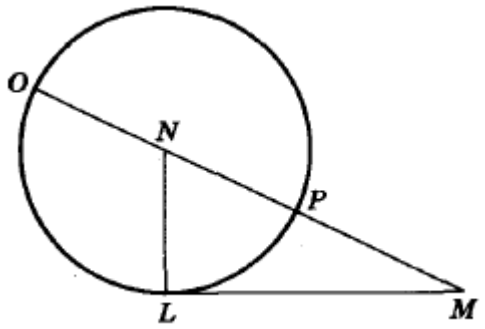
Pascal, Fermat and Descartes

Descartes and Analytic Geometry

- Rene Descartes (1596-1650) discovered analytic geometry. The essential idea was to study geometry through co-ordinatization. Today, we speak of the x-y axis as the Cartesian co-ordinate plane.
- In his work, Discours de la méthode, he opens with the statement that ``any problem in geometry can easily be reduced to such terms that a knowledge of the lengths of certain lines is sufficient for its construction.''
- We saw this method in our proof of Pappus's theorem.

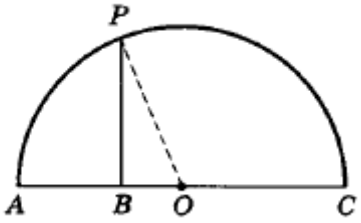
Descartes' geometric solution of quadratic equations

- To solve the equation $z^2 = az + b^2$, Descartes proceeded geometrically as follows and assumed that a, b were both positive.
- He first constructed a line segment LM of length b.
- At L he erected a perpendicular line segment LN of length a/2.
- With center N and radius a/2, he drew a circle. Then extending the line segment MN so that it intersects the circle at O, we find that OM is the desired root z.
- Since the sum of the roots is a, the other root is z-a.
- But Descartes ignored this root because it is negative!



Two problems of antiquity

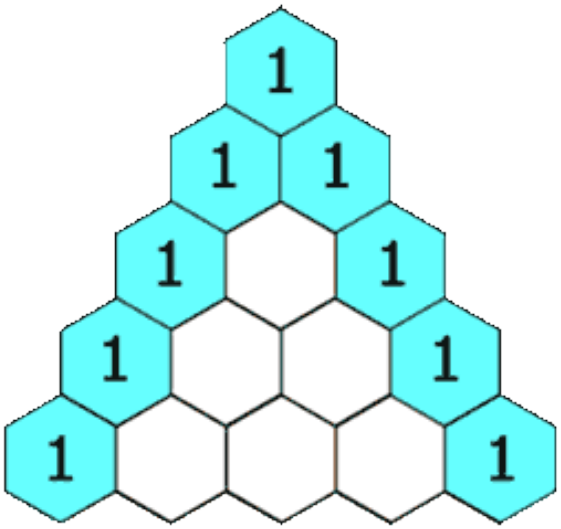
- Descartes was aware that his new method of "geometric algebra" can shed light on some of the classical problems such as trisecting a given angle using straightedge and compass, or doubling the cube.
- Both problems lead to cubic equations, a fact already known to Viete. He then stated without any proof that neither of these problems can be solved using straightedge and compass..
- What he may have discovered using his Cartesian co-ordinate methods is the fact that if a line segment of length x is constructible then so is $\sqrt{x}$.
- The proof can be deduced from the diagram using the Pythagorean theorem.

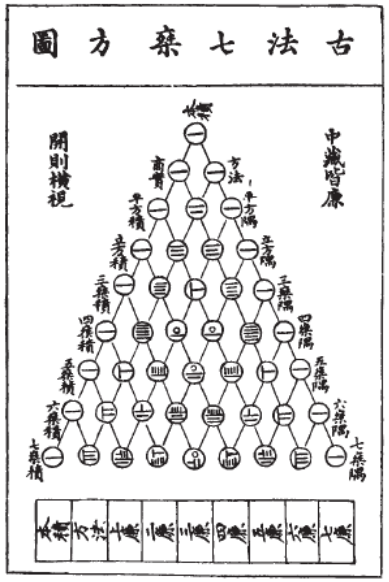


Let AB have length 1.
Let BC have length x.
Then, BP has length $\sqrt{x}$.
Thus, given x, to construct a line segment of length $\sqrt{x}$, we need only construct a circle of radius (x+1)/2 centered at O, mark off one unit from A at B and draw a perpendicular at B.

Blaise Pascal (1623-1662)

- Pascal was a contemporary of Descartes and wrote extensively on mathematics, philosophy and religion. He suffered from frail health throughout his life and died at a young age.
- In mathematics, he is known for his famous "triangle" as well as his work in elementary probability theory.





A page from the Book of Chu Shih Chieh's book "The Precious Mirror of Four Elements" written in 1303.

The binomial theorem

- Pascal's triangle is related to the binomial theorem:

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

Important observation: if p is prime, all the binomial coefficients in the expansion of $(a+b)^p$ are divisible by p, except for the first and the last, are divisible by p:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
and so on

$$(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

Fermat and his conjectures

- Pierre de Fermat (1601-1665) was a lawyer by day and an amateur mathematician by night.
- He made many conjectures in number theory the most famous being his "marginal note" called Fermat's Last Theorem, solved only in 1995 by Andrew Wiles, as a culmination of major developments in 20th century mathematics.

