

Fermat's Last Theorem

A Journey from Ancient to Modern Mathematics

Stefan Erickson

Department of Mathematics & Computer Science
Colorado College

September 18, 2007

Number Theory

Number Theory is the study of the integers.

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

- ▶ Patterns in sequences of integers.
- ▶ Prime numbers and factorization.
- ▶ Integral solutions to equations.

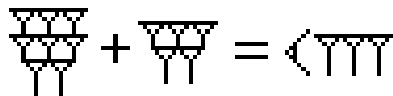
God made the integers; all else is the work of man.
- Leopold Kronecker

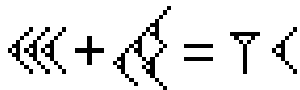
Babylonian Numerals

1		11		21		31		41		51	
2		12		22		32		42		52	
3		13		23		33		43		53	
4		14		24		34		44		54	
5		15		25		35		45		55	
6		16		26		36		46		56	
7		17		27		37		47		57	
8		18		28		38		48		58	
9		19		29		39		49		59	
10		20		30		40		50			

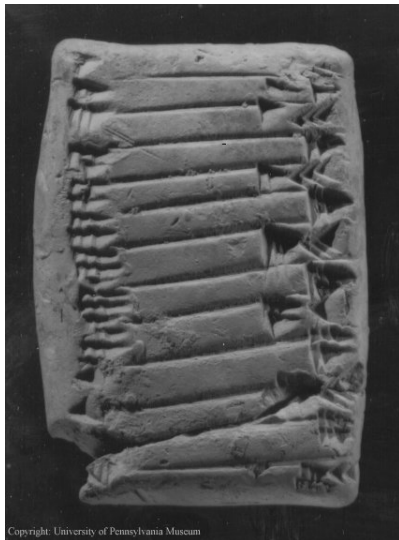
Addition

$$\Upsilon = 1 = 60 = 3600 = \dots$$


$$\begin{array}{c} \triangle \\ \triangle \\ \triangle \\ \triangle \\ \triangle \\ \triangle \end{array} + \begin{array}{c} \triangle \\ \triangle \\ \triangle \end{array} = \begin{array}{c} \triangle \\ \triangle \\ \triangle \end{array}$$

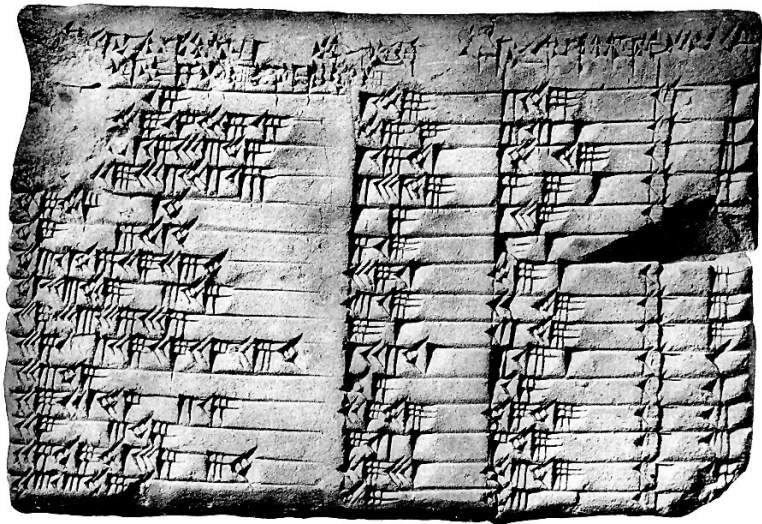

$$\begin{array}{c} \triangle \\ \triangle \\ \triangle \end{array} + \begin{array}{c} \triangle \\ \triangle \end{array} = \begin{array}{c} \triangle \\ \triangle \end{array}$$

Multiplication



1	0; 30
2	1; 0
3	1; 30
4	2; 0
5	2; 30
6	3; 0
7	3; 30
8	4; 0
9	4; 30
10	5; 0
11	5; 30
12	6; 0

Plimpton 322 (circa 1800 BC)



