The area of a right-angled triangle

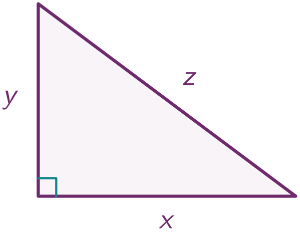
Jack Shotton
Durham University

21 September 2026

Ask questions on Slido

https://qr.sli.do/geXcoYUpSPJPo7kYQhiLNk

A familiar triangle



Pythagoras's theorem

$$x^2 + y^2 = z^2$$

Area

$$\frac{xy}{2}$$

Guiding question

If x, y, z are rational, what can the area be?

Rational sides

x	y	z	Area
3	4	5	6
5	12	13	30
8	15	17	60
7	24	25	84

x	y	z	Area
4	$\frac{15}{2}$	$\frac{17}{2}$	15
16	30	34	240
$\frac{8}{17}$	$\frac{15}{17}$	1	$\frac{60}{289}$

Plimpton 322

Row 5 (in base 10)
1.815007716 . . . 65 97 5

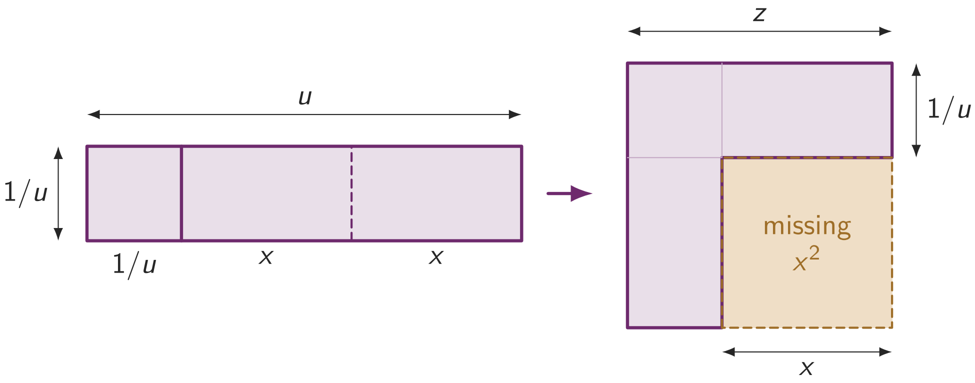
Photograph: Christine Proust, in Britton, Proust, and Shnider (2011).

- From Larsa, southern Iraq, around 1800 BCE.
- Row 5:

$$65^2 + 72^2 = 97^2$$

and $\left(\frac{97}{72}\right)^2 = 1.815007716\ldots.$

Construction



$$x = \frac{u - 1/u}{2}, \qquad z = \frac{u + 1/u}{2}, \qquad x^2 + 1 = z^2.$$

$$u = \frac{9}{4} \implies x = \frac{65}{72}, \qquad z = \frac{97}{72}, \qquad x^2 + 1 = z^2.$$

A recipe

Write $u = m/n > 1$ in lowest terms. Then

$$\left(\frac{u - 1/u}{2}, 1, \frac{u + 1/u}{2}\right) = \left(\frac{m^2 - n^2}{2mn}, 1, \frac{m^2 + n^2}{2mn}\right).$$

Clearing denominators gives a Pythagorean triple

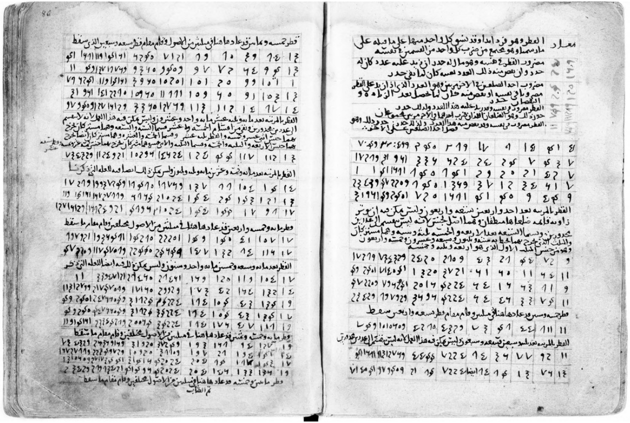
$$(m^2 - n^2, 2mn, m^2 + n^2).$$

Theorem

Every primitive[1] Pythagorean triple (x, y, z) with y even[2] can be written in this form.

