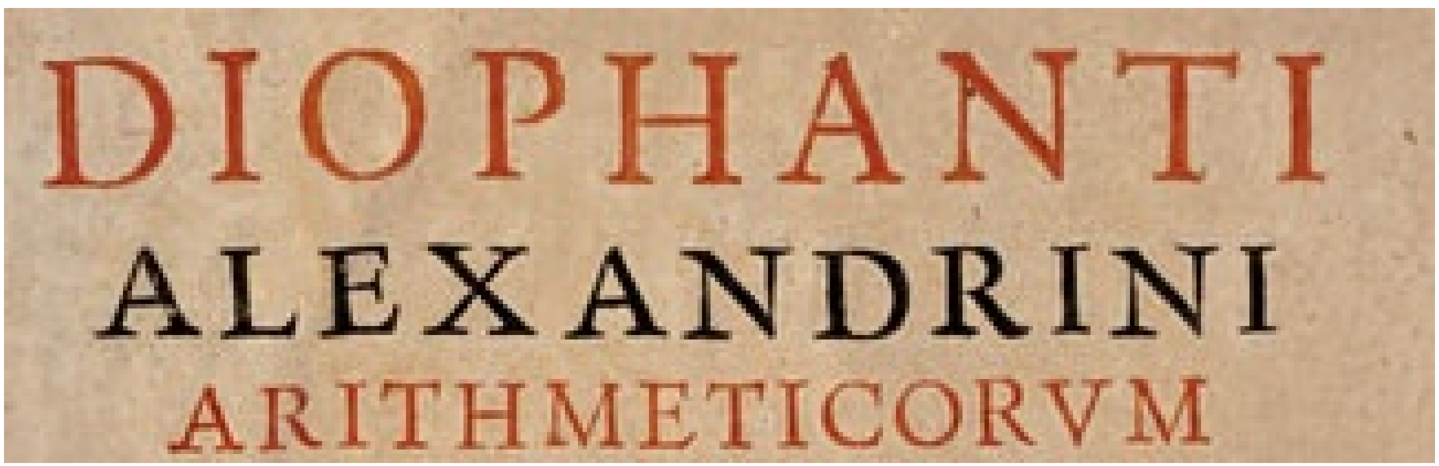
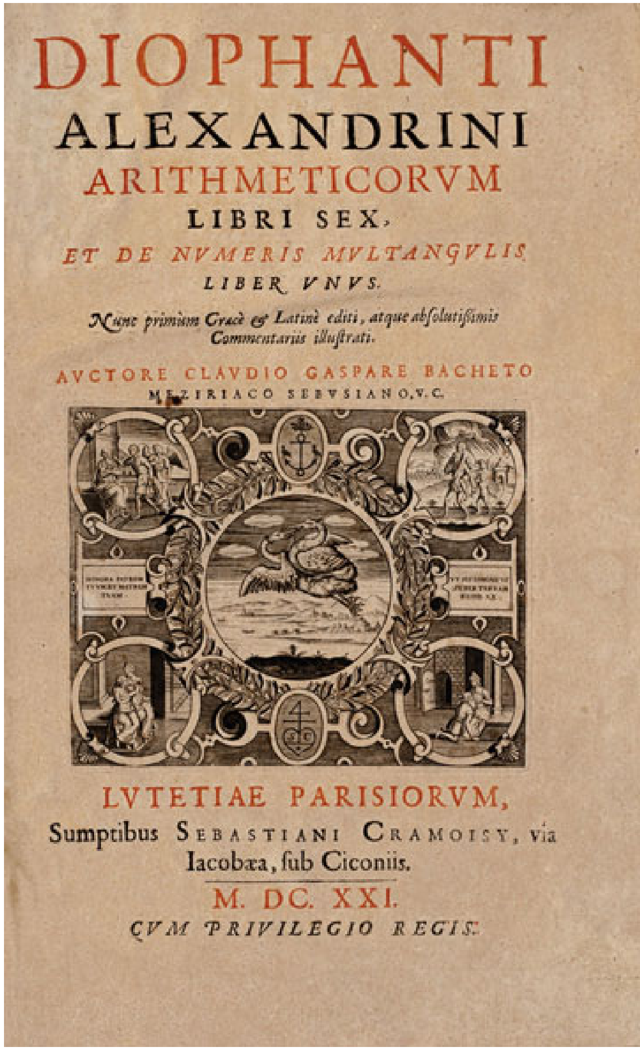
# Diophantus, Pappus and the decline of Greek mathematics



# Diophantus of Alexandria

- Diophantus is often dated as living around 250 CE.
- His major work is called Arithmetica and consists of 13 books, of which only 6 have survived.
- This was essentially a treatise on number theory and dealt with integer solutions of equations.
- Such equations are called Diophantine equations today.



