^2 + p^2}, \qquad \text{and} \qquad \frac{c}{d} = \frac{m^2 - n^2 - p^2}{m^2 + n^2 + p^2}.$$

Parametrizations?

Several types of families can be derived from these parametrizations.

- One obvious family is

$$a = 2\,m\,n\,q, \qquad c = (m^2 - n^2 - p^2)\,q,$$
$$b = 2\,m\,p\,q, \qquad d = (m^2 + n^2 + p^2)\,q;$$

- Other Pythagorean quadruples are in the form

$$a = 2\,\alpha\,\beta + 2\,\gamma\,\delta, \qquad c = \alpha^2 - \beta^2 - \gamma^2 + \delta^2,$$
$$b = 2\,\alpha\,\gamma - 2\,\beta\,\delta, \qquad d = \alpha^2 + \beta^2 + \gamma^2 + \delta^2;$$

These formulas may look different, but they are related by setting

$$m = \alpha^2 + \delta^2, \qquad n = \alpha\,\beta + \gamma\,\delta, \qquad p = \alpha\,\gamma - \beta\,\delta \qquad q = \frac{1}{\alpha^2 + \delta^2}.$$

- For example, consider the quadruple $(36, 8, 3, 37)$.

$$\alpha = 2, \quad \beta = 1, \quad \gamma = 4, \quad \delta = 4; \qquad m = 10, \quad n = 9, \quad p = 2, \quad q = \frac{1}{5}.$$

- These two families do **not** exhaust all possibilities of Pythagorean quadruples!

What about these

Parametrizations?

Mason-Stothers Theorem

Theorem (W. W. Stothers, 1981; R. C. Mason, 1983)

Denote $n(A\,B\,C)$ as the number distinct zeroes of the product of relatively prime polynomials $A(t)$, $B(t)$, and $C(t)$ satisfying $A+B=C$. Then

$$\max\left\{deg(A),\ deg(B),\ deg(C)\right\} \leq n(A\,B\,C) - 1.$$

Proof: We follow Lang's "Algebra". Explicitly write

$$A(t) = A_0 \prod_{i=1}^{a} (t-\alpha_i)^{p_i} \qquad \deg(A) = \sum_{i=1}^{a} p_i$$

$$B(t) = B_0 \prod_{j=1}^{b} (t-\beta_j)^{q_j} \qquad \deg(B) = \sum_{j=1}^{b} q_j$$

$$C(t) = C_0 \prod_{k=1}^{c} (t-\gamma_k)^{r_k} \qquad \deg(C) = \sum_{k=1}^{c} r_k$$

$$\operatorname{rad}\bigl(ABC\bigr)(t) = \prod_{i=1}^{a}(t-\alpha_i) \prod_{j=1}^{b}(t-\beta_j) \prod_{k=1}^{c}(t-\gamma_k) \qquad n(ABC) = a+b+c$$

$$\left. \begin{aligned} F(t) &= \frac{A(t)}{C(t)} \\ G(t) &= \frac{B(t)}{C(t)} \end{aligned} \right\} \implies -\frac{B(t)}{A(t)} = \frac{\dfrac{F'(t)}{F(t)}}{\dfrac{G'(t)}{G(t)}} = \frac{\displaystyle\sum_{i=1}^{a} \frac{p_i}{t-\alpha_i} - \sum_{i=k}^{c} \frac{r_k}{t-\gamma_k}}{\displaystyle\sum_{j=1}^{b} \frac{q_j}{t-\beta_j} - \sum_{k=1}^{c} \frac{r_k}{t-\gamma_k}}$$

Clearing, we find polynomials of degrees $\max\{\deg(A),\ \deg(B)\} \leq n-1$:

$$\mathrm{rad}\big(ABC\big)(t) \cdot \frac{F'(t)}{F(t)} = \sum_{i=1}^{a} p_i \prod_{e \neq i} (t-\alpha_e) \prod_{j=1}^{b} (t-\beta_j) \prod_{k=1}^{c} (t-\gamma_k) - \sum_{k=1}^{c} r_k \prod_{i=1}^{a} (t-\alpha_i) \prod_{j=1}^{b} (t-\beta_j) \prod_{e \neq k} (t-\gamma_e)$$

$$\mathrm{rad}\big(ABC\big)(t) \cdot \frac{G'(t)}{G(t)} = \sum_{j=1}^{b} q_j \prod_{i=1}^{a} (t-\alpha_i) \prod_{e \neq j} (t-\beta_e) \prod_{k=1}^{c} (t-\gamma_k) - \sum_{k=1}^{c} r_k \prod_{i=1}^{a} (t-\alpha_i) \prod_{j=1}^{b} (t-\beta_j) \prod_{e \neq k} (t-\gamma_e)$$

Examples

The Mason-Stothers Theorem is sharp. Here is a list of relatively prime polynomials such that $A(t) + B(t) = C(t)$ and

$$\max\left\{\deg(A),\ \deg(B),\ \deg(C)\right\} = n(A\,B\,C) - 1.$$

$A(t)$	$B(t)$	$C(t)$	n
$(2\,t)^2$ $8\,t\,(t^2+1)$	$(t^2-1)^2$ $(t-1)^4$	$(t^2+1)^2$ $(t+1)^4$	5
$16\,t$ $16\,t^3$	$(t+1)^3\,(t-3)$ $(t+1)\,(t-3)^3$	$(t+3)\,(t-1)^3$ $(t+3)^3\,(t-1)$	5
$(2\,t)^4$ $16\,t\,(t^2-1)\,(t^2+1)^2$	$(t^4-6\,t^2+1)\,(t^2+1)^2$ $(t^2-2\,t-1)^4$	$(t^2-1)^4$ $(t^2+2\,t-1)^4$	9

Restatement of Theorem

The polynomial ring $\overline{\mathbb{Q}}[t]$ has an absolute value

$$|\cdot|: \ \overline{\mathbb{Q}}[t] \to \mathbb{Z}_{\geq 0} \qquad \text{defined by} \qquad \big|A(t)\big| = \begin{cases} 0 & \text{if } A(t) \equiv 0, \\ 2^{\deg(A)} & \text{otherwise.} \end{cases}$$

It has the following properties:

- **Multiplicativity:** $|A \cdot B| = |A| \cdot |B|$
- **Non-degeneracy:** $|A| = 0$ iff $A = 0$; $|A| = 1$ iff $A(t) = A_0$ is a unit.
- **Ordering:** $|A| \leq |B|$ iff $\deg(A) \leq \deg(B)$.

Corollary

For each $\epsilon > 0$ there exists a uniform $\mathcal{C}_\epsilon > 0$ such that the following holds: For any relatively prime polynomials A, B, $C \in \overline{\mathbb{Q}}[t]$ with $A + B = C$,

$$\max\Big\{|A|, \ |B|, \ |C|\Big\} \leq \mathcal{C}_\epsilon \ \Big|\text{rad}(A\,B\,C)\Big|^{1+\epsilon}.$$

Proof: Using Mason-Stothers, we may choose $\mathcal{C}_\epsilon = 1/2$.

Multiplicative Dedekind-Hasse Norms

Let R be a Principal Ideal Domain with quotient field K:

- $\overline{\mathbb{Q}}[t]$ in $\overline{\mathbb{Q}}(t)$ with primes $t - \alpha$.
- $\mathbb{Z}$ in $\mathbb{Q}$ with primes p.

Define $\mathrm{rad}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ is the intersection of primes $\mathfrak{p}$ containing it:

- $\mathrm{rad}(A) = \prod_i (t - \alpha_i)$ for $A(t) = A_0 \prod_i (t - \alpha_i)^{e_i}$ in $\overline{\mathbb{Q}}[t]$.
- $\mathrm{rad}(A) = \prod_i p_i$ for $A = \prod_i p_i^{e_i}$ in $\mathbb{Z}$.

Theorem (Richard Dedekind; Helmut Hasse)

R is a Principal Ideal Domain if and only if there exists an absolute value $|\cdot| : R \to \mathbb{Z}_{\geq 0}$ with the following properties:

- **Multiplicativity:** $|A \cdot B| = |A| \cdot |B|$
- **Non-degeneracy:** $|A| = 0$ *iff* $A = 0$; $|A| = 1$ *iff A is a unit.*
- **Ordering:** $|A| \leq |B|$ *if A divides B.*

We may define $|\mathfrak{a}| = |A|$ as $\mathfrak{a} = A\,R$. Hence $|rad(\mathfrak{a})| \leq |\mathfrak{a}|$ as $rad(\mathfrak{a}) \subseteq \mathfrak{a}$.

ABC Conjecture

Conjecture (David Masser, 1985; Joseph Oesterlé, 1985)

For each $\epsilon > 0$ there exists a uniform $\mathcal{C}_\epsilon > 0$ such that the following holds: For any relatively prime integers A, B, $C \in \mathbb{Z}$ with $A + B = C$,

$$\max\Big\{|A|,\ |B|,\ |C|\Big\} \leq \mathcal{C}_\epsilon\,\Big|\text{rad}(A\,B\,C)\Big|^{1+\epsilon}.$$

Lemma

The symmetric group on three letters acts on the set of *ABC* Triples:

$$\sigma : \begin{bmatrix} A \\ B \\ C \end{bmatrix} \mapsto \begin{bmatrix} B \\ -C \\ -A \end{bmatrix}, \quad \tau : \begin{bmatrix} A \\ B \\ C \end{bmatrix} \mapsto \begin{bmatrix} B \\ A \\ C \end{bmatrix} \qquad \text{where} \qquad \begin{aligned} \sigma^3 &= 1 \\ \tau^2 &= 1 \\ \tau \circ \sigma \circ \tau &= \sigma^2 \end{aligned}$$

In particular, we may assume $0 < A \leq B < C$.

