The experiments of Birch and Swinnerton-Dyer

Comp-nt Day 1

Monday, 25th October 2021

Introduction

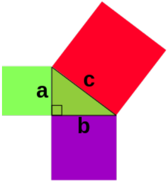
Integral right triangles

Integral right triangles

Recall the Theorem of Pythagoras:

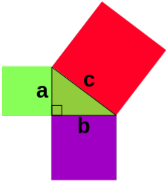
Integral right triangles

Recall the Theorem of Pythagoras:



Integral right triangles

Recall the Theorem of Pythagoras:



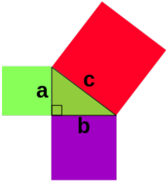
Theorem (Pythagoras)

Let a, b, c be the sides of a right angled triangle. Then

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

Integral right triangles

Recall the Theorem of Pythagoras:



Theorem (Pythagoras)

Let a, b, c be the sides of a right angled triangle. Then

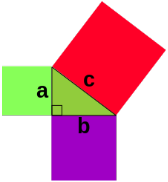
$$a^2 + b^2 = c^2.$$

Question (Ancient Greeks)

Do there exist integral right triangles?

Integral right triangles

Recall the Theorem of Pythagoras:



Theorem (Pythagoras)

Let a, b, c be the sides of a right angled triangle. Then

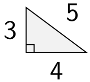
$$a^2 + b^2 = c^2.$$

Question (Ancient Greeks)

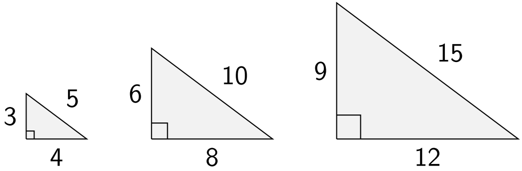
Do there exist integral right triangles? i.e. $a, b, c \in \mathbb{Z}$ *such that* $a^2 + b^2 = c^2$*?*

Yes they do!

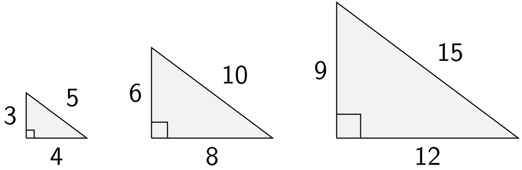
Yes they do!



Yes they do!

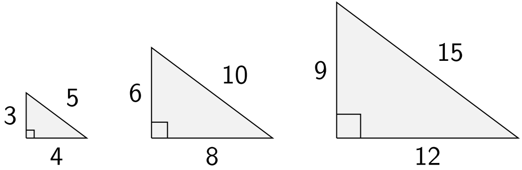


Yes they do!



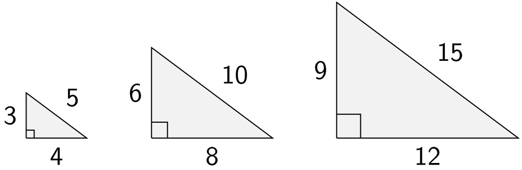
These are all essentially the same triangle. Are there any genuinely different integral right triangles?

Yes they do!

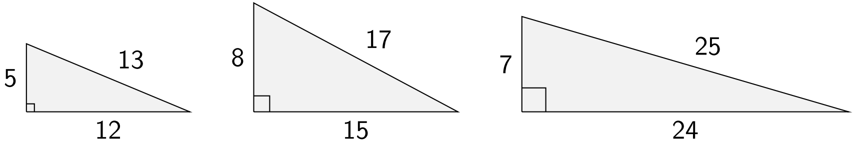


These are all essentially the same triangle. Are there any genuinely different integral right triangles? Yes there are:

Yes they do!

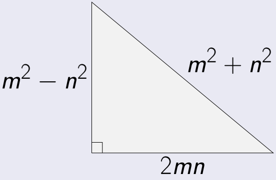


These are all essentially the same triangle. Are there any genuinely different integral right triangles? Yes there are:



Theorem (Euclid, ca. 200 BC)

Every integral right triangle is of the form



for integers $m > n > 0$.

