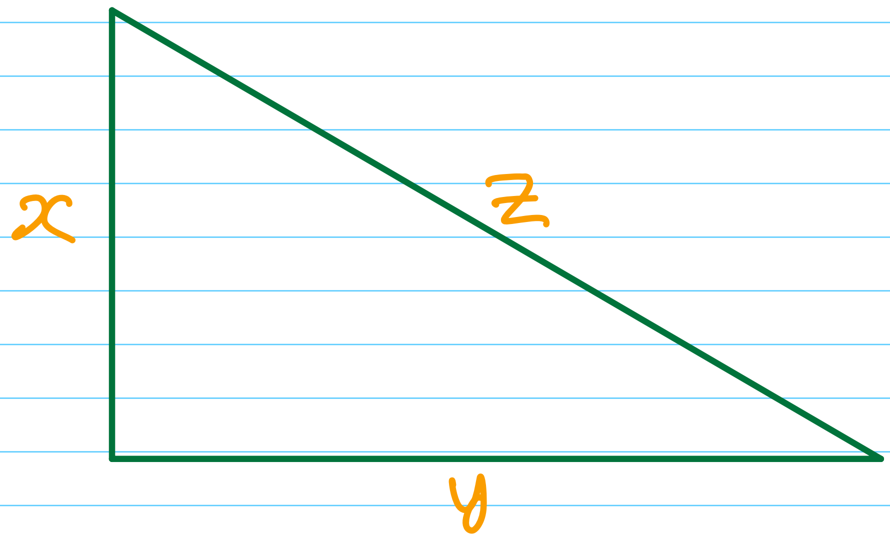
Pythagorean triples

$$x^2 + y^2 = z^2, \quad x, y, z \in \mathbb{Z}_{\geq 1}$$



Euclid's formula

Given $m > n \in \mathbb{Z}_{\geq 1}$

$$x = m^2 - n^2$$

$$y = 2mn$$

$$z = m^2 + n^2$$

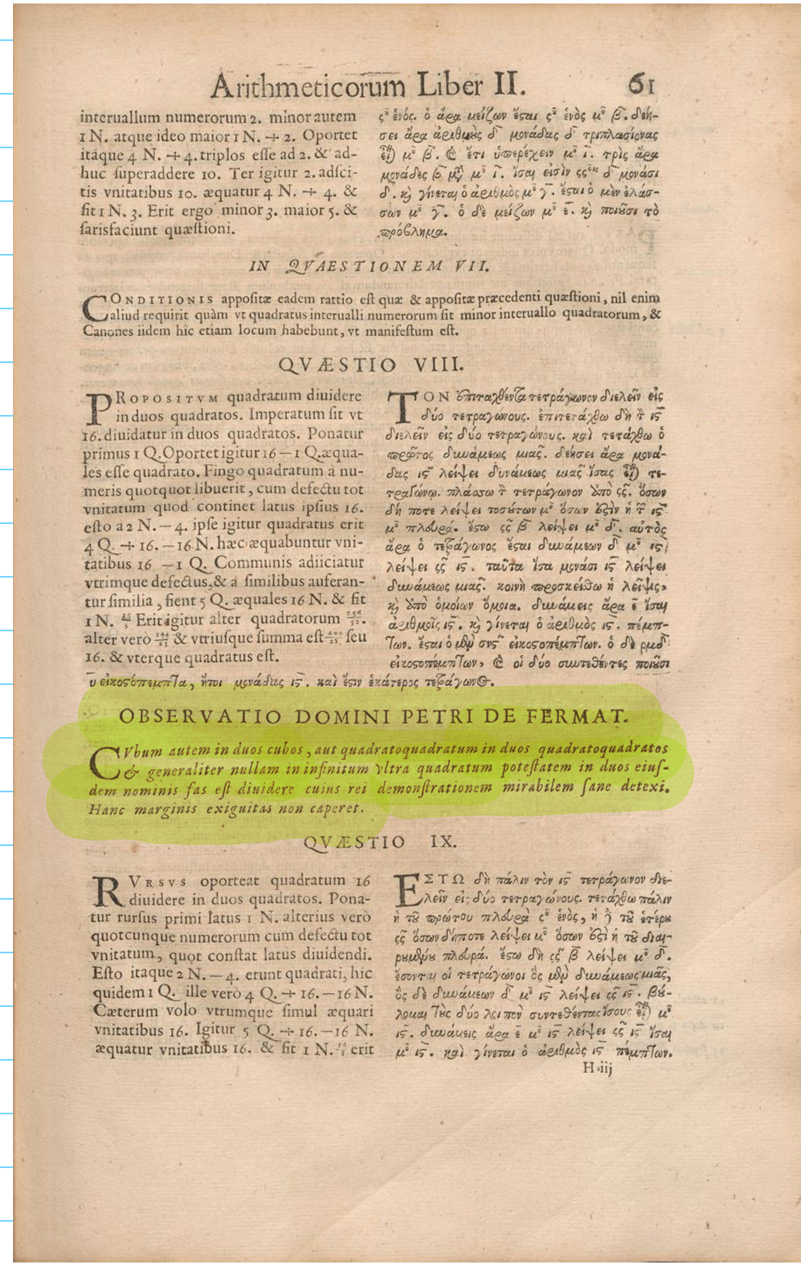
is a Pythagorean triple

In fact, all Pythagorean triples can be obtained in this way (up to scaling

Can be shown using unique factorization in the Gaussian integers $\mathbb{Z}[i]$

Fermat's Last Theorem
(1634)

Fermat's Last Theorem



interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

ϛοῦ ἑνός. ὁ ἄρα μείζων ἔσται ϛοῦ ἑνὸς μο β. δεήσει ἄρα ἀριθμοὺς δ μονάδας δ τριπλασίονας εἶναι μο β. καὶ ἔτι ὑπερέχειν μο ι. τρὶς ἄρα μονάδες β μετὰ μο ι. ἴσαι εἰσὶν ϛϛοῖς δ μονάσι δ. καὶ γίνεται ὁ ἀριθμὸς μο γ. ἔσται ὁ μὲν ἐλάσσων μο γ. ὁ δὲ μείζων μο ε. καὶ ποιοῦσι τὸ πρόβλημα.