Quality of *ABC* Triples

Corollary

If the *ABC* Conjecture holds, then $\limsup q(A,B,C) \leq 1$ for the quality

$$q(A,B,C) = \frac{\max\bigl\{\ln|A|,\ \ln|B|,\ \ln|C|\bigr\}}{\ln\bigl|\mathrm{rad}(A\,B\,C)\bigr|}.$$

Proof: Say $\epsilon = \bigl(\limsup q(P) - 1\bigr)/3$ is positive. Choose a sequence $P_k = (A_k, B_k, C_k)$ with $q(P_k) \geq 1 + 2\,\epsilon$. But this must be finite because

$$\max\bigl\{|A_k|, |B_k|, |C_k|\bigr\} \leq \mathcal{C}_\epsilon \bigl|\mathrm{rad}(A_k B_k C_k)\bigr|^{1+\epsilon} \leq \exp\left[\frac{q(P_k)}{q(P_k) - 1 - \epsilon}\ \ln \mathcal{C}_\epsilon\right].$$

Question

For each $\epsilon > 0$, there are only finitely many *ABC* Triples $P = (A,B,C)$ with $q(P) \geq 1 + \epsilon$. What is the largest $q(P)$ can be?

Exceptional Quality

Proposition (Bart de Smit, 2010)

There are only 233 known *ABC* Triples $P = (A, B, C)$ with $q(P) \geq 1.4$.

Rank	A	B	C	$q(A, B, C)$
1	2	$3^{10} \cdot 109$	23^5	1.6299
2	11^2	$3^2 \cdot 5^6 \cdot 7^3$	$2^{21} \cdot 23$	1.6260
3	$19 \cdot 1307$	$7 \cdot 29^2 \cdot 31^8$	$2^8 \cdot 3^{22} \cdot 5^4$	1.6235
4	283	$5^{11} \cdot 13^2$	$2^8 \cdot 3^8 \cdot 17^3$	1.5808
5	1	$2 \cdot 3^7$	$5^4 \cdot 7$	1.5679
6	7^3	3^{10}	$2^{11} \cdot 29$	1.5471
7	$7^2 \cdot 41^2 \cdot 311^3$	$11^{16} \cdot 13^2 \cdot 79$	$2 \cdot 3^3 \cdot 5^{23} \cdot 953$	1.5444
8	5^3	$2^9 \cdot 3^{17} \cdot 13^2$	$11^5 \cdot 17 \cdot 31^3 \cdot 137$	1.5367
9	$13 \cdot 19^6$	$2^{30} \cdot 5$	$3^{13} \cdot 11^2 \cdot 31$	1.5270
10	$3^{18} \cdot 23 \cdot 2269$	$17^3 \cdot 29 \cdot 31^8$	$2^{10} \cdot 5^2 \cdot 7^{15}$	1.5222

http://www.math.leidenuniv.nl/~desmit/abc/index.php?set=2

THE ABC CONJECTURE HOME PAGE

ABC

La conjecture abc est aussi difficile que la conjecture ... xyz. (P. Ribenboim) (read the story)

The abc conjecture is the most important unsolved problem in diophantine analysis. (D. Goldfeld)

Created and maintained by Abderrahmane Nitaj

Last updated May 27, 2010

Index

- **The *abc* conjecture**
- **Generalizations**
- **Consequences**
- **Tables**
  - The top ten good *abc* examples
  - The top ten good *abc*-Szpiro examples
  - The top ten good algebraic *abc* examples
  - New good *abc* examples new
  - New hunters of *abc* examples **rekenmeemetabc, abc@home** new
  - Largest good *abc* examples new
  - The list of good triples up to 20 digits is now complete new
- **Bibliography**
- **Download abc papers**
- **abc Theses**
- **abc links**
- **Contact**

ABC **Conjecture Home Page**

`http://www.math.unicaen.fr/~nitaj/abc.html`

ABC @home

What is ABC@home?
ABC@home is an educational and non-profit distributed computing project finding abc-triples related to the **ABC conjecture**.

JOIN ABC@HOME

1. Read our rules and policies
2. Download BOINC
3. When prompted, enter **http://abcathome.com/**

PROJECT
Collected data
Forums
Server status
Applications
Project personnel

PARTICIPANTS
Participant profiles
Your account
Teams
Certificate

BOINC STATISTICS
Top participants
Top computers
Top teams
Other statistics

ABC INFO
ABC conjecture
Top ABC triples
Reken mee met ABC

BOINC INFO
Main
Wiki

WHAT IS THE ABC CONJECTURE?

The ABC conjecture involves abc-triples: positive integers a,b,c such that a+b=c, a < b < c, a,b,c have no common divisors and c > rad(abc), the so-called radical of abc. The ABC conjecture says that there are only finitely many a,b,c such that log(c)/log(rad(abc)) > h for any real h > 1. The ABC conjecture is currently one of the greatest open problems in mathematics. If it is proven to be true, a lot of other open problems can be answered directly from it.

WHY SHOULD I JOIN?

The ABC conjecture is one of the greatest open mathematical questions, one of the holy grails of mathematics. It will teach us something about our very own numbers. Furthermore, the application of ABC@home is tiny, secure and stable, we like to keep things simple.

WHO IS INVOLVED?

The project is run by the Mathematical Institute of Leiden University as part of Reken mee met ABC

MINIMUM SYSTEM REQUIREMENTS

- min. 256MB ram free
- 2 MB of free disk space
- windows, linux, mac (recommended with a 64bit cpu)

USER OF THE DAY

Kajunfisher

NEWS

25 March 2012
We've encountered a problem with our feed of new work units, so there's no new work available right now. Sorry! We're working on fixing it.

10 September 2011
Due to a flood of spam, we've temporarily restricted who can post to the project forums.

9 April 2011
A quick update: A lot of spam profiles were removed in the last few days, do complain if we removed any legitimate ones by mistake! Also, preliminary data for all triples with c no more than 10^18 has been available from our data page for a while now, although it is (of course) still preliminary at this point. Many thanks to our dedicated users, and we've now moved onward to further reaches of the search space!

...more

News is available as an RSS feed XML.

ABC at Home

`http://abcathome.com/`

Frey's Observation

Theorem (Gerhard Frey, 1989)

Let $P = (A, B, C)$ be an ABC Triple, that is, a triple of relatively prime integers such that $A + B = C$. Then the corresponding curve

$$E_{A,B,C} : \qquad y^2 = x\,(x - A)\,(x + B)$$

has "remarkable properties."

Question

How do you explain this to undergraduates?

Answer: You don't!

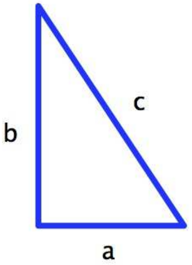
Can you find a right triangle

with rational sides

having area $A = 6$?

Consider positive rational numbers a, b, and c satisfying

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}\, a\, b = 6.$$



Recall the $(a, b, c) = (3, 4, 5)$ triangle.

Cubic Equations

Are there more rational solutions (a, b, c) to

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}\, a\, b = 6?$$

Proposition

Let x and y be rational numbers, and denote the rational numbers

$$a = \frac{x^2 - 36}{y}, \qquad b = \frac{12\, x}{y}, \qquad \text{and} \qquad c = \frac{x^2 + 36}{y}.$$

Then

$$\left. \begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}\, a\, b &= 6 \end{aligned} \right\} \qquad \text{if and only if} \qquad \left\{ y^2 = x^3 - 36\, x. \right.$$

Example: $(x, y) = (12, 36)$ corresponds to $(a, b, c) = (3, 4, 5)$.

Can we find **infinitely many** rational solutions (a, b, c)?

What types of properties

does do these

cubic equations have?

Thank You!

Questions?

Modern Math Workshop

Break

2:30 PM – 2:40 PM

SACNAS National Convention

Room 212

Henry B. Gonzalez Convention Center

Modern Math Workshop

Undergraduate Mini-Course #2: Part II

2:45 PM – 3:40 PM

SACNAS National Convention

Room 210B

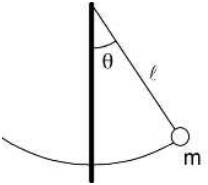
Henry B. Gonzalez Convention Center

Elliptic Curves

Simple Pendulum

Question

Say we have a mass m attached to a rigid rod of length ℓ that is allowed to swing back and forth at one end. What is the period of the oscillation given an initial angle θ_0?



In 1602, the Italian physicist **Galileo Galilei** believed that its period was independent of of the initial angle θ_0 and began a series of experiments to determine whether this observation was correct.

Period: Approximate Value

Theorem (Galileo Galilei, 1602)

$$\text{Period} = 2\,\pi\,\sqrt{\frac{\ell}{g}}$$

where $g = 9.81 \text{ m/sec}^2 = 32.17 \text{ ft/sec}^2$ is gravitational acceleration.