Euclid, from *The School of Athens* by Raphael, 1511

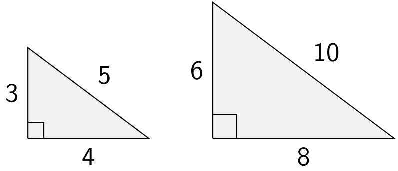
Rational right triangles

Rational right triangles

Recall that we were scaling triangles up:

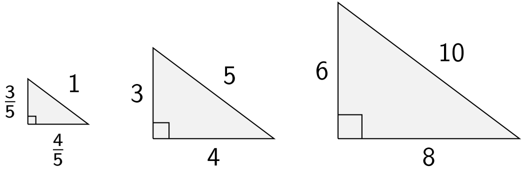
Rational right triangles

Recall that we were scaling triangles up:



Rational right triangles

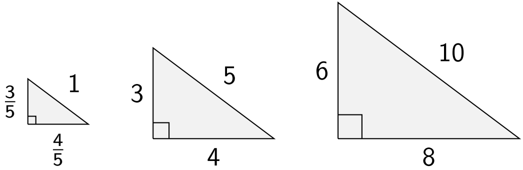
Recall that we were scaling triangles up:



However, we can also scale down.

Rational right triangles

Recall that we were scaling triangles up:



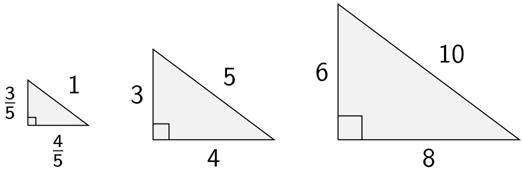
However, we can also scale down.

Definition

A right triangle is called rational if its sides have lengths in the field of rationals $\mathbb{Q}$.

Rational right triangles

Recall that we were scaling triangles up:



However, we can also scale down.

Definition

A right triangle is called rational if its sides have lengths in the field of rationals $\mathbb{Q}$.

Remark

By clearing denominators, every rational right triangle is essentially the same as an integral right triangle. But working with rational triangles instead of integral triangles is often easier because $\mathbb{Q}$ *is a field, whereas* $\mathbb{Z}$ *is not.*

Congruent numbers

Definition

An integer D is called a congruent number if it is the area of a rational right triangle.

Congruent numbers

Definition

An integer D is called a congruent number if it is the area of a rational right triangle.

Question (Anonymous Arab Manuscript, $\leq$ 972 AD)

Which numbers are congruent?

Congruent numbers

Definition

An integer D is called a congruent number if it is the area of a rational right triangle.

Question (Anonymous Arab Manuscript, $\leq$ 972 AD)

Which numbers are congruent?

Example

(3,4,5) $\triangle$ $\Rightarrow$ 6 is congruent.

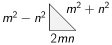
(5,12,13) $\triangle$ $\Rightarrow$ 30 is congruent.

D is congruent $\Leftrightarrow D = \mathrm{Area}\Big($ 

$\Big)$ for $x, y, z \in \mathbb{Q}^+$

D is congruent $\Leftrightarrow D = \text{Area}\Big($ 

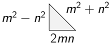
$\Big)$ for $x, y, z \in \mathbb{Q}^+$

(clearing denominators) $\Leftrightarrow Dw^2 = \text{Area}\Big($ 

$\Big)$ for $w, m, n \in \mathbb{Z}^+,\ m > n > 0$

D is congruent $\Leftrightarrow D = \text{Area}\Big($ 

$\Big)$ for $x, y, z \in \mathbb{Q}^+$

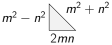
(**clearing denominators**) $\Leftrightarrow Dw^2 = \text{Area}\Big($ 

$\Big)$ for $w, m, n \in \mathbb{Z}^+, \;\; m > n > 0$

$$\Leftrightarrow Dw^2 = mn(m^2 - n^2) \;\; \text{for } w, m, n \in \mathbb{Z}^+, \;\; m > n > 0$$

D is congruent $\Leftrightarrow D = \text{Area}\Big($ 

$\Big)$ for $x, y, z \in \mathbb{Q}^+$

(**clearing denominators**) $\Leftrightarrow Dw^2 = \text{Area}\Big($ 

$\Big)$ for $w, m, n \in \mathbb{Z}^+,\ m > n > 0$

$$\Leftrightarrow Dw^2 = mn(m^2 - n^2) \text{ for } w, m, n \in \mathbb{Z}^+,\ m > n > 0$$