A brief chronology of FLT

1637	Fermat makes his conjecture and proves it for $n = 4$.
1753	Euler proves FLT for $n = 3$ (his proof has a fixable error).
1800s	Sophie Germain proves FLT for $n \nmid xyz$ for all $n < 100$.
1825	Dirichlet and Legendre complete the proof for $n = 5$.
1839	Lamé addresses $n = 7$.
1847	Kummer proves FLT for all primes $n \nmid h(\mathbb{Q}(\zeta_n))$, called *regular* primes. This leaves 37, 59, and 67 as the only open cases for $n < 100$.
1857	Kummer addresses 37, 59, and 67, but his proof has gaps.
1926	Vandiver fills the gaps and addresses all irregular primes $n < 157$.
1937	Vandiver and assistants handle all irregular primes $n < 607$.
1954	Lehmer, Lehmer, and Vandiver introduce techniques better suited to mechanical computation and use a computer to address all $n < 2521$.
1954-1993	Computers verify FLT for all $n < 4,000,000$.

- In 1972, Hellegouarch suggested a connection between elliptic curves and FLT. In 1984, Gerhard Frey made the connection to Taniyama's conjecture.
- In 1987, Serre made his famous epsilon conjecture, if proved, would show that Taniyama's conjecture implies FLT. The epsilon conjecture was proved by Ken Ribet in 1995. Shortly after, Wiles proved the Taniyama conjecture which from Ribet's work, implies FLT.

Fermat's little theorem (1640)

- Fermat's little theorem is the assertion that if p is a prime then p divides a^p-a for any number a.
- The result is clear if p divides a. So let us suppose that p is coprime to a.
- The non-zero residue classes mod p are represented by 1, 2, …, (p-1). The numbers a, 2a, …, (p-1)a are also distinct non-zero residue classes (mod p) and so (p-1)! $\equiv a^{p-1}$ (p-1)! (mod p) so the theorem is now immediate.
- However, Fermat never wrote up a proof though he claimed he had one.
- One can derive it by induction as follows. For a=1, the result is obvious.
- Assume the result has been proved for (a-1). Then, writing a= (a-1)+1, we see that a^p= ((a-1) + 1)^p which can now be expanded using the binomial theorem and noting that all the binomial coefficients apart from the first and last one are divisible by p.
- This proof using binomial coefficients was given almost a century later by Euler in 1742.

Euler's generalization (1750)

- Eight years after his proof using binomial coefficients, Euler obtained in 1750 a generalization of Fermat's theorem which was to have far reaching implications, such as RSA cryptography developed in the 20th century.
- If m is any natural number, and $\varphi(m)$ is the number of residue classes coprime to m, then for any a coprime to m, we have $a^{\varphi(m)} \equiv 1 \pmod{m}$.
- The earlier proof generalizes: if $r_1, \ldots, r_t$ are the coprime residue classes with $t=\varphi(m)$, $ar_1, \ldots, ar_t$ is again a permutation of the coprime residue classes. Thus the two products are congruent (mod m) and the result is now immediate.
- This result allowed Euler to disprove a famous conjecture of Fermat regarding what are now called Fermat numbers.

Fermat's conjecture

- A Fermat number is a number of the form:

$$F_n = 2^{2^n} + 1$$

Fermat conjectured that all these numbers are prime numbers. Here are the first five:

5, 17, 257, 65537, 4294967297,

Fermat checked his conjecture for the first four, but the last one may have been too big a number for him to deal with.

Euler's counterexample

- In 1732, Euler proved that:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

Here is the proof:

The fact that 641 is a factor of F_5 can be deduced from the equalities $641 = 2^7 \times 5 + 1$ and $641 = 2^4 + 5^4$. It follows from the first equality that $2^7 \times 5 \equiv -1 \pmod{641}$ and therefore (raising to the fourth power) that $2^{28} \times 5^4 \equiv 1 \pmod{641}$. On the other hand, the second equality implies that $5^4 \equiv -2^4 \pmod{641}$. These congruences imply that $-2^{32} \equiv 1 \pmod{641}$.

No more Fermat primes are known. It is conjectured that there are only finitely many Fermat primes.

How would Euler have guessed this factor for F_5 ?

- Let p be a prime factor of $2^a + 1$. Then 2a is the order of 2 (mod p).
- This means that 2a divides p-1 (Exercise)
- We apply this to a=32, so that any prime p dividing $2^{32} + 1$ has to be of the form 64k+1.
- It is now a question of checking k=1, 2, …, 10 which is not a tedious computation.

Fermat's letter to Pascal (1654)

- In a letter written in 1654, Fermat tried to interest Pascal in number theory and formulated the following problems (which were not solved until the 19th century):

Every integer is composed of one, two, or three triangular numbers, of one, two, three, or four squares, of one, two, three, four, or five pentagons, of one, two, three, four, five, or six hexagons, and thus to infinity.

This is the precursor of what later would be called Waring's problem of representing natural numbers as a sum of fixed number of k-th powers.