For example, the pendulum in a Grandfather clock is around $\ell = 1 \text{ m} = 3.28 \text{ ft}$ in length because the pendulum has period

$$\text{Period} = 2\,\pi\,\sqrt{\frac{\ell}{g}} = 2 \cdot 3.14 \cdot \sqrt{\frac{3.28}{32.17}} \text{ sec} = 2 \text{ sec.}$$

Question

Unfortunately this formula is only an approximation assuming the initial angle θ_0 is small. What happens as $\theta_0 \to \pi$?

Period: True Value

Theorem

The period of a pendulum with mass m, length ℓ, and initial angle θ_0 is

$$\text{Period} = 4\sqrt{\frac{\ell}{g}} \int_0^{\pi/2} \frac{d\phi}{\sqrt{1 - k^2 \sin^2 \phi}} \qquad \text{where} \qquad k = \sin \frac{\theta_0}{2}.$$

If $\theta_0 \approx 0$ then $k \approx 0$ as well, so that the integral has the value $\pi/2$. We recover Galileo's original formula in this limiting approximation.

$$\text{Period} \approx 4\sqrt{\frac{\ell}{g}} \cdot \frac{\pi}{2} = 2\pi\sqrt{\frac{\ell}{g}}.$$

The formula above works for all angles θ_0. **Why?**

Proof of Period Formula

The energy of an oscillating system such as a pendulum must be conserved, so the kinetic plus potential energy must be a constant.

$$\text{Kinetic} + \text{Potential} = \frac{1}{2}\, m \left(\ell\, \frac{d\theta}{dt} \right)^2 + m\, g\, \ell \,(1 - \cos\theta)$$

In particular, the energy is all kinetic when $\theta = 0$ and it is all potential when $\theta = \pm\theta_0$ (i.e., $\frac{d\theta}{dt} = 0$).

Lemma

$$\text{Energy} = \frac{1}{2}\, m \left(\ell\, \frac{d\theta}{dt} \right)^2 + m\, g\, \ell \,(1 - \cos\theta) = m\, g\, \ell \,(1 - \cos\theta_0)\,.$$

To compute the period of this pendulum, we integrate the differential dt with respect to time over one complete oscillation.

$$\frac{d\theta}{dt} = \sqrt{2\, \frac{g}{\ell}\, (\cos\theta - \cos\theta_0)} \qquad \Longrightarrow \qquad dt = \sqrt{\frac{\ell}{g}}\, \frac{d\theta}{\sqrt{2\,(\cos\theta - \cos\theta_0)}}.$$

Proof of Period Formula

We'll simplify this expression a bit.

$$\phi = \arcsin \frac{\sin \frac{\theta}{2}}{\sin \frac{\theta_0}{2}} \quad \Longrightarrow \quad \frac{d\theta}{\sqrt{2\left(\cos\theta - \cos\theta_0\right)}} = \frac{d\phi}{\sqrt{1 - \sin^2 \frac{\theta_0}{2} \, \sin^2 \phi}}$$

The period of the simple pendulum is

$$\begin{aligned} \text{Period} &= \int_{\text{One Oscillation}} dt = 2\sqrt{\frac{\ell}{g}} \int_{-\theta_0}^{\theta_0} \frac{d\theta}{\sqrt{2\left(\cos\theta - \cos\theta_0\right)}} \\ &= 4\sqrt{\frac{\ell}{g}} \cdot K\left(\sin\frac{\theta_0}{2}\right) \end{aligned}$$

in terms of the **elliptic integral**:

$$K(k) = \int_0^{\pi/2} \frac{d\phi}{\sqrt{1 - k^2 \, \sin^2\phi}} = \int_0^1 \frac{dt}{\sqrt{\left(1 - t^2\right)\left(1 - k^2\, t^2\right)}}, \qquad |k| < 1.$$

Limiting Values

- As $\theta_0 \to \pi$, the value $k = \sin \frac{\theta_0}{2} \to 1$. Then $K(k) \to \infty$. Hence the becomes infinitely long because the pendulum hangs at the top.

- As $\theta_0 \to 0$, the value $k = \sin \frac{\theta_0}{2} \to 0$. Expand $K(k)$ in a Taylor series around $k = 0$:

$$K(k) = \frac{\pi}{2} + \frac{\pi}{8}\, k^2 + \frac{9\pi}{128}\, k^4 + \cdots \qquad \text{for } k \text{ small.}$$

Hence the period of a pendulum has the approximate value

$$\text{Period} = 2\pi \sqrt{\frac{\ell}{g}} \left(1 + \frac{1}{4} \sin^2 \frac{\theta_0}{2} + \cdots \right) \qquad \text{for } \theta_0 \text{ small.}$$

Where else do we see

Elliptic Integrals?

Arc Length of Circle

Theorem

Consider the circle $x^2 + y^2 = r^2$. The arc length is given by the integral

$$z = \int_0^{2\pi} r \, d\theta = 2\pi \, r.$$

In general, the arc length from P to Q on a curve $f(x,y) = 0$ is given by the integral

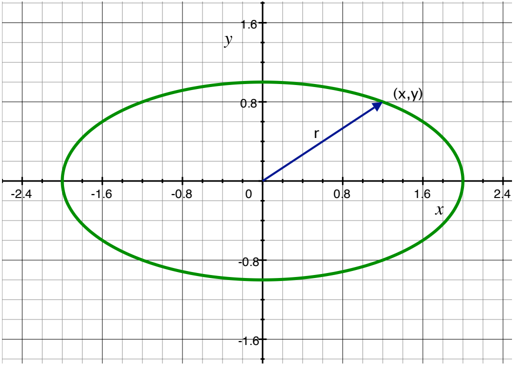
$$z = \int_P^Q \sqrt{1 + \left(\frac{dy}{dx}\right)^2} \, dx \qquad \text{where} \qquad \frac{dy}{dx} = -\frac{\dfrac{\partial f}{\partial x}}{\dfrac{\partial f}{\partial y}}.$$

We will use polar coordinates by setting $x = r \cos\theta$ and $y = r \sin\theta$:

$$dz = \sqrt{1 + \left(\frac{dy}{dx}\right)^2} \, dx = \sqrt{(dx)^2 + (dy)^2} = \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2} \, d\theta.$$

Arc Length of an Ellipse

Consider the ellipse $x^2/a^2 + y^2/b^2 = 1$ with $0 < a \leq b$. We set $x = r\,\cos\theta$ and $y = r\,\sin\theta$ so that $r = \dfrac{a\,b}{\sqrt{b^2\,\cos^2\theta + a^2\,\sin^2\theta}}$:



Arc Length of an Ellipse

We have the differential

$$dz = \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2}\, d\theta = a \sqrt{\frac{1-k^2\,t^2}{1-t^2}}\, dt, \qquad t = \sin\theta.$$

Theorem

The arc length of the ellipse is

$$z = 4 \int_0^{\pi/2} \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2}\, d\theta = 4\,a\,E(k), \qquad k = \frac{\sqrt{b^2-a^2}}{b};$$

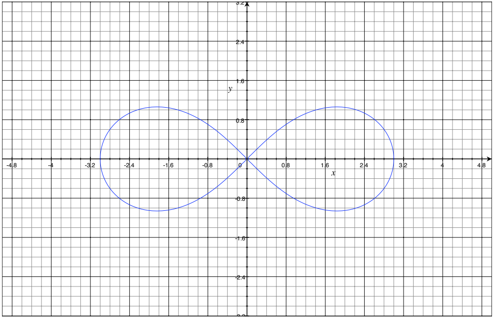
in terms of the **elliptic integral**

$$E(k) = \int_0^1 \sqrt{\frac{1-k^2\,t^2}{1-t^2}}\, dt, \qquad k \neq \pm 1.$$

Here k is the **eccentricity** of the ellipse. For a circle, $k=0$.

Lemniscate

Now consider the curve $\left(x^2+y^2\right)^2 = a^2\left(x^2-y^2\right)$.



In 1694, Swiss mathematician **Jakob Bernoulli** called this curve **Lemniscus** or "Pendant Ribbon."

Question

What is the arc length of this curve?

Arc Length of Lemniscate

We set $x = r\cos\theta$ and $y = r\sin\theta$:

$$\left(x^2 + y^2\right)^2 = a^2\left(x^2 - y^2\right) \qquad \Longrightarrow \qquad r^2 = a^2\cos 2\theta.$$

We also evaluate

$$dz = \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2}\,d\theta = a\,\frac{dt}{\sqrt{1-t^4}}, \qquad t = \frac{r}{a} = \sqrt{\cos 2\theta}.$$

Theorem

The complete arc length of the lemniscate is

$$z = 4\int_0^{\pi/4}\sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2}\,d\theta = 4\,a\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 4\,a\,K(\sqrt{-1}).$$

This integral cannot be evaluated in terms of elementary functions.

Are there

any other applications of

Elliptic Integrals?

