

A Survey of Diophantine Equations

Edray Herber Goins

Department of Mathematics
Pomona College

M@X: Math at Xavier Seminar
Xavier University of Louisiana

October 30, 2025



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 talk, we'll focus on various types of so-called Diophantine Equations, discussing such topics as Pythagorean Triples, Pell's Equations, Elliptic Curves, and Fermat's Last Theorem.

<https://www.xula.edu/departments/departments-of-mathematics.html>

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author, and do not necessarily reflect the views of the National Science Foundation.

My Personal Journey



William Dailey and Edray (1972)



Edray and Dwight (1974)



Edray in Kindergarten (1978)



Edray in 6th Grade (1984)



Portrait of Nimray (1989)



Playing the Piano (December 1993)



Dwight, Nimray, and Edray (1993)



Edray, Eddi B., and Dwight (January 2010)



Washington Prep



Academic Decathlon (1989)



San Francisco Examiner (April 1990)



Valedictorian Speech (June 1990)



Caltech NSBE Meeting (February 1991)



Ditch Day Stack (April 1991)



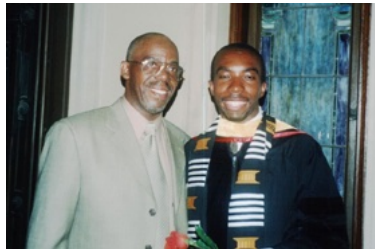
The California Tech (February 1994)



Black History Month Display (1994)



Black Grad Students Assoc Meeting (1997)



Nimray and Edray (1999)



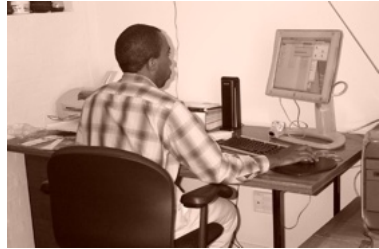
Stanford Black Graduation (1999)



Eddi B. and Edray (1999)



Institute for Advanced Study (1999)



Institute for Advanced Study (1999)



Berliner Dom (April 2001)



Eiffel Tower (May 2001)



Edray and John Tate (November 2001)



Harvard University (January 2003)



Caltech (February 2003)



Black Issues in Higher Ed (January 2004)



Purdue University



MAA Section Meeting (October 2012)

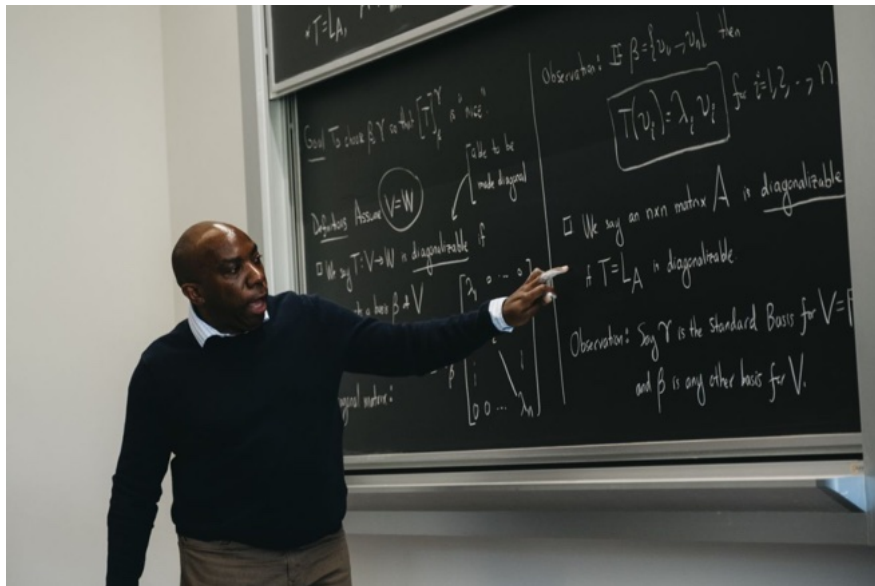


Kevin Mugo's Graduation (July 2014)



Alex Barrios's Graduation (May 2018)







<https://www.pomona.edu/academics/departments/mathematics>

Academics / Departments and Programs / Mathematics Department

Mathematics Department



◀ Professor Edray Goins hosted a dinner for African American freshmen who expressed an interest in majoring in the mathematical sciences. ▶

