Right triangles and elliptic curves

Karl Rubin

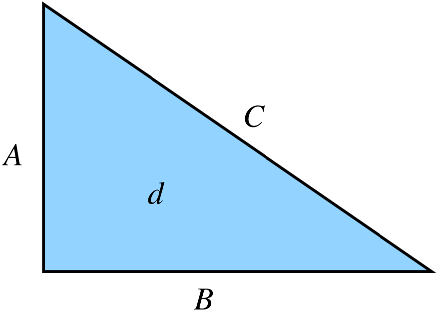
UCIrvine
UNIVERSITY OF CALIFORNIA, IRVINE

Ross Reunion July 2007

Rational right triangles

Question

Given a positive integer d, is there a right triangle with rational sides and area d?



- Pythagorean Theorem:

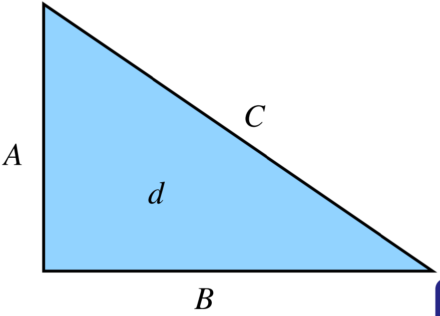
$$A^2 + B^2 = C^2$$

- Area: $d = \dfrac{AB}{2}$

Rational right triangles

Question

Given a positive integer d, is there a right triangle with rational sides and area d?



Examples:

- $A = 3, \; B = 4, \; C = 5$

  $d = 6$

- $A = \frac{3}{2}, \; B = \frac{20}{3}, \; C = \frac{41}{6}$

  $d = 5$

Theorem (Fermat, ∼1640)

There is no rational right triangle with area 1.

“Answer”

Suppose d is a positive integer, not divisible by the square of an integer bigger than 1. Let $a = 1$ if d is odd, and $a = 2$ if d is even, and

$$n = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2ay^2 + 8z^2 = d/a\}$$
$$m = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2ay^2 + 32z^2 = d/a\}$$

counting *integer* solutions (positive, negative, or zero) x, y, z.

Theorem (Tunnell, 1983)

If $n \neq 2m$, then there is no rational right triangle with area d.

Conjecture

If $n = 2m$, then there is a rational right triangle with area d.

"Answer"

Suppose d is a positive squarefree integer, and $a = (d,2)$. Let

$$n = \#\{(x,y,z) : x^2 + 2ay^2 + 8z^2 = d/a\}$$
$$m = \#\{(x,y,z) : x^2 + 2ay^2 + 32z^2 = d/a\}$$

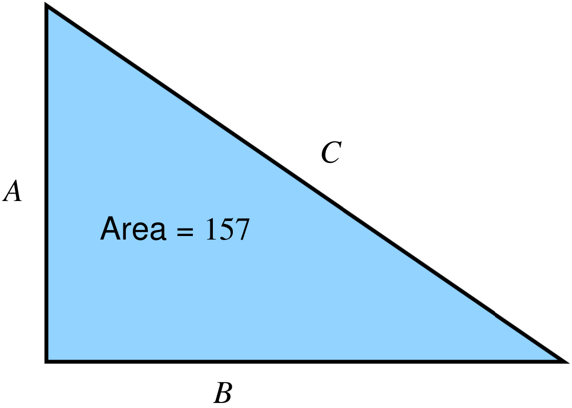
d	1	2	3	5	6	7	11	41	$\cdots$	157	$\cdots$	$5, 6,$ or $7 \pmod 8$
n	2	2	4	0	0	0	12	32		0		0
m	2	2	4	0	0	0	4	16		0		0

“Answer”

d	right triangle with area d
1	none
2	none
3	none
5	$(3/2, 20/3, 41/6)$
6	$(3, 4, 5)$
7	$(24/5, 35/12, 337/60)$
11	none
41	$(40/3, 123/20, 881/60)$
157	?

d	1	2	3	5	6	7	11	41	$\cdots$	157	$\cdots$	$5, 6,$ or $7 \pmod 8$
n	2	2	4	0	0	0	12	32		0		0
m	2	2	4	0	0	0	4	16		0		0

$d = 157$



$$A = \frac{411340519227716149383203}{21666555693714761309610}$$

$$B = \frac{6803298487826435051217540}{411340519227716149383203}$$

$$C = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

5, 6, and 7 $\pmod 8$

Conjecture

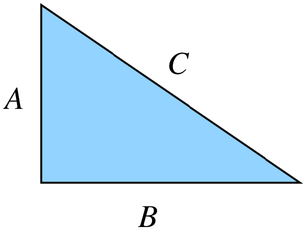
If d is positive, squarefree, and $d \equiv 5, 6,$ or $7 \pmod 8$, then there is a rational right triangle with area d.