Fagnano's Duplication Formula

In 1750, Italian mathematician **Giulio Fagnano** considered the **incomplete elliptic integral**

$$z(w) = \int_0^w \frac{dt}{\sqrt{1-t^4}}.$$

Theorem

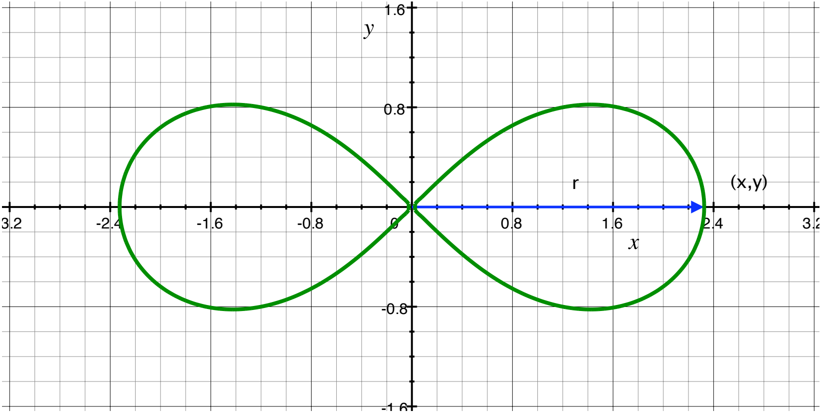
$$z(W) = 2 \cdot z(w) \qquad \text{when} \qquad W = \frac{2\,w\sqrt{1-w^4}}{1+w^4}.$$

Equivalently, if $w = w(z)$ is the inverse of $z = z(w)$, then

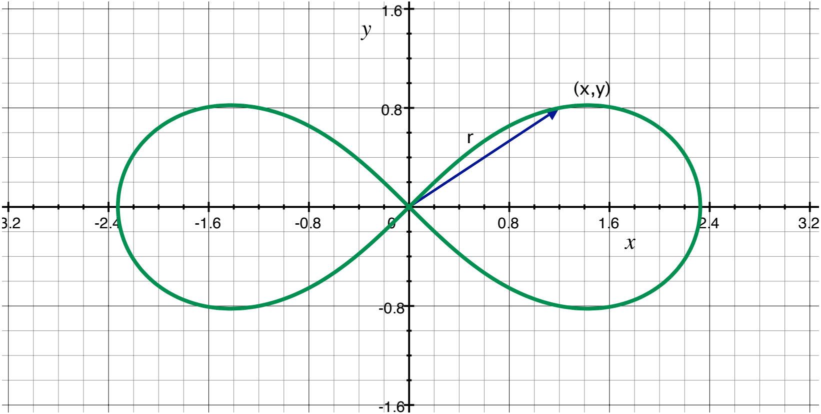
$$w(2\,z) = \frac{2\,w(z)\,w'(z)}{1+w(z)^4} \qquad \text{where} \qquad (w')^2 = 1 - w^4.$$

Question

Are there more formulas like this one?



$$\left(x^2+y^2\right)^2 = a^2\left(x^2-y^2\right)$$



$$\left(x^2+y^2\right)^2 = a^2\left(x^2-y^2\right)$$

Euler's Addition Formula

In 1751, Swiss mathematician **Leonhard Euler**, while reading through Fagnano's work, considered the integral for a fixed modulus k

$$z(w) = \int_0^w \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}}.$$

Theorem

$z(W) = z(w_1) \pm z(w_2)$ where

$$W = \frac{w_1\sqrt{(1-w_2^2)\,(1-k^2\,w_2^2)} \pm w_2\sqrt{(1-w_1^2)\,(1-k^2\,w_1^2)}}{1-k^2\,w_1^2\,w_2^2}.$$

Equivalently, if $w = w(z)$ is the inverse of $z = z(w)$ then

$$w(z_1 \pm z_2) = \frac{w(z_1)\,w'(z_2) \pm w'(z_1)\,w(z_2)}{1-k^2\,w(z_1)^2\,w(z_2)^2}.$$

where $(w')^2 = \left(1-w^2\right)\left(1-k^2\,w^2\right)$.

Corollaries

As $k \to \sqrt{-1}$ we find the integral studied by Fagnano:

$$z(w) = \int_0^w \frac{dt}{\sqrt{(1-t^2)\,(1+t^2)}} = \int_0^w \frac{dt}{\sqrt{1-t^4}}.$$

Corollary

$$z(W) = z(w_1) \pm z(w_2) \quad \text{where} \quad W = \frac{w_1\sqrt{1-w_2^4} \pm w_2\sqrt{1-w_1^4}}{1+w_1^2\,w_2^2}.$$

As $k \to 0$ we find the trigonometric functions:

$$z(w) = \int_0^w \frac{dt}{\sqrt{1-t^2}} = \arcsin w \qquad \Longrightarrow \qquad \begin{cases} w(z) = \sin z \\ w'(z) = \cos z \end{cases}$$

Corollary

$$\sin(z_1 \pm z_2) = \sin(z_1)\,\cos(z_2) \pm \cos(z_1)\,\sin(z_2).$$

For arbitrary k, the function $w(z) = \mathrm{sn}(z)$ is a **Jacobi elliptic function**.

Proof of Addition Formula

$$z(w) = \int_0^w \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}}$$

$$\iff \qquad dz(w) = \frac{dw}{\sqrt{(1-w^2)\,(1-k^2\,w^2)}} \qquad \text{and} \qquad z(0)=0.$$

Hence $(w')^2 = \left(1-w^2\right)\left(1-k^2\,w^2\right)$. Using the Chain Rule,

$$dz(W) = \underbrace{\frac{\frac{\partial W}{\partial w_1}}{\sqrt{\frac{(1-W^2)\,(1-k^2\,W^2)}{(1-w_1^2)\,(1-k^2\,w_1^2)}}}}_{c_1}\,dz(w_1) + \underbrace{\frac{\frac{\partial W}{\partial w_2}}{\sqrt{\frac{(1-W^2)\,(1-k^2\,W^2)}{(1-w_2^2)\,(1-k^2\,w_2^2)}}}}_{c_2}\,dz(w_2)$$

To conclude $z(W) = z(w_1) + z(w_2)$ it suffices to show $c_1 = c_2 = 1$. We use this to define $W = W(w_1,\,w_2)$.

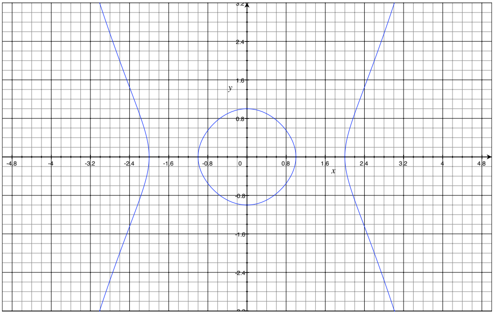
Parametrization of Quartic Curves

Fix a complex number k, and define a function $w = w(z)$ implicitly by

$$z = \int_0^{w(z)} \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}} \qquad \Longleftrightarrow \qquad w(z) = \mathrm{sn}(z).$$

Theorem

The point $(x, y) = \left(\mathrm{sn}(z),\, \mathrm{sn}'(z)\right)$ satisfies $y^2 = \left(1 - x^2\right)\left(1 - k^2\,x^2\right)$.



Elliptic Functions and Elliptic Integrals

Unfortunately, the map $w = \mathrm{sn}(z)$ is not well-defined because the integrand has poles at $t = \pm 1, \pm 1/k$. We make branch cuts then integrate in closed loops around them:

$$\omega_1 = 2 \int_{-1/k}^{1/k} \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}} = \frac{4}{k}\,K\left(\frac{1}{k}\right),$$

$$\omega_2 = 2 \int_{-1}^{1} \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}} = 4\,K(k)$$

in terms of the **complete elliptic integral** of the first kind

$$K(k) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}}, \qquad k \neq -1, 0, 1.$$

Theorem

The Jacobi elliptic function $\mathrm{sn} : \mathbb{C}/\Lambda \to \mathbb{C}$ is well-defined for the lattice $\Lambda = \{m\,\omega_1 + n\,\omega_2 \mid m,\, n \in \mathbb{Z}\}$.

Parametrization of Cubic Curves

Fix a complex number $k \neq -1, 0, 1$.

- We will consider the **torus** $\mathbb{C}/\Lambda$ as defined in terms of the lattice

$$\Lambda = \left\{ m \cdot \frac{1}{k} K\left(\frac{1}{k}\right) + n \cdot K(k) \;\middle|\; m, n \in \mathbb{Z} \right\}.$$

- The map $z \mapsto (x, y) = \big(\mathrm{sn}(z), \mathrm{sn}'(z)\big)$ gives a correspondence with

$$y^2 = \left(1 - x^2\right)\left(1 - k^2 x^2\right).$$

- The map

$$(x, y) \mapsto (X, Y) = \left(\frac{3\,(5\,k^2 - 1)\,x + 3\,(k^2 - 5)}{x - 1}, \; \frac{54\,(1 - k^2)\,y}{(x-1)^2} \right)$$

gives a one-to-one correspondence with the cubic curve

$$Y^2 = X^3 + A\,X + B \quad \text{where} \quad \begin{cases} A = -27\left(k^4 + 14\,k^2 + 1\right) \\ B = -54\left(k^6 - 33\,k^4 - 33\,k^2 + 1\right) \end{cases}$$

Example

When $k = \sqrt{-1}$:

- The complete elliptic integrals have the values

$$\left.\begin{aligned} \omega_1 &= -4\,\sqrt{-1}\,K(\sqrt{-1}) \\ \omega_2 &= +4\,K(\sqrt{-1}) \end{aligned}\right\} \quad \text{where} \quad K(\sqrt{-1}) = \int_0^1 \frac{dt}{\sqrt{1-t^4}};$$

  so that $\Lambda \simeq \mathbb{Z}[\sqrt{-1}]$ is just the Gaussian integers.