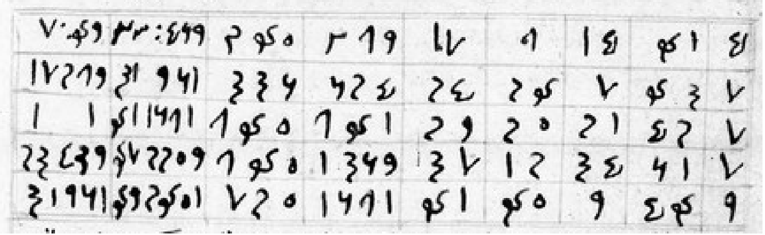
[1] No common factor of x, y, z.
[2] If not, switch x and y.

Another table of triangles



Anonymous author, perhaps 10th century CE; https://gallica.bnf.fr/ark:/12148/bpt6k99646z

What can the area be?



$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2.$$

$m+n$	(m,n)	x	y	z	z^2	$2xy$	$(x+y)^2$	$x+y$	$(x-y)^2$	$\lvert x-y \rvert$
5	4, 1	15	8	17	289	$240 = 4 \cdot 60$	529	23	49	7
7	4, 3	7	24	25	625	$336 = 4 \cdot 84$	961	31	289	17
7	5, 2	21	20	29	841	$840 = 4 \cdot 210$	1681	41	1	1
7	6, 1	35	12	37	1369	$840 = 4 \cdot 210$	2209	47	529	23
9	5, 4	9	40	41	1681	$720 = 4 \cdot 180$	2401	49	961	31

Columns reversed for left-to-right reading; translation by Franz Woepcke (1861).

Congruent numbers

Question

A positive integer is congruent if it is the area of a right-angled triangle with rational side lengths.
Which numbers are congruent?

Remember:

x	y	z	Area
8	15	17	60
4	$\frac{15}{2}$	$\frac{17}{2}$	15
16	30	34	240

Scaling all sides by t scales the area by t^2.
An integer N is congruent if and only if its *squarefree part*, $\mathrm{sf}(N)$, is.

The problem in Bachet's Diophantus

PROBLEMA XX.

Inuenire triangulum rectangulum, cuius area ſit datus numerus. Oportet autem vt quadratus areæ duplicatæ additus alicui quadratoquadrato, faciat quadratum.

Find a right-angled triangle whose area is a given number.

Bachet's 1621 edition of Diophantus' *Arithmetica* (c. 250CE).

Generating congruent numbers

(m,n)	(x,y,z)	A	sf(A)
$(2,1)$	$(3,4,5)$	6	6
$(3,2)$	$(5,12,13)$	30	30
$(4,1)$	$(15,8,17)$	60	15
$(4,3)$	$(7,24,25)$	84	21
$(5,2)$	$(21,20,29)$	210	210
$(5,4)$	$(9,40,41)$	180	5
$(6,1)$	$(35,12,37)$	210	210
$(6,5)$	$(11,60,61)$	330	330

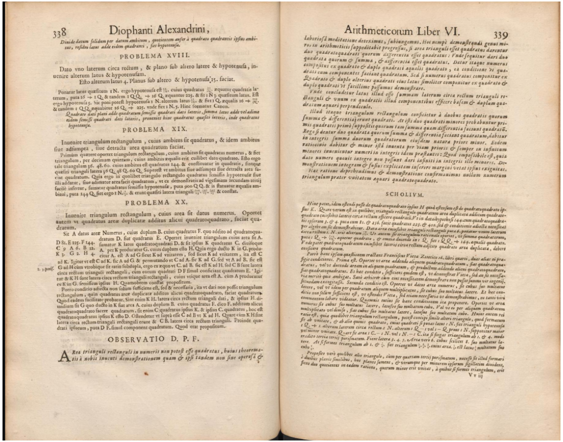
(m,n)	(x,y,z)	A	sf(A)
$(7,2)$	$(45,28,53)$	630	70
$(7,4)$	$(33,56,65)$	924	231
$(7,6)$	$(13,84,85)$	546	546
$(8,1)$	$(63,16,65)$	504	14
$(8,3)$	$(55,48,73)$	1320	330
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(16,9)$	$(175,288,337)$	25200	7

Generating congruent numbers

(m, n)	$\mathrm{sf}(A)$
$(325, 36)$	13
$(24\,336, 17\,689)$	23
$(8\,780\,605\,285\,453\,456, 7\,551\,929\,273\,974\,569)$	103

Question

Is 1 congruent?