(**setting** $x := \frac{Dm}{n}, y = \frac{D^2 w}{n}$) $\Leftrightarrow y^2 = x^3 - D^2 x$ for $x, y \in \mathbb{Q},\ x \neq 0 \neq y$

$$D \text{ is congruent } \Leftrightarrow D = \text{Area}\left({}^{x}\triangle^{z}_{y} \right) \text{ for } x, y, z \in \mathbb{Q}^+$$

$$(\textbf{clearing denominators}) \Leftrightarrow Dw^2 = \text{Area}\left({}^{m^2-n^2}\triangle^{m^2+n^2}_{2mn} \right) \text{ for } w, m, n \in \mathbb{Z}^+,\ m > n > 0$$

$$\Leftrightarrow Dw^2 = mn(m^2 - n^2) \text{ for } w, m, n \in \mathbb{Z}^+,\ m > n > 0$$

$$\left(\textbf{setting } x := \tfrac{Dm}{n}, y = \tfrac{D^2 w}{n}\right) \Leftrightarrow y^2 = x^3 - D^2 x \text{ for } x, y \in \mathbb{Q},\ x \neq 0 \neq y$$

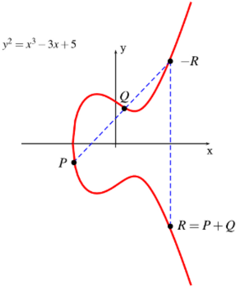
This equation $E_D : y^2 = x^3 - D^2 x$ is an example of an **elliptic curve**, which in general has equation

$$y^2 = x^3 + Ax + B$$

for $A, B \in K$, where K is (almost) *any* field.

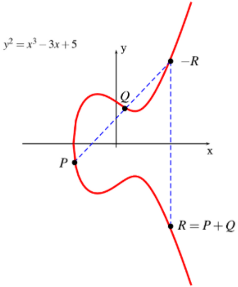
The chord and tangent process

Elliptic curves are remarkable because their set of solutions form a group under the chord and tangent process:



The chord and tangent process

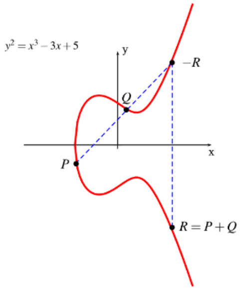
Elliptic curves are remarkable because their set of solutions form a group under the chord and tangent process:



The identity of the group law is the point at infinity O_E, infinitely far up the y-axis.

The chord and tangent process

Elliptic curves are remarkable because their set of solutions form a group under the chord and tangent process:



The identity of the group law is the point at infinity O_E, infinitely far up the y-axis. Most[1] projective curves do not admit a group structure with a geometrical interpretation, making elliptic curves a rather special class among all curves.

[1] If the genus of the curve is ≥ 2

The Mordell-Weil Theorem

Theorem (Mordell-Weil)

Let K be a global field (e.g. a number field), and let E/K be an elliptic curve. Then the group of K-rational points $E(K)$ is a finitely generated abelian group:

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r.$$

The integer r is called the rank of E over K.

Back to congruent numbers ...

D is congruent $\Leftrightarrow y^2 = x^3 - D^2 x$ for $x, y \in \mathbb{Q},\ x \neq 0 \neq y$

Back to congruent numbers ...

$$
\begin{aligned}
D \text{ is congruent } &\Leftrightarrow y^2 = x^3 - D^2x \text{ for } x, y \in \mathbb{Q},\ x \neq 0 \neq y \\
&\Leftrightarrow E_D : y^2 = x^3 - D^2x \text{ admits point } P = (x, y) \text{ with } y \neq 0
\end{aligned}
$$

Back to congruent numbers ...

