CO 480 Lecture 13

Pierre de Fermat and Fermat's Last Theorem

June 15th, 2017

Final 15th Century Person - François Viète

- Born in 1540 in western France (Fontenay-le-Comte). Died 1603.
- Had a legal reputation - worked for King Henri III as a cryptanalyst. [Kat93, p. 369]
- Father of modern notation (that is, using an x to denote a number)
- Coefficients could be either positive or negative!
- Wrote *The Analytic Art*, effectively reformulating Algebra.
- Descarte's *Géométrie* took this further and used early letters for known quantities and later letters (specifically x) for unknown quantities.

https://commons.wikimedia.org/wiki/File:Francois_Viete.jpg

Elementary Symmetric Functions (Viète's Formulas)

Viète wrote the coefficients of polynomials using their roots. For example, if we look at the polynomial $ax^3 + bx^2 + cx + d$ with roots x_1, x_2 and x_3, then, we see that

$$\begin{aligned} x_1 + x_2 + x_3 &= -\frac{b}{a} \\ x_1x_2 + x_2x_3 + x_3x_1 &= \frac{c}{a} \\ x_1x_2x_3 &= -\frac{d}{a} \end{aligned}$$

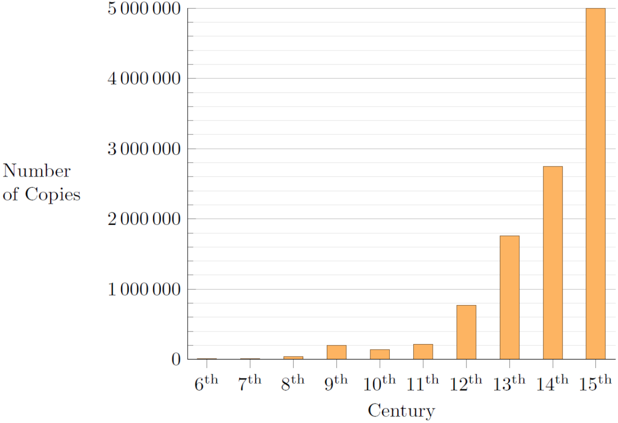
First Infinite Product (Vièta's Formula)

$$\pi = 2 \cdot \frac{2}{\sqrt{2}} \cdot \frac{2}{\sqrt{2+\sqrt{2}}} \cdot \frac{2}{\sqrt{2+\sqrt{2+\sqrt{2}}}} \cdots$$

Dark Ages (c. 600-1200 AD)

"... [there] existed great ignorance and wretchedness - these were the Dark Ages" (Voltaire, An Essay on Universal History, 1758)

European Output of Manuscripts 500–1500*



*without Southeast Europe (Byzantine realm) and Russia

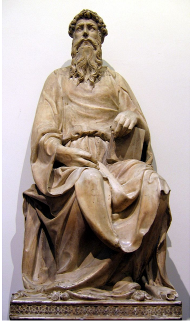
Renaissance (14th century to 16th century)

- European movement - began in Italy, particularly Florence and moved north
- Cultural movement that deeply influenced European intellectual life.

Artists

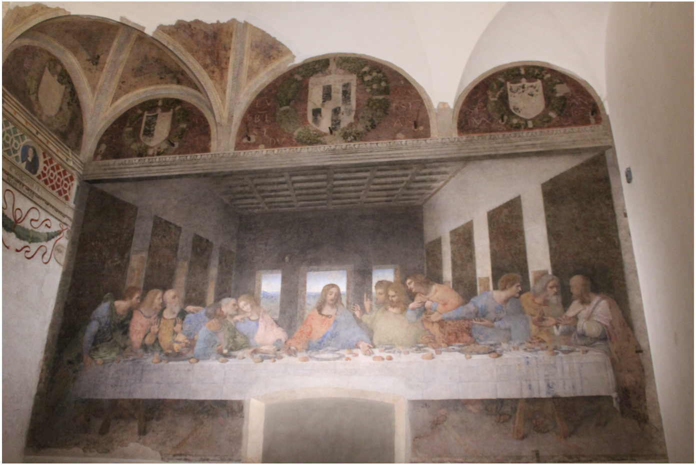
- Italy's "Ninja Turtles": Donatello (1386-1466), Leonardo Da Vinci (1452-1519), Michelangelo (1475-1564) and Raphael (1483-1520)
- Netherlands: Jan van Eyck (1395-1441)
- Germany: Durer (1471-1528)

Donatello



St. John the Evangelist (1409-1411) - Wikimedia Commons

Da Vinci

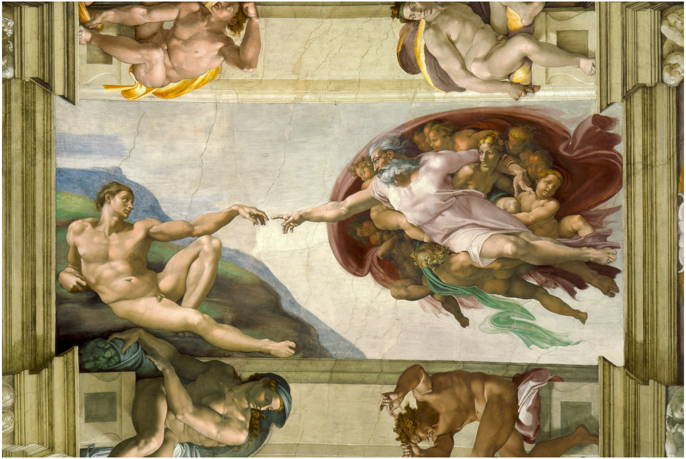


The Last Supper (currently in Milan- 1498)

Duomo in Milan

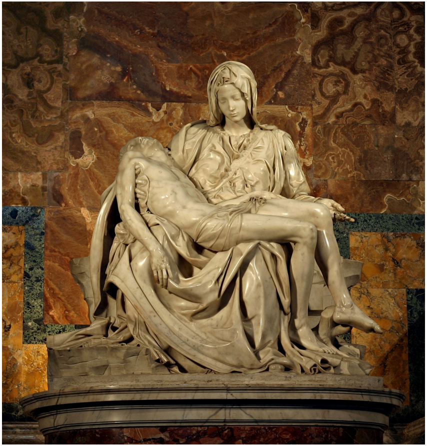
Duomo in Milan - Largest church in Italy.

