The world of Diophantine equations

B.Sury
Indian Statistical Institute
Bangalore, India
sury@isibang.ac.in
National seminar on Algebra and Number Theory
Pavanatma College, Idukki, Kerala
December 5, 2014

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:
'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.
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

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!
The subject of Diophantine equations is an area of mathematics where solutions to very similar-looking problems can vary from the elementary to the deep.
Typically, problems are easy to state, but it is usually far from clear whether a given one is trivial to solve or whether it must involve deep ideas.
Even the type of mathematical tools used varies drastically for equations which seem similar on the first glance.

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

There is the as-yet-unsolved conjecture on the generalized Fermat equation:
This conjecture (for which a businessman and mathematics lover Robert Beals has offered a million dollar prize) asserts that $x^a + y^b = z^c$ for $a, b, c > 2$ implies that x, y, z must have a common prime factor.
The conditions are necessary as shown by the examples

$$7^3 + 13^2 = 2^9$$

$$27^4 + 162^3 = 9^7$$

I mention briefly that the ancient Indians contributed to a famous Diophantine equation known as Pell's equation which has nothing to do with Pell!
Brahmagupta (6th century) and Bhaskara (12th century) not only solved equations of the form $x^2 - dy^2 = \pm 1$ completely when d is a square-free positive integer, they gave the marvellous chakravala algorithm to do that.
In 1150 A.D., Bhaskara II gave the explicit solutions

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

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

In fact, Brahmagupta had already solved this equation in 628 A.D. for several values like $N = 83$ and $N = 92$.
He is said to have remarked, "*a person who is able to solve these two cases within a year is truly a mathematician*"' !

A 1657 challenge of Fermat "*to the English mathematicians and all others*" was posed in a letter to his friend Frenicle; he posed the problem of finding a solution of $x^2 - Ny^2 = 1$ "*pour ne vous donner pas trop de peine*" like $N = 61,109$.
André Weil, one of the greatest mathematicians of the 20th century, who is also an Indophile, says of this:
"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?".
In this talk, we concentrate on some relatively elementary problems and their pretty connections which are quite amazing already!

• 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 $3/2, 20/3, 41/6$.
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?
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.
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.
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 unsolvability 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!
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 $y^2 = x^3 - d^2x$.
Such equations define **elliptic curves.**
It is easy to show:
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 $y^2 = x^3 - d^2x$.
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.
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.
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!

Here is a set of questions on arithmetic progressions of natural numbers which leads us to some very interesting Diophantine equations.
Can we have a finite arithmetic progression

$$a, a+d, a+2d, \cdots, a+nd$$

such that a first part $a, a+d, \cdots, a+(r-1)d$ has the same sum as that of the second part $a+rd, a+(r+1)d, \cdots, a+nd$?
Note

$$20+25+30 = 35+40$$

$$14+21+28+35+42+49 = 56+63+70$$

This question is very easy to settle and we leave this as an exercise and proceed to a more general case as follows.

Can we break an arithmetic progression into THREE parts with equal sums?
Here, we mean that each of the three parts consist of consecutive terms.
Another question: Can we have four perfect squares of positive integers in arithmetic progression?
If a^2, b^2, c^2, d^2 are in arithmetic progression, then

$$b^2 - a^2 = c^2 - b^2 = d^2 - c^2$$

So

$$2a + 1, 2a + 3, \cdots, 2b - 1$$

$$2b + 1, 2b + 3, \cdots, 2c - 1$$

$$2c + 1, 2c + 3, \cdots, 2d - 1$$

are 3 parts of an A.P. whose sums are all equal.

Therefore, if the answer to the second question is 'yes', then the answer to the first question is 'yes'.
The answer to the first question is NO as we show now. In fact, we prove more generally:

Theorem.

(i) *If an A.P. is broken into three parts of lengths $a > b > c$ with equal sums, then*

$$(a-c)^2 b = (a+c)(ac-b^2).$$

(ii) *If*

$$(a-c)^2 b = (a+c)(ac-b^2)$$

has solutions in integers $a > b > c$, then there are four consecutive terms of an A.P. of integers whose product is a square.
Further, the latter is impossible.