$$
\begin{aligned}
D \text{ is congruent } &\Leftrightarrow y^2 = x^3 - D^2x \text{ for } x, y \in \mathbb{Q},\ x \neq 0 \neq y \\
&\Leftrightarrow E_D : y^2 = x^3 - D^2x \text{ admits point } P = (x, y) \text{ with } y \neq 0 \\
&\Leftrightarrow E_D \text{ admits a point } P = (x, y) \text{ of infinite order}
\end{aligned}
$$

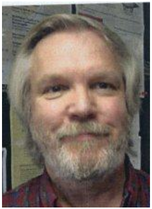
Back to congruent numbers ...

$$
\begin{aligned}
D \text{ is congruent } &\Leftrightarrow y^2 = x^3 - D^2x \text{ for } x, y \in \mathbb{Q},\ x \neq 0 \neq y \\
&\Leftrightarrow E_D : y^2 = x^3 - D^2x \text{ admits point } P = (x, y) \text{ with } y \neq 0 \\
&\Leftrightarrow E_D \text{ admits a point } P = (x, y) \text{ of infinite order} \\
&\Leftrightarrow E_D(\mathbb{Q}) \text{ has positive rank.}
\end{aligned}
$$

Back to congruent numbers ...

$$\begin{aligned} D \text{ is congruent } &\Leftrightarrow y^2 = x^3 - D^2x \text{ for } x, y \in \mathbb{Q},\ x \neq 0 \neq y \\ &\Leftrightarrow E_D : y^2 = x^3 - D^2x \text{ admits point } P = (x, y) \text{ with } y \neq 0 \\ &\Leftrightarrow E_D \text{ admits a point } P = (x, y) \text{ of infinite order} \\ &\Leftrightarrow E_D(\mathbb{Q}) \text{ has positive rank.} \end{aligned}$$

The rank of an elliptic curve is an elusive quantity, so this description doesn't immediately solve the congruent number problem.

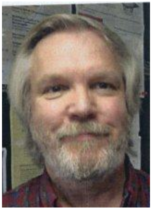


Jerrold B. Tunnell

Theorem (Tunnell, 1983)

For $D \in \mathbb{Z}$, define

$$\begin{aligned} P_D &= \#\left\{(x,y,z) \in \mathbb{Z}^3 | D = 2x^2 + y^2 + 32z^2\right\} \\ Q_D &= \#\left\{(x,y,z) \in \mathbb{Z}^3 | D = 2x^2 + y^2 + 8z^2\right\} \\ R_D &= \#\left\{(x,y,z) \in \mathbb{Z}^3 | D = 8x^2 + 2y^2 + 64z^2\right\} \\ S_D &= \#\left\{(x,y,z) \in \mathbb{Z}^3 | D = 8x^2 + 2y^2 + 16z^2\right\}. \end{aligned}$$



Jerrold B. Tunnell

Theorem (Tunnell, 1983)

For $D \in \mathbb{Z}$, define

$$\begin{aligned}
P_D &= \#\left\{(x, y, z) \in \mathbb{Z}^3 | D = 2x^2 + y^2 + 32z^2\right\} \\
Q_D &= \#\left\{(x, y, z) \in \mathbb{Z}^3 | D = 2x^2 + y^2 + 8z^2\right\} \\
R_D &= \#\left\{(x, y, z) \in \mathbb{Z}^3 | D = 8x^2 + 2y^2 + 64z^2\right\} \\
S_D &= \#\left\{(x, y, z) \in \mathbb{Z}^3 | D = 8x^2 + 2y^2 + 16z^2\right\}.
\end{aligned}$$

Then, assuming the Birch-Swinnerton-Dyer conjecture for elliptic curves,

$$E_D \text{ has positive rank } \Leftrightarrow \begin{cases} 2P_D = Q_D & \text{if } D \text{ is odd} \\ 2R_D = S_D & \text{if } D \text{ is even.} \end{cases}$$

Tunnell's theorem gives a resolution to the ancient Congruent number problem, but assuming a very major conjecture!

Tunnell's theorem gives a resolution to the ancient Congruent number problem, but assuming a very major conjecture!

H.P.F. Swinnerton-Dyer with B. Birch

The Birch-Swinnerton-Dyer conjecture is one of the six Clay Millenium Problems - solving it will earn you $1,000,000!