Michelangelo



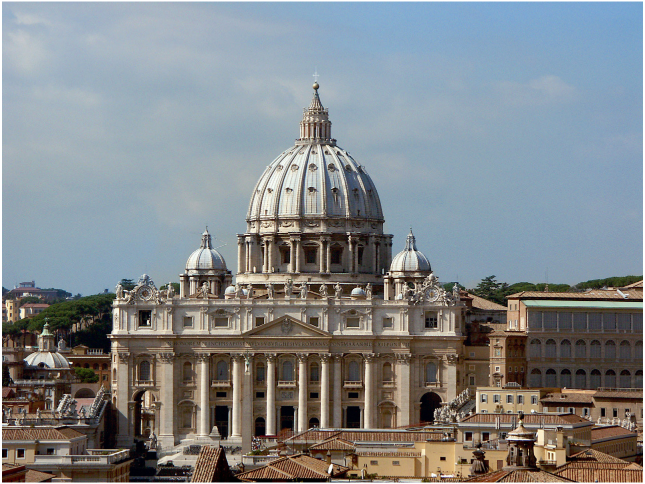
Creation of Adam (Sistine Chapel, Michelangelo 1512) - Wikimedia Commons

Michelangelo



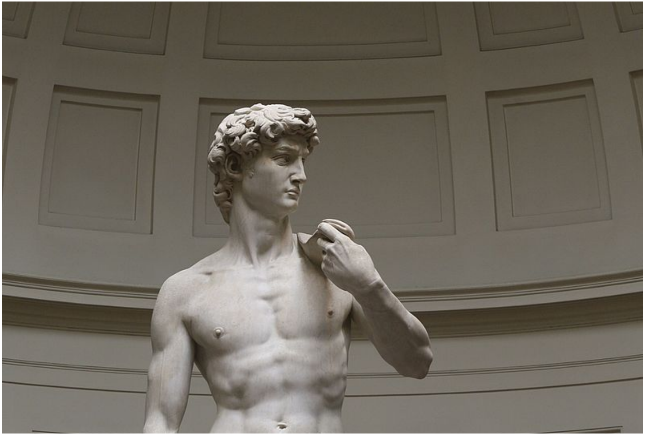
Pieta (St. Peter's Basilica, Michelangelo - 1499) - Wikimedia Commons

St. Peter's Basilica


IN HONOREM PRINCIPIS APOST PAVLVS V BVRGHESIVS ROMANVS PONT MAX AN MDCXII PONT VII

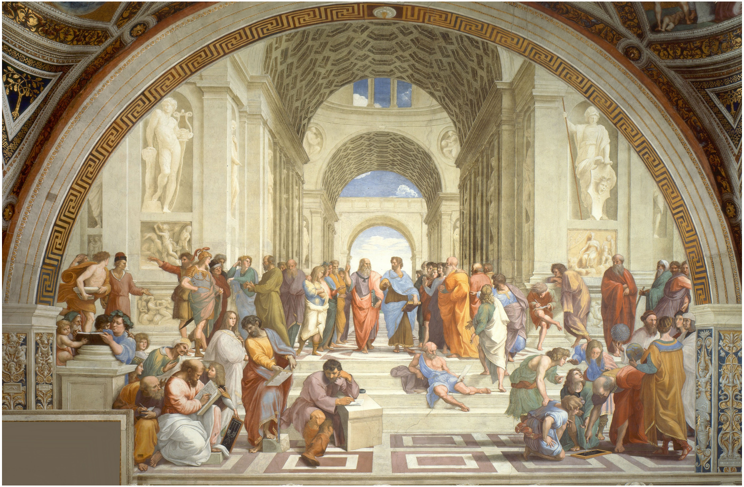
St. Peter's Basilica (Vatican, Redesigned by Michelangelo - 1546) - Wikimedia Commons

Michelangelo



Michelangelo's David (1501-1504) - Wikimedia Commons

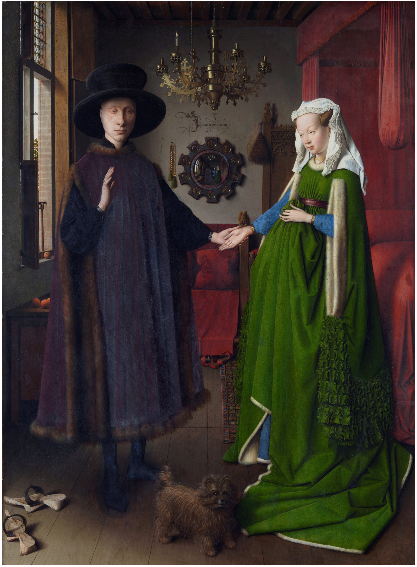
Raphael



School of Athens (1505) - Raphael Wikimedia Commons

Van Eyck

Arnolfini Portrait (1434)
Jan van Eyck
Wikimedia Commons.