- The quotient $\mathbb{C}/\mathbb{Z}[\sqrt{-1}]$ is equivalent to the quartic curve

$$y^2 = 1 - x^4.$$

- The quartic curve is equivalent to the cubic curve

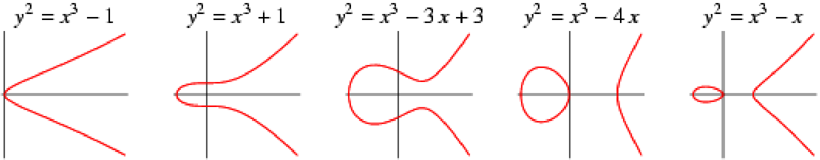
$$Y^2 = X^3 + 4\,X.$$

Elliptic Curves

More generally, we consider cubic curves

$$E : \quad Y^2 = X^3 + A\,X + B$$

where the rational numbers A and B satisfy $4\,A^3 + 27\,B^2 \neq 0$.



Given a field K such as either $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, denote

$$E(K) = \left\{ (X, Y) \in K \times K \,\middle|\, Y^2 = X^3 + A\,X + B \right\} \cup \{\mathcal{O}\}.$$

Here $\mathcal{O}$ is the "point at infinity" coming from $(x, y) = (1, 0)$.

Why do people care about

Elliptic Curves?

Can you find a right triangle

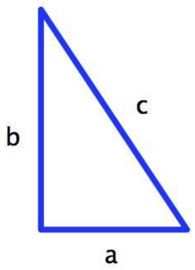
with rational sides

having area $A = 6$?

Motivating Question

Consider positive rational numbers a, b, and c satisfying

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}\, a\, b = 6.$$



Recall the $(a, b, c) = (3, 4, 5)$ triangle.

Cubic Equations

Are there **more** rational solutions (a, b, c) to

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}\, a\, b = 6?$$

Proposition

Let x and y be rational numbers, and denote the rational numbers

$$a = \frac{x^2 - 36}{y}, \qquad b = \frac{12\,x}{y}, \qquad \text{and} \qquad c = \frac{x^2 + 36}{y}.$$

Then

$$\left. \begin{array}{c} a^2 + b^2 = c^2 \\ \frac{1}{2}\, a\, b = 6 \end{array} \right\} \quad \text{if and only if} \quad \left\{ y^2 = x^3 - 36\,x. \right.$$

Example: $(x, y) = (12, 36)$ corresponds to $(a, b, c) = (3, 4, 5)$.

Can we find **infinitely many** rational solutions (a, b, c)?

What types of properties

does this

cubic equation have?

What is an Elliptic Curve?

Definition

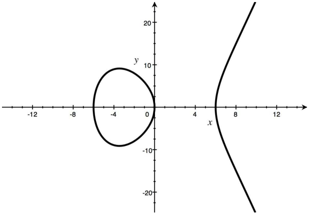
Let A and B be rational numbers such that $4\,A^3 + 27\,B^2 \neq 0$. An **elliptic curve** E is the set of all (x, y) satisfying the equation

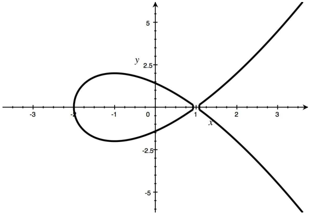
$$y^2 = x^3 + A\,x + B.$$

We will also include the "point at infinity" $\mathcal{O}$.

Example: $y^2 = x^3 - 36\,x$ is an elliptic curve.

Non-Example: $y^2 = x^3 - 3\,x + 2$ is **not** an elliptic curve.





What is an Elliptic Curve?

Formally, an **elliptic curve** E over $\mathbb{Q}$ is a nonsingular projective curve of genus 1 possessing a $\mathbb{Q}$-rational point $\mathcal{O}$.

Such a curve is birationally equivalent over $\mathbb{Q}$ to a cubic equation in Weierstrass form:

$$E: \qquad y^2 = x^3 + A\,x + B;$$

with rational coefficients A and B, and nonzero discriminant $\Delta(E) = -16\left(4\,A^3 + 27\,B^2\right)$.

For any field K, define

$$E(K) = \left\{ (x_1 : x_2 : x_0) \in \mathbb{P}^2(K) \;\middle|\; x_2^2\,x_0 = x_1^3 + A\,x_1\,x_0^2 + B\,x_0^3 \right\};$$

where $\mathcal{O} = (0:1:0)$ is on the projective line at infinity $x_0 = 0$.

Remark: In practice we choose either $K = \mathbb{Q}$ or $\mathbb{F}_p$.

Chord-Tangent Method

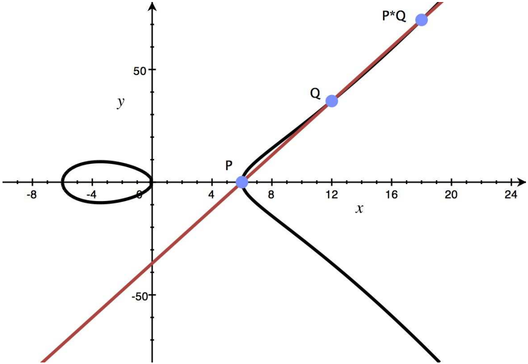
Given two rational points on an elliptic curve E, we explain how to construct more.

1. Start with two rational points P and Q.
2. Draw a line through P and Q.
3. The intersection, denoted by $P * Q$, is another rational point on E.

Example: $y^2 = x^3 - 36\,x$

Consider the two rational points

$$P = (6, 0) \qquad \text{and} \qquad Q = (12, 36).$$

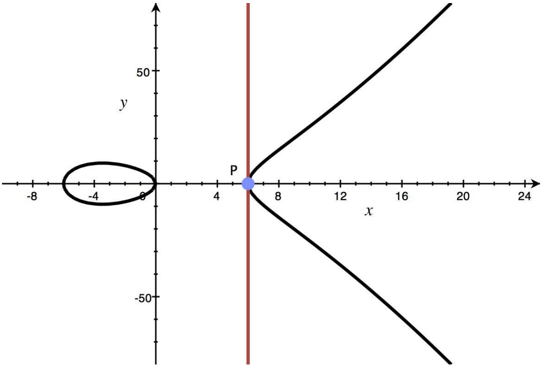


$$P * Q = (18, 72)$$

Example: $y^2 = x^3 - 36\,x$

Consider the two rational points

$$P = (6, 0) \qquad \text{and} \qquad Q = (12, 36).$$

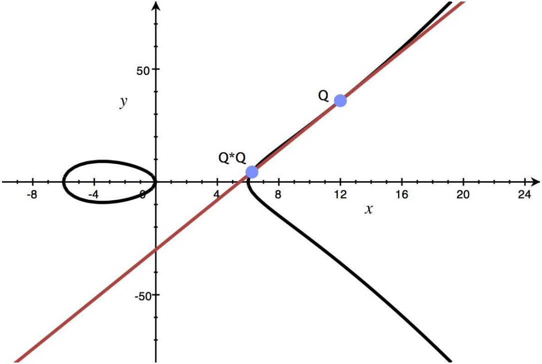


$$P * P = \mathcal{O}$$

Example: $y^2 = x^3 - 36\,x$

Consider the two rational points

$$P = (6, 0) \qquad \text{and} \qquad Q = (12, 36).$$



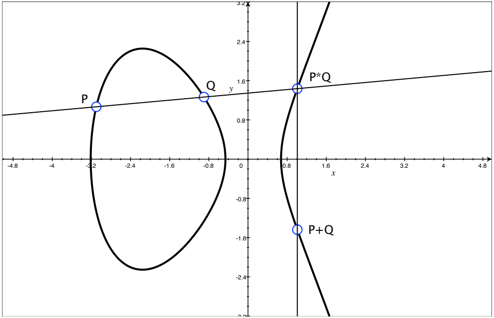
$$Q * Q = (25/4, 35/8)$$

Group Law

Definition

Let E be an elliptic curve defined over a field K, and denote $E(K)$ as the set of K-rational points on E. Define the operation $\oplus$ as

