The world of $\Delta\iota o\phi\alpha\nu\tau o\varsigma$

B.Sury
Indian Statistical Institute
Bangalore, India
sury@isibang.ac.in; surybang@gmail.com
https:www.isibang.ac.in/ sury

Celebrating Pi Day 2025
IIT Roorkee


Terrace 428 - the highes


z
a


VOL-YUM =
pi zz a

Diophantus of Alexandria, Egypt lived during the 3rd century AD. Here he is:

Diophantus of Alexandria, Egypt lived during the 3rd century AD. Here he is:

Диофант из Александрии
(Diophantus of Alexandria, Διοφαντος ο Αλεξανδρευς)
(гг. рождения и смерти неизвестны, вероятно, 200/214 - 284/298 гг.)

Metrodorus indicated the life span of Diophantus through a puzzle poetically as:

Metrodorus indicated the life span of Diophantus through a puzzle poetically as:
'Here lies Diophantus,' the wonder behold.
Through art algebraic, the stone tells how old:
'God gave him his boyhood one-sixth of his life,
One twelfth more as youth while whiskers grew rife;
And then yet one-seventh ere marriage begun;
In five years there came a bouncing new son.
Alas, the dear child of master and sage
after attaining half the measure of his father's life chill fate took him.
After consoling his fate by the science of numbers for four years, he ended his life.'

Metrodorus indicated the life span of Diophantus through a puzzle poetically as:
'Here lies Diophantus,' the wonder behold.
Through art algebraic, the stone tells how old:
'God gave him his boyhood one-sixth of his life,
One twelfth more as youth while whiskers grew rife;
And then yet one-seventh ere marriage begun;
In five years there came a bouncing new son.
Alas, the dear child of master and sage
after attaining half the measure of his father's life chill fate took him.
After consoling his fate by the science of numbers for four years, he ended his life.'
This puzzle implies that Diophantus's age $x = 84$ is a solution of the equation

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4.$$

Diophantus was interested in solving polynomial equations in many variables where he sought solutions in integers or, more generally, in rational numbers.

Diophantus was interested in solving polynomial equations in many variables where he sought solutions in integers or, more generally, in rational numbers.
He wrote a number of books titled '*Arithmetica*' many of which have got lost.

Diophantus was interested in solving polynomial equations in many variables where he sought solutions in integers or, more generally, in rational numbers.
He wrote a number of books titled '*Arithmetica*' many of which have got lost.
The amateur mathematician Pierre de Fermat had, in his copy of Bachet's translation of Diophantus's *Arithmetica*, made a famous marginal note which came to be known as Fermat's last theorem.

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

Waring conjectured (in 1770)

Waring conjectured (in 1770)
Every positive integer N is a sum of at the most 9 cubes of positive integers -

Waring conjectured (in 1770)
Every positive integer N is a sum of at the most 9 cubes of positive integers -
proved by Wieferich (1909) and Kempner (1912).

Waring conjectured (in 1770)
Every positive integer N is a sum of at the most 9 cubes of positive integers -
proved by Wieferich (1909) and Kempner (1912).

In fact, if N is large enough, 7 cubes suffice (Linnik 1942); can 7 be reduced to 6 or 5 or 4? -

Waring conjectured (in 1770)
Every positive integer N is a sum of at the most 9 cubes of positive integers -
proved by Wieferich (1909) and Kempner (1912).

In fact, if N is large enough, 7 cubes suffice (Linnik 1942); can 7 be reduced to 6 or 5 or 4? -

unknown.

Allow cubes of negative integers also; then 5 cubes suffice but it is as yet unknown if 4 cubes suffice.

Allow cubes of negative integers also; then 5 cubes suffice but it is as yet unknown if 4 cubes suffice.

Therefore, the problem as to which integers are sums of three integer cubes becomes very interesting.

Regarding this, by 2021, the only two elusive cases of 33 and 42 remained among the numbers up to 100.

Regarding this, by 2021, the only two elusive cases of 33 and 42 remained among the numbers up to 100.
Finally settled by Andrew Booker from Bristol, and Andrew Sutherland from MIT - authorities on parallel computations.

Regarding this, by 2021, the only two elusive cases of 33 and 42 remained among the numbers up to 100.
Finally settled by Andrew Booker from Bristol, and Andrew Sutherland from MIT - authorities on parallel computations.

They used 'Charity Engine', a world-wide computer that harnessed idle, unused computing power from over 500000 home PCs to create a crowd-sourced platform.

The most difficult case of 42 resolved using a computing platform reminiscent of ‘Deep Thought’, the giant machine which gave the answer 42 in Douglas Adams’s Hitchhiker’s Guide to the Galaxy.

The most difficult case of 42 resolved using a computing platform reminiscent of ‘Deep Thought’, the giant machine which gave the answer 42 in Douglas Adams’s Hitchhiker’s Guide to the Galaxy.

The Earth was actually a giant supercomputer, created by another supercomputer, Deep Thought.

The most difficult case of 42 resolved using a computing platform reminiscent of ‘Deep Thought’, the giant machine which gave the answer 42 in Douglas Adams’s Hitchhiker’s Guide to the Galaxy.

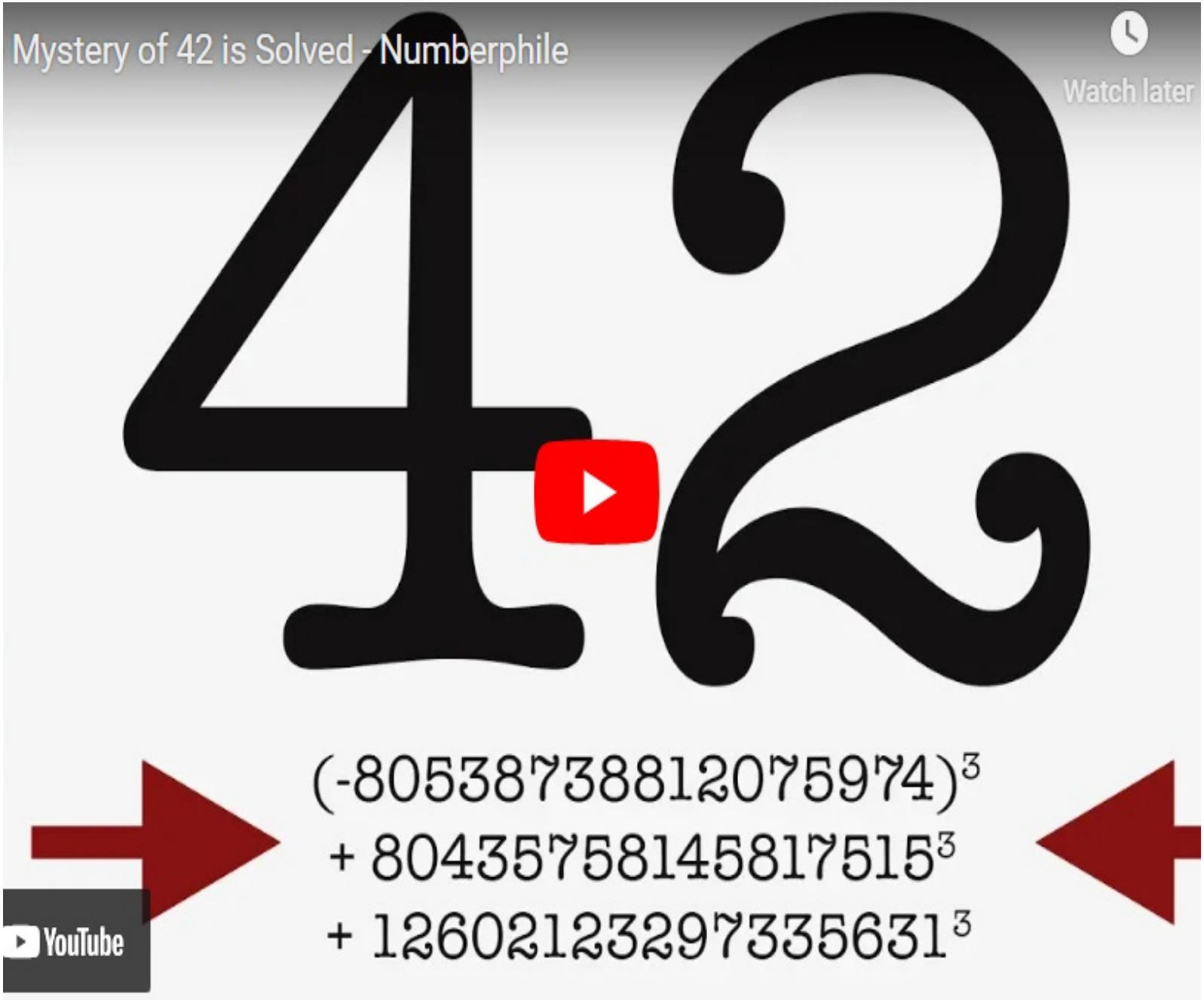
The Earth was actually a giant supercomputer, created by another supercomputer, Deep Thought.
‘Deep Thought’ built by its creators to give the answer to the “Ultimate Question of Life, the Universe, and Everything”.