Proof (i).
Suppose, more generally, that we have an A.P. of real numbers. By dividing out all terms by the common difference, we may assume that the A.P. is

$$t+1, t+2, \cdots, t+a, t+a+1, \cdots, t+a+b, t+a+b+1, \cdots, t+a+b+c$$

with

$$\sum_{i=1}^{a}(t+i) = \sum_{i=1}^{b}(t+a+j) = \sum_{i=1}^{c}(t+a+b+i).$$

As $2\sum_{i=1}^{a}(t+i) = 2ta + a(a+1)$,
$2\sum_{i=1}^{b}(t+a+j) = 2b(t+a) + b(b+1)$, and
$2\sum_{i=1}^{c}(t+a+b+i) = 2c(t+a+b) + c(c+1)$,
are equal, we have
$2t+1 = \frac{2ab}{a-b} - (a+b)$ from the first two, and
$2t+1 = \frac{2bc}{b-c} - (2a+b+c)$ from the 2nd and 3rd equations.
Subtracting and rearranging, we have the equality
$(a-c)^2 b = (a+c)(ac-b^2)$.

Proof of (ii).
The equation $b(a-c)^2 = (a+c)(ac-b^2)$ **can be rewritten as** $(a-c)^2(a+c+4b) = (a+c)(a+c-2b)(a+c+2b)$.
Multiplying by $a+c+4b$**, the LHS is a perfect square while the RHS is a product of 4 consecutive terms of an A.P. of positive integers.**

Leonhard Euler proved that four consecutive terms of an A.P. of positive integers cannot have product a square.
Therefore, Euler's result shows by the theorem above that:
There does not exist a A.P. of positive integers which has length $a+b+c$ and such that the sum of the first a terms, the sum of the next b terms and then the sum of the last c terms are all equal.

Euler's theorem can be proved easily by first observing that the 4-term A.P. with a square product can be reduced to a 4-term A.P. $a+d, a+2d, a+3d, a+4d$ with a, d coprime; then observing that each of the 4 terms must be a square up to extra factor of 2 or 3. We leave the completion of this proof as an exercise and discuss another approach.
Before that, we mention in passing that Euler's theorem has an even easier proof when the common difference is 1:
Note that

$$(a+1)(a+2)(a+3)(a+4) = (a^2+5a+5)^2 - 1.$$

So, if there were b^2, we would have a solution to the equation $y^2 = x^2 - 1$ in positive integers, which is impossible.

Recall that if we have a decomposition of an A.P. into parts of sizes a, b, c, we have

$$(a-c)^2 b = (a+c)(ac-b^2)$$

which is also expressible as:
$(a+c)b^2 + (a-c)^2 b - ac(a+c) = 0$.
Writing $u = a+c, v = a-c$, the discriminant

$$(a-c)^4 + 4ac(a+c)^2 = u^4 - u^2v^2 + v^4.$$

So $u^4 - u^2v^2 + v^4$ is a square, which can be shown to be possible in positive integers only if $u = v$ (this is not possible in our case as $c \neq 0$).
The way to show the above impossibility is by considering it as an equation

$$(u^2 - v^2)^2 + (uv)^2 = w^2$$

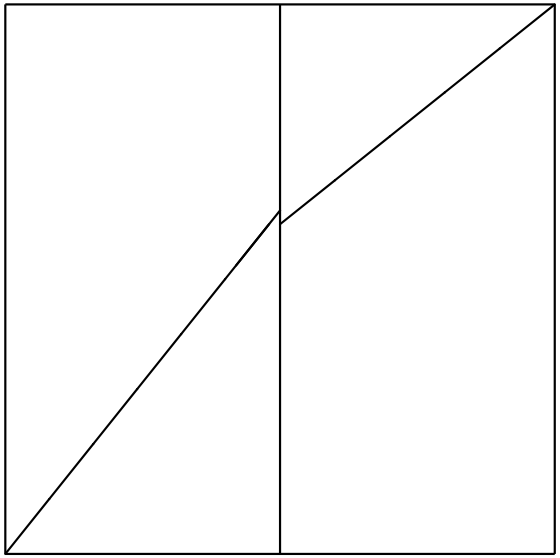
and showing that any solution leads to a 'smaller' solution; this method is known as descent.