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem rattio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hîc etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ϛϛ. ὅσων δή ποτε λείψει τοσούτων μο ὅσων ἐστὶν ἡ τῶν ιϛ μο πλευρά. ἔστω ϛϛ β λείψει μο δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μο ιϛ λείψει ϛϛ ιϛ. ταῦτα ἴσα μονάσι ιϛ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ πέμπτων. ἔσται ὁ μὲν σνϛ εἰκοσοπέμπτων. ὁ δὲ ρμδ εἰκοσοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοσόπεμπτα, ἤτοι μονάδας ιϛ. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

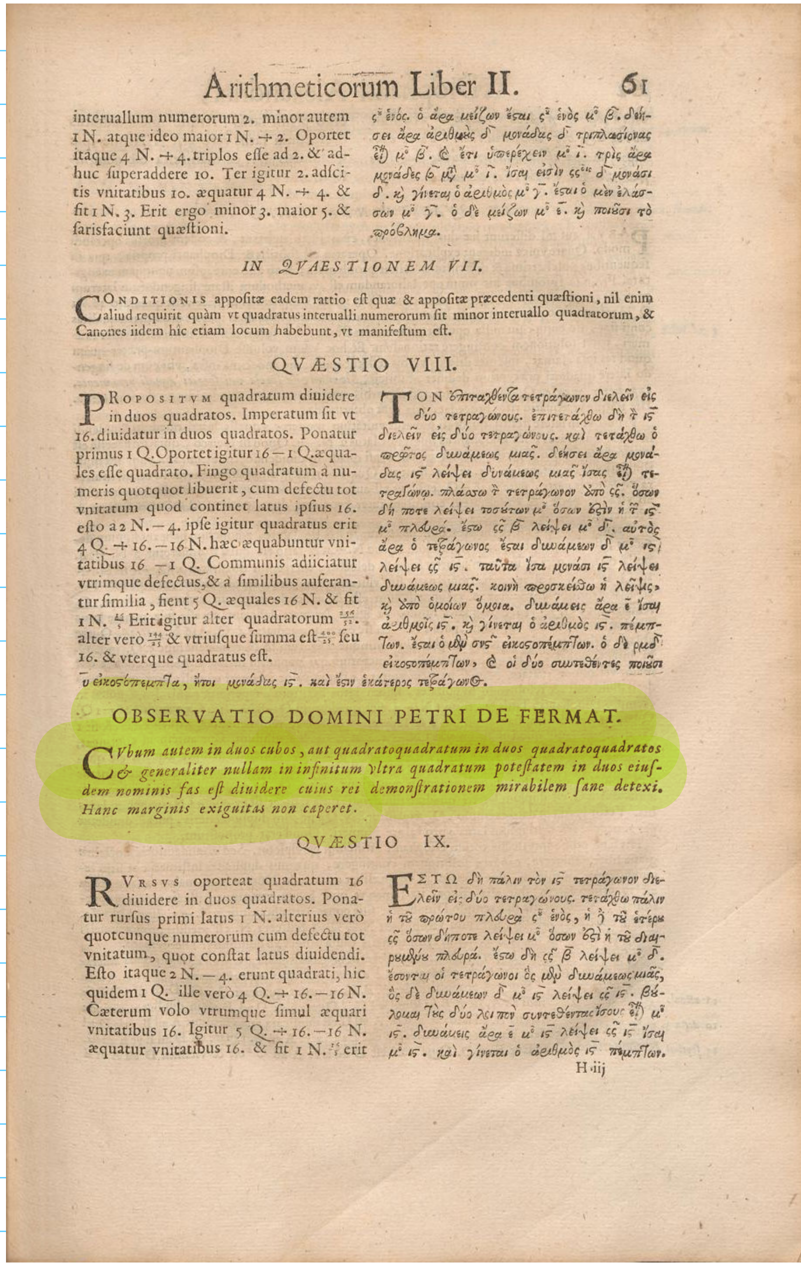
CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