The most difficult case of 42 resolved using a computing platform reminiscent of ‘Deep Thought’, the giant machine which gave the answer 42 in Douglas Adams’s Hitchhiker’s Guide to the Galaxy.

The Earth was actually a giant supercomputer, created by another supercomputer, Deep Thought.
‘Deep Thought’ built by its creators to give the answer to the “Ultimate Question of Life, the Universe, and Everything”.
After eons of calculations, the answer was given simply as “42”.

The most difficult case of 42 resolved using a computing platform reminiscent of ‘Deep Thought’, the giant machine which gave the answer 42 in Douglas Adams’s Hitchhiker’s Guide to the Galaxy.

The Earth was actually a giant supercomputer, created by another supercomputer, Deep Thought.
‘Deep Thought’ built by its creators to give the answer to the “Ultimate Question of Life, the Universe, and Everything”.
After eons of calculations, the answer was given simply as “42”.
Deep Thought was then instructed to design the Earth supercomputer to determine what the Question actually is!


Mystery of 42 is Solved - Numberphile
Watch later
42
$(-80538738812075974)^3$
$+ 80435758145817515^3$
$+ 12602123297335631^3$
YouTube


569936821221962380720^3
+
$(-569936821113563493509)^3$
+
$(-472715493453327032)^3$
=
3

Challenge for the clairvoyant

"It occurs to me that these sorts of questions would be excellent challenge questions to pose to any psychics who claim to be in contact with super-intelligent aliens, since the solutions are already expected to be produced by computer search in a few years but would be instantly verifiable evidence of some extraordinary computational or intellectual resource if produced sooner".

Everyone must have heard of the famous taxicab number 1729 and Ramanujan's story thanks to Mahalanobis, who was a contemporary of Ramanujan at Cambridge.

Everyone must have heard of the famous taxicab number 1729 and Ramanujan's story thanks to Mahalanobis, who was a contemporary of Ramanujan at Cambridge.

The Ramanujan taxicab number concerns the Diophantine equation $x^3 + y^3 = 1729$ for which Ramanujan observed two integer solutions; $(12, 1)$ and $(10, 9)$ are the only ones.

Everyone must have heard of the famous taxicab number 1729 and Ramanujan's story thanks to Mahalanobis, who was a contemporary of Ramanujan at Cambridge.

The Ramanujan taxicab number concerns the Diophantine equation $x^3 + y^3 = 1729$ for which Ramanujan observed two integer solutions; $(12, 1)$ and $(10, 9)$ are the only ones.

However, what may not be so well-known is that it has infinitely many rational solutions. For instance, if u, v is a solution, then so is $U = u(u^3 - 3458)/(1729 - 2u^3)$ and $V = v(u^3 + 1729)/(1729 - 2u^3)$.

Determining which integers n are sums of two rational cubes, has a rich history tracing back to Sylvester.

Determining which integers n are sums of two rational cubes, has a rich history tracing back to Sylvester.

Sylvester predicted that:

Determining which integers n are sums of two rational cubes, has a rich history tracing back to Sylvester.

Sylvester predicted that:
primes $p \equiv 2, 5 \pmod 9$ are not sums of two rational cubes,

Determining which integers n are sums of two rational cubes, has a rich history tracing back to Sylvester.

Sylvester predicted that:
primes $p \equiv 2, 5 \pmod 9$ are not sums of two rational cubes,
primes $p \equiv 4, 7, 8 \pmod 9$ are sums of two rational cubes.

Determining which integers n are sums of two rational cubes, has a rich history tracing back to Sylvester.

Sylvester predicted that:
primes $p \equiv 2, 5 \pmod 9$ are not sums of two rational cubes,
primes $p \equiv 4, 7, 8 \pmod 9$ are sums of two rational cubes.
In contrast, primes $p \equiv 1 \pmod 9$ may or may not be sums of two rational cubes.

The notion of Diophantine approximation arises in many situations - we briefly mention one, where π occurs.

The notion of Diophantine approximation arises in many situations - we briefly mention one, where π occurs.

Here is a routine-looking question? Is the infinite series $\sum \frac{1}{n^3 \sin^2(n)}$ convergent?

The notion of Diophantine approximation arises in many situations - we briefly mention one, where π occurs.

Here is a routine-looking question? Is the infinite series $\sum \frac{1}{n^3 \sin^2(n)}$ convergent?

The convergence of the series depends on the behavior of the sequence $n|\sin(n)|$ as $n \to \infty$ and, this is mysterious. It depends on something unknown as yet - how well can π be approximated by rational numbers?

The *irrationality measure* $\mu(\alpha)$ of an irrational number α is the infimum of all $a > 0$ such that the inequality $|\alpha - p/q| < 1/q^a$ has only finitely many solutions p, q.

The *irrationality measure* $\mu(\alpha)$ of an irrational number α is the infimum of all $a > 0$ such that the inequality $|\alpha - p/q| < 1/q^a$ has only finitely many solutions p, q.

The Dirichlet box principle implies that $\mu(\alpha) \geq 2$ and generically (that is, almost all) α have $\mu(\alpha) = 2$.

The *irrationality measure* $\mu(\alpha)$ of an irrational number α is the infimum of all $a > 0$ such that the inequality $|\alpha - p/q| < 1/q^a$ has only finitely many solutions p, q.

The Dirichlet box principle implies that $\mu(\alpha) \geq 2$ and generically (that is, almost all) α have $\mu(\alpha) = 2$.

For a specific number, it is difficult to find μ; for instance, $\mu(e) = 2$ but, the constant $\mu(\pi)$ is still unknown.

One knows $\mu(\pi) < 8$ but not much more is known.

One knows $\mu(\pi) < 8$ but not much more is known.

Here is the shocker - the series $\sum \frac{1}{n^3 \sin^2(n)}$ diverges if $\mu(\pi) > 5/2$ and converges if, $\mu(\pi) < 5/2$. So, take your pick!

Many problems of mathematics can be formulated as seeking solutions of certain Diophantine equations. In fact, in a sense of mathematical logic, every problem can be so formulated!

Many problems of mathematics can be formulated as seeking solutions of certain Diophantine equations. In fact, in a sense of mathematical logic, every problem can be so formulated!

Hilbert's famous 10th problem asserted: *Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Many problems of mathematics can be formulated as seeking solutions of certain Diophantine equations. In fact, in a sense of mathematical logic, every problem can be so formulated!