# Arithmetica and its use of symbology

- Arithmetica seems to be the first work where symbols are introduced for unknowns.
- An unknown number is represented by the symbol indicated here.
- In some editions, he uses ζ.
- Squares, cubes, fourth powers, fifth powers and sixth powers are represented by various symbols:

ς

$\Delta^{\Upsilon}$

$K^{\Upsilon}$

$\Delta^{\Upsilon}\Delta$

$\Delta K^{\Upsilon}$

$K^{\Upsilon}K$

# Bachet's translation of Diophantus

- In 1621, Claude Gaspard de Bachet (1591-1639) translated the Arithmetica of Diophantus into Latin.
- This made a deep impression on Pierre de Fermat who is considered today as the one who revived number theory in the 17th century.

# Fermat's method of descent

- Diophantus seemed to have used in his proofs, a method of descent that we attribute today to Fermat.

illustration of his process of infinite descent, let us apply it to an old and familiar problem—the proof that $\sqrt{3}$ is not rational. Let us assume that $\sqrt{3} = a_1/b_1$, where $a_1$ and $b_1$ are positive integers with $a_1 > b_1$. Since

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$$

upon replacing the first $\sqrt{3}$ by its equal $a_1/b_1$, we have

$$\sqrt{3} = \frac{3b_1 - a_1}{a_1 - b_1}$$

In view of the inequality $\frac{3}{2} < a_1/b_1 < 2$, it is clear that $3b_1 - a_1$ and $a_1 - b_1$ are positive integers, $a_2$ and $b_2$, each less than $a_1$ and $b_1$ respectively, and such that $\sqrt{3} = a_2/b_2$. This reasoning can be repeated indefinitely, leading to an infinite descent in which $a_n$ and $b_n$ are ever smaller integers such that $\sqrt{3} = a_n/b_n$. This implies the false conclusion that there is no smallest positive integer. Hence the premise that $\sqrt{3}$ is a quotient of integers must be false.

# Fermat's Last Theorem

- Perhaps the most famous of Fermat's 1637 marginal comments in his edition of Bachet's translation is what has since been called Fermat's Last Theorem.

He wrote his famous marginal note: to split a cube into a sum of two cubes
or a fourth power into a sum of two fourth powers and in general an n-th power as a sum of two n-th powers is impossible.
I have a truly marvellous proof of this but this margin is too narrow to contain it.

# The method of descent for n=4

- What Fermat may have had is a valid proof for n=4 which he derived by the method of descent, as we will soon demonstrate.
- He may have been premature to conclude that his proof was valid for all n.
- Here is the precise statement:

For integers $n > 2$ the equation

$$a^n + b^n = c^n$$

cannot be solved with positive integers $a$, $b$, $c$.

# From Pythagorean triples to Fermat's study of n=4

- The trick is to consider a seemingly more "difficult" problem.
- Fermat showed the equation $x^4 + y^4 = z^2$ has no non-trivial integer solutions.
- He did this by assuming that there is a non-trivial solution and then choosing the solution with $|z|$ minimal.
- Then he showed that there is a solution with a smaller $|z|$, which is a contradiction.

**Solution.** Suppose that $x^4 + y^4 = z^2$ has a nontrivial solution. Take $|z|$ to be minimal. By Euclid's result, we can write

$$
\begin{aligned}
x^2 &= 2ab, && (1.1)\\
y^2 &= b^2 - a^2, && (1.2)\\
z &= b^2 + a^2, && (1.3)
\end{aligned}
$$

with $(x, y) = 1$ and $a$ and $b$ having opposite parity.