We end this circle of problems with the following one which can be investigated further.
Suppose an A.P. of $a+b+c$ positive integers has the sum of first a terms to that of the next b terms to that of the next c terms in the ration $u:v:w$.
What are the possible u, v, w?
In fact, our earlier discussion can be generalized without any extra effort to show that such an A.P. gives rise to a Diophantine equation

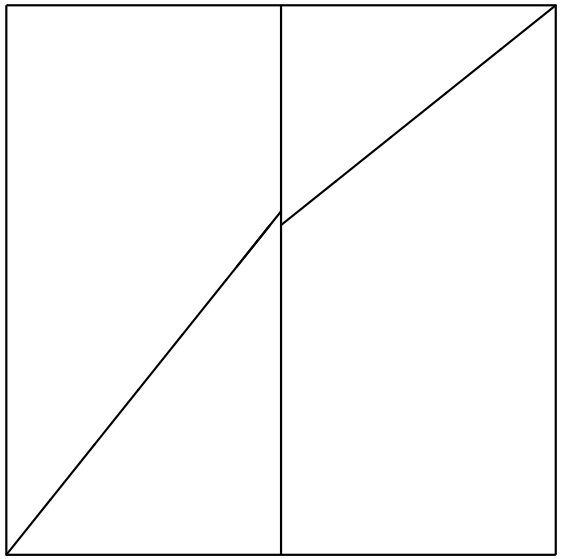
$$(ub-va)c(b+c)+(wb-vc)a(a+b)=0.$$

In the above equation, we are looking for solutions under the condition $u/a, v/b, w/c$ must be distinct.
We leave the investigation open for students to try.

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



The rule is to walk from the bottom left corner on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the top right 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. Suppose such a 'rational' path is possible.
Let us call the vertical distance x on the middle line from the bottom to the point we reach on it; of course, the rest of the vertical distance is $1 - x$.



Now,

$$r^2 - \frac{1}{4} = x^2$$

$$s^2 - \frac{1}{4} = (1-x)^2$$

This gives $2x = 1 + r^2 - s^2$, which is then rational.
Then, writing $r = p/q$ and $s = u/v$, we have two equations

$$\frac{\sqrt{4p^2 - q^2}}{2q} = x \ , \frac{\sqrt{4u^2 - v^2}}{2v} = 1 - x$$

Therefore, since the square-roots in

$$\frac{\sqrt{4p^2-q^2}}{2q}=x$$

$$\frac{\sqrt{4u^2-v^2}}{2v}=1-x$$

are rational, they must be integers and so, $q=2Q$ (if q were odd, the number $4p^2-q^2$ would be -1 modulo 4 which cannot be a square).

Thus, $x=\frac{\sqrt{p^2-Q^2}}{2Q}=\frac{I}{2Q}$ for some I with $(I,Q)=1$.

Similarly, $v=2V$ and $1-x=\frac{\sqrt{u^2-V^2}}{2V}=\frac{m}{2V}$ with $(m,V)=1$.

Thus, $1=\frac{I}{2Q}+\frac{m}{2V}$ gives $2QV=IV+mQ$.

As $(I,Q)=1=(m,V)$, we get $Q|V, V|Q$; that is, $Q=V$ as both are positive integers.

Hence, we have obtained:

$l^2 + Q^2 = p^2, m^2 + Q^2 = u^2, l + m = 2Q$ with
$(l, Q) = 1 = (m, Q)$.
We leave it as an exercise to show that these equations are solvable if and only if the equation $X^4 - Y^4 = Z^2$ is solvable in positive integers.
The last equation is not solvable in integers (equivalently, 1 is not a congruent number!).
Therefore, such a 'rational' walk is impossible because 1 is not a congruent number!