ΕΣΤΩ δὴ πάλιν τὸν ιϛ τετράγωνον διελεῖν εἰς δύο τετραγώνους. τετάχθω πάλιν ἡ τοῦ πρώτου πλευρὰ ϛοῦ ἑνός, ἡ δὲ τοῦ ἑτέρου ϛϛ ὅσων δήποτε λείψει μο ὅσων ἐστὶν ἡ τοῦ διαιρουμένου πλευρά. ἔστω δὴ ϛϛ β λείψει μο δ. ἔσονται οἱ τετράγωνοι ὃς μὲν δυνάμεως μιᾶς, ὃς δὲ δυνάμεων δ μο ιϛ λείψει ϛϛ ιϛ. βούλομαι τοὺς δύο λοιπὸν συντεθέντας ἴσους εἶναι μο ιϛ. δυνάμεις ἄρα ε μο ιϛ λείψει ϛϛ ιϛ ἴσαι μο ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ πέμπτων.

Fermat's Last Theorem



interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hîc etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

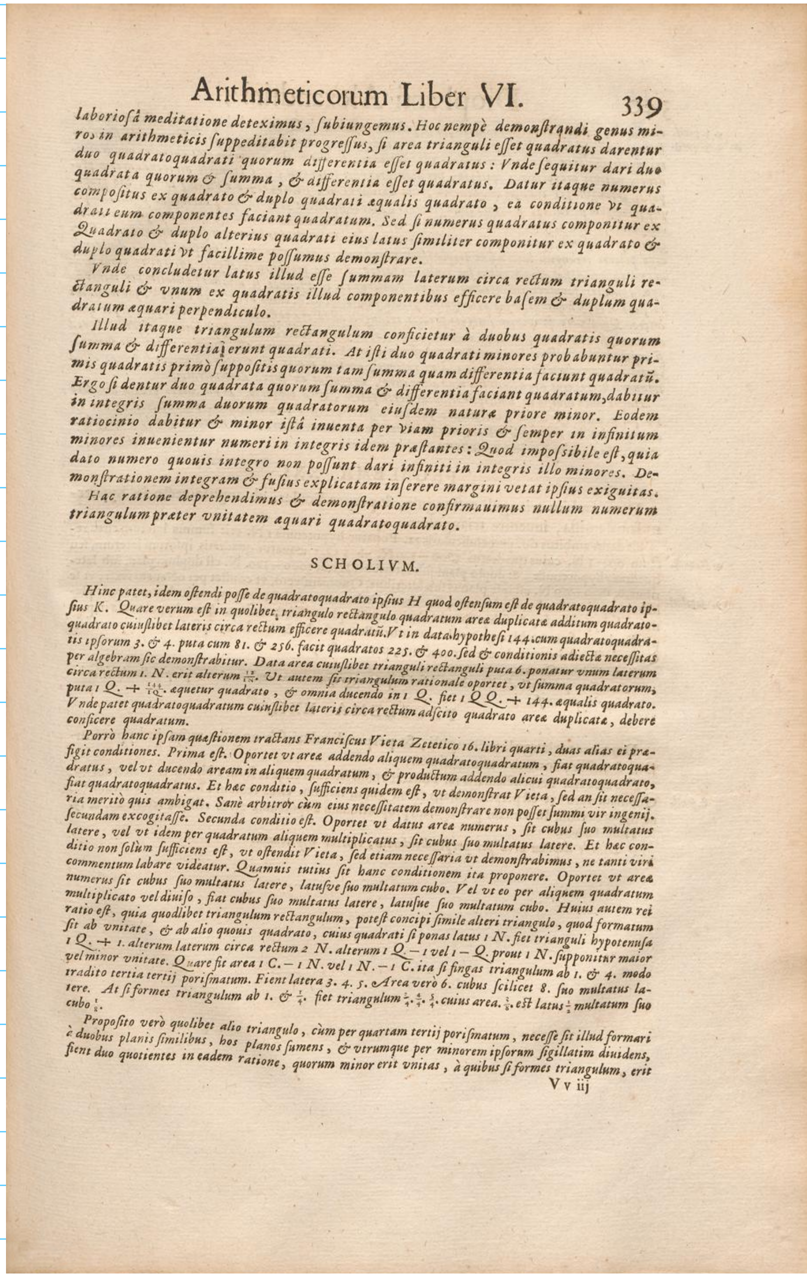
CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