Suppose that $b$ is even. Then we see that

$$y^2 = b^2 - a^2 \equiv -1 \equiv 3 \pmod 4.$$

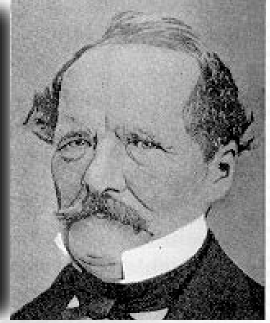
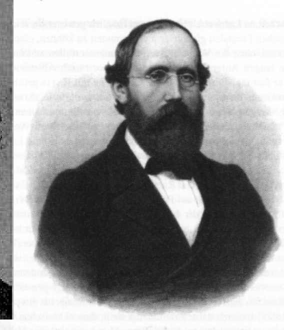
This is impossible. Hence $a$ is even. Then $\exists c \in \mathbb{Z}$ such that $a = 2c$ and $(c, b) = 1$. Then $x^2 = 2 \cdot 2bc = 4bc$. Since $(b, c) = 1$, $b$ and $c$ are perfect squares by unique factoriz. Hence $\exists m, n \in \mathbb{Z}$ such that $b = m^2, c = n^2$ where $(m, n) = 1$. By (1.2), we see that $y^2 = b^2 - a^2 = m^4 - 4n^4$. Hence $(2n^2)^2 + y^2 = (m^2)^2$ and $(2n^2, y) = (y, m^2) = (2n^2, m^2) = 1$.

By Exercise 1.2.2, $2n^2 = 2\alpha\beta$, $y = \beta^2 - \alpha^2$, and $m^2 = \alpha^2 + \beta^2$ where $(\alpha, \beta) = 1$ and $\alpha$ and $\beta$ have opposite parity. Thus we can see that $n^2 = \alpha\beta$. Hence by Euclid again., $\exists p, q \in \mathbb{Z}$ such that $\alpha = p^2$ and $\beta = q^2$. Hence we have $m^2 = p^4 + q^4$. This is a solution of the equation $x^4 + y^4 = z^2$. But $m < b < |z|$ since $m^2 = b < b^2 + a^2 = z$. This is a contradiction to the minimality of $|z|$. Therefore $x^4 + y^4 = z^2$ has no nontrivial solution.

# The development of algebraic number theory

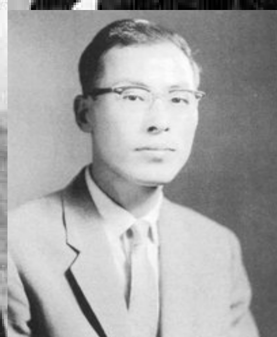
- Fermat's last theorem is a superb example of how a single conjecture can inspire the rapid development of mathematics.
- After Fermat, Euler began a systematic study and showed that for n=3, there are no non-trivial solutions.
- Important reduction: it suffices to solve the problem for prime exponents.