MATHEMATICS DEPARTMENT

DEPARTMENT A-Z

MATHEMATICS MAJOR

COURSES & REQUIREMENTS

UNDERGRADUATE RESEARCH

EVENTS & COLLOQUIA

STUDENTS

RESOURCES

DEPARTMENTAL NEWS

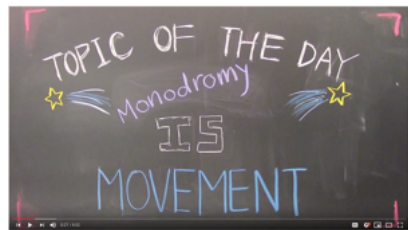
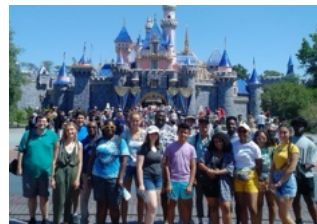
EMPLOYMENT

OUR FACULTY & STAFF

CONTACT US

<https://www.pomona.edu/academics/departments/mathematics>

Pomona Research in Mathematics Experience



<http://research.pomona.edu/prime>

We have funding from the National Science Foundation (DMS-2113782) for **\$548,786** to encourage underrepresented undergraduates, graduate students, and faculty:

- **Research with Undergraduate Participation.** In the past, PRiME employed 8 undergraduate students, 2 graduate students, and 2 faculty in order to host two research teams. Now PRiME employs 15 undergraduate students, 5 graduate students, and 5 faculty in order to host **five research teams**.
- **Mentoring Clusters.** There are **three mentoring clusters**, each consisting of graduate students and faculty. Each week, the mentoring clusters have lunch at least once to discuss topics such as the academic job market, writing funding proposals, and forming potential research collaborations.
- **Professional Development.** There are various development activities for both undergraduates and staff (graduate students and faculty) on Fridays. Undergraduates will attend a series of workshops run by local faculty to prepare for the Graduate Record Examination, gain $\text{\LaTeX}$ proficiency, and strengthen graduate school and fellowship applications. Every other week, the staff have focused, literature-based discussions led by local faculty who are experts in the field.
- **Community Building.** There is a lecture series during Friday afternoons featuring underrepresented minority faculty. Speakers are encouraged to stay for Saturday outings to help build community and facilitate social interactions.



Alex Barrios



Luis Garcia Puente



Edray Goins



Haydee Lindo



Lori Watson



Mark Curiel



Olivia Del Guercio



Fabian Ramirez



Cameron Thomas



Japheth Varlack

➤ **Wednesday June 28**

12:00 PM - 2:00 PM: *Embracing Differences* with **Brandon Jackson** (POM)

➤ **Friday June 30**

10:00 AM - 12:00 PM: *PRiME Alumni Panel*

2:00 PM - 4:00 PM: *Combatting Imposter Syndrome* with **Ellie Ash-Balá** (POM)

➤ **Friday July 7**

10:00 AM - 12:00 PM: *Opportunities at NSF-Math Institutes Panel*

2:00 PM - 4:00 PM: *L^AT_EX Tutorial* with **Sireesh Vinnakota** (UCI)

➤ **Friday July 14**

10:00 AM - 12:00 PM: *Grad School 101 Panel*

2:00 PM - 4:00 PM: *Computational Software* with **Youngsu Kim** (CSUSB)

➤ **Friday July 21**

10:00 AM - 12:00 PM: *NSF GRFP Workshop* with **Tomislav Pintauer** (NSF)

2:00 PM - 4:00 PM: *Writing Winning Résumés* with **Wanda Gibson** (POM)

➤ **Friday July 28**

10:00 AM - 12:00 PM: *Careers at the Department of Defense* with **Bill Christian** (DOD)

2:00 PM - 4:00 PM: *Giving Effective Mathematical Presentations* with **Bahar Acu** (PZR)



Friday June 30: *Apollonian Circle Packings, Integers, and Higher-Dimensional Sphere Packings*

Edna Jones (Duke University)

<https://services.math.duke.edu/~elj31/index.html>



Friday July 7: *Lines and Curves in the Tropics*

María Angélica Cueto (Ohio State University)

<https://people.math.osu.edu/cueto.5/>



Friday July 14: *Fourier Coefficients of Modular Forms and Arithmetic*

Jennifer Johnson-Leung (University of Idaho)

<https://www.uidaho.edu/sci/mathstat/our-people/faculty/jenfns>



Friday July 21: *Curves, Surfaces, and Applied Algebraic Geometry*

Jose Israel Rodriguez (University of Wisconsin at Madison)

<https://sites.google.com/wisc.edu/jose/home>



Friday July 28: *Finite Element Exterior Calculus with Smoother Spaces*

Johnny Guzmán (Brown University)

<https://appliedmath.brown.edu/people/johnny-guzman>

<https://researchseminars.org/seminar/PRiME2020>





Stipend and Travel

Undergraduate participants in the PRiME program will receive:

- a stipend of \$4,000 upon successful completion of the program;
- travel to and from Claremont, housing at Pomona, and dining hall meals;
- a \$1,000 allowance for travel to future conferences.