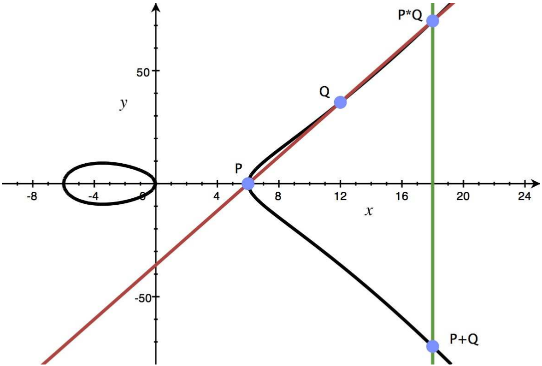
$$P \oplus Q = (P * Q) * \mathcal{O}.$$



Example: $y^2 = x^3 - 36\,x$

Consider the two rational points

$$P = (6, 0) \qquad \text{and} \qquad Q = (12, 36).$$

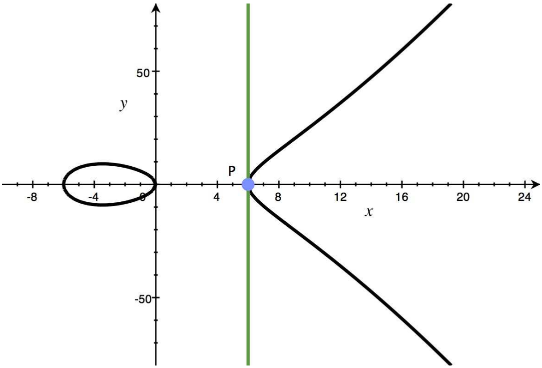


$$P \oplus Q = (18, -72)$$

Example: $y^2 = x^3 - 36\,x$

Consider the two rational points

$$P = (6, 0) \qquad \text{and} \qquad Q = (12, 36).$$

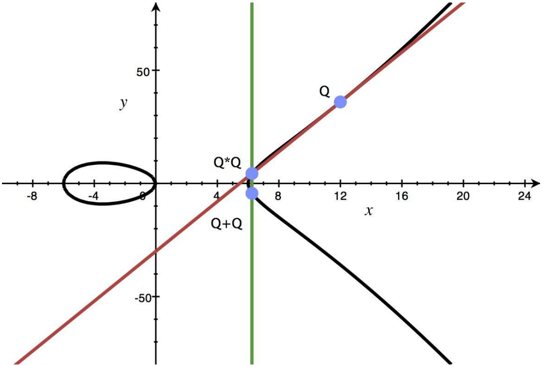


$$P \oplus P = \mathcal{O}$$

Example: $y^2 = x^3 - 36\,x$

Consider the two rational points

$$P = (6, 0) \qquad \text{and} \qquad Q = (12, 36).$$



$$Q \oplus Q = (25/4, -35/8)$$

Poincaré's Theorem

Theorem (Henri Poincaré, 1901)

Let E be an elliptic curve defined over a field K. Then $E(K)$ is an abelian group under $\oplus$.

Recall that to be an **abelian group**, the following five axioms must be satisfied:

- **Closure:** If P, $Q \in E(K)$ then $P \oplus Q \in E(K)$.
- **Associativity:** $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.
- **Commutativity:** $P \oplus Q = Q \oplus P$.
- **Identity:** $P \oplus \mathcal{O} = P$ for all P.
- **Inverses:** $[-1]P = P * \mathcal{O}$ satisfies $P \oplus [-1]P = \mathcal{O}$.

What types of properties

does this

abelian group have?

Poincaré's Conjecture

Conjecture (Henri Poincaré, 1901)

Let E be an elliptic curve. Then $E(\mathbb{Q})$ is finitely generated.

Recall that an abelian group G is said to be **finitely generated** if there exists a **finite** generating set $\{a_1, a_2, \ldots, a_n\}$ such that, for each given $g \in G$, there are integers $m_1, m_2, \ldots, m_n$ such that

$$g = [m_1]a_1 \circ [m_2]a_2 \circ \cdots \circ [m_n]a_n.$$

Example: $G = \mathbb{Z}$ is a finitely generated abelian group because all integers are generated by $a_1 = 1$.

Example: For a positive integer d which is not a square, the set

$$G = \left\{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \,\middle|\, x^2 - d\, y^2 = 1 \right\} \simeq Z_2 \times \mathbb{Z}$$

is a finitely generated abelian group because all integral solutions $g = (x, y)$ are generated by $a_1 = -1$ and the fundamental solution $a_2 = (x_1, y_1)$.

Mordell's Theorem

Theorem (Louis Mordell, 1922)

Let E be an elliptic curve. Then $E(\mathbb{Q})$ is finitely generated.

That is, there exists a finite group $E(\mathbb{Q})_{tors}$ and a nonnegative integer r such that

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

- The set $E(\mathbb{Q})$ is called the **Mordell-Weil group** of E.
- The finite set $E(\mathbb{Q})_{\text{tors}}$ is called the **torsion subgroup** of E. It contains all of the points of finite order, i.e., those $P \in E(\mathbb{Q})$ such that

$$[m]P = \mathcal{O} \qquad \text{for some positive integer } m.$$

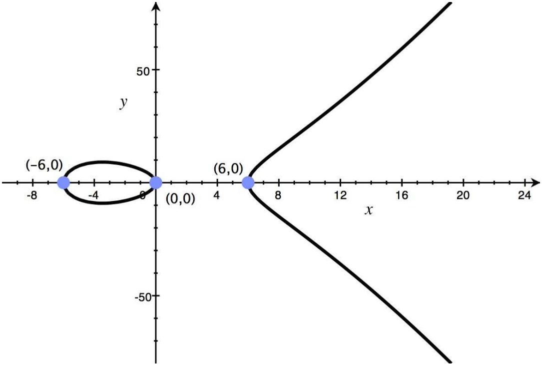
- The nonnegative integer r is called the **Mordell-Weil rank** of E.

Example: $y^2 = x^3 - 36\,x$

Consider the three rational points

$$P_1 = (0,0), \qquad P_2 = (6,0), \qquad \text{and} \qquad P_3 = (12,36).$$

$[2]P_1 = [2]P_2 = \mathcal{O}$, i.e., both P_1 and P_2 have order 2. They are torsion.



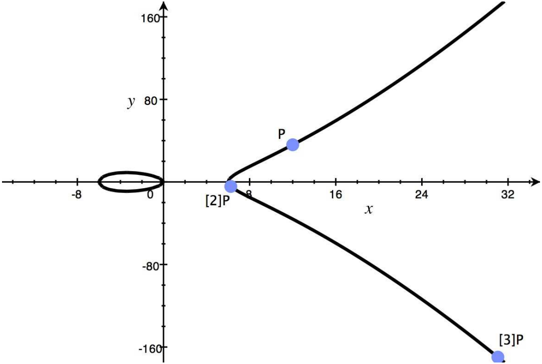
$$E(\mathbb{Q})_{\text{tors}} = \langle P_1,\ P_2 \rangle \simeq Z_2 \times Z_2$$

Example: $y^2 = x^3 - 36\,x$

Consider the three rational points

$$P_1 = (0,0), \qquad P_2 = (6,0), \qquad \text{and} \qquad P_3 = (12,36).$$

$[2]P_3 = (25/4, -35/8)$ and $[3]P_3 = (16428/529, -2065932/12167)$.



$$E(\mathbb{Q}) = \langle P_1,\ P_2,\ P_3 \rangle \simeq Z_2 \times Z_2 \times \mathbb{Z}$$

Classification of Torsion Subgroups

Theorem (Barry Mazur, 1977)

Let E is an elliptic curve, then

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} Z_n & \text{where } 1 \leq n \leq 10 \text{ or } n = 12; \\ Z_2 \times Z_{2m} & \text{where } 1 \leq m \leq 4. \end{cases}$$

Remark: Z_n denotes the cyclic group of order n.

Example: The elliptic curve $y^2 = x^3 - 36\,x$ has torsion subgroup $E(\mathbb{Q})_{tors} \simeq Z_2 \times Z_2$ generated by $P_1 = (0,0)$ and $P_2 = (6,0)$.

Mordell's Theorem states that

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$

What can we say about the Mordell-Weil rank r?

Records for Prescribed Torsion and Rank

$E(\mathbb{Q})_{\text{tors}}$	Highest Known Rank r	Found By	year Discovered
Trivial	28	Elkies	2006
Z_2	19	Elkies	2009
Z_3	13	Eroshkin	2007, 2008, 2009
Z_4	12	Elkies	2006
Z_5	8	Dujella, Lecacheux Eroshkin	2009 2009
Z_6	8	Eroshkin Dujella, Eroshkin Elkies Dujella	2008 2008 2008 2008
Z_7	5	Dujella, Kulesz Elkies Eroshkin Dujella, Lecacheux Dujella, Eroshkin	2001 2006 2009 2009 2009
Z_8	6	Elkies	2006
Z_9	4	Fisher	2009
Z_{10}	4	Dujella Elkies	2005, 2008 2006
Z_{12}	4	Fisher	2008
$Z_2 \times Z_2$	15	Elkies	2009
$Z_2 \times Z_4$	8	Elkies Eroshkin Dujella, Eroshkin	2005 2008 2008
$Z_2 \times Z_6$	6	Elkies	2006
$Z_2 \times Z_8$	3	Connell Dujella **Campbell, Goins** Rathbun **Flores, Jones, Rollick, Weigandt, Rathbun** Fisher	2000 2000, 2001, 2006, 2008 **2003** 2003, 2006 **2007** 2009

http://web.math.hr/~duje/tors/tors.html

How does this

help answer

the motivating questions?

Rational Triangles Revisited

Can we find **infinitely many** right triangles (a, b, c) having rational sides and area $A = 6$?

Proposition

Let x and y be rational numbers, and denote the rational numbers

$$a = \frac{x^2 - 36}{y}, \qquad b = \frac{12\,x}{y}, \qquad \text{and} \qquad c = \frac{x^2 + 36}{y}.$$

Then

$$\left.\begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}\,a\,b &= 6 \end{aligned}\right\} \quad \text{if and only if} \quad \left\{ y^2 = x^3 - 36\,x. \right.$$

Example: $(x, y) = (12, 36)$ corresponds to $(a, b, c) = (3, 4, 5)$.