Hilbert's famous 10th problem asserted: *Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Theorem (Davis-Putnam-Robinson-Matiyasevich) There is no general algorithm that, given any Diophantine equation, decides whether it has solutions in positive integers or not. In more technical terms, the notions of 'effectively enumerable' sets and 'Diophantine' sets coincide.

a to z

The ideas appearing in the resolution of the 10th problem yield interesting implications such as:

a to z

The ideas appearing in the resolution of the 10th problem yield interesting implications such as:

The set of positive values of the following polynomial in 26 variables when the variables take positive integer values, equals the set of prime numbers!

$$
\begin{aligned}
(k+2)\{\quad 1 \quad & -[wz+h+j-q]^2 \\
& -[(gk+2g+k+1)(h+j)+h-z]^2 \\
& -[2n+p+q+z-e]^2 \\
& -\left[16(k+1)^3(k+2)(n+1)^2+1-f^2\right]^2 \\
& -\left[e^3(e+2)(a+1)^2+1-o^2\right]^2 \\
& -\left[(a^2-1)y^2+1-x^2\right]^2 \\
& -\left[16r^2y^4(a^2-1)+1-u^2\right]^2-[n+l+v-y]^2 \\
& -\left[\left((a+u^2(u^2-a))^2-1\right)(n+4dy)^2+1-(x+cu)^2\right]^2 \\
& -\left[(a^2-1)l^2+1-m^2\right]^2 \\
& -\left[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\right]^2 \\
& -\left[z+pl(a-p)+t(2ap-p^2-1)-pm\right]^2 \\
& -[ai+k+1-l-i]^2 \\
& -\left[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\right]^2\ \}
\end{aligned}
$$

There are several questions like Fermat's last theorem asserting the nonexistence of solutions in positive integers of the equations $x^n + y^n = z^n$ for $n > 2$ (which is solved now),

There are several questions like Fermat's last theorem asserting the nonexistence of solutions in positive integers of the equations $x^n + y^n = z^n$ for $n > 2$ (which is solved now),

Catalan's conjecture asserting that the only solution in positive integers of $x^m - y^n - 1$ is $x = 3, m = 2, y = 2, n = 2$ (which is also solved now)

There are several questions like Fermat's last theorem asserting the nonexistence of solutions in positive integers of the equations $x^n + y^n = z^n$ for $n > 2$ (which is solved now),

Catalan's conjecture asserting that the only solution in positive integers of $x^m - y^n - 1$ is $x = 3, m = 2, y = 2, n = 2$ (which is also solved now)

which require very different techniques; we will say more about them in a while but first, let us discuss a more elementary problem.

Think of a fruit-seller arranging her fruits in a triangular pattern in the morning and in a square pattern in the evening.

Think of a fruit-seller arranging her fruits in a triangular pattern in the morning and in a square pattern in the evening.

Can she do both of these with the same number of fruits?

Think of a fruit-seller arranging her fruits in a triangular pattern in the morning and in a square pattern in the evening.

Can she do both of these with the same number of fruits?

For instance, if he has 36 fruits, he can do this because $6^2 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8$.

Think of a fruit-seller arranging her fruits in a triangular pattern in the morning and in a square pattern in the evening.

Can she do both of these with the same number of fruits?

For instance, if he has 36 fruits, he can do this because $6^2 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8$.

Which other squares are so expressible as 'triangular numbers'?

If $n^2 = 1 + 2 + \cdots + k = k(k+1)/2$, then

If $n^2 = 1 + 2 + \cdots + k = k(k+1)/2$, then
$8n^2 = 4k(k+1) = (2k+1)^2 - 1$

If $n^2 = 1 + 2 + \cdots + k = k(k+1)/2$, then
$8n^2 = 4k(k+1) = (2k+1)^2 - 1$
Thus, $(2k+1, 2n)$ is a solution of the equation $x^2 - 2y^2 = 1$.

If $n^2 = 1 + 2 + \cdots + k = k(k+1)/2$, then
$8n^2 = 4k(k+1) = (2k+1)^2 - 1$
Thus, $(2k+1, 2n)$ is a solution of the equation $x^2 - 2y^2 = 1$.

Being aesthetically-minded fruit-sellers, all of us of course want to know what the solutions of $x^2 - 2y^2 = 1$ are !

Here is another instance when the above equation occurs and involves Ramanujan:

December 22, 1887 to April 26, 1920

December 22, 1887 to April 26, 1920

In the Strand magazine, Mahalanobis had seen the following problem which he mentioned to Ramanujan:

In the Strand magazine, Mahalanobis had seen the following problem which he mentioned to Ramanujan:
Imagine that you are on a street with houses marked 1 through n. There is a house in between such that the sum of the house numbers to the left of it equals the sum of the house numbers to its right. If n is between 50 and 500, what are n and the house number?

In the Strand magazine, Mahalanobis had seen the following problem which he mentioned to Ramanujan:
Imagine that you are on a street with houses marked 1 through n. There is a house in between such that the sum of the house numbers to the left of it equals the sum of the house numbers to its right. If n is between 50 and 500, what are n and the house number?

Ramanujan thought for a moment and replied "Take down the solution" and dictated a continued fraction saying that it contained the solution!

In the Strand magazine, Mahalanobis had seen the following problem which he mentioned to Ramanujan:
Imagine that you are on a street with houses marked 1 through n. There is a house in between such that the sum of the house numbers to the left of it equals the sum of the house numbers to its right. If n is between 50 and 500, what are n and the house number?

Ramanujan thought for a moment and replied "Take down the solution" and dictated a continued fraction saying that it contained the solution!

Evidently, Ramanujan wanted to have some fun instead of directly giving the answer! So, what is behind this?

If the house number is r, then we have

$$1 + 2 + \cdots + (r-1) = (r+1) + \cdots + n$$

If the house number is r, then we have

$$1 + 2 + \cdots + (r-1) = (r+1) + \cdots + n$$

The LHS is $\frac{(r-1)r}{2}$ and if we add $1 + 2 + \cdots + r = \frac{r(r+1)}{2}$ to both sides, we have:

If the house number is r, then we have

$$1 + 2 + \cdots + (r-1) = (r+1) + \cdots + n$$

The LHS is $\frac{(r-1)r}{2}$ and if we add $1 + 2 + \cdots + r = \frac{r(r+1)}{2}$ to both sides, we have:

$r^2 = \frac{n(n+1)}{2}$.

If the house number is r, then we have

$$1 + 2 + \cdots + (r-1) = (r+1) + \cdots + n$$

The LHS is $\frac{(r-1)r}{2}$ and if we add $1 + 2 + \cdots + r = \frac{r(r+1)}{2}$ to both sides, we have:

$r^2 = \frac{n(n+1)}{2}$.

Multiplying by 8 and adding 1, we have $8r^2 + 1 = (2n+1)^2$, the very same equation encountered by the fruit-seller!

One can similarly look at $m^2 - dn^2$ for any square-free positive integer d.

One can similarly look at $m^2 - dn^2$ for any square-free positive integer d.
Can it take the value 1? Can it take the value -1? How many solutions are there?

One can similarly look at $m^2 - dn^2$ for any square-free positive integer d.
Can it take the value 1? Can it take the value -1? How many solutions are there?
This rich area of mathematics is popularly (and erroneously!) known as the theory of the Pell equations.

One can similarly look at $m^2 - dn^2$ for any square-free positive integer d.
Can it take the value 1? Can it take the value -1? How many solutions are there?
This rich area of mathematics is popularly (and erroneously!) known as the theory of the Pell equations.
Interestingly, it turns out that there are infinitely many pairs m, n for which $m^2 - dn^2 = 1$ and essentially, they are all generated from a single pair.

The ancient Indian mathematicians (especially Brahmagupta, Bhaskara II and Jayadeva) studied the equations $x^2 - dy^2 = \pm 1$ and solved them!

The ancient Indian mathematicians (especially Brahmagupta, Bhaskara II and Jayadeva) studied the equations $x^2 - dy^2 = \pm 1$ and solved them!
What is more - they gave an algorithm (the so-called Chakravala or cyclic method) which produces all the solutions.

Brahmagupta lived during 598-670 AD

Bhaskaracharya lived from 1114 to 1185 AD.

In 1657, Fermat, writing to his friend Frenicle, he posed "to the English mathematicians and all others" the problem of finding a solution of $x^2 - Ny^2 = 1$ "pour ne vous donner pas trop de peine" like $N = 61,109$.

Fermat : August 17, 1601 to January 12, 1665

The 20th century great André Weil's comment on this was:

The 20th century great André Weil's comment on this was: "What would have been Fermat's astonishment if some missionary, just back from India, had told him that his problem had been successfully tackled there by native mathematicians almost six centuries earlier ?"

Andre Weil : May 6, 1906 to August 6, 1998

Indeed, in 1150 A.D., Bhaskara II gave the explicit solutions

$$1766319049^2 - 61(226153980)^2 = 1$$

$$158070671986249^2 - 109(15140424455100)^2 = 1!$$

Indeed, in 1150 A.D., Bhaskara II gave the explicit solutions

$$1766319049^2 - 61(226153980)^2 = 1$$

$$158070671986249^2 - 109(15140424455100)^2 = 1!$$

Indeed, Brahmagupta (598-665) had already solved this equation in 628 A.D. for several values like $N = 83$ and $N = 92$.