"It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain."

The method of infinite descent



laborioſâ meditatione deteximus, ſubiungemus. Hoc nempè demonſtrandi genus miros in arithmeticis ſuppeditabit progreſſus, ſi area trianguli eſſet quadratus darentur duo quadratoquadrati quorum differentia eſſet quadratus: Vnde ſequitur dari duo quadrata quorum & ſumma, & differentia eſſet quadratus. Datur itaque numerus compoſitus ex quadrato & duplo quadrati æqualis quadrato, ea conditione vt quadrati eum componentes faciant quadratum. Sed ſi numerus quadratus componitur ex Quadrato & duplo alterius quadrati eius latus ſimiliter componitur ex quadrato & duplo quadrati vt facillime poſſumus demonſtrare.

Vnde concludetur latus illud eſſe ſummam laterum circa rectum trianguli rectanguli & vnum ex quadratis illud componentibus efficere baſem & duplum quadratum æquari perpendiculo.

Illud itaque triangulum rectangulum conficietur à duobus quadratis quorum ſumma & differentia erunt quadrati. At iſti duo quadrati minores probabuntur primis quadratis primò ſuppoſitis quorum tam ſumma quam differentia faciunt quadratũ. Ergo ſi dentur duo quadrata quorum ſumma & differentia faciant quadratum, dabitur in integris ſumma duorum quadratorum eiuſdem naturæ priore minor. Eodem ratiocinio dabitur & minor iſtâ inuenta per viam prioris & ſemper in infinitum minores inuenientur numeri in integris idem præſtantes: Quod impoſſibile eſt, quia dato numero quouis integro non poſſunt dari infiniti in integris illo minores. Demonſtrationem integram & fuſius explicatam inſerere margini vetat ipſius exiguitas.

Hac ratione deprehendimus & demonſtratione confirmauimus nullum numerum triangulum præter vnitatem æquari quadratoquadrato.

SCHOLIVM.

Hinc patet, idem oſtendi poſſe de quadratoquadrato ipſius H quod oſtenſum eſt de quadratoquadrato ipſius K. Quare verum eſt in quolibet triangulo rectangulo quadratum areæ duplicatæ additum quadratoquadrato cuiuſlibet lateris circa rectum efficere quadratũ. Vt in data hypotheſi 144. cum quadratoquadratis ipſorum 3. & 4. puta cum 81. & 256. facit quadratos 225. & 400. ſed & conditionis adiectæ neceſſitas per algebram ſic demonſtrabitur. Data area cuiuſlibet trianguli rectanguli puta 6. ponatur vnum laterum circa rectum 1. N. erit alterum $\frac{12}{1N}$. Vt autem ſit triangulum rationale oportet, vt ſumma quadratorum, puta 1 Q. + $\frac{144}{1Q}$. æquetur quadrato, & omnia ducendo in 1 Q. fiet 1 QQ. + 144. æqualis quadrato. Vnde patet quadratoquadratum cuiuſlibet lateris circa rectum adſcito quadrato areæ duplicatæ, debere conficere quadratum.