Rational Triangles Revisited

The elliptic curve $E: \ y^2 = x^3 - 36\,x$ has Mordell-Weil group

$$E(\mathbb{Q}) = \langle P_1,\ P_2,\ P_3 \rangle \simeq Z_2 \times Z_2 \times \mathbb{Z}$$

as generated by the rational points

$$P_1 = (0,0), \qquad P_2 = (6,0), \qquad \text{and} \qquad P_3 = (12,36).$$

P_3 is not a torsion element, so we find triangles for each $[m]P_3$:

$$[1]P_3 = (12,\ 36) \qquad \Longrightarrow \qquad (a,b,c) = (3,\ 4,\ 5)$$

$$[-2]P_3 = \left(\frac{25}{4},\ \frac{35}{8}\right) \qquad \Longrightarrow \qquad (a,b,c) = \left(\frac{49}{70},\ \frac{1200}{70},\ \frac{1201}{70}\right)$$

$$[-3]P_3 = \left(\frac{16428}{529},\ \frac{2065932}{12167}\right) \qquad \Longrightarrow \qquad (a,b,c) = \left(\frac{7216803}{1319901},\ \frac{2896804}{1319901},\ \frac{7776485}{1319901}\right)$$

There are **infinitely many** rational right triangles with area $A = 6$!

Are the torsion subgroups

useful for anything?

ABC Conjecture

Conjecture (David Masser, 1985; Joseph Oesterlé, 1985)

For each $\epsilon > 0$ there exists a uniform $\mathcal{C}_\epsilon > 0$ such that the following holds: For any relatively prime integers A, B, $C \in \mathbb{Z}$ with $A + B = C$,

$$\max\{|A|, \; |B|, \; |C|\} \leq \mathcal{C}_\epsilon \, \Big|\text{rad}(A\,B\,C)\Big|^{1+\epsilon}.$$

Lemma

The symmetric group on three letters acts on the set of *ABC* Triples:

$$\sigma : \begin{bmatrix} A \\ B \\ C \end{bmatrix} \mapsto \begin{bmatrix} B \\ -C \\ -A \end{bmatrix}, \quad \tau : \begin{bmatrix} A \\ B \\ C \end{bmatrix} \mapsto \begin{bmatrix} B \\ A \\ C \end{bmatrix} \quad \text{where} \quad \begin{matrix} \sigma^3 = 1 \\ \tau^2 = 1 \\ \tau \circ \sigma \circ \tau = \sigma^2 \end{matrix}$$

In particular, we may assume $0 < A \leq B < C$.

Frey's Observation

Theorem (Gerhard Frey, 1989)

Let $P = (A, B, C)$ be an ABC Triple, that is, a triple of relatively prime integers such that $A + B = C$. Then the corresponding curve

$$E_{A,B,C}: \qquad y^2 = x\,(x - A)\,(x + B)$$

has "remarkable properties."

Question

How do you explain this to undergraduates?

Answer: You don't!

Classification of Torsion Subgroups

Theorem (Barry Mazur, 1977)

Let E is an elliptic curve over $\mathbb{Q}$. Then

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} Z_N & \text{where } 1 \leq N \leq 10 \text{ or } N = 12; \\ Z_2 \times Z_{2N} & \text{where } 1 \leq N \leq 4. \end{cases}$$

Corollary (Gerhard Frey, 1989)

For each *ABC* Triple, the elliptic curve

$$E_{A,B,C}: \qquad y^2 = x\,(x - A)\,(x + B)$$

has discriminant $\Delta(E_{A,B,C}) = 16\,A^2\,B^2\,C^2$ and $E_{A,B,C}(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2N}$.

Question

For each *ABC* Triple, which torsion subgroups **do** occur?

Proposition (EHG and Jamie Weigandt, 2009)

All possible subgroups do occur – and infinitely often.

Proof: Choose relatively prime integers m and n. We have the following N-isogeneous curves:

A	B	C	$E_{A,B,C}(\mathbb{Q})_{\text{tors}}$
$(2\,m\,n)^2$ $8\,m\,n\,(m^2+n^2)$	$(m^2-n^2)^2$ $(m-n)^4$	$(m^2+n^2)^2$ $(m+n)^4$	$Z_2 \times Z_4$ $Z_2 \times Z_2$
$16\,m\,n^3$ $16\,m^3\,n$	$(m+n)^3\,(m-3\,n)$ $(m+n)\,(m-3\,n)^3$	$(m+3\,n)\,(m-n)^3$ $(m+3\,n)^3\,(m-n)$	$Z_2 \times Z_6$ $Z_2 \times Z_2$
$(2\,m\,n)^4$ $16\,m\,n\,(m^2-n^2)\cdot(m^2+n^2)^2$	$(m^4-6\,m^2\,n^2+n^4)\cdot(m^2+n^2)^2$ $(m^2-2\,m\,n-n^2)^4$	$(m^2-n^2)^4$ $(m^2+2\,m\,m-n^2)^4$	$Z_2 \times Z_8$ $Z_2 \times Z_2$

Examples

Rank of Quality	$E_{A,B,C}(\mathbb{Q})_{\text{tors}}$	m	n	Quality $q(A,B,C)$
– –	$Z_2 \times Z_4$ $Z_2 \times Z_2$	1029	1028	1.2863664657 1.3475851066
– 35	$Z_2 \times Z_4$ $Z_2 \times Z_2$	4	3	1.2039689894 1.4556731002
– 113	$Z_2 \times Z_6$ $Z_2 \times Z_2$	5	1	1.0189752355 1.4265653296
45 –	$Z_2 \times Z_6$ $Z_2 \times Z_2$	729	7	1.4508584088 1.3140518205
– 35	$Z_2 \times Z_8$ $Z_2 \times Z_2$	3	1	1.0370424407 1.4556731002
– –	$Z_2 \times Z_8$ $Z_2 \times Z_2$	577	239	1.2235280800 1.2951909301

Exceptional Quality Revisited

Proposition

There are infinitely many *ABC* Triples $P = (A, B, C)$ with $q(P) > 1$.

Proof: For each positive integer k, define the relatively prime integers

$$A_k = 1, \qquad B_k = 2^{k+2}\left(2^k - 1\right), \qquad \text{and} \qquad C_k = \left(2^{k+1} - 1\right)^2.$$

Then $P_k = (A_k, B_k, C_k)$ is an *ABC* Triple. Moreover,

$$\operatorname{rad}\left(A_k B_k C_k\right) = \operatorname{rad}\left((2^{k+1} - 2)\,(2^{k+1} - 1)\right) \leq (2^{k+1} - 2)\,(2^{k+1} - 1) < C_k.$$

Hence

$$q(P_k) = \frac{\max\left\{\ln|A_k|,\ \ln|B_k|,\ \ln|C_k|\right\}}{\ln\left|\operatorname{rad}(A_k\, B_k\, C_k)\right|} = \frac{\ln|C_k|}{\ln\left|\operatorname{rad}(A_k\, B_k\, C_k)\right|} > 1.$$

Corollary

If the *ABC* Conjecture holds, then $\limsup q(A, B, C) = 1$.

Quality by Torsion Subgroup

Question

Fix $N = 1, 2, 3, 4$. Let $\mathcal{F}(N)$ denote the those *ABC* Triples (A, B, C) such that $E_{A,B,C}(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2N}$. What can we say about

$$\limsup_{(A,B,C)\in\mathcal{F}(N)} q(A, B, C)?$$

Theorem (Alexander Barrios, Caleb Tillman and Charles Watts, 2010)

Fix $N = 1, 2, 4$. There are infinitely many ABC Triples with

$$E_{A,B,C}(\mathbb{Q})_{tors} \simeq Z_2 \times Z_{2N} \qquad \text{and} \qquad q(A, B, C) > 1.$$

In particular, if the ABC Conjecture holds, then $\limsup_{P\in\mathcal{F}(N)} q(P) = 1$.

Proof: Use the formulas above to create a dynamical system!

Can we use elliptic curves

to find *ABC* Triples

with exceptional quality $q(A, B, C)$?

In what follows, we will substitute $A_k = m$, $B_k = n$, and $C_k = m + n$.