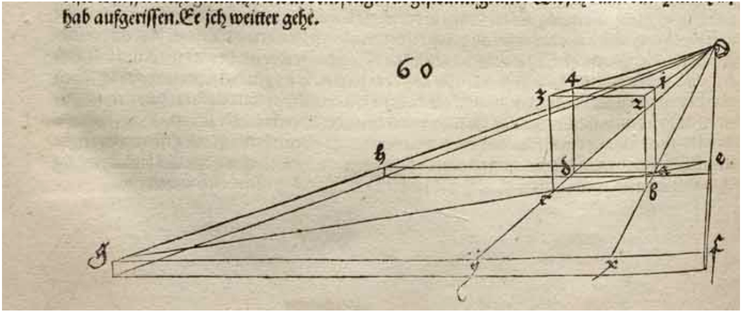


Durer - Projective Art

Albrecht Durer
Self-Portrait (1500)
Wikipedia Commons

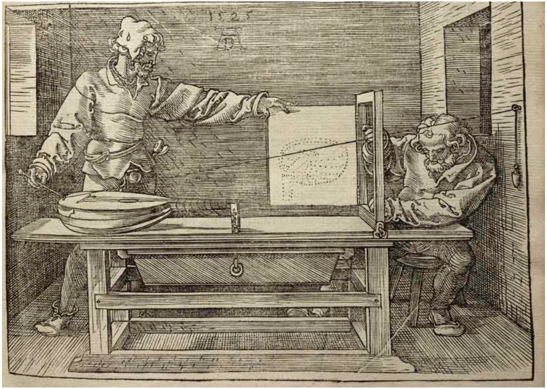
1500
AD
Albertus Durerus Noricus
ipsum me propriis sic effin-
gebam coloribus aetatis
anno XXVIII.

Durer - Projective Geometry

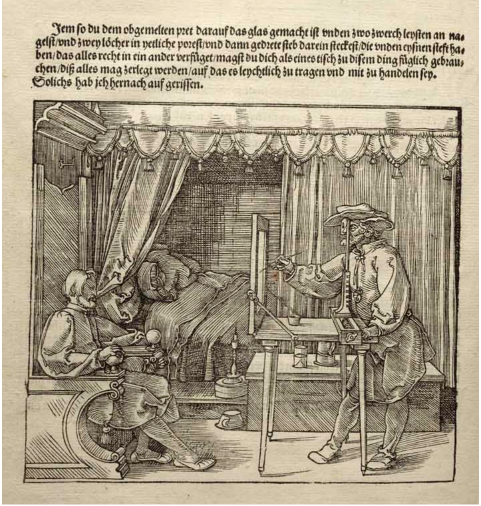


hab aufgeriſſen.Ee jch weitter gehe.

Durer - Projective Geometry



Durer - Projective Geometry



Jem ſo du dem obgemelten pret darauf das glas gemacht iſt vnden zwo zwerch leyſten an nagelſt/vnd zwey löcher in yetliche poreſt/vnd dann gedrete ſteb darein ſteckeſt/die vnden eyſnen ſteft haben/das alles recht in ein ander verfüget/magſt du dich als eines tiſch zu diſem ding füglich gebrauchen/diß alles mag zerlegt werden/auf das es leychtlich zu tragen vnd mit zu handelen ſey.
Solichs hab jch hernach auf geriſſen.

Northern Renaissance

https://www.youtube.com/watch?v=lob0zb28_wM (van Eyck)
https://www.youtube.com/watch?v=gFhR8xUE5ZU (Durer esp. 32:00/33:20)

Writers

- 1439, invention of printing press by Gutenberg (1398-1468)
- Italy: Machiavelli (1469-1527) [arguably the founder of political science]
- England: Thomas More (1478-1535), Shakespeare (1564-1616)

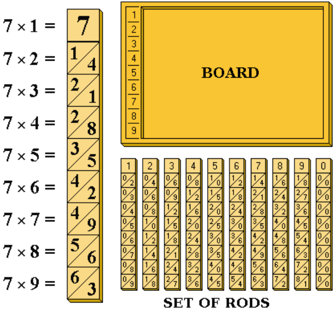
The Scientific Revolution

- End of Renaissance period marked the beginning of the Scientific Revolution
- Arguably begins with Copernicus' *De revolutionibus orbium coelestium* (On the Revolution of Heavenly Spheres) in 1543 and continued into the late 18th century.
- Founding of the scientific method
- Francis Bacon (1561-1626) - Father of Empiricism
- Began applying quantitative analysis to observations

Some Highlights

- Heliocentric model of our solar system (Copernicus, Kepler, Galileo, Brahe)
- Gravity (Newton's *Principia* - 1687)
- Human anatomy (Vesalius - 1543 *De humani corporis fabrica*)
- Refining ores and extracting metals (Georg Agricola *De re metallica*)
- Telescope (Lippershey, Galileo), refraction of light (Newton)
- Electricity (Gilbert *De Magnete*)

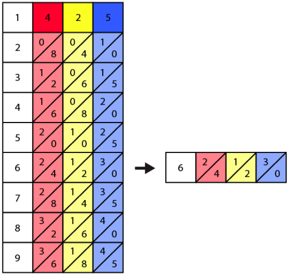
Mechanical Devices - Napier's Bones



(Wikimedia Commons)

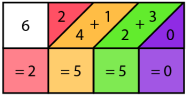
How They Worked (Wikimedia Commons)

- eg. $425 \cdot 6$
- Take the appropriate bones and stack them beside each other
- Take the row corresponding to 6.
- Add the diagonals (watching for carry overs)
- Get the result.
- If 6 is a multi-digit number, repeat for other digits, padding for zeroes at the end then add the result.



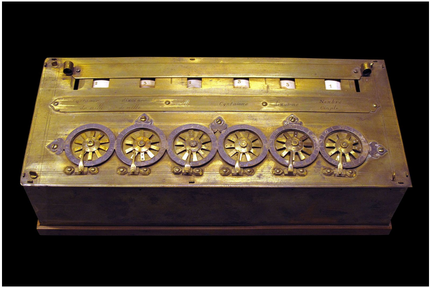
1	4	2	5
2	0/8	0/4	1/0
3	1/2	0/6	1/5
4	1/6	0/8	2/0
5	2/0	1/0	2/5
6	2/4	1/2	3/0
7	2/8	1/4	3/5
8	3/2	1/6	4/0
9	3/6	1/8	4/5

6	2/4	1/2	3/0



6	2	4 + 1	2 + 3	0
	= 2	= 5	= 5	= 0

Blaise Pascal (Mechanical Calculator -1642)



Created at the age of 18, Pascal used this to help his father perform tedious tax accounting in Rouen. Uses 'Nine's Complement'. First to get the addition carry over. Only performed + and −.