Indeed, in 1150 A.D., Bhaskara II gave the explicit solutions

$$1766319049^2 - 61(226153980)^2 = 1$$

$$158070671986249^2 - 109(15140424455100)^2 = 1!$$

Indeed, Brahmagupta (598-665) had already solved this equation in 628 A.D. for several values like $N = 83$ and $N = 92$.

Brahmagupta had remarked, "Kurvannaavatsaraad ganakah" - meaning (approximately), "*a person who is able to solve these within a year is truly a mathematician*"' !

The wrong attribution to Pell of these equations is due to the most prolific of mathematicians - Leonhard Euler, but the name has stuck.

The wrong attribution to Pell of these equations is due to the most prolific of mathematicians - Leonhard Euler, but the name has stuck.

In view of the above understanding of mathematical history, now the equations can better be referred to as the Brahmagupta-Pell equations.

- The Congruent Number Problem:

- The Congruent Number Problem:

A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.

• The Congruent Number Problem:
A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.
For example, $5, 6, 7$ are congruent numbers.

• The Congruent Number Problem:

A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.

For example, $5, 6, 7$ are congruent numbers.

Why?

• The Congruent Number Problem:

A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.

For example, $5, 6, 7$ are congruent numbers.

Why?

6 is easy from the usual $3, 4, 5$ triangle.

To see that 5 is a congruent number, consider the right-angled triangle with sides $3/2, 20/3, 41/6$.

To see that 5 is a congruent number, consider the right-angled triangle with sides $3/2, 20/3, 41/6$.
What about 7?

To see that 5 is a congruent number, consider the right-angled triangle with sides $3/2, 20/3, 41/6$.
What about 7?
Look at a right triangle with sides $35/12, 24/5, 337/60$.

To see that 5 is a congruent number, consider the right-angled triangle with sides $3/2, 20/3, 41/6$.
What about 7?
Look at a right triangle with sides $35/12, 24/5, 337/60$.
How did we guess this? More importantly, how do we decide if a given number is a congruent number?

To see that 5 is a congruent number, consider the right-angled triangle with sides $3/2, 20/3, 41/6$.
What about 7?
Look at a right triangle with sides $35/12, 24/5, 337/60$.
How did we guess this? More importantly, how do we decide if a given number is a congruent number?
This will be done by relating it to another problem!

Question. Can we have an arithmetic progression of three terms which are all squares of rational numbers and the common difference d?

Question. Can we have an arithmetic progression of three terms which are all squares of rational numbers and the common difference d?
That is, can $x^2 - d, x^2, x^2 + d$ be squares of rational numbers and x rational?

Question. Can we have an arithmetic progression of three terms which are all squares of rational numbers and the common difference d?
That is, can $x^2 - d, x^2, x^2 + d$ be squares of rational numbers and x rational?
The congruent number problem and the above question are equivalent!

Indeed, Let $u \leq v < w$ be the sides of a right triangle with rational sides.

Indeed, Let $u \leq v < w$ be the sides of a right triangle with rational sides.
Then $x = w/2$ is such that $(v-u)^2/4, w^2/4, (u+v)^2/4$ form an arithmetic progression.

Indeed, Let $u \leq v < w$ be the sides of a right triangle with rational sides.
Then $x = w/2$ is such that $(v-u)^2/4, w^2/4, (u+v)^2/4$ form an arithmetic progression.
Conversely, if $x^2 - d = y^2, x^2, x^2 + d = z^2$ are three rational squares in arithmetic progression, then:
$z - y, z + y$ are the legs of a right angled triangle with rational legs, area $(z^2 - y^2)/2 = d$ and rational hypotenuse $2x$ because $2(y^2 + z^2) = 4x^2$.

$1, 2, 3$ are not congruent numbers.

$1, 2, 3$ are not congruent numbers.
Why?

$1, 2, 3$ are not congruent numbers.
Why?
The fact that $1, 2$ are not congruent numbers is essentially equivalent to Fermat's last theorem for the exponent 4(!)

$1, 2, 3$ are not congruent numbers.
Why?
The fact that $1, 2$ are not congruent numbers is essentially equivalent to Fermat's last theorem for the exponent 4(!)
Indeed, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 1$ for some rational numbers a, b, c then $x = c/2, y = |a^2 - b^2|/4$ are rational numbers satisfying $y^2 = x^4 - 1$.

$1, 2, 3$ are not congruent numbers.
Why?
The fact that $1, 2$ are not congruent numbers is essentially equivalent to Fermat's last theorem for the exponent 4(!)
Indeed, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 1$ for some rational numbers a, b, c then $x = c/2, y = |a^2 - b^2|/4$ are rational numbers satisfying $y^2 = x^4 - 1$.
Similarly, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 2$ for rational numbers a, b, c, then $x = a/2, y = ac/4$ are rational numbers satisfying $y^2 = x^4 + 1$.

The equations $y^2 = x^4 \pm 1$ over rational numbers, reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat using the method of descent not to have nontrivial solutions.

The equations $y^2 = x^4 \pm 1$ over rational numbers, reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat using the method of descent not to have nontrivial solutions.
The un-solvability of $y^2 = x^4 \pm 1$ in rational numbers are exactly equivalent to showing $1, 2$ are not congruent.

The equations $y^2 = x^4 \pm 1$ over rational numbers, reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat using the method of descent not to have nontrivial solutions.
The un-solvability of $y^2 = x^4 \pm 1$ in rational numbers are exactly equivalent to showing $1, 2$ are not congruent.
In fact $y^2 = x^4 - 1$ for rational x, y gives a right-angled triangle with sides $y/x, 2x/y, (x^4 + 1)/xy$ and area 1.

The equations $y^2 = x^4 \pm 1$ over rational numbers, reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat using the method of descent not to have nontrivial solutions.

The un-solvability of $y^2 = x^4 \pm 1$ in rational numbers are exactly equivalent to showing $1, 2$ are not congruent.

In fact $y^2 = x^4 - 1$ for rational x, y gives a right-angled triangle with sides $y/x, 2x/y, (x^4 + 1)/xy$ and area 1.

Similarly, $y^2 = x^4 + 1$ for rational x, y gives a right-angled triangle with sides $2x, 2/x, 2y/x$ and area 2.

Here is a (rather unusual!) way of using the above fact that 1 is not a congruent number to show that $\sqrt{2}$ is irrational!

Here is a (rather unusual!) way of using the above fact that 1 is not a congruent number to show that $\sqrt{2}$ is irrational! Indeed, consider the right-angled triangle with legs $\sqrt{2}, \sqrt{2}$ and hypotenuse 2. If $\sqrt{2}$ were rational, this triangle would exhibit 1 as a congruent number!

Though it is an ancient problem to determine which natural numbers are congruent, it is only in late 20th century that substantial results were obtained and progress has been made which is likely to lead to its complete solution.

The rephrasing in terms of arithmetic progressions of squares emphasizes a connection of the problem with rational solutions of the equation $y^2 = x^3 - d^2x$.

The rephrasing in terms of arithmetic progressions of squares emphasizes a connection of the problem with rational solutions of the equation $y^2 = x^3 - d^2x$.
Such equations define "elliptic curves".

The rephrasing in terms of arithmetic progressions of squares emphasizes a connection of the problem with rational solutions of the equation $y^2 = x^3 - d^2x$.
Such equations define "elliptic curves".
It is easy to show that:
d is a congruent number if, and only if, the elliptic curve $E_d : y^2 = x^3 - d^2x$ has a solution with $y \neq 0$.

In fact, $a^2+b^2=c^2, \frac{1}{2}ab=d$ implies $bd/(c-a), 2d^2/(c-a)$ is a rational solution of $y^2=x^3-d^2x$.

In fact, $a^2 + b^2 = c^2, \frac{1}{2}ab = d$ implies $bd/(c-a), 2d^2/(c-a)$ is a rational solution of $y^2 = x^3 - d^2x$.
Conversely, a rational solution of $y^2 = x^3 - d^2x$ with $y \neq 0$ gives the rational, right-angled triangle with sides $(x^2 - d^2)/y, 2xd/y, (x^2 + d^2)/y$ and area d.