Tunnell's theorem gives a resolution to the ancient Congruent number problem, but assuming a very major conjecture!

H.P.F. Swinnerton-Dyer with B. Birch

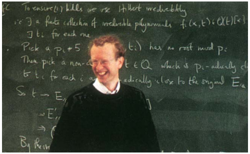
The Birch-Swinnerton-Dyer conjecture is one of the six Clay Millenium Problems - solving it will earn you $1,000,000!

Tunnell's theorem uses the theory of modular forms of half-integral weight. There are many other deep connections between elliptic curves and modular forms.

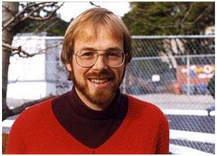
Modularity Theorem (Wiles, Taylor-Wiles, 1995)

Every elliptic curve $E/\mathbb{Q}$ arises from a (weight-2 cuspidal of level $\Gamma_0(N)$) modular form f_E such that the L-functions coincide:

$$L(E, s) = L(f_E, s).$$



Andrew J. Wiles



Richard L. Taylor

Modularity Theorem (Wiles, Taylor-Wiles, 1995)

Every elliptic curve $E/\mathbb{Q}$ arises from a (weight-2 cuspidal of level $\Gamma_0(N)$) modular form f_E such that the L-functions coincide:

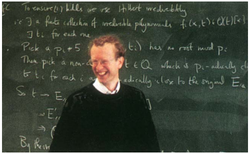
$$L(E, s) = L(f_E, s).$$

Corollary

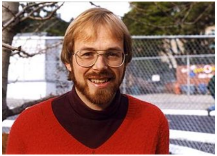
Fermat's Last Theorem is true: for $n > 2$, the equation

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

admits only the trivial solutions (i.e. when $xyz = 0$).



Andrew J. Wiles



Richard L. Taylor

What did Birch and Swinnerton-Dyer actually do?

Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve, e.g.

Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve, e.g.

$$E/\mathbb{Q} : y^2 = x^3 - 17x + 17.$$

Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve, e.g.

$$E/\mathbb{Q} : y^2 = x^3 - 17x + 17.$$

Consider "reading E modulo p", for p a prime:

Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve, e.g.

$$E/\mathbb{Q} : y^2 = x^3 - 17x + 17.$$

Consider "reading E modulo p", for p a prime:

$$E/\mathbb{F}_p : y^2 = x^3 - 17x + 17 \pmod{p}.$$

Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve, e.g.

$$E/\mathbb{Q} : y^2 = x^3 - 17x + 17.$$

Consider "reading E modulo p", for p a prime:

$$E/\mathbb{F}_p : y^2 = x^3 - 17x + 17 \pmod{p}.$$

e.g. $p = 3$, we get

$$\tilde{E}/\mathbb{F}_3 : y^2 = x^3 - 2x + 2 \pmod{3}.$$

Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve, e.g.

$$E/\mathbb{Q} : y^2 = x^3 - 17x + 17.$$

Consider "reading E modulo p", for p a prime:

$$E/\mathbb{F}_p : y^2 = x^3 - 17x + 17 \pmod{p}.$$

e.g. $p = 3$, we get

$$\tilde{E}/\mathbb{F}_3 : y^2 = x^3 - 2x + 2 \pmod{3}.$$

For now, let's not worry about what happens if we take $p = 17$ ...

Number of points mod p

Since $\tilde{E}(\mathbb{F}_p)$ is contained inside $\mathbb{P}^2(\mathbb{F}_p)$ which has only finitely many points, we get that

Number of points mod p

Since $\tilde{E}(\mathbb{F}_p)$ is contained inside $\mathbb{P}^2(\mathbb{F}_p)$ which has only finitely many points, we get that

$N_p := |\tilde{E}(\mathbb{F}_p)|$ is finite.

Number of points mod p

Since $\tilde{E}(\mathbb{F}_p)$ is contained inside $\mathbb{P}^2(\mathbb{F}_p)$ which has only finitely many points, we get that

$N_p := |\tilde{E}(\mathbb{F}_p)|$ is finite.

Until the mid-50s, actually computing these numbers required "lots of pencils and paper" (essentially a quote from Swinnerton-Dyer).