This has been verified for $d < 1,000,000$.

Theorem

If p is a prime, and $p \equiv 5$ or $7 \pmod 8$, then there is a rational right triangle with area p.

Translating the question

If 

has area d …

…then $x = \frac{1}{2}A(A-C)$, $y = \frac{1}{2}A^2(C-A)$ is a solution of

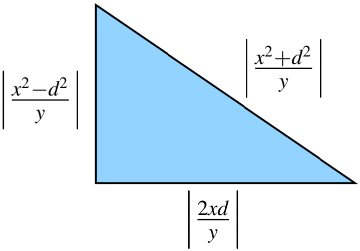
$$y^2 = x^3 - d^2x.$$

For example, the $(3,4,5)$ triangle with area 6 gives the solution $(-3,9)$ of $y^2 = x^3 - 36x$.

Translating the question

If (x, y) is a solution of $y^2 = x^3 - d^2x$, and $y \neq 0$ ...

then



is a right triangle with area d.

Translating the question

Theorem

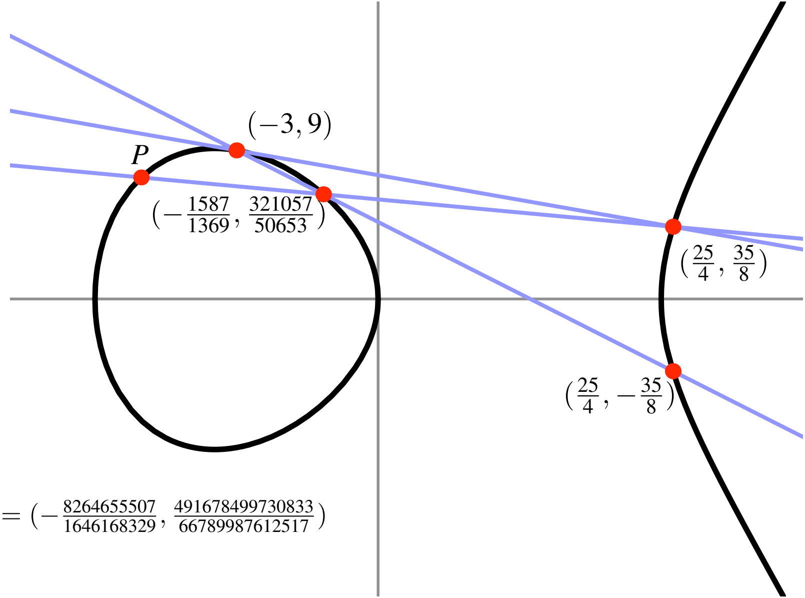
There is a rational right triangle with area d

if and only if

there are rational numbers x and y, $y \neq 0$, such that $y^2 = x^3 - d^2x$.

The equation $y^2 = x^3 - d^2x$ is an elliptic curve.

$y^2 = x^3 - 36x$



$$P = \left(-\frac{8264655507}{1646168329}, \frac{491678499730833}{66789987612517}\right)$$

$y^2 = x^3 - 36x$

In fact, this procedure gives *infinitely many* rational solutions (x, y) of the equation $y^2 = x^3 - 36x$, so there are *infinitely many* rational right triangles with area 6.

Some right triangles with area 6

$3 \quad 4 \quad 5$

$\frac{7}{10} \quad \frac{120}{7} \quad \frac{1201}{70}$

$\frac{4653}{851} \quad \frac{3404}{1551} \quad \frac{7776485}{1319901}$

$\frac{1437599}{168140} \quad \frac{2017680}{1437599} \quad \frac{2094350404801}{241717895860}$

$\frac{3122541453}{2129555051} \quad \frac{8518220204}{1040847151} \quad \frac{18428872963986767525}{2216541307731009701}$

$\frac{43690772126393}{20528380655970} \quad \frac{246340567871640}{43690772126393} \quad \frac{5405257799550679424342410801}{896900801363839325090016210}$