Europe in the 17th Century

A few mathematicians:

- Galileo (1564-1642) [Planetary motion]
- Kepler (1571-1630) [Planetary motion]
- Napier (1550-1617) [Logarithms]
- Descartes (1596-1650) [Analytic geometry]
- Newton (c. 1642-1726) [Physics/Calculus]
- Leibniz (1646 - 1716) [Calculus]
- Pascal (1623-1662) [Probability]
- **Fermat (1607-1665)**

This day June 20th, 1800.

Abraham Kaestner, teacher of Gauss and of Farkas Bolyai, died in Gottingen, Germany. He interested these two men directly, along with Farkas' son Janos Bolyai and Lobachevsky indirectly, in Euclid's parallel postulate.

Pierre de Fermat

- The last of the great amateur mathematicians [Bur91, p. 511]
- Was a lawyer and magistrate by trade
- No known of evidence of interest in mathematics until after 30.
- Contributions in many fields (analytic geometry, calculus, probability theory, number theory).

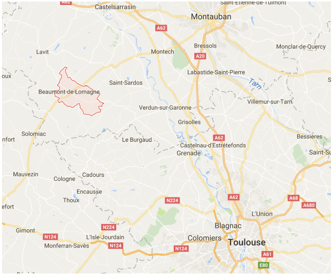
`https://en.wikipedia.org/wiki/File:Pierre_de_Fermat.jpg`

Quotes [Mah94]

- “Braggart” (Descartes)
- “the greatest mathematician in all of Europe” (Pascal)
- “the learned councilor from Toulouse” (Mersenne)
- “that damned Frenchman” (Wallis)

A Bit About Fermat [Wei84, p. 37]

- Born in Beaumont de Lomagne (southern France) to a middle class family.
- Baptized “Pierre Fermat” on August 20th, 1601.
- Attended University of Toulouse before moving to Bordeaux in the late 1620s.
- From Bourdeaux, he went north to Orléans where he studied law at university, graduating before 1631 with a civil law degree. [OR]



More on His Career

- May 14th, 1631, got into “parlement” as councilor of the provincial High Court of Judicature in Toulouse
- Bought the seat from wide of former holder at a price of 43,500 *livres* [Mah94, p. 16] (200 *livres* = annual wages for 1 labourer)
- Could then change his hame to “Pierre de Fermat”. [OR]
- Many of his contemporaries felt that Fermat was an average (if not below average) lawyer - probably because he spent so much of his time doing mathematics.

More on Fermat [Wei84]

- Married Louise de Long on June 1st, 1631 (a distant cousin of his mother's)
- Dowry was 12,000 *livres* [Mah94, p. 16]
- Was a polyglot (spoke Latin, Greek, Italian and Spanish)
- Was a homebody, Never went further than Bordeaux/Orléans.
- Would send letters to prominent mathematicians both French and English challenging them to problems he could solve.
- Had 5 children; 2 sons (Clément-Samuel [eldest], Jean) and 3 daughters (Claire, Louise, Cathérine)
- Had relatively good health until around 1652/1653 - plague hit Toulouse.
- Erroneously reported dead by friend and philosopher Bernard Medon [Mah94, p. 17]
- Died January 12th, 1665

Bourdeaux (250 km from Bordeaux to Toulouse)

E606
A89
A89
A10
A20
Les Eyzies-de-Tayac-Sireuil
Bordeaux
Libourne
Bergerac
Sarlat-la-Canéda
Padirac
Rocamad
Parc naturel régional des Causses du Quercy
A63
A62
Parc naturel régional des Landes de Gascogne
Marmande
Cahors
Villeneuve-sur-Lot
A65
A62
Villefra
Agen
Boé
A20
Montauban
Condom
Ga
A65
Mont-de-Marsan
A62
A68
Aire-sur-l'Adour
Auch
Toulouse
A65
A64

Digression - Plague(s)

- Europe was riddled with plagues during this time.
- Biggest was Black Death from 1346-1350 killing 75-250 million people (from 30%-60%) of the total population. (see Wikipedia on Black Death)
- In the 1600's, there were several bad plagues:
- Italian Plague 1629-1631 (killed 280,000)
- Great Plague of Seville 1647-1652 (killed 500,000, say 5% of population - probably bubonic plague)
- Great Plague of London 1665-1666 (killed 100,000)
- Plague in France 1668 (killed 40,000)
- Great Plague of Marseille 1720 (killed 100,000 people)

Dispute [OR]

- Fermat was given a copy of Descartes' La Diotrique (by Beaugrand)
- Mersenne wanted his opinion on the book to which Fermat says it was "groping about in the shadows" [Mah94]
- Fermat claimed that Descartes was not correctly deducing the law of refraction properly due to faulty assumptions. (Fermat was vindicated later see next slide)

https://en.wikipedia.org/wiki/Ren%C3%A9_Descartes

Descartes to Fermat [OR]

... seeing the last method that you used for finding tangents to curved lines, I can reply to it in no other way than to say that it is very good and that, if you had explained it in this manner at the outset, I would have not contradicted it at all.