Cambridge University gets EDSAC2

In the late 50s, Cambridge University got one of the first computers.

Cambridge University gets EDSAC2

In the late 50s, Cambridge University got one of the first computers.

Swinnerton-Dyer got a job at the Computer Lab as a “tame mathematician” to run the machine for various queries.

Cambridge University gets EDSAC2

In the late 50s, Cambridge University got one of the first computers.

Swinnerton-Dyer got a job at the Computer Lab as a "tame mathematician" to run the machine for various queries.

In his spare time (in the evenings) he used it to compute N_p values for large primes p.

Cambridge University gets EDSAC2

In the late 50s, Cambridge University got one of the first computers.

Swinnerton-Dyer got a job at the Computer Lab as a "tame mathematician" to run the machine for various queries.

In his spare time (in the evenings) he used it to compute N_p values for large primes p.

He was super-excited to be able to do this for all primes $p \leq 1000$ on some of the E_D elliptic curves from earlier.

It turns out that $N_p = p + 1 - a_p$ for some "error" term a_p, so to get a sense of "how often N_p differs from p" as one varies over all primes p, Birch and Swinnerton-Dyer considered the function

It turns out that $N_p = p + 1 - a_p$ for some "error" term a_p, so to get a sense of "how often N_p differs from p" as one varies over all primes p, Birch and Swinnerton-Dyer considered the function

$$y = f(x) = \prod_{p \leq x} \frac{N_p}{p}$$

for different elliptic curves.

It turns out that $N_p = p + 1 - a_p$ for some "error" term a_p, so to get a sense of "how often N_p differs from p" as one varies over all primes p, Birch and Swinnerton-Dyer considered the function

$$y = f(x) = \prod_{p \leq x} \frac{N_p}{p}$$

for different elliptic curves.

This function may be called the poor-mans L-function of an elliptic curve.

It turns out that $N_p = p + 1 - a_p$ for some "error" term a_p, so to get a sense of "how often N_p differs from p" as one varies over all primes p, Birch and Swinnerton-Dyer considered the function

$$y = f(x) = \prod_{p \leq x} \frac{N_p}{p}$$

for different elliptic curves.

This function may be called the poor-mans L-function of an elliptic curve.

Question

How does $f(x)$ grow as $x \to \infty$?

Based on this, they conjectured

$$\prod_{p \leq x} \frac{N_p}{p} \to C(\log(x))^r \quad \text{as} \quad x \to \infty$$

for C a constant.

Based on this, they conjectured

$$\prod_{p \leq x} \frac{N_p}{p} \to C(\log(x))^r \quad \text{as} \quad x \to \infty$$

for C a constant.

It was only after travelling to the US and meeting Weil that the "gradient of the asymptotic growth" got interpreted as the order of vanishing of the L-function at $s = 1$, which is the modern formulation:

Based on this, they conjectured

$$\prod_{p \leq x} \frac{N_p}{p} \to C(\log(x))^r \quad \text{as} \quad x \to \infty$$

for C a constant.

It was only after travelling to the US and meeting Weil that the "gradient of the asymptotic growth" got interpreted as the order of vanishing of the L-function at $s = 1$, which is the modern formulation:

Conjecture (The Birch and Swinnerton-Dyer conjecture (weak))

Let E/K be an elliptic curve over a number field, and $L(E/K, s)$ its L-function. Then

$$ord_{s=1}(L(E/K, s) = rank(E(K)).$$

Based on this, they conjectured

$$\prod_{p \leq x} \frac{N_p}{p} \to C(\log(x))^r \quad \text{as} \quad x \to \infty$$

for C a constant.

It was only after travelling to the US and meeting Weil that the "gradient of the asymptotic growth" got interpreted as the order of vanishing of the L-function at $s = 1$, which is the modern formulation:

Conjecture (The Birch and Swinnerton-Dyer conjecture (weak))

Let E/K be an elliptic curve over a number field, and $L(E/K, s)$ its L-function. Then

$$ord_{s=1}(L(E/K, s) = rank(E(K)).$$

(The strong version relates the leading coefficient of the Taylor expansion of $L(E/K, s)$ to arithmetic data of E/K.)