A	B	C	$E_{A,B,C}(\mathbb{Q})_{\text{tors}}$
$(2\,m\,n)^2$ $8\,m\,n\,(m^2+n^2)$	$(m^2-n^2)^2$ $(m-n)^4$	$(m^2+n^2)^2$ $(m+n)^4$	$Z_2 \times Z_4$ $Z_2 \times Z_2$
$16\,m\,n^3$ $16\,m^3\,n$	$(m+n)^3\,(m-3\,n)$ $(m+n)\,(m-3\,n)^3$	$(m+3\,n)\,(m-n)^3$ $(m+3\,n)^3\,(m-n)$	$Z_2 \times Z_6$ $Z_2 \times Z_2$
$(2\,m\,n)^4$ $16\,m\,n\,(m^2-n^2) \cdot (m^2+n^2)^2$	$(m^4-6\,m^2\,n^2+n^4) \cdot (m^2+n^2)^2$ $(m^2-2\,m\,n-n^2)^4$	$(m^2-n^2)^4$ $(m^2+2\,m\,m-n^2)^4$	$Z_2 \times Z_8$ $Z_2 \times Z_2$

Motivation

Consider a sequence $\{P_0, \dots, P_k, P_{k+1}, \dots\}$ defined recursively by

$$\begin{bmatrix} A_{k+1} \\ B_{k+1} \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} A_k^2 \\ B_k^2 - A_k^2 \\ B_k^2 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 4\, A_k\, B_k \\ \left(A_k - B_k\right)^2 \\ C_k^2 \end{bmatrix}.$$

Proposition (EHG and Jamie Weigandt, 2009)

If the following properties hold for $k = 0$, they hold for all $k \geq 0$:

i. A_k, B_k, and C_k are relatively prime, positive integers.
ii. $A_k + B_k = C_k$.
iii. $A_k \equiv 0 \pmod{16}$ and $C_k \equiv 1 \pmod{4}$.

Corollary

- For $\epsilon > 0$, there exists δ such that $\max\left\{\ln|A_k|,\ \ln|B_k|,\ \ln|C_k|\right\} > \epsilon$ when $k \geq \delta$. Hence $q(P_k) > 1$ for all $k \geq 0$ if and only if $q(P_0) > 1$.
- There exists an infinite sequence with $q(P_k) > 1$.

$Z_2 \times Z_2$ and $Z_2 \times Z_4$

Consider a sequence $\{P_0, \dots, P_k, P_{k+1}, \dots\}$ defined recursively by

$$\begin{bmatrix} A_{k+1} \\ B_{k+1} \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} 8\, A_k\, B_k \left(A_k^2 + B_k^2\right) \\ \left(A_k - B_k\right)^4 \\ C_k^4 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \left(2\, A_k\, B_k\right)^2 \\ \left(A_k^2 - B_k^2\right)^2 \\ \left(A_k^2 + B_k^2\right)^2 \end{bmatrix}.$$

Proposition (Alexander Barrios, Caleb Tillman and Charles Watts, 2010)

If the following properties hold for $k = 0$, they hold for all $k \geq 0$:

i. A_k, B_k, and C_k are relatively prime, positive integers.
ii. $A_k + B_k = C_k$.
iii. $A_k \equiv 0 \pmod{16}$ and $C_k \equiv 1 \pmod{4}$.

Corollary

- For $\epsilon > 0$, there exists δ such that $\max\left\{\ln|A_k|,\ \ln|B_k|,\ \ln|C_k|\right\} > \epsilon$ when $k \geq \delta$. Hence $q(P_k) > 1$ for all $k \geq 0$ if and only if $q(P_0) > 1$.
- There exist infinitely $E_{P_k}(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_{2N}$ for $N = 1, 2$; $q(P_k) > 1$.

$Z_2 \times Z_6$

Consider a sequence $\{P_0, \ldots, P_k, P_{k+1}, \ldots\}$ defined recursively by

$$\begin{bmatrix} A_{k+1} \\ B_{k+1} \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} 16\, A_k\, B_k^3 \\ (A_k + B_k)^3\,(A_k - 3\,B_k) \\ (A_k + 3\,B_k)\,(A_k - B_k)^3 \end{bmatrix}.$$

Proposition (Alexander Barrios, Caleb Tillman and Charles Watts, 2010)

If the following properties hold for $k = 0$, they hold for all $k \geq 0$:

i. A_k, B_k, and C_k are relatively prime integers.
ii. $A_k + B_k = C_k$.
iii. $A_k \equiv 0 \pmod{16}$ and $C_k \equiv 1 \pmod{4}$.

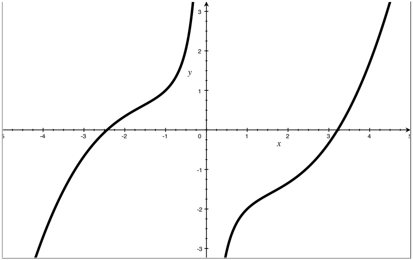
Question

What condition do we need to guarantee that these are **positive** integers?

$Z_2 \times Z_6$?

We sketch why perhaps $3.214\,B_k > A_k$. Define the rational number

$$x_k = \frac{A_k}{B_k} \qquad \Longrightarrow \qquad \begin{cases} \dfrac{1}{x_{k+1}} - \dfrac{1}{x_k} & = \dfrac{\left(A_k + B_k\right)^3 \left(A_k - 3\,B_k\right)}{16\,A_k\,B_k^3} - \dfrac{B_k}{A_k} \\ & = \dfrac{x_k^4 - 6\,x_k^2 - 8\,x_k - 19}{16\,x_k}. \end{cases}$$



The largest root is $x_0 = 3.2138386$, so $0 < x_{k+1} < x_k < x_0$ is decreasing.

$Z_2 \times Z_8$

Consider a sequence $\{P_0, \ldots, P_k, P_{k+1}, \ldots\}$ defined recursively by

$$\begin{bmatrix} A_{k+1} \\ B_{k+1} \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} \left(2\,A_k\,B_k\right)^4 \\ \left(A_k^4 - 6\,A_k^2\,B_k^2 + B_k^4\right)\left(A_k^2 + B_k^2\right)^2 \\ \left(A_k^2 - B_k^2\right)^4 \end{bmatrix}.$$

Proposition (Alexander Barrios, Caleb Tillman and Charles Watts, 2010)

If the following properties hold for $k = 0$, they hold for all $k \geq 0$:

i. A_k, B_k, and C_k are relatively prime, positive integers.
ii. $A_k + B_k = C_k$ and $B_k > 3.174\,A_k$.
iii. $A_k \equiv 0 \pmod{16}$ and $C_k \equiv 1 \pmod{4}$.

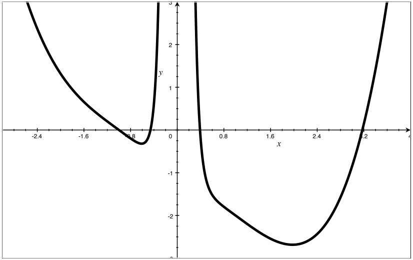
Corollary

- For $\epsilon > 0$, there exists δ such that $\max\left\{\ln|A_k|,\ \ln|B_k|,\ \ln|C_k|\right\} > \epsilon$ when $k \geq \delta$. Hence $q(P_k) > 1$ for all $k \geq 0$ if and only if $q(P_0) > 1$.
- There exists a sequence $E_{P_k}(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$ and $q(P_k) > 1$.

$Z_2 \times Z_8$

We sketch why $B_k > 3.174\, A_k$. Define the rational number

$$x_k = \frac{B_k}{A_k} \quad \Longrightarrow \quad \begin{cases} x_{k+1} - x_k = \dfrac{\left(A_k^4 - 6\, A_k^2\, B_k^2 + B_k^4\right)\left(A_k^2 + B_k^2\right)^2}{\left(2\, A_k\, B_k\right)^4} - \dfrac{B_k}{A_k} \\ \qquad\qquad\;\; = \dfrac{x_k^8 - 4\, x_k^6 - 16\, x_k^5 - 10\, x_k^4 - 4\, x_k^2 + 1}{16\, x_k^4}. \end{cases}$$



The largest root is $x_0 = 3.1737378$, so $x_0 < x_k < x_{k+1}$ is increasing.

Example

We can generate many examples of *ABC* Triples $P = (A, B, C)$ with

$$E_{A,B,C}(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8 \qquad \text{and} \qquad q(A, B, C) > 1.$$

We consider the recursive sequence defined by

$$\begin{bmatrix} A_{k+1} \\ B_{k+1} \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} \left(2\,A_k\,B_k\right)^4 \\ \left(A_k^4 - 6\,A_k^2\,B_k^2 + B_k^4\right)\left(A_k^2 + B_k^2\right)^2 \\ \left(A_k^2 - B_k^2\right)^4 \end{bmatrix}.$$

Initialize with $P_0 = \left(16^2, 63^2, 65^2\right)$ so that we have

i. A_k, B_k, and C_k are relatively prime, positive integers.
ii. $A_k + B_k = C_k$ and $B_k > 3.174\,A_k$.
iii. $A_k \equiv 0 \pmod{16}$ and $C_k \equiv 1 \pmod{4}$.

k	A_k	B_k	C_k	$q(P_k)$
0	2^8	$3^4 \cdot 7^2$	$5^2 \cdot 13^2$	1.05520
1	$2^{36} \cdot 3^{16} \cdot 7^8$	$41^2 \cdot 881 \cdot 20113 \cdot 385817^2 \cdot 13655297$	$5^8 \cdot 13^8 \cdot 47^4 \cdot 79^4$	1.00676

Further Topics for Elliptic Curves

- How can we find curves of large rank? Play around with k (or t) to find a curve E with group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^4$.

  `http://www.math.purdue.edu/~egoins/site//SUMSRI.html`

- Will this win me $1,000,000? Yes, according to the Clay Mathematics Institute!

  `http://www.claymath.org/millennium/`

- Work of Wiles' on Fermat's Last Theorem used elliptic curves. What's being studied now? Modular Forms, Quaternion Algebras, and Shimura Varieties!

  `http://en.wikipedia.org/wiki/Shimura_variety`

Number Theory is COOL!