Porrò hanc ipſam quæſtionem tractans Franciſcus Vieta Zetetico 16. libri quarti, duas alias ei præfigit conditiones. Prima eſt. Oportet vt area addendo aliquem quadratoquadratum, fiat quadratoquadratus, vel vt ducendo aream in aliquem quadratum, & productum addendo alicui quadratoquadrato, fiat quadratoquadratus. Et hæc conditio, ſufficiens quidem eſt, vt demonſtrat Vieta, ſed an ſit neceſſaria meritò quis ambigat. Sanè arbitror cùm eius neceſſitatem demonſtrare non poſſet ſummi vir ingenij, ſecundam excogitaſſe. Secunda conditio eſt. Oportet vt datus areæ numerus, ſit cubus ſuo multatus latere, vel vt idem per quadratum aliquem multiplicatus, ſit cubus ſuo multatus latere. Et hæc conditio non ſolùm ſufficiens eſt, vt oſtendit Vieta, ſed etiam neceſſaria vt demonſtrabimus, ne tanti viri commentum labare videatur. Quamuis tutius ſit hanc conditionem ita proponere. Oportet vt areæ numerus ſit cubus ſuo multatus latere, latuſve ſuo multatum cubo. Vel vt eo per aliquem quadratum multiplicato vel diuiſo, fiat cubus ſuo multatus latere, latuſue ſuo multatum cubo. Huius autem rei ratio eſt, quia quodlibet triangulum rectangulum, poteſt concipi ſimile alteri triangulo, quod formatum ſit ab vnitate, & ab alio quouis quadrato, cuius quadrati ſi ponas latus 1 N. fiet trianguli hypotenuſa 1 Q. + 1. alterum laterum circa rectum 2 N. alterum 1 Q. − 1 vel 1 − Q. prout 1 N. ſupponitur maior vel minor vnitate. Quare ſit area 1 C. − 1 N. vel 1 N. − 1 C. ita ſi fingas triangulum ab 1. & 4. modo tradito tertia tertij poriſmatum. Fient latera 3. 4. 5. Area verò 6. cubus ſcilicet 8. ſuo multatus latere. At ſi formes triangulum ab 1. & $\frac{1}{4}$. fiet triangulum $\frac{3}{4}$. $\frac{4}{4}$. $\frac{5}{4}$. cuius area. $\frac{3}{8}$. eſt latus $\frac{1}{2}$ multatum ſuo cubo $\frac{1}{8}$.

Propoſito verò quolibet alio triangulo, cùm per quartam tertij poriſmatum, neceſſe ſit illud formari à duobus planis ſimilibus, hos planos ſumens, & vtrumque per minorem ipſorum ſigillatim diuidens, fient duo quotientes in eadem ratione, quorum minor erit vnitas, à quibus ſi formes triangulum, erit

$$x^4+y^4=z^2,$$ x, y, z rel. prime, y <u>even</u>

$\exists\ m>n \in \mathbb{Z}_{\geq 1}$ s.t.

$$\boxed{x^2=m^2-n^2},\ y^2=2mn,\ z=m^2+n^2$$

$$\Downarrow$$

(x, n, m) is a Pythagorean triple

$$\Downarrow$$

$\exists\ p>q \in \mathbb{Z}_{\geq 1}$ s.t.

$$x=p^2-q^2,\ \boxed{n=2pq,\ m=p^2+q^2}$$

$$\Downarrow$$

$$y^2=4pq(p^2+q^2) \Rightarrow p=a^2,\ q=b^2,\ p^2+q^2=c^2$$

$$\Downarrow$$

$$a^4+b^4=c^2$$

But $c \leq c^2 = m < z$

Sophie Germain
(1776–1831)

$p > 2$: odd prime

$x^p + y^p = z^p$: x, y, z rel. prime

Sophie Germain's theorem

Suppose there is an auxiliary prime q s.t.
(a) There is no integer m s.t. m & $m+1$ are both p-th powers modulo q.
(b) $x^p \equiv p \pmod{q}$ has no solns

Then:

p^2 divides one of x, y, z

Sophie Germain primes: p s.t. $2p+1$ is <u>prime</u>

In this case, $2p+1$ is an <u>auxiliary prime</u>.