In fact, $a^2 + b^2 = c^2, \frac{1}{2}ab = d$ implies $bd/(c-a), 2d^2/(c-a)$ is a rational solution of $y^2 = x^3 - d^2x$.
Conversely, a rational solution of $y^2 = x^3 - d^2x$ with $y \neq 0$ gives the rational, right-angled triangle with sides $(x^2 - d^2)/y, 2xd/y, (x^2 + d^2)/y$ and area d.
In a nutshell, here is the reason we got this elliptic curve.

In fact, $a^2 + b^2 = c^2, \frac{1}{2}ab = d$ implies $bd/(c-a), 2d^2/(c-a)$ is a rational solution of $y^2 = x^3 - d^2x$.
Conversely, a rational solution of $y^2 = x^3 - d^2x$ with $y \neq 0$ gives the rational, right-angled triangle with sides $(x^2 - d^2)/y, 2xd/y, (x^2 + d^2)/y$ and area d.
In a nutshell, here is the reason we got this elliptic curve.
The real solutions of the equation $a^2 + b^2 = c^2$ defines a surface in 3-space and so do the real solutions of $\frac{1}{2}ab = d$.
The intersection of these two surfaces is a curve whose equation in suitable co-ordinates is the above curve!

The set of rational solutions of an elliptic curve over $\mathbf{Q}$ forms a group and, it is an easy fact from the way the group law is defined, that there is a solution with $y \neq 0$ if and only if there are infinitely many rational solutions.

The set of rational solutions of an elliptic curve over $\mathbf{Q}$ forms a group and, it is an easy fact from the way the group law is defined, that there is a solution with $y \neq 0$ if and only if there are infinitely many rational solutions.
Therefore, if d is a congruent number, there are infinitely many rational-sided right-angled triangles with area d(!)

The connection with elliptic curves has been used, more generally, to show that numbers which are $1, 2$ or 3 mod 8 are not congruent. This is rather deep.

The connection with elliptic curves has been used, more generally, to show that numbers which are $1, 2$ or 3 mod 8 are not congruent. This is rather deep.
Further, assuming the truth of a famous, deep, open conjecture known as the *weak Birch & Swinnerton-Dyer conjecture*, it has been shown that this is a complete characterization of congruent numbers!

The system of Diophantine equations that describes a rectangular box whose sides are X, Y, Z, face diagonals are U, V, W, and the long diagonal is T (with all these lengths rational) is:

The system of Diophantine equations that describes a rectangular box whose sides are X, Y, Z, face diagonals are U, V, W, and the long diagonal is T (with all these lengths rational) is:

$$X^2 + Y^2 = U^2, Y^2 + Z^2 = V^2,$$
$$Z^2 + X^2 = W^2, X^2 + Y^2 + Z^2 = T^2.$$

The system of Diophantine equations that describes a rectangular box whose sides are X, Y, Z, face diagonals are U, V, W, and the long diagonal is T (with all these lengths rational) is:

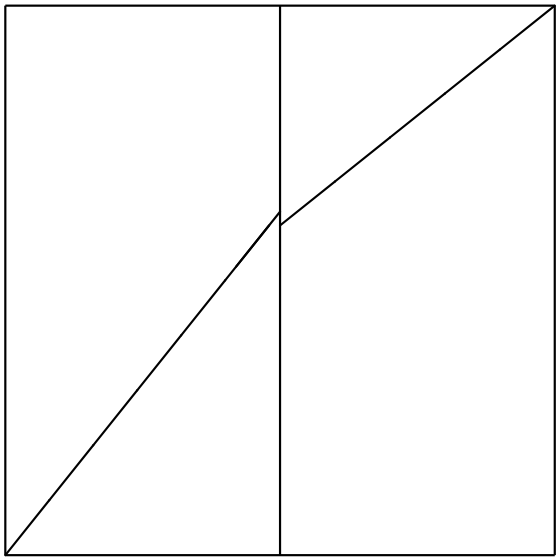
$$X^2 + Y^2 = U^2, Y^2 + Z^2 = V^2,$$
$$Z^2 + X^2 = W^2, X^2 + Y^2 + Z^2 = T^2.$$

No solutions are known.

Now, we discuss a natural problem which leads to a Diophantine equation discussed above.

Now, we discuss a natural problem which leads to a Diophantine equation discussed above.
Look at the figure below.

Now, we discuss a natural problem which leads to a Diophantine equation discussed above.
Look at the figure below.



The rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line.

The rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment of length r until the middle line is reached and the other of length s from that point to the opposite corner.

The rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment of length r until the middle line is reached and the other of length s from that point to the opposite corner. The question is whether we can follow such a path with both the distances r, s rational numbers.

The rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment of length r until the middle line is reached and the other of length s from that point to the opposite corner. The question is whether we can follow such a path with both the distances r, s rational numbers.
It is an easy exercise to prove that such a 'rational' walk is impossible because 1 is not a congruent number!

The fact that a product of $r > 1$ consecutive numbers can not be a perfect power was settled 50 years back by Erdös & Selfridge.

The fact that a product of $r > 1$ consecutive numbers can not be a perfect power was settled 50 years back by Erdös & Selfridge.

Erdös-Selfridge theorem is so simple to state that one may be tempted to think it could perhaps have an elementary proof.

The fact that a product of $r > 1$ consecutive numbers can not be a perfect power was settled 50 years back by Erdös & Selfridge.

Erdös-Selfridge theorem is so simple to state that one may be tempted to think it could perhaps have an elementary proof.

For instance, these are easy to observe when $r = 2, 3$.

The fact that a product of $r > 1$ consecutive numbers can not be a perfect power was settled 50 years back by Erdös & Selfridge.

Erdös-Selfridge theorem is so simple to state that one may be tempted to think it could perhaps have an elementary proof.

For instance, these are easy to observe when $r = 2, 3$.

However, for $r > 3$, the proof needs deeper properties of prime numbers, such as:

a classical theorem due to Sylvester which asserts that any set of k consecutive numbers with the smallest one $> k$ contains a multiple of a prime $> k$.

a classical theorem due to Sylvester which asserts that any set of k consecutive numbers with the smallest one $> k$ contains a multiple of a prime $> k$.

The special case of this when the numbers are $k+1, \cdots, 2k$ is known as Bertrand's postulate.

a classical theorem due to Sylvester which asserts that any set of k consecutive numbers with the smallest one $> k$ contains a multiple of a prime $> k$.

The special case of this when the numbers are $k+1, \cdots, 2k$ is known as Bertrand's postulate.

By the way, the product of any four consecutive integers is one less than a perfect square:

$$n(n+1)(n+2)(n+3) = (n^2+3n+1)^2 - 1.$$

Which natural numbers have all their digits to be 1 *with respect to two different bases?*

Which natural numbers have all their digits to be 1 *with respect to two different bases?*

Equivalently, solve

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

in natural numbers $x, y > 1; m, n > 2$.

For example 31 and 8191 have this property;

$$(11111)_2 = (111)_5 \quad , \quad (111)_{90} = 2^{13} - 1.$$

(Observed by Goormaghtigh nearly a century ago).

For example 31 and 8191 have this property;

$$(11111)_2 = (111)_5 \quad , \quad (111)_{90} = 2^{13} - 1.$$

(Observed by Goormaghtigh nearly a century ago).

However, it is still unknown whether there are only finitely many solutions in x, y, m, n. In fact, no other solutions are known.

For example 31 and 8191 have this property;

$$(11111)_2 = (111)_5 \quad , \quad (111)_{90} = 2^{13} - 1.$$

(Observed by Goormaghtigh nearly a century ago).

However, it is still unknown whether there are only finitely many solutions in x, y, m, n. In fact, no other solutions are known.

For any *fixed bases* x, y, it was proved only as recently as in 2002 that the number of solutions for m, n is at the most 2.

Another problem is:

- *Can one have different finite arithmetic progressions with the same product?*

Another problem is:

- *Can one have different finite arithmetic progressions with the same product?*

Note that

$$2.6 \cdots (4n-2) = (n+1)(n+2) \cdots (2n)$$

for all natural numbers n.