Descartes to Fermat [OR]

> *... seeing the last method that you used for finding tangents to curved lines, I can reply to it in no other way than to say that it is very good and that, if you had explained it in this manner at the outset, I would have not contradicted it at all.*

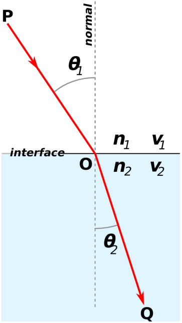
.. this was, of course, after Descartes attacked Fermat's methods of finding maxima, minima and tangents. (Yes, Fermat knew calculus before calculus!)

Descartes Was Not Done!

- Sadly, the feud doesn't end here.
- Descartes proceeds to attack Fermat's reputation.
- He praised Fermat's work on the tangent to a cycloid to his face (which was correct)
- However, in letters to Mersenne, he claims it was incorrect, citing Fermat as an "inadequate mathematician and inadequate thinker" [OR].

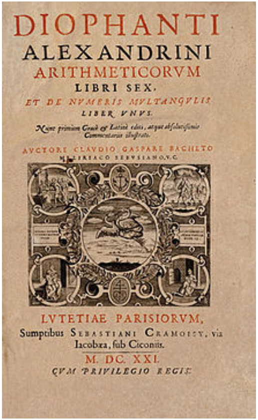
20 Years Later

- Eventually, Descartes (and Snell) settled on a description of the refraction of light (the sine law from refraction)
- However, Fermat had deduced it as well from a fundamental property of light that he proposed, namely that light follows the shortest path. This is now one of the most basic properties of optics! (Yet many mathematicians disputed this with him) [OR].



Fermat's Contributions to Number Theory

- Fermat was largely influenced by Diophantus' Arithmetica
- Given that it was a Greek book, one begs the question "How did the book arrive in France"?



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque abſolutiſſimis
Commentariis illuſtrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, ſub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

(Bachet's translation of Arithmetica
Wikimedia Commons)

Lineage of Arithmetica [Ore88]

- First mention in Europe in 1462 by Regiomontanus (mathematician active in Vienna)
- Wanted to translate Arithmetica from Greek to Latin but never did.
- First successful translation was by Holzman (changed from Greek Xylander) in Heidelberg in 1575 (see next quote from his foreword)
- "When I first came upon the work of Diophantos, his method and reasoning so overwhelmed me that I scarcely knew whether to think of my former self with pity or with laughter." [Ore88, p. 195]
- In 1621, Bachet de Méziriac produced a new edition, "sharply and ungratefully criticiz[ing] Xylander" [Ore88, p. 196] (probably unjust since Xylander's edition helped Bachet).

Reminder Book II Problem 8

- Reminder: To divide a square into the sum of two squares
- Fermat wrote in the margin of this question Fermat's Last Theorem, that $x^n + y^n = z^n$ has no nontrivial solutions and claimed to have a proof "that the margin was too narrow to contain"
- Original book is lost but was kept alive in Bachet's Latin copy of Arithmetica written by Fermat's son Samuel.
- We'll focus on key players who had a part in proving Fermat's Last Theorem.

Fermat's and Others

- Fermat never really met with other mathematicians
- Only met for three days with Father Mersenne [Wei84, p. 42]
- Despite this, he had many correspondences with mathematicians, including Huygens, Carcavi and Pascal (Both Etienne (died 1651) and son Blaise)
- In 1654, he asked the two aforementioned men to help write his work in a book (never came to be - see next slide)
- Bulk of this job fell on Samuel

Letter to Carcavi [Mah94, p. 61]

I am delighted to have had opinions conforming to those of M. Pascal, for I have infinite esteem for his genius and believe him capable of succeeding in anything he might undertake. The friendship he has offered is so dear to me and so thoughtful that I believe there should be no difficulty in making some use of it in the publication of my treatises.

If that did not shock you, the two of you may undertake that publication of which I consent to your being the masters; you may clarify or supplement whatever seems too concise and relieve me of a burden that my duties prevent me from taking on. I even desire that the work appear without my name, leaving pretty much up to you the choice of any designation that will be able to mark the name of the author whom you deem your friend.

Fermat and Viète [Wei84]

- Fermat actually managed to obtain some of Viète's work - including some of his unpublished work which Fermat studied closely.
- Provided most of the symbolism that Fermat used throughout his life.

Mathematics of Fermat

- Defied usual norms of mathematics (eg. did most of his work after the age of 30, didn't write many proofs)
- Fermat worked in many fields, including geometry (analytical and on Apollonius' Plane Loci), optimization, probability and for us, most notably, number theory.
- At the time, few people were working on number theory.
- One in particular, Bernard Frénicle de Bessy (c. 1604-1674) had many correspondences with Fermat. However Fermat's skills were far greater than those of Bessy and the correspondence ended quickly [OR]

Mathematical Skills of Fermat

- Fermat published only one paper in his life [Bur91, p. 513].
- Motivation came from personal pleasure.

Two Very Interesting Propositions

Fermat posed as a challenge that the equation

$$y^2 + 4 = x^3$$

had exactly 4 integer solutions and that the equation

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

has exactly 2 integer solutions. We believe he solved this using infinite descent however we to this day don't know exactly how Fermat solved these two problems.

Note to self: Elements of Algebra by Euler (1822 - p. 401) has a proof. Note to self: Compare to Diophantine Equations we've seen.

Binomial Theorem

Setting $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, we have that for $n \geq 0$ an integer and x, y numbers, that

$$\begin{aligned}(x+y)^n &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \\ &= x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + ... + \binom{n}{n-1} x y^{n-1} + y^n\end{aligned}$$

Theorem of Fermat (see assignment 4)

Let m and n be positive integers. Prove that

$$n \cdot \binom{n+m-1}{m-1} = m\binom{n+m-1}{m}$$

Note that for $m = 2$, the binomial coefficient on the right represents the triangular numbers and for $m = 3$, the pyramidal numbers.