Ernst Kummer
(1810 - 1893)

Kummer's theorem (1850)

FLT holds for regular primes

Expectation

About 60.65% of primes are regular

Example

The only irregular primes < 100 are 37, 59, 67

Mordell conjecture (Faltings' theorem)

(1983)

Louis Mordell

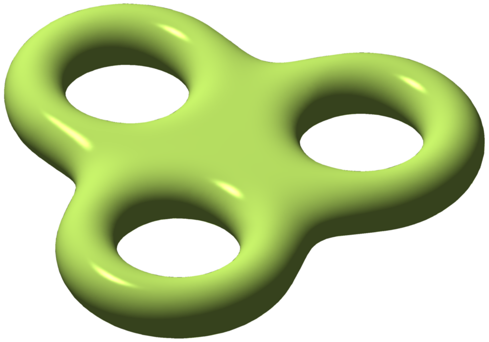
(1888 – 1972)

For any $n \geq 3$, there are only <u>finitely</u> many integer solutions to the Fermat equation

$$x^n + y^n = z^n$$

Gerd Faltings

(1954 –)



Topology

$\Rightarrow$ (≥ 2 holes)

Finitely many integer solutions (!!)

Arithmetic

The Frey-Hellegouarch Curve

(1975/1982) (p: odd prime)

Gerhard Frey
(1944 -)

Yves Hellegouarch
(1936 - 2022)

Suppose that
$a^p + b^p = c^p$, a, b, c rel. prime
is a non-trivial solution to the Fermat equation.
Then the equation

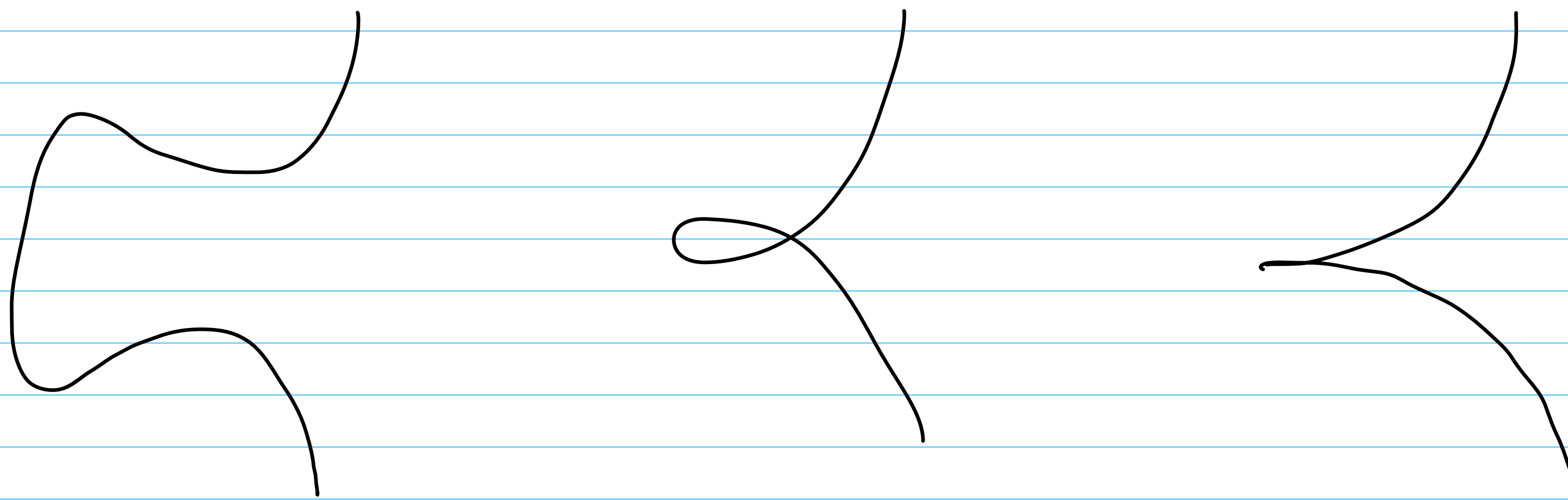
$$y^2 = x(x-a^p)(x+b^p)$$

has very interesting geometric properties
if
- b is even
- $a \equiv 3 \pmod 4$

It is a semi-stable elliptic curve over $\mathbb{Q}$

The trichotomy of cubic equations

$$y^2 = x(x-A)(x-B)$$



Elliptic curve	Nodal cubic	Cuspidal cubic
$0 \neq A \neq B \neq 0$	$0 = A \neq B$	$A = B = 0$