Another problem is:

- *Can one have different finite arithmetic progressions with the same product?*

Note that

$$2.6 \cdots (4n-2) = (n+1)(n+2) \cdots (2n)$$

for all natural numbers n.

Are there other solutions to the equation

$$x(x+d_1) \cdots (x+(m-1)d_1) = y(y+d_2) \cdots (y+(n-1)d_2)$$

where d_1, d_2 are positive rational numbers and $d_1 \neq d_2$ if $m = n$?

Another problem is:

- *Can one have different finite arithmetic progressions with the same product?*

Note that

$$2.6 \cdots (4n-2) = (n+1)(n+2) \cdots (2n)$$

for all natural numbers n.

Are there other solutions to the equation

$$x(x+d_1) \cdots (x+(m-1)d_1) = y(y+d_2) \cdots (y+(n-1)d_2)$$

where d_1, d_2 are positive rational numbers and $d_1 \neq d_2$ if $m = n$?

It is only in 1999 that using ideas from algebraic geometry, it was proved that if m, n, d_1, d_2 are fixed, then the equation has only finitely many solutions in integers apart from some exceptions which occur when $m = 2, n = 4$.

A deep conjecture due to Erdös in 1975 asserts that:

A deep conjecture due to Erdös in 1975 asserts that:

For each $c \in \mathbb{Q}$, the number of (x, y, m, n) satisfying

$$x(x+1)\cdots(x+m-1) = cy(y+1)\cdots(y+n-1)$$

with $y \geq x+m$, $\min(m, n) \geq 3$, is finite.

A deep conjecture due to Erdös in 1975 asserts that:

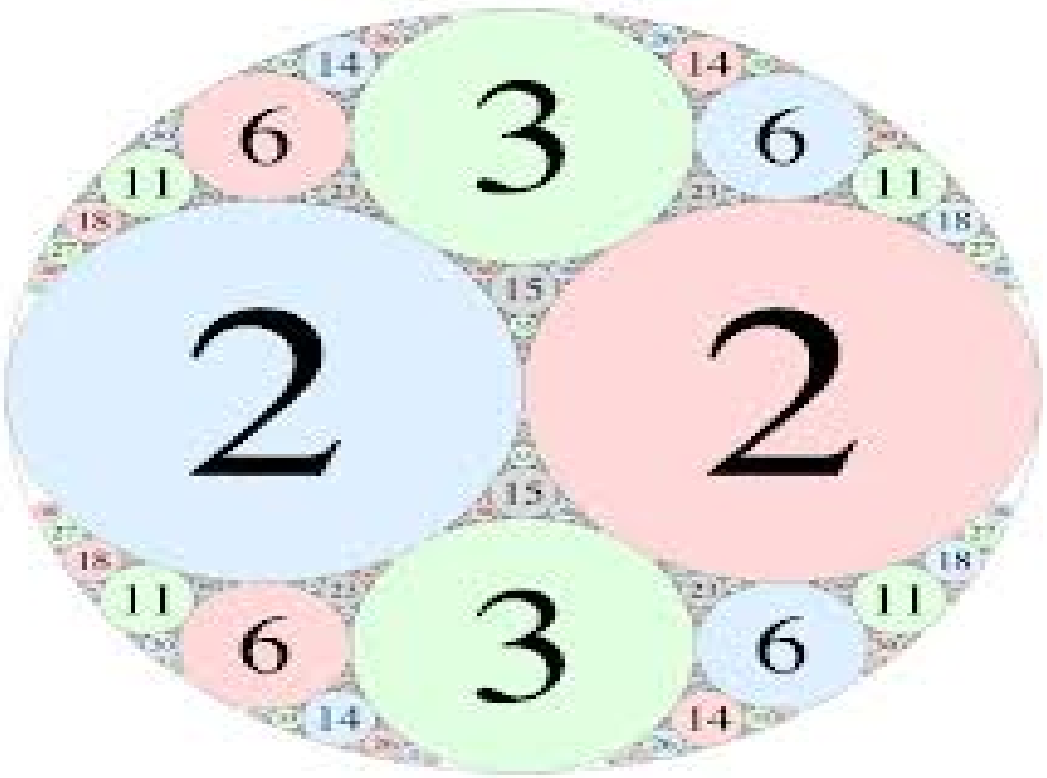
For each $c \in \mathbb{Q}$, the number of (x, y, m, n) satisfying

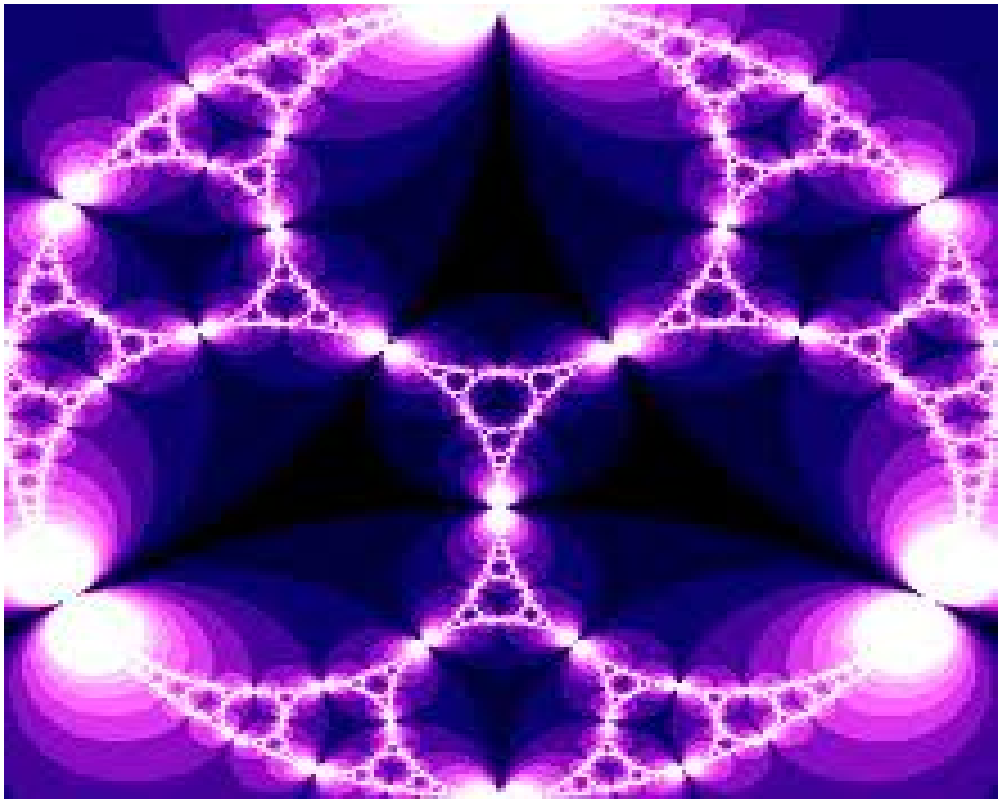
$$x(x+1)\cdots(x+m-1) = cy(y+1)\cdots(y+n-1)$$