Fermat's Little Theorem

One of Fermat's most famous results in number theory

Fermat's Little Theorem

Let a be an integer and $p > 0$ a prime number. Then

$$a^p \equiv a \mod p$$

Where did This Come From? [Bur91]

Fermat wrote to Mersenne in June 1640 about a discovery he had while dealing with perfect numbers.

Recall that a number n is perfect if $2n = \sum_{\substack{d|n \\ d>0}} d$.

Alain proved in class that a even number is perfect if and only if $n = 2^{p-1}(2^p - 1)$ for some prime p.

Discovery

While playing around with these, Fermat noted that $2p$ would always divide $(2^p - 1) - 1$. Taking out the factor of 2, this means that $2^{p-1} - 1$ is always divisible by p. From here, it wasn't a matter of time before he wrote to Bernard Frénicle de Bessy on October 18th, 1640 that

> *If p is a prime and a is any integer not divisible by p, then $a^{p-1} - 1$ is divisible by p.*

A Small Lemma

Claim: $p \mid \binom{p}{k}$ where $0 < k < p$ is any integer.
Proof: We see that by definition

$$k!\binom{p}{k} = p(p-1)(p-2)...(p-k+1)$$

Since p divides the right hand side and $p > k$ so $p \nmid k!$, we must have that $p \mid \binom{p}{k}$ by Euclid's Lemma.

Proof of FLT

When $p = 2$, $a^2 - a = a(a-1) \equiv 0 \mod 2$ since $a(a-1)$, the product of consecutive integers, is even. So we assume $p > 2$. If a is negative, then $b = -a$ is positive and

$$a^p - a = (-b)^p - (-b) = -(b^p - b)$$

so it suffices to prove the claim for nonnegative integers a (for then the right hand side above is divisible by p)

Induction

The claim is by induction. When $a = 0$ or $a = 1$, a simple plug in reveals these cases. Now, assume that $k^p - k \equiv 0 \mod p$ for some $k > 1$. Then, with $k + 1$, we have

$$\begin{aligned} (k+1)^p &= k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + ... + \binom{p}{p-1}k + 1 \\ &\equiv k^p + 1 \mod p \quad \text{By lemma} \\ &\equiv k^p - k + k + 1 \mod p \\ &\equiv k + 1 \mod p \quad \text{By IH} \end{aligned}$$

hence $(k+1)^p \equiv k + 1 \mod p$ and thus, by induction, $a^p \equiv a \mod p$.

This day June 22nd...

... 1633:

Galileo recanted Copernicanism. Under the threat of torture, he was forced by the Inquisition to recant.

... 1925

Felix Klein died. In 1905 the famous geometer recommended the teaching of calculus in German secondary schools.

Announcements

- Extension granted on Assignment 3 due to popular demand. Due Next Friday at 2:30pm.
- Check for your Crowdmark link!
- Assignment 4 has been posted.
- Editorial Reviews should be given out within the next 48 hours. These are due on Thursday July 6th.

Editorial Review

- You will each get a project to edit individually.
- Must submit two anonymous copies: One via a Crowdmark Link and one on LEARN's Dropbox (sadly I cannot download assignments from Crowdmark... yes I know this is frustrating).
- Due Thursday July 6th at 2:30pm.
- Be courteous in your reviews while still being critical.
- Check out the editorial guidelines.

Method of Infinite Descent

Main outline:

- Assume some statement is true (usually that some equation has an integer solution).
- Take that integer solution and find a smaller positive integer solution (usually by taking the previous solution and dividing the values by something)
- Argue that one can continue to do this forever, finding more and more smaller positive integer solutions.
- Since the point above cannot continue forever, we have a contradiction.

Fermat writes this in the margin of Book VI, Problem 26 in Arithmetica while solving the problem at the end of these slides. (Not surprisingly, he runs out of room in the margin to complete his proof!)

Fermat's Last Theorem for $n = 4$

Let's use the method of infinite descent to show that $x^2 + y^4 = z^4$ has no nontrivial integer solutions, that is, no solutions when $xyz \neq 0$ (Note this implies that Fermat's Last Theorem for $n = 4$ is true!)

Of significant importance is that this is the only example we have in full of Fermat explicitly writing down his infinite descent argument. [Bur91, p. 517]

As always, assume towards a contradiction that (x, y, z) are nonzero positive integers satisfying $x^2 + y^4 = z^4$. Without loss of generality, we can assume x, y and z are pairwise coprime.

Recall Assignment 2

In assignment 2, you proved the following:

Assignment 2

If $X^2 + Y^2 = Z^2$ with X, Y, Z pairwise coprime (and Y even), then there exists integers $m > n > 0$ coprime such that

$$X = m^2 - n^2 \qquad Y = 2mn \qquad Z = m^2 + n^2.$$

We apply this with $x^2 + (y^2)^2 = (z^2)^2$ to get one of two cases:

1. $x = 2mn$, $y^2 = m^2 - n^2$ and $z^2 = m^2 + n^2$ OR
2. $x = m^2 - n^2$, $y^2 = 2mn$ and $z^2 = m^2 + n^2$

Case 1

If $x = 2mn$, $y^2 = m^2 - n^2$ and $z^2 = m^2 + n^2$, we can find a smaller solution by taking y^2z^2 and noting that

$$(yz)^2 = m^4 - n^4$$

This gives

$$(yz)^2 + n^4 = m^4$$

Now, $n < y$ and $m < z$ and so we have descended to a smaller solution.

Case 2

If instead $x = m^2 - n^2$, $y^2 = 2mn$ and $z^2 = m^2 + n^2$, we have more work to do.

Case 2

If instead $x = m^2 - n^2$, $y^2 = 2mn$ and $z^2 = m^2 + n^2$, we have more work to do.

Since $y^2 = 2mn$ and m and n are coprime, we know that $m = 2u^2$ and $n = v^2$ (or vice versa). Without loss of generality, we suppose the first case.