We have seen some Diophantine equations arising naturally while considering the congruent number problem or while looking at some natural questions on A.P's.
Another natural question is:
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).
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?*

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 $m = 2, n = 4$.

The fact that a product of k consecutive numbers (where $k \geq 3$) can not be a perfect power was settled in 1975 by Erdös & Selfridge.
They used 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.

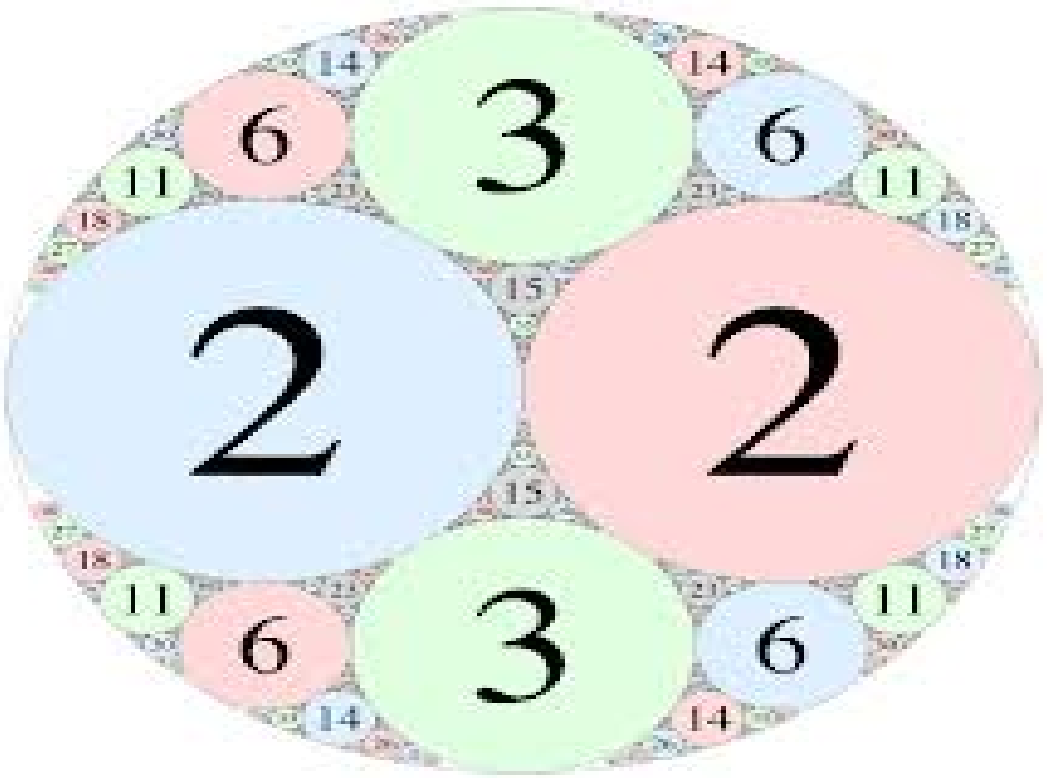
In contrast with the above Erdös- Selfridge result, there is a much deeper conjecture due to Erdös in 1975 that:
For each $c \in \mathbb{Q}$, the number of (x, y, m, n) satisfying