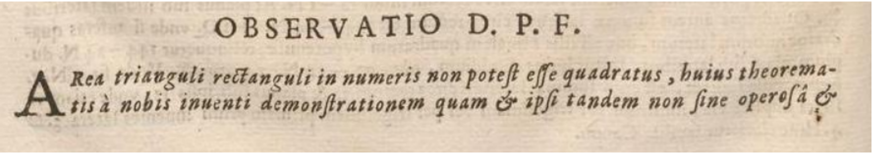


Bachet

Fermat

Spread: Fermat–Bachet's 1621/1670 edition of Diophantus's *Arithmetica* (c. 250CE).
Portraits: Wikimedia Commons, Fermat and Bachet (public domain).

Fermat's "only theorem"


OBSERVATIO D. P. F.

AREA trianguli rectanguli in numeris non poteſt eſſe quadratus, huius theorematis à nobis inuenti demonſtrationem quam & ipſi tandem non ſine operoſâ &

Fermat (c. 1637)

> *"The area of a right-angled triangle cannot be a square in integers. We shall append a proof of this theorem, discovered by us—a proof which we ourselves finally found only through effort and painstaking reflection."*

Fermat's marginal observation in Bachet's 1621 edition of Diophantus, *Arithmetica*, p. 338.

Infinite descent

1. Suppose we have a solution:
$$x^2 + y^2 = z^2, \qquad \frac{xy}{2} = a^2.$$
We will take z *as small as possible*, and find one with z *even smaller*.

2. Parametrise it:
$$(x, y, z) = (m^2 - n^2,\ 2mn,\ m^2 + n^2).$$
Then
$$mn(m+n)(m-n) = a^2.$$

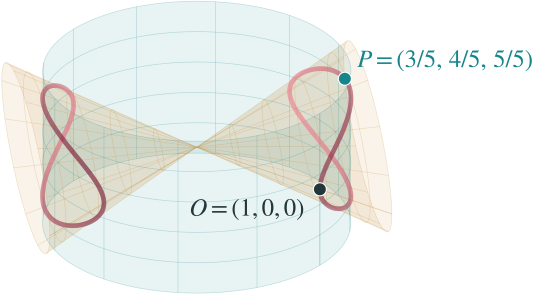
3. The four factors are pairwise coprime, so
$$m = p^2, \qquad n = q^2, \qquad m + n = r^2, \qquad m - n = s^2.$$

4. Let
$$(x', y', z') = \left(\frac{r+s}{2},\ \frac{r-s}{2},\ p \right).$$
Then
$$(x')^2 + (y')^2 = (z')^2, \qquad \frac{x'y'}{2} = \left(\frac{q}{2}\right)^2, \qquad \mathbf{z' = p < z}.$$
This is a solution with a smaller value of z. **Contradiction!!**

Drawing solutions: $N = 6$

Look for rational right-angled triangles with area 6. Rescale:

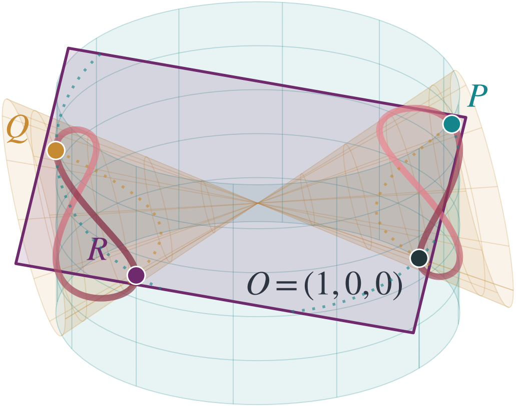
$$x^2 + y^2 = 1 \qquad \tfrac{1}{2}xy = 6w^2$$



This is an elliptic curve.