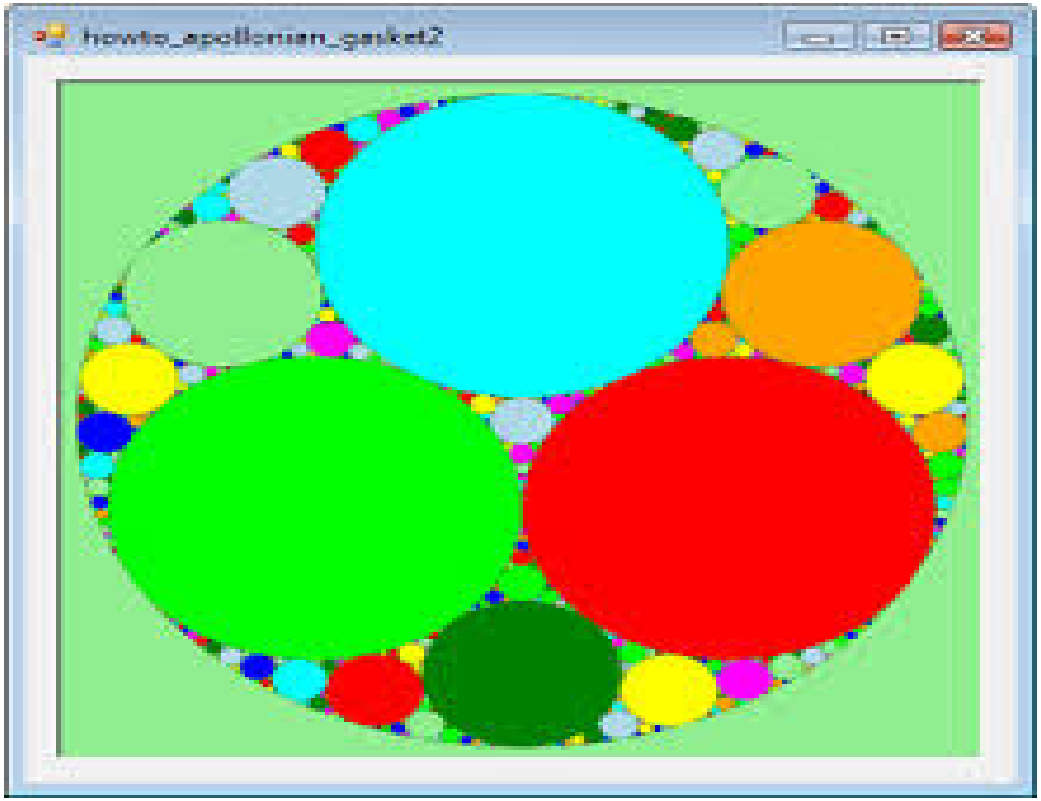
with $y \geq x+m$, $\min(m, n) \geq 3$, is finite.
This is unsettled as yet.

Apollonian circle packing

Apollonius from 200 BC discovered something beautiful.


14
6
3
14
6
11
11
18
18
15
2
2
15
18
18
11
11
6
3
6
14
14




howto_apollonian_gasket2

If we have three circles touching each other, one may place another circle touching all three.

If we have three circles touching each other, one may place another circle touching all three.
In the 17th century, Descartes discovered the remarkable fact that the radii satisfy the equation

If we have three circles touching each other, one may place another circle touching all three.
In the 17th century, Descartes discovered the remarkable fact that the radii satisfy the equation

$$\left(\sum_{i=1}^{4} \frac{1}{r_i} \right)^2 = 2 \sum_{i=1}^{4} \frac{1}{r_i^2}.$$

If we have three circles touching each other, one may place another circle touching all three.
In the 17th century, Descartes discovered the remarkable fact that the radii satisfy the equation

$$\left(\sum_{i=1}^{4} \frac{1}{r_i}\right)^2 = 2\sum_{i=1}^{4} \frac{1}{r_i^2}.$$

Here, the circles are supposed to have no common interior point which means by convention that the outermost circle's exterior is the interior and the interior is the exterior and the radius is negative.

In terms of the curvature, which is the reciprocal of the radius, the equation becomes

$$(C_1 + C_2 + C_3 + C_4)^2 = 2(C_1^2 + C_2^2 + C_3^2 + C_4^2).$$

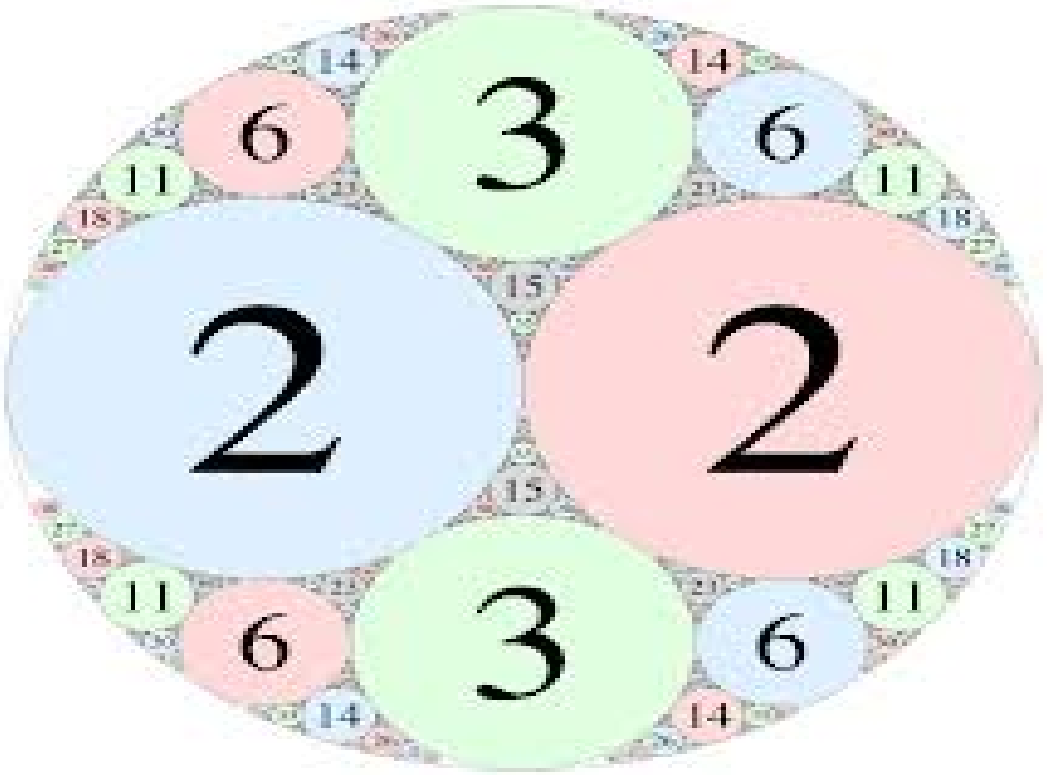
In terms of the curvature, which is the reciprocal of the radius, the equation becomes

$$(C_1 + C_2 + C_3 + C_4)^2 = 2(C_1^2 + C_2^2 + C_3^2 + C_4^2).$$

Thus, if we are given 3 of the circles and they have integer curvatures,t he fourth must also have integral curvature because of the equation!

In the figure here, the curvatures are $-1, 2, 2, 3$.

In the figure here, the curvatures are $-1, 2, 2, 3$.



In this manner, we can get a packing by circles and it is a nontrivial problem to find all solutions of the above Diophantine equation.

In this manner, we can get a packing by circles and it is a nontrivial problem to find all solutions of the above Diophantine equation.
Recently, very deep mathematical tools have been brought to bear on these problems and there is a veritable treasure for the eye as well as the brain awaiting you if you are interested!

Upping the ante

Questions on counting (and many questions we considered above) often involve finding integer solutions of equations of the form $f(x) = g(y)$ for integer polynomials f, g.

Upping the ante

Questions on counting (and many questions we considered above) often involve finding integer solutions of equations of the form $f(x) = g(y)$ for integer polynomials f, g.

An example comes from counting lattice points in generalized octahedra.

Upping the ante

Questions on counting (and many questions we considered above) often involve finding integer solutions of equations of the form $f(x) = g(y)$ for integer polynomials f, g.

An example comes from counting lattice points in generalized octahedra.

The number of integral points on the n-dimensional octahedron $|x_1| + |x_2| + \cdots + |x_n| \leq r$ is given by the expression $p_n(r) = \sum_{i=0}^{n} 2^i \binom{n}{i} \binom{r}{i}$.

The question of whether two octahedra of different dimensions m, n can contain the same number of integral points becomes equivalent to the solvability of $p_m(x) = p_n(y)$ in integers x, y; this is proved now to have only finitely many solutions.

Modus operandi - Siegel's theorem

Theorem (Siegel, 1929). If $F \in \mathbb{Z}[X, Y]$ is absolutely irreducible and the curve $F = 0$ has genus > 0, then the number of integral points on the curve is finite. Further, the finiteness of the number of integer points holds good except when the (projective completion of the) curve defined by $F = 0$ has genus 0 and at most 2 points at infinity.