Expectations

In order to successfully complete this project, undergraduate participants will:

- Give a presentation at MAA's MathFest.
- Write a technical paper explaining the details of the project.
- Design a poster giving an overview of the project.

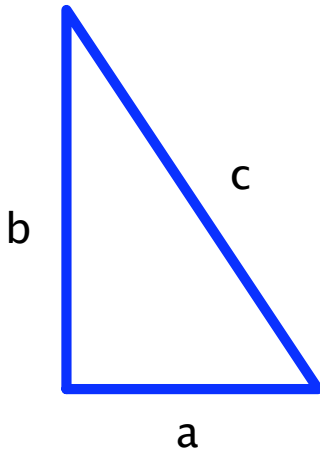
Prerequisites

Students must be undergraduates in good standing, although preference will be given to applicants who will begin their junior or senior year in Fall 2023. Participants must be either US Citizens or Permanent Residents.



<http://research.pomona.edu/prime>

Some Motivating Questions



Motivating Question

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

$$3^2 + 4^2 = 5^2$$

$$8^2 + 15^2 = 17^2$$

$$10^2 + 24^2 = 26^2$$

$$6^2 + 8^2 = 10^2$$

$$12^2 + 16^2 = 20^2$$

$$20^2 + 21^2 = 29^2$$

$$5^2 + 12^2 = 13^2$$

$$7^2 + 24^2 = 25^2$$

$$16^2 + 30^2 = 34^2$$

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

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

Proof: Define the integers m and n by the relation

$$\frac{m}{n} = \frac{a}{c-b} \quad \Rightarrow \quad \begin{aligned} a &= \frac{m}{n}(c-b) \\ a^2 &= c^2 - b^2 \end{aligned} \quad \Rightarrow \quad \begin{aligned} \frac{a}{c} &= \frac{2mn}{m^2 + n^2} \\ \frac{b}{c} &= \frac{m^2 - n^2}{m^2 + n^2} \end{aligned}$$

$$3^2 + 4^2 = 5^2$$

$$8^2 + 15^2 = 17^2$$

$$10^2 + 24^2 = 26^2$$

$$6^2 + 8^2 = 10^2$$

$$12^2 + 16^2 = 20^2$$

$$20^2 + 21^2 = 29^2$$

$$5^2 + 12^2 = 13^2$$

$$7^2 + 24^2 = 25^2$$

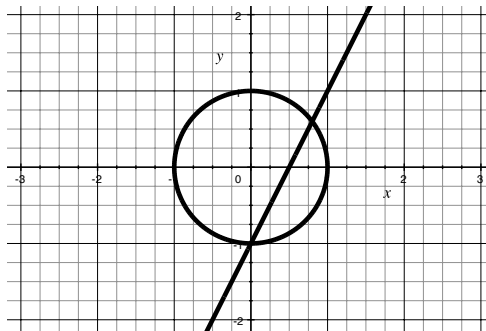
$$16^2 + 30^2 = 34^2$$

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

$$\begin{aligned}
 x = \frac{a}{c} = \frac{2mn}{m^2 + n^2} & \quad \Rightarrow \quad \frac{m}{n} = \frac{y+1}{x} & \Rightarrow & \quad y = (m/n)x - 1 \\
 y = \frac{b}{c} = \frac{m^2 - n^2}{m^2 + n^2} & & & \quad x^2 + y^2 = 1
 \end{aligned}$$



Where does this
“draw a line” trick
come from?

Pythagorean Triples correspond to the quadratic equation

$$a^2 + b^2 - c^2 = 0.$$

Consider a more general quadratic equation

$$Aa^2 + Bab + Cb^2 + Dac + Ebc + Fc^2 = 0$$

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

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

Motivating Questions

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

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM

LIBRI SEX.

ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

*Hanc primum Graecè & Latine editi, atque absolutissimis
Commentariis illustrati.*

AVCTORE CLAVDIO GASPARI BACHETO
MEXICANO SEBASTIANO, V.C.



LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, VIRI
IACOBI, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIÆ

Cover of the 1621 translation of Diophantus' *Arithmetica*

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

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

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

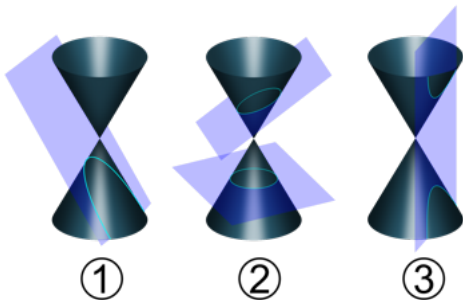
➤ **Step #2:** Substitute

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

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

$$\begin{aligned}
 x &= x_0 - \frac{(2 A x_0 + B y_0 + D) n^2 + (B x_0 + 2 C y_0 + E) m n}{A n^2 + B m n + C m^2} \\
 y &= y_0 - \frac{(2 A x_0 + B y_0 + D) m n + (B x_0 + 2 C y_0 + E) m^2}{A n^2 + B m n + C m^2}
 \end{aligned}$$

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$$



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

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) .