New solutions from old

$x^2 + y^2 = 1 \qquad xy = 12w^2$



Given two points P and Q, we can generate a third point R.

So many rational triangles of area 6

x	y	z
3	4	5
$\frac{7}{10}$	$\frac{120}{7}$	$\frac{1201}{70}$
$\frac{4653}{851}$	$\frac{3404}{1551}$	$\frac{7776485}{1319901}$
$\frac{1437599}{168140}$	$\frac{2017680}{1437599}$	$\frac{2094350404801}{241717895860}$

Gotta catch them all.

Theorem

If there is one rational right triangle of area N, then there are infinitely many.

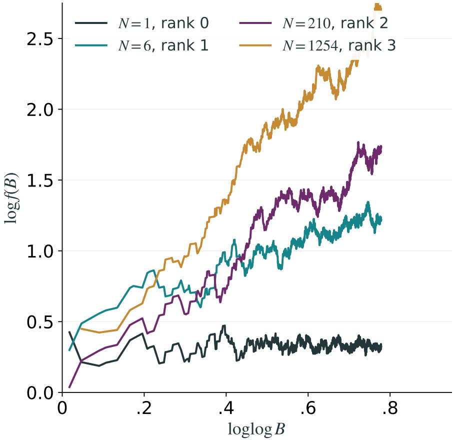
For $N = 6$, every rational triangle comes from $(3, 4, 5)$ by the preceding construction combined with swapping the legs and changing signs.
For $N = 210$, one starting triangle is no longer enough. Two independent basis triangles are needed:

$$(21, 20, 29) \qquad \text{and} \qquad (35, 12, 37).$$

Rank

The *rank* of (the curve associated to) N is the number of independent rational triangles needed to generate all of them (combined with swapping legs and changing signs).

The Birch and Swinnerton-Dyer conjecture



Let S_p be the number of solutions to $x^2 + y^2 = 1$, $xy = 2Nw^2$ modulo p.
For example, when $N = 2$ and $p = 11$, can have $x = 3$, $y = 5$, $w = 1$.
Define

$$f(B) = \prod_{p \leq B} \frac{S_p}{p}.$$

The growth of $f(B)$ seems to remember the rank.

The Birch and Swinnerton-Dyer conjecture

The BSD conjecture[3] (1965)

For r the *rank* of N (number of generating triangles):

$$\prod_{p \leq B} \frac{S_p}{p}$$

grows like $C_N(\log B)^r$.

[3] This is actually stronger than what we usually call BSD.

Some things we know

- (Tunnell, 1983, plus Coates–Wiles 1977) A simple procedure that takes N and outputs "no" or "maybe" as the answer to "is N congruent?". If BSD holds, can upgrade "maybe" to "yes".
- If BSD holds, then any squarefree N of the form $8k+5$, $8k+6$, or $8k+7$ is congruent.[4]
- (Smith, 2017) 100% of the squarefree N of the form $8k+1$, $8k+2$ and $8k+3$ are not congruent.[5]

[4] Known without BSD for N prime.
[5] But note that 210 is congruent, as we have seen, and of the form $8k+2$.

Some things we don't know

- BSD! Partial results in rank 0 and rank 1.
- Without knowing BSD, we don't know a sure-fire way to determine whether a given N is congruent.
- The highest known rank is 7 (achieved by $N = 797\,507\,543\,735$). Can the rank be 8?
- Are there infinitely many *primes* of the form $8k + 1$ which are congruent?

Rank-7 example and rank-8 search: Fisher, Watkins, Donnelly, Elkies, Granville and Rogers (2014).

Summary

- Rational right-angled triangles have been contemplated since ancient times.
- Their possible areas are the *congruent numbers*.
- Fermat showed that 1 is not congruent, or equivalently: no right-angled triangle with integer sides has square area.
- Modern setting is elliptic curves and the Birch–Swinnerton-Dyer conjecture. Much is still not known.

Any questions?

Scan to join Slido

`https://qr.sli.do/geXcoYUpSPJPo7kYQhiLNk`