Contents of Plimpton 322

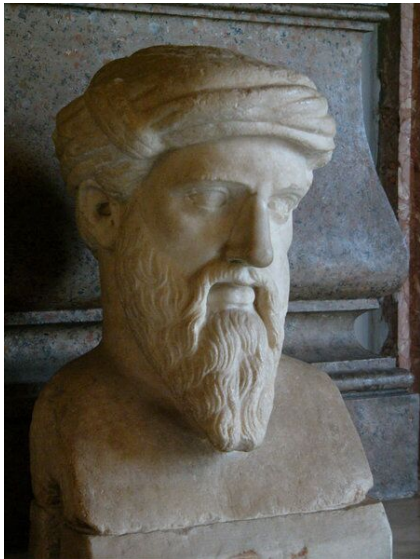
119	169
3367	4825
4601	6649
12709	18541
65	97
319	481
2291	3541
799	1249
481	769
4961	8161
45	75
1679	2929
161	289
1771	3229
56	106

Contents of Plimpton 322

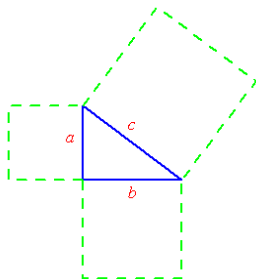
<i>Width</i>	<i>Length</i>	<i>Diagonal</i>
120	119	169
3456	3367	4825
4800	4601	6649
13500	12709	18541
72	65	97
360	319	481
2700	2291	3541
960	799	1249
600	481	769
6480	4961	8161
60	45	75
2400	1679	2929
240	161	289
2700	1771	3229
90	56	106

$$a^2 + b^2 = c^2$$

Pythagoras (6th century BC)



Pythagorean Theorem



$$a^2 + b^2 = c^2$$

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

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

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

⋮

Our offense is like the Pythagorean Theorem – there is no answer!
- Shaquille O'Neal

Diophantus (3th century AD)

DIOPHANTI ALEXANDRINI ARITHMETICORVM

LIBRI SEX.

ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

*Nunc primum Graecè & Latini editi, atque absolutissimi
Commentarijs illustrati.*

AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, G.



LVRETIAE PARISIORVM,

Sumptibus SEBASTIANI CRAMOISY, via

Jacobæ, sub Ciconiis.

M. DC. XXI.

CVM PRIVILEGIO REGIÆ

Diophantus is called “the father of algebra.”

Arithmetica contains many problems with solutions in the integers, now called Diophantine equations.

Proves there are infinitely many *primitive* Pythagorean triples (triples with no common factors).

Pierre de Fermat (1601-1665)



$$a^2 + b^2 = c^2$$

$$a^3 + b^3 = c^3?$$

$$a^4 + b^4 = c^4?$$

$$a^5 + b^5 = c^5?$$

⋮

Proofs for various values of n

$n = 4$: Fermat (1640)

$n = 3$: Euler (1753)

$n = 5$: Dirichlet, Legendre (1825)

$n = 7$: Lamé (1839)

$n < 37$: Kummer (1847)

$n \leq 100$: Kummer (1857)

$n \leq 4,000,000$: Buhler, et. al. (1992)

Uniqueness of Prime Factorization

Every integer has a unique factorization into prime numbers.

$$6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3)$$

are considered to be the same factorization of 6.

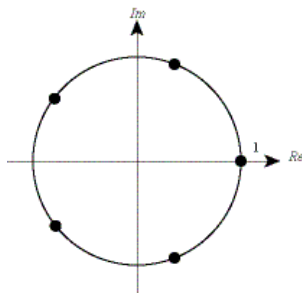
Uniqueness breaks down in extensions of the rationals.

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

are two different factorizations of 6.

The lack of unique factorization is the main obstacle to proving Fermat's Last Theorem.

Roots of Unity



$$\zeta = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

$$\zeta^n = 1$$

$$c^n = a^n + b^n = (a + b)(a + \zeta b)(a + \zeta^2 b) \dots (a + \zeta^{n-1} b)$$

Lamé's Flawed Proof (1847)

$$c^n = a^n + b^n = (a + b)(a + \zeta b)(a + \zeta^2 b) \dots (a + \zeta^{n-1} b)$$

Assume that a , b , and c have no common factors.