$$\Delta = \frac{1}{256} A^2 B^2 (A+B)^2$$: Discriminant of the cubic

$\Delta \neq 0 \iff$ elliptic curve

Back to the Frey curve

$y^2 = x(x-a^p)(x+b^p)$ $a^p + b^p = c^p$

If we view a^p, b^p as rational numbers then we get an elliptic curve over $\mathbb{Q}$

Discriminant

$$\frac{1}{256} a^{2p} b^{2p} c^{2p}$$

The discriminant is a geometric invariant but it is keeping track of arithmetic information

Semistability of the Frey curve

But we can also view a, b, c as integers <u>modulo</u> ℓ for <u>any</u> <u>prime</u> ℓ

(i.e. as elements of $\mathbb{Z}/\ell\mathbb{Z}$)

In this case, the conditions on a, b, c tell us that we obtain:

<u>Note</u>:
- $a^p \equiv 0 \pmod{\ell} \iff \ell \mid a$
- $(-b)^p \equiv 0 \pmod{\ell} \iff \ell \mid b$
- $a^p \equiv -b^p \pmod{\ell} \iff \ell \mid c$

An elliptic curve if $\ell \nmid abc$

A nodal cubic otherwise

This is telling us that the Frey-Hellegouarch curve is <u>semistable</u> of conductor abc

Shimura-Taniyama & modularity

Goro Shimura

(1930 - 2019)

Yutaka Taniyama

(1927 - 1958)

Conjecture: Every elliptic curve over $\mathbb{Q}$ with conductor N is modular of level $\Gamma_0(N)$

(1950s)

Cuspidal Modular forms

(of wt 2 & level $\Gamma_0(N)$)

$f : \mathbb{H} \to \mathbb{C}$ s.t.

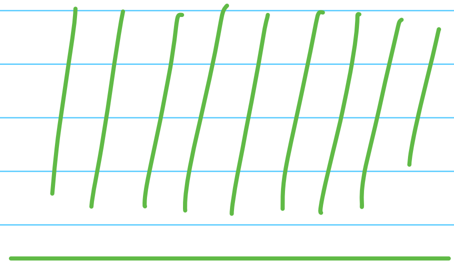
(i) f is complex diff'ble or **holomorphic**

(ii) $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $\tau \in \mathbb{H}$ **weight 2 level $\Gamma_0(N)$**

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau)$$

(iii) **cuspidal condition**

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}$$



$\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Re}\,\tau > 0\}$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{array}{l} a,b,c,d \in \mathbb{Z} \\ ad-bc=1 \\ c \equiv 0 \pmod N \end{array} \right\}$$

$\Gamma_0(N) \curvearrowright \mathbb{H}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau = \frac{a\tau+b}{c\tau+d}$$

Modularity

An elliptic curve

$(*)$ $y^2 = x(x-A)(x-B)$ is

modular if $\exists f$ s.t.

For almost all primes ℓ,

$$\ell + 1 - a_\ell = \#\text{ of solns to } (*) \text{ in } \mathbb{Z}/\ell\mathbb{Z}$$

modular mod p if $\exists f$ s.t. for almost all ℓ

$$\ell + 1 - a_\ell \equiv \#\text{ of solns to } (*) \text{ in } \mathbb{Z}/\ell\mathbb{Z} \pmod p$$

S-T conjecture $\Rightarrow$ FLT
(1986)

Barry Mazur
(1937–)

Ken Ribet
(1948–)

Theorem

If the Taniyama-Shimura conjecture holds for $\boxed{\text{semistable}}$ elliptic curves $/\mathbb{Q}$ then

$a^p + b^p = c^p$ $\Rightarrow$ Semistable Frey curve of discriminant $\frac{1}{256}a^{2p}b^{2p}c^{2p}$