Case 2

If instead $x = m^2 - n^2$, $y^2 = 2mn$ and $z^2 = m^2 + n^2$, we have more work to do.

Since $y^2 = 2mn$ and m and n are coprime, we know that $m = 2u^2$ and $n = v^2$ (or vice versa). Without loss of generality, we suppose the first case.

Now, as $z^2 = m^2 + n^2$, again we can use Assignment 2 to see that there are coprime positive integers $r > s > 0$ such that $z = r^2 + s^2$, $m = 2rs$ and $n = r^2 - s^2$. Since $m = 2u^2$, we see that $u^2 = rs$ and as before $r = a^2$ and $s = b^2$ for some positive integers a and b.

Case 2

If instead $x = m^2 - n^2$, $y^2 = 2mn$ and $z^2 = m^2 + n^2$, we have more work to do.

Since $y^2 = 2mn$ and m and n are coprime, we know that $m = 2u^2$ and $n = v^2$ (or vice versa). Without loss of generality, we suppose the first case.

Now, as $z^2 = m^2 + n^2$, again we can use Assignment 2 to see that there are coprime positive integers $r > s > 0$ such that $z = r^2 + s^2$, $m = 2rs$ and $n = r^2 - s^2$. Since $m = 2u^2$, we see that $u^2 = rs$ and as before $r = a^2$ and $s = b^2$ for some positive integers a and b.

Since $n = r^2 - s^2$, we have $v^2 = a^4 - b^4$, which gives a solution with $a < z$ and $b < y$.

Conclusion

So in either case, we have a solution with z coordinate strictly smaller than the original. This can go on forever which is a contradiction because there are only finitely many positive integers less than z. This is the idea behind a proof by infinite descent and this is a contradiction.

Recall: Numbers as the Sums of Two Squares

Recall from Diophantus' Arithmetica we show that if $n \equiv 3 \mod 4$, then n is not the sum of two squares, that is $x^2 + y^2 = n$ has no integer solutions.

What about...

... the numbers (in this case primes) $p \not\equiv 3 \mod 4$. Well 2 clearly is the sum of two squares so let's ask about primes $p \equiv 1 \mod 4$.

Try some out!

Primes Congruent to 1 Modulo 4

$$\begin{aligned} 5 &= 1^2 + 2^2 \\ 13 &= 2^2 + 3^3 \\ 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2 \\ 37 &= 1^2 + 6^2 \\ 41 &= 4^2 + 5^2 \end{aligned}$$

$$\begin{aligned} 53 &= 7^2 + 2^2 \\ 61 &= 5^2 + 6^2 \\ 73 &= 3^2 + 8^2 \\ 89 &= 5^2 + 8^2 \\ 97 &= 4^2 + 9^2 \\ 101 &= 1^2 + 10^2 \end{aligned}$$

Sums of Primes as Two Squares

Recall some of these facts:

Part of Arithmetica Book III Problem 19

For a, b, c, d numbers, we have

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2 = (ac+bd)^2+(ad-bc)^2$$

that is, we can write a product of sums of two squares as itself the sum of two squares.

this is sometimes called the Diophantus-Fibonacci identity. [Hea64, p.105, 167]

Composition Rule Revisited

Brahmagupta-Fibonacci identity

For a, b, c, d, n numbers, we have

$$\begin{aligned}(a^2 + nb^2)(c^2 + nd^2) &= (ac - nbd)^2 + n(ad + bc)^2 \\ &= (ac + nbd)^2 + n(ad - bc)^2.\end{aligned}$$

this is sometimes called the Brahmagupta-Fibonacci identity (our composition rule).

Main Theorem

Sum of Two Squares

Every prime number $p \equiv 1 \mod 4$ can be expressed as the sum of two squares.

The first proof written down was by Euler in 1749 when he was 42.

Four Major Lemmas

Lemma 1

The product of sums of two squares is again the sum of two squares

This is the identity of Diophantus/Brahmagupta.

Four Major Lemmas

Lemma 2

If the sum of two squares $a^2 + b^2$ is divisible by a prime that is the sum of two squares $p^2 + q^2$, then that quotient is the sum of two squares.

Four Major Lemmas

Lemma 2

If the sum of two squares $a^2 + b^2$ is divisible by a prime that is the sum of two squares $p^2 + q^2$, then that quotient is the sum of two squares.

Main Idea: Since by Lemma 1

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2$$

We would like to show that $p^2 + q^2$ divides one of the squares on the right.

Proof

Clever insight:

$$\begin{aligned}(pb - aq)(pb + aq) &= p^2 b^2 - a^2 q^2 \\ &= p^2 b^2 + p^2 a^2 - p^2 a^2 - a^2 q^2 \\ &= p^2(a^2 + b^2) - a^2(p^2 + q^2)\end{aligned}$$

Since $p^2 + q^2$ divides both terms on the right, it divides the term on the left. By Euclid's Lemma, since this is a prime number, it must divide one of the factors. We'll show the case where $(p^2 + q^2) \mid pb - aq$.

Wrapping up

As $(a^2+b^2)(p^2+q^2) = (ap+bq)^2 + (aq-bp)^2$, we see that p^2+q^2 divides two of these three terms and hence it divides the third, which in this case is $(ap+bq)^2$. Again by Euclid's Lemma, $(p^2+q^2) \mid (ap+bq)^2$ implies that $(p^2+q^2) \mid (ap+bq)$ Thus, we can divide everything by p^2+q^2 giving

$$\frac{a^2+b^2}{p^2+q^2} = \left(\frac{ap+bq}{p^2+q^2}\right)^2 + \left(\frac{aq-bp}{p^2+q^2}\right)^2$$

completing the proof in this case (and the case where $(p^2+q^2) \mid pb+aq$ is similar; just switch p^2+q^2 to q^2+p^2 in Lemma 1)

Four Major Lemmas

Lemma 3

If the sum of two squares $a^2 + b^2$ is divisible by a number x that is not the sum of two squares, then the quotient must also not be the product of the sum of two squares.