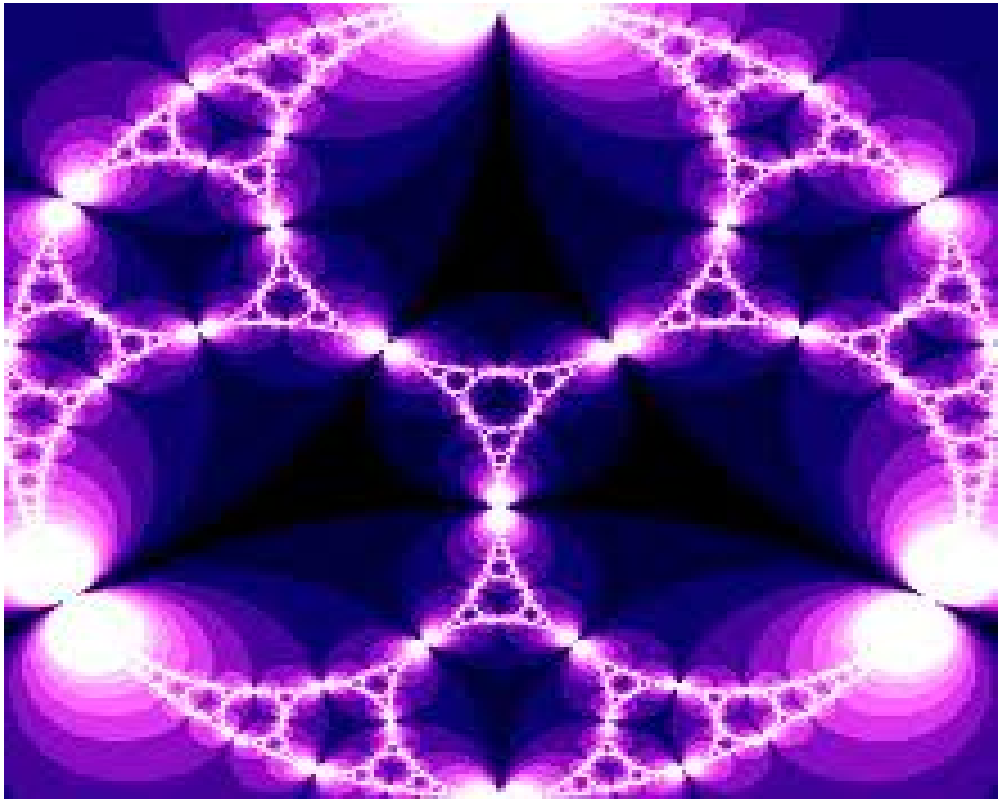
$$x(x+1)\cdots(x+m-1) = cy(y+1)\cdots(y+n-1)$$

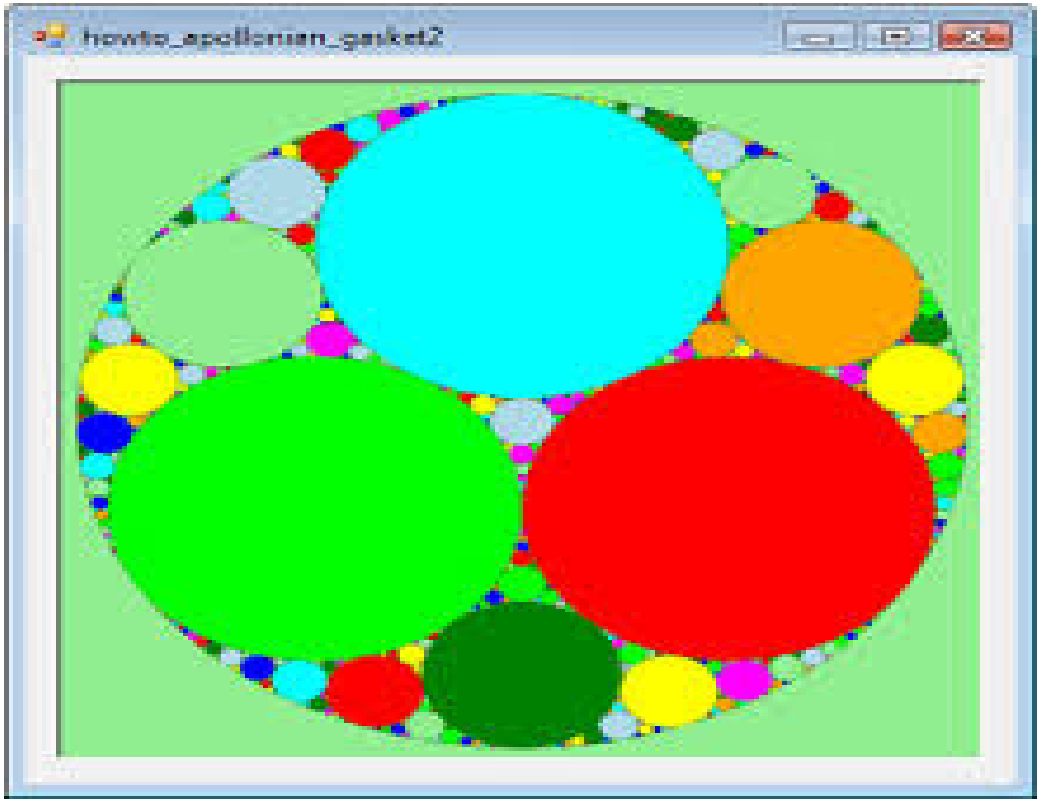
with $y \geq x+m$, $\min(m, n) \geq 3$, is finite.
This is unsettled as yet.