$\Downarrow$ Taniyama-Shimura

cuspidal modular form of weight 2 & level $\Gamma_0(abc)$

Level lowering

Mazur-Wiles

cuspidal modular form of weight 2 & level $\Gamma_0(2)$

$\uparrow$

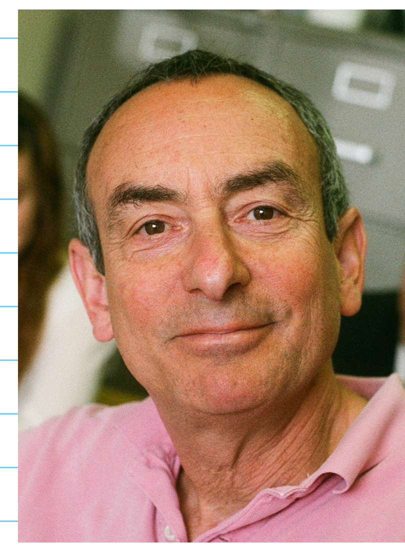
Doesn't exist!!

Hopeless ? ?

John Coates

impossible to actually prove

completely inaccessible



Wiles (& Taylor-Wiles)

Andrew Wiles

(1953 –)

Richard Taylor

(1962 –)

Theorem (1994-95)

The Taniyama-Shimura conjecture holds for semistable elliptic curves over $\mathbb{Q}$ (!!!)

Modularity lifting

Theorem (Wiles) Suppose that E is a semistable elliptic curve $/\mathbb{Q}$ s.t. for some prime $\ell > 2$:

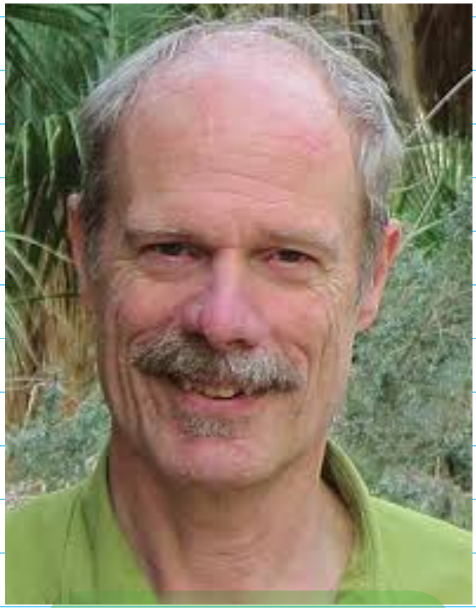
(i) E is modular mod ℓ

(ii) E is absolutely irreducible mod ℓ

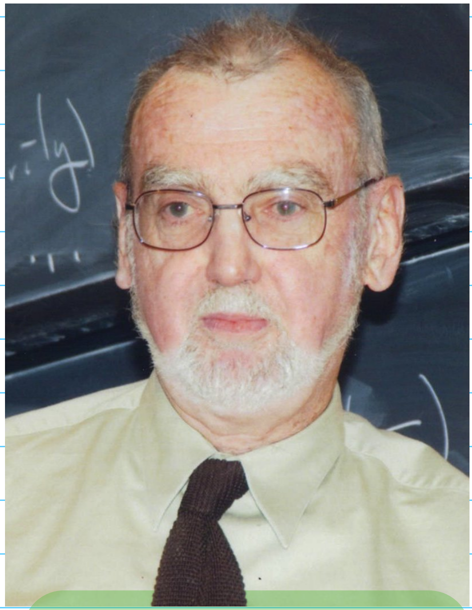
Then E is modular!

We still need a starting point!

Langlands - Tunnell



Jerry Tunnell
(1950 - 2022)



Robert Langlands
(1936 –   )

Theorem Suppose that E is absolutely irreducible mod 3. Then E is modular mod 3.
(eek!)

Wiles's strategy

$E/\mathbb{Q}$: semistable elliptic curve

Want to show it's modular

Abs. irred mod 3? $\xrightarrow{\text{No}}$ Abs. irred mod 5!

Yes

Langlands-Tunnell + Modularity lifting

Theorem If E is abs. irred mod 5, $\exists$ another s.stable ell. curve $E'/\mathbb{Q}$

s.t. (i) $|E(\mathbb{Z}/\ell\mathbb{Z})| \equiv |E'(\mathbb{Z}/\ell\mathbb{Z})| \pmod 5$ for almost all ℓ

(ii) E' is abs. irred. mod 3

$\Longrightarrow$ E' is modular $\Longrightarrow$ E is modular mod 5 $\xrightarrow[\text{lifting}]{\text{Mod.}}$ E is modular!