- 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

$$(x, y) = \left(\frac{2mn}{m^2 + n^2}, \frac{m^2 - n^2}{m^2 + n^2} \right).$$

- For any integer d , the curve $x^2 - dy^2 = 1$ has a rational point $(x_0, y_0) = (1, 0)$, so all rational points are in the form

$$(x, y) = \left(\frac{dm^2 + n^2}{dm^2 - n^2}, \frac{2mn}{dm^2 - n^2} \right).$$

- The equation $x^2 + y^2 = -1$ has no rational points at all.

Motivating Questions

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

- 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

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

There are infinitely many rational solutions:

$$\begin{array}{l} y = (m/n)(x-1) \\ x^2 - 2y^2 = 1 \end{array} \quad \implies \quad (x, y) = \left(\frac{2m^2 + n^2}{2m^2 - n^2}, \frac{2mn}{2m^2 - n^2} \right).$$

We can find a few integral solutions:

$$\begin{array}{l} (x_0, y_0) = (1, 0) \\ (x_1, y_1) = (3, 2) \\ (x_2, y_2) = (17, 12) \\ (x_3, y_3) = (99, 70) \\ (x_4, y_4) = (577, 408) \end{array} \quad \implies \quad x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n.$$

For $d = 61$, we have the equation $x^2 - 61y^2 = 1$.



Proposition (Fermat, 1657)

One nontrivial integral solution (x, y) to $x^2 - 61y^2 = 1$ is

$$(x_1, y_1) = (1766319049, 226153980).$$

How did Fermat find this solution?

Proposition

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

- 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 $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$, we consider the ring

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

We denote the norm of $a = x + y\sqrt{d}$ as $\mathbb{N}a = x^2 - dy^2$ 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

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

Proposition

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

- We have a one-to-one correspondence

$$\left\{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 - dy^2 = 1 \right\} \longrightarrow G = \left\{ a \in \mathbb{Z}[\sqrt{d}] \mid \mathbb{N}a = 1 \right\},$$

$$(x, y) \longmapsto a = x + y\sqrt{d}.$$

- The collection of integer solutions (x, y) to $x^2 - dy^2 = 1$ 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, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}$ 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 $b = 1$. $\square$

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 $x^2 - dy^2 = 1$.

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

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

Motivating Question

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

Given a real number x , define the following sequence

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

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

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

Denote the **n th convergent** as the rational number

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

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

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

We find the specific numbers

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

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

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}}.$$

Theorem (Joseph-Louis Lagrange, 1771)

Fix a positive integer d which is not a square.

➤ $\sqrt{d} = \{a_0; \overline{a_1, \dots, a_{h-1}}, 2a_0\}$, where the overline denotes that h terms repeat indefinitely.

➤ If we consider the h th convergent, say $\{a_0; a_1, \dots, a_{h-1}\} = p_h/q_h$, then

$$p_h^2 - dq_h^2 = (-1)^h.$$

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

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

Consider $d = 2$. The continued fraction is

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}} = \{1; \overline{2}\}$$

which has $h = 1$. Consider the convergent

$$\frac{p_1}{q_1} = \{1\} = \frac{1}{1} \quad \implies \quad p_1^2 - 2q_1^2 = -1.$$

On the other hand,

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

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

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

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

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

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

$$\delta = 1766319049 + 226153980\sqrt{61} = (29718 + 3805\sqrt{61})^2,$$

so every integral solution (x, y) to $x^2 - 61 y^2 = 1$ satisfies

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

- We have seen identities such as $3^2 + 4^2 = 5^2$ and $1^2 + 2^2 + 2^2 = 3^2$. We can generalize to **Pythagorean Triples** $a^2 + b^2 = c^2$ and **Pythagorean Quadruples** $a^2 + b^2 + c^2 = d^2$.

- We have focused on rational and integral solutions (x, y) to $x^2 - dy^2 = 1$. We can generalize to **conic sections**

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0.$$

These are examples of **quadratic equations**.

- What about **cubic equations**? There are identities such as $3^3 + 4^3 + 5^3 = 6^3$ discovered by Plato, and $1^3 + 12^3 = 9^3 + 10^3$ discovered by G. H. Hardy and Srinivasa Ramanujan. What can we say about equations such as $a^3 + b^3 + c^3 = d^3$ and $x^3 + y^3 = d$?
- What about **quartic equations**? Euler discovered $59^4 + 158^4 = 133^4 + 134^4$. What about equations such as $x^4 + y^4 = d$?
- There are many, many more questions involving **Diophantine Equations**!