Let $f, g \in \mathbb{C}[X]$ be two polynomials such that the polynomial $f(X) - g(Y) \in \mathbb{C}[X, Y]$ in two variables is irreducible. Suppose the stationary points of f and g are simple. For each stationary point $a \in S_f$, define

$$r_a := |\{b \in S_g : f(a) = g(b)\}|.$$

Then, the genus g of the curve $f(X) = g(Y)$ is given by

$$2g = \sum_{a \in S_f} (\deg(g) - 2r_a) - \deg(f) + 2 - GCD(\deg(f), \deg(g)).$$

Given $F \in \mathbb{Q}[X, Y)$, one may homogenize this polynomial to a homogeneous polynomial of three variables X, Y, Z. Then, the points in the projective space corresponding to the solutions of $F(x, y, 0) = 0$ are called the points at infinity of the curve $F = 0$.

Given $F \in \mathbb{Q}[X, Y)$, one may homogenize this polynomial to a homogeneous polynomial of three variables X, Y, Z. Then, the points in the projective space corresponding to the solutions of $F(x, y, 0) = 0$ are called the points at infinity of the curve $F = 0$.

Yuri Bilu and Robert Tichy found a novel way to use Siegel's theorem in a more effective manner.

The power of these geometric methods can be exemplified by one application as follows:

The power of these geometric methods can be exemplified by one application as follows:

The following theorems address Erdös's conjecture and gives finiteness of integral solutions when the genus is > 0 and the finiteness of rational solutions when the genus is > 1.

Theorem 2.1. *Let m and n be positive integers with $m \leq n$ and let $\lambda \in \mathbb{C}^*$. If $X(X+1)\cdots(X+m-1) - \lambda Y(Y+1)\cdots(Y+n-1)$ is reducible in $\mathbb{C}[X,Y]$ then one of the following possibilities holds:*

1. *$m = n$, $\lambda = 1$, in which case $X - Y$ is a factor,*
2. *$m = n$ is odd, $\lambda = -1$, in which case $X + Y + m - 1$ is a factor,*
3. *$m = 2$, $n = 4$, $\lambda = \frac{1}{4}$, in which case we have*

$$4X(X+1) - Y(Y+1)(Y+2)(Y+3) = (2X - Y^2 - 3Y)(2X + 2 + 3Y + Y^2).$$

Theorem 2.2. *Consider the curve*

$$X(X+1)\cdots(X+m-1) = \lambda Y(Y+1)\cdots(Y+n-1)$$

with $n \geq m > 1$ *and* $\lambda \in \mathbb{C}^*$. *Suppose it is irreducible. Then its genus is zero in the following cases:*

1. $m = 2, n = 2,$
2. $m = 2, n = 3, \lambda = \pm 3\sqrt{3}/8,$
3. $m = 2, n = 4, \lambda = -4/9,$
4. $m = 2, n = 6, \lambda = (-10 \pm 7\sqrt{7})/576.$

The genus is one in the following cases:

1. $m = 2, n = 3, \lambda \neq \pm 3\sqrt{3}/8,$
2. $m = 2, n = 4, \lambda \neq -4/9,$
3. $m = 2, n = 5, \lambda = -1/4t, 3125t^4 - 47500t^2 + 82944 = 0,$
4. $m = 2, n = 6, \lambda = 16/225,$
5. $m = 2, n = 8, \lambda = -1/4t, t^3 + 567t^2 - 54432t - 4665600 = 0,$
6. $m = 3, n = 3,$
7. $m = 3, n = 4, \lambda = \pm 3\sqrt{3}/2,$
8. $m = n = 4, \lambda = -9/16, -16/9.$

In all other cases the genus is strictly bigger than one.

ABC

The dilemma of using transcendental methods due to Alan Baker and others is that although one may prove the finiteness of the number of solutions, the result may not be effective.

ABC

The dilemma of using transcendental methods due to Alan Baker and others is that although one may prove the finiteness of the number of solutions, the result may not be effective.

Even when we have an effective result, the bound may be so big as to rule out any checking by powerful computers also.

ABC

The dilemma of using transcendental methods due to Alan Baker and others is that although one may prove the finiteness of the number of solutions, the result may not be effective.

Even when we have an effective result, the bound may be so big as to rule out any checking by powerful computers also.

For instance, for the Catalan equation $x^m - y^n = 1$, Robert Tijdeman's finiteness result was made effective by Langevin who obtained an upper bound for x, y, m, n that was of the order of $exp(exp(exp(exp(730))))$.

Later, in 20024, the Catalan equation was completely solved by Preda Mihailescu, showing that the only perfect powers differing by 1 are 8 and 9.

Later, in 20024, the Catalan equation was completely solved by Preda Mihailescu, showing that the only perfect powers differing by 1 are 8 and 9.

A more general conjecture due to S S Pillai is still open; it asserts that the gaps in the sequence of perfect powers tends to infinity.

The ABC conjecture - formulated independently by Masser and Oesterlé - supercedes many conjectures in Diophantine equations and implies many of them.

The ABC conjecture - formulated independently by Masser and Oesterlé - supercedes many conjectures in Diophantine equations and implies many of them.

It formalizes the observation that when two numbers A and B are divisible by large powers of small primes, then $A + B$ tends to be divisible by small powers of large primes.

The ABC conjecture - formulated independently by Masser and Oesterlé - supercedes many conjectures in Diophantine equations and implies many of them.

It formalizes the observation that when two numbers A and B are divisible by large powers of small primes, then $A + B$ tends to be divisible by small powers of large primes.

More precisely:

For any $\epsilon > 0$, there are only finitely many triples A, B, C of relatively prime integers satisfying $A + B = C$, and $max(A, B, C) > Rad(ABC)^{1+\epsilon}$, where $Rad(n)$ is the product of all distinct prime divisors of n.

For any $\epsilon > 0$, there are only finitely many triples A, B, C of relatively prime integers satisfying $A + B = C$, and $max(A, B, C) > Rad(ABC)^{1+\epsilon}$, where $Rad(n)$ is the product of all distinct prime divisors of n.

For instance, the ABC-conjecture implies Fermat's last theorem for sufficiently large exponents; in fact, it implies finiteness of the number of solutions of the generalized Fermat equation $Ax^r + By^s = Cz^t$.

I end with two remarkable results from a century back:

Ritt's first theorem. Let $f_1 \circ f_2 \circ \cdots f_r = g_1 \circ g_2 \circ \cdots g_s$ where $f_i, g_j \in \mathbf{C}[X]$ be nontrivial decompositions into indecomposables. Then, $r = s$ and the sets of degrees $\{deg(f_1), \cdots, deg(f_r)\} = \{deg(g_1), \cdots, deg(g_s)\}$.

Ritt's second theorem. let $f_1 \circ g_1 = f_2 \circ g_2$ be two proper decompositions over $\mathbf{C}$ where $deg(f_1) = deg(g_2)$ is relatively prime to $deg(g_1) = deg(f_2)$.
Then, either

$$f_1(X) = X^r P(X)^s = g_2(X) \ , \ g_1(X) = f_2(X) = X^s$$

or

$$f_1(X) = g_2(X) = D_m(X) \ , \ g_1(X) = f_2(X) = D_n(X)$$

where $D_n(X)$ is the Dickson polynomial of degree n defined by

$$D_n(X + 1/X) = X^n + 1/X^n.$$

We had this year's Pi Day

We had this year's Pi Day
just now - last Friday.

We had this year's Pi Day
just now - last Friday.
To Pi, 22 by 7 is closer

We had this year's Pi Day
just now - last Friday.
To Pi, 22 by 7 is closer
but somehow 3.14 is kosher.

We had this year's Pi Day
just now - last Friday.
To Pi, 22 by 7 is closer
but somehow 3.14 is kosher.
But who cares? Let's celebrate any way!

Thank You For Listening!

Which numbers are popular in IIT?

Which numbers are popular in IIT?
All love Pi, and know by sight e.

Which numbers are popular in IIT?
All love Pi, and know by sight e.
Last Friday was Pi Day,

Which numbers are popular in IIT?
All love Pi, and know by sight e.
Last Friday was Pi Day,
celebrate despite delay,

Which numbers are popular in IIT?
All love Pi, and know by sight e.
Last Friday was Pi Day,
celebrate despite delay,
- the best way to start is with High Tea!