Apollonian circle packing

Apollonius from 200 BC discovered something beautiful.


6
3
6
2
2
6
3
6




howto_apollonian_gasket2

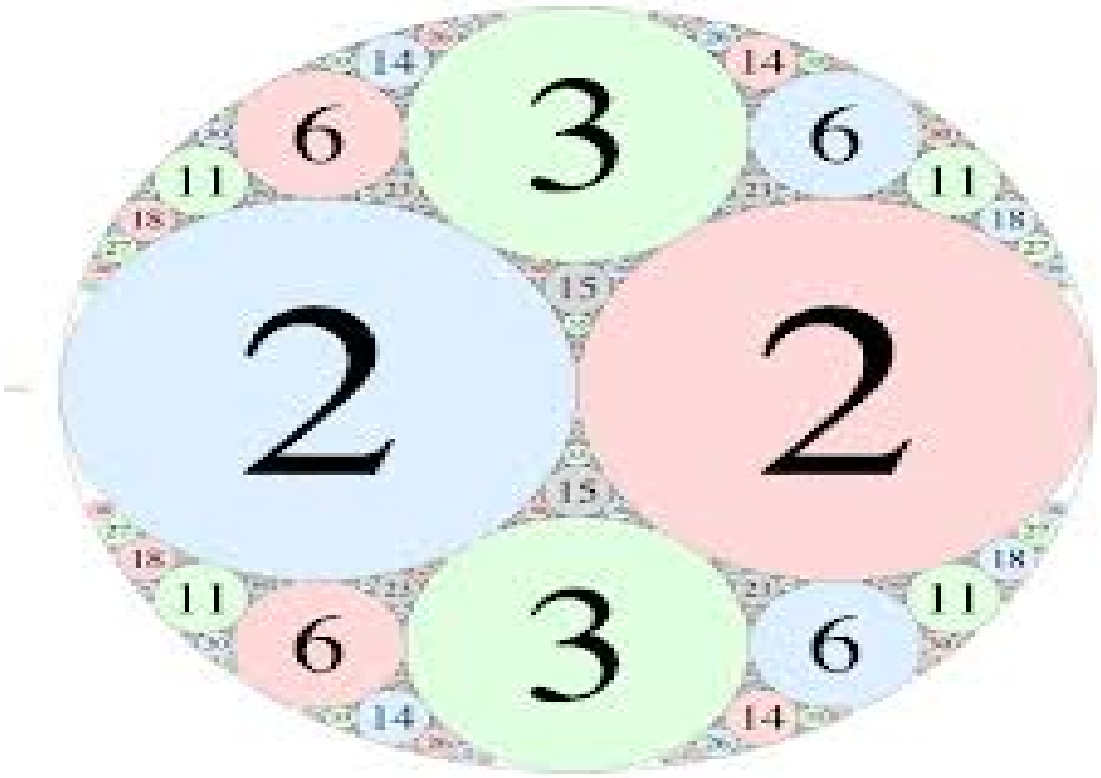
If we have three circles touching each other, one may place another circle touching all three.
In the 17th century, Descartes discovered the remarkable fact that the radii satisfy the equation
$\left(\sum_{i=1}^{4} \frac{1}{r_i}\right)^2 = 2\sum_{i=1}^{4} \frac{1}{r_i^2}$.
Here, the circles are supposed 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

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

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 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!