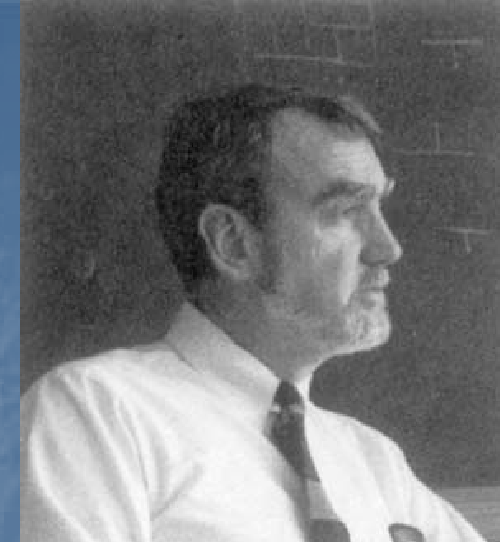




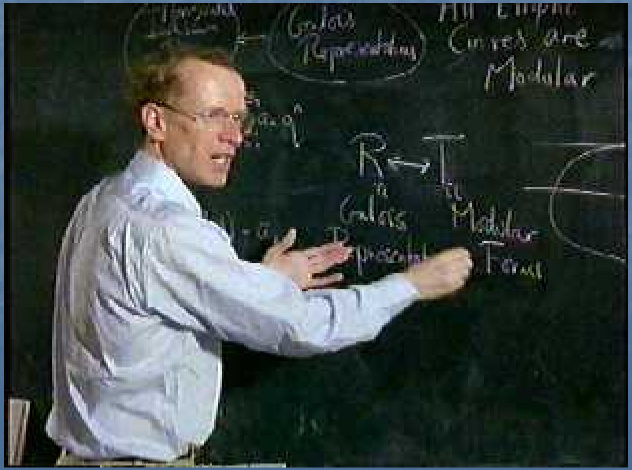




Kenneth A. Ribet

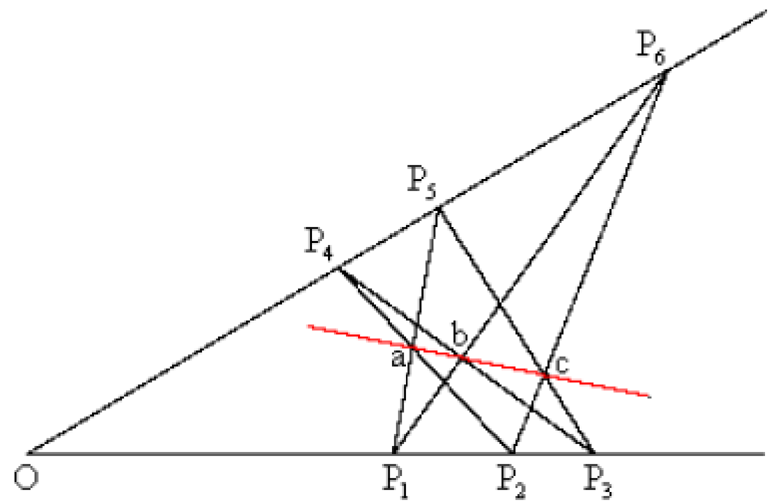


FLT solved in 1995.

# Pappus's theorem

- Pappus (c. 300 CE) is considered the last great geometer of the Alexandrian school before it was destroyed.
- His geometric theorem is a precursor to the theory of elliptic curves.



# A simple proof using co-ordinate geometry

- Using Cartesian co-ordinates, one can give a simple, but a bit tedious proof.

An explicit analytical demonstration of this theorem by determining the coordinates of the points a,b,c is straight-forward, but algebraically less trivial than one might expect. Let $x_i, y_i$ denote the coordinates of the point $P_i$, and note that $y_i = 0$ for $i = 1,2,3$ and $y_i = kx_i$ for $i = 4,5,6$ where k signifies the slope of the line $OP_6$. (We have drawn the line $OP_3$ along the x axis for convenience, but we can obviously rotate the entire figure without affecting the co-linearity of any set of points.) The coordinates $x_a, y_a$ of point a satisfy the conditions

$$\frac{y_a}{x_a - x_1} = \frac{kx_5}{x_5 - x_1} \quad \text{and} \quad \frac{y_a}{x_2 - x_a} = \frac{kx_4}{x_2 - x_4}$$

# We can solve for $x_a$ and $y_a$:

$$x_a = \frac{x_2x_4x_5 - x_1x_4x_5 + x_1x_2x_5 - x_1x_2x_4}{x_2x_5 - x_1x_4} \qquad y_a = \frac{x_2x_4x_5 - x_1x_4x_5}{x_2x_5 - x_1x_4}k$$

- Put $u_i = 1/x_i$. Then,

$$x_a = \frac{u_1 - u_2 + u_4 - u_5}{u_1u_4 - u_2u_5} \qquad y_a = \frac{u_1 - u_2}{u_1u_4 - u_2u_5}k$$

$$x_b = \frac{u_1 - u_3 + u_4 - u_6}{u_1u_4 - u_3u_6} \qquad y_b = \frac{u_1 - u_3}{u_1u_4 - u_3u_6}k$$

$$x_c = \frac{u_2 - u_3 + u_5 - u_6}{u_2u_5 - u_3u_6} \qquad y_c = \frac{u_2 - u_3}{u_2u_5 - u_3u_6}k$$

# The condition for collinearity

- The condition for collinearity of the points a,b,c is:

$$\frac{y_a - y_b}{x_a - x_b} = \frac{y_b - y_c}{x_b - x_c}$$

This is now easily verified with the above formulas.