Proof of Lemma 3

Take $a^2 + b^2 = xp_1p_2...p_n$ where the p_i are all prime factors. Assume towards a contradiction that each of these p_i is the sum of two squares. Then applying Lemma 2 a total of n times gives us that x is also the sum of two squares. This is a contradiction and hence the claim is true.

Four Major Lemmas

Lemma 4

Suppose $\gcd(a, b) = 1$. Then every positive factor of $a^2 + b^2$ is the sum of two squares.

Proof of Lemma 4

Let $x \mid (a^2 + b^2)$ be a positive factor and assume towards a contradiction that x is not the sum of two squares. We try to find a smaller $w \leq x$ with the same property . Find c and d satisfying

$$a \equiv c \mod x \qquad b \equiv d \mod x \qquad -\frac{|x|}{2} \leq c, d \leq \frac{|x|}{2}$$

Now, notice that $0 \equiv a^2 + b^2 \equiv c^2 + d^2 \mod x$ and so $x \mid (c^2 + d^2)$. If $\gcd(c, d) = \delta$, and if $\gcd(\delta, x) \neq 1$, then this $\gcd(\delta, x)$ divides a since $a \equiv c \mod x$ and similarly for b. This contradicts the assumption that $\gcd(a, b) = 1$ and so we know that $\gcd(\delta, x) = 1$.

Continuing

So $x \mid (c^2 + d^2)$ and $\delta = \gcd(c, d)$ is coprime to x. Write $xy = c^2 + d^2$ for some positive integer y. Then $\delta^2 \mid xy$ and since $\gcd(\delta^2, x) = 1$, we see that $\delta^2 \mid y$. Let $z\delta^2 = y$ for some positive integer z. Then, we see that $zx = e^2 + f^2$ where $e = c\delta$ and $f = d\delta$ are two integers. Then

$$zx = e^2 + f^2 \leq c^2 + d^2 \leq (x/2)^2 + (x/2)^2 = x^2/2$$

and so, $z = (e^2 + f^2)/x$ is the quotient of a sum of squares and a number that cannot be expressed as the sum of squares. Hence by Lemma 3, z has a factor that is not the sum of two squares call it w and $w \leq z \leq (x^2/2)/x = x/2$. Thus, we have descended to a smaller value w with the same properties of x and so we can repeat the above with w instead of x and so on. This is a contradiction by infinite descent.

On June 27th...

1831: Sophie Germain died in Paris. She is famous for her work on number theory and on elastic surfaces.

1908: Award for proof of Fermat's Last Theorem announced. The Academy of Sciences of Gottingen announced a prize of one hundred thousand marks, according to the will of Dr. Paul Wolfskehl, of Darmstadt, for the proof of Fermat's great theorem.

Main Theorem

Sum of Two Squares

Every prime number $p \equiv 1 \mod 4$ can be expressed as the sum of two squares.

Recall

Lemma 4

Suppose $\gcd(a, b) = 1$. Then every positive factor of $a^2 + b^2$ is the sum of two squares.

Proof

Clever again! Let x be a positive integer less than $p = 4n + 1$ (for some positive integer n). We see that

$$(x^{2n} - 1)(x^{2n} + 1) = x^{4n} - 1 \equiv 0 \mod p$$

the last equality holding by Fermat's Little Theorem. So $p \mid (x^{2n} + 1)$ of $p \mid (x^{2n} - 1)$. If $p \mid (x^{2n} + 1)$, then Lemma 4 says it is the sum of two squares. Hence assume towards a contradiction that $p \mid (x^{2n} - 1)$ for all possible values of x. Notice that this implies that $x^{2n} \equiv 1 \mod p$.

Reminder

This is a math 135 result that you likely don't remember (it can be proved by induction).

Roots in a Field (Lagrange's Theorem)

A polynomial equation $x^{2n} = c$ can only have at most $2n$ roots in $\mathbb{Z}_p$ (or $\mathbb{C}$ or $\mathbb{R}$ etc.)

Finishing the proof

Since we know that $x^{2n} \equiv 1 \mod p$ can only have $2n$ roots but we know this must hold for all $4n$ numbers, we have reached a contradiction and thus for some value of x, we see that $p \mid (x^{2n} + 1)$

Generalizing

With a bit of thought, you can convince yourself that

Theorem

A number $N = mn^2$ with m squarefree can be written as the sum of two squares if and only if the only divisors of m are 2 and/or primes p congruent to 1 modulo 4.

Exercise: Which of these numbers can be written as the sum of two squares? Can you exhibit such a way?

$$103, 109, 234, 365, 1947$$

Exercise in Descent

Prove: The area of a rational right triangle cannot be a square number. [Ore88, p. 200]

References I

David M. Burton, *The history of mathematics*, second ed., W. C. Brown Publishers, Dubuque, IA, 1991, An introduction. MR 1223776

T. L. Heath, *Diophantus of Alexandria: A study in the history of Greek algebra*, Second edition. With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler, Dover Publications, Inc., New York, 1964. MR 0175731

Victor J. Katz, *A history of mathematics*, HarperCollins College Publishers, New York, 1993, An introduction. MR 1200894

Michael Sean Mahoney, *The mathematical career of pierre de fermat, 1601-1665*, 2 revised ed., Princeton University Press, 1994.

J. J. O'Connor and E.F. Robertson, *Pierre de fermat*, `http://www-groups.dcs.st-and.ac.uk/history/Biographies/Fermat.html`, visited 2017-06-12.

Oystein Ore, *Number theory and its history*, Dover, New York, 1988.

References II

André Weil, *Number theory*, Birkhäuser Boston, Inc., Boston, MA, 1984, An approach through history, From Hammurapi to Legendre. MR 734177