$(a + b)$, $(a + \zeta b)$, \dots , $(a + \zeta^{n-1} b)$ have no common factors.

Suppose a prime p divides c . Then p^n divides c^n .

Hence, p^n divides $(a + \zeta^i b)$ for some i . Using unique factorization, one can show that p must also divide a and b .

The problem is that unique factorization very rarely occurs!

Two Types of Number Theory

Algebraic Number Theory:

Use roots of polynomials to prove number theoretical results.

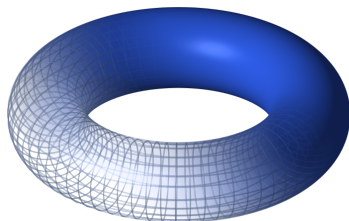
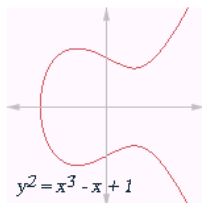
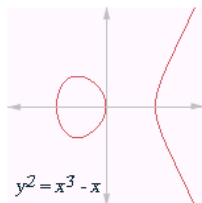
Analytic Number Theory:

Use “smooth” functions to prove number theoretical results.

Developed as separate theories throughout the late nineteenth and early twentieth centuries.

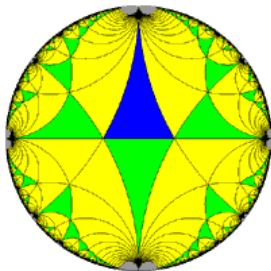
Elliptic Curves

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



Modular Forms

Complex analytic functions with many symmetries.



Taniyama-Shimura Conjecture (1955, 1962):

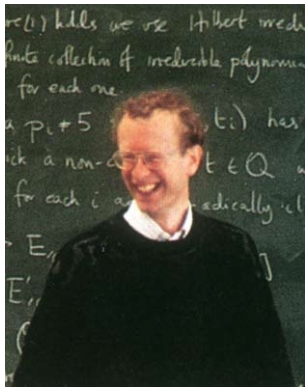
Every elliptic curve is modular.

From Taniyama-Shimura to Fermat

Gerhard Frey (early 1980's) - Suggests that a counterexample to Fermat's Last Theorem would produce an elliptic curve which is not modular.

Jean-Pierre Serre, Ken Ribet (1986) - Prove Frey's hunch, thus showing that Taniyama-Shimura implies Fermat's Last Theorem.

Wiles Proves Fermat's Last Theorem...



After hearing of Serre's and Ribet's results, Andrew Wiles decides to try proving the Taniyama-Shimura Conjecture.

He worked in total isolation for seven years.

In June 1993, Wiles announced that he had proven the Taniyama-Shimura Conjecture. The paper was 200 pages long.

...Or Did He?

Over the summer, the paper was reviewed and checked carefully.

In December 1993, Wiles announces there is a gap in the proof.

Proof Resolved

Along with Richard Taylor, Wiles fills the gap in September 1994.

After 357 years, Fermat's Last Theorem is finally proven!

Idea of Proof

Suppose $a^n + b^n = c^n$ is a counterexample to Fermat's Last Theorem.

Frey's Curve:

$$E : y^2 = x(x - a^n)(x + b^n)$$

Ribet proves that E cannot be modular.

Wiles proves that E must be modular.

Therefore, no such counterexample could exist!

Aftermath

Did Fermat have a proof? Probably not.

Did Fermat have Wiles's proof? Definitely not.

Any applications to the real world? None.

The greatest contribution is the deep mathematical theory generated by the problem.

Elliptic curves are currently the fastest method in cryptography.

Millennium Problems

- ▶ Riemann Hypothesis
- ▶ Birch Swinnerton-Dyer Conjecture
- ▶ Hodge Conjecture
- ▶ Navier-Stokes Equations
- ▶ Yang-Mills Theory
- ▶ $P = NP$
- ▶ Poincare Conjecture (Solved?)