$\frac{139321523551022904 03}{884619602260392601} \quad \frac{3538478409041570404}{4644050785034096801} \quad \frac{64777297161660083702224674830494320965}{4108218358333926731621213541698169401}$

$\frac{41561188085489679417 69601}{10124839460840739240477 20} \quad \frac{1214980735300888708857 2640}{41561188085489679417 69601} \quad \frac{2120599530936633126752254320635080079967772 8019201}{4208003571673898812953630313884276610165569359720}$

$\frac{5628773675353652252514840 84003}{9096802581030701081135787921001}$

$\frac{318497209829094206727124168815460900807}{81696716359207757071479211742813520050}$

$\frac{8552954436381428255942182374519699202802928 2253}{454789373799282177611248467630262117949339 9749}$

$\frac{2192913891960404693804016374075761895352212725856781 8399}{969596010399029433102598494384114956082566977513816 8420}$

$\frac{107678491232504214629027366203609143706610045561881253147888227347}{80304789058118229075736578976728059627039657981964461933622942851}$

$\frac{4176501831301593836542885342768698632287714214832228338980765292538706358393}{532238562805568241491490558109034414979225647633848461831768367334071583930}$

$\frac{1079105871168987121006453902668412947766665234341778960385423262791622087404656103595203}{185464238582965240005930623598461000901089939509317879474651315129697183338323743861199}$

$\frac{147041175918614622878834609763844737863238509623432216983017702582510228429899319383526553807398401}{178469808005426933574772082424814735318789288015046635216293058541114735982691961198186826871967440}$

$\frac{4070056675448836579024879370271267980956229345588329478596840641287521113637800807862653771565199120693031057597}{1429074121970706033855720824145960825829305397068390644927313224349582184764846147591378216841482986847582555601}$

$\frac{109565800840255303348288858797431823906809310407172779909217038823592251715733191650183352374951410179667208161417205417936007}{1129923003469755304557346049544320420591109221557621543965948977234077059160030475517429354890371843356582997577908093920090}$

The numerator and denominator of a side of the n-th triangle each have about $.38n^2$ digits.

Elliptic curves

An *elliptic curve* is a curve defined by a cubic equation

$$y^2 = x^3 + ax + b$$

with constants $a, b \in \mathbb{Z}$, and

$$\Delta := -16(4a^3 + 27b^2) \neq 0.$$

(One should really think of it as a curve

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

in 2-dimensional projective space.)

Elliptic curves

Basic Problem

If E *is the elliptic curve* $y^2 = x^3 + ax + b$, *find all rational solutions (rational points):*

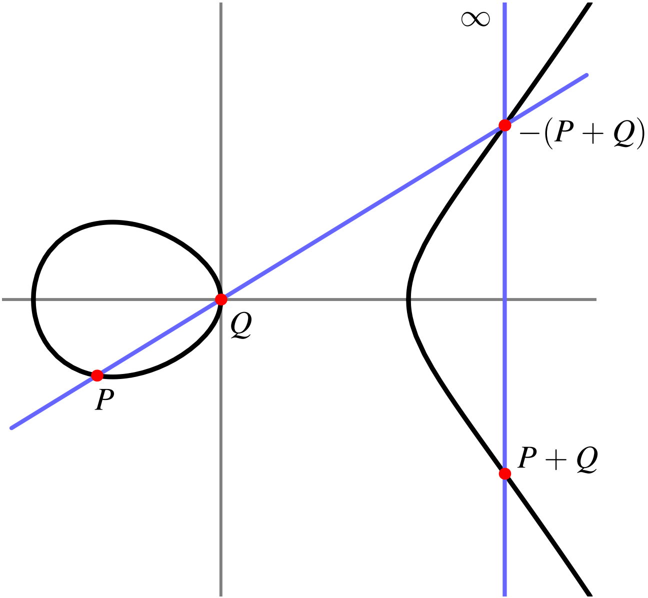
$$E(\mathbb{Q}) := \{(x,y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

Example (Fermat)

If E *is* $y^2 = x^3 - x$, *then* $E(\mathbb{Q}) = \{(0,0),(1,0),(-1,0),\infty\}$.
(*In particular, there is no rational right triangle with area* 1.)

The chord-and-tangent process can be used to define an addition law on $E(\mathbb{Q})$, making $E(\mathbb{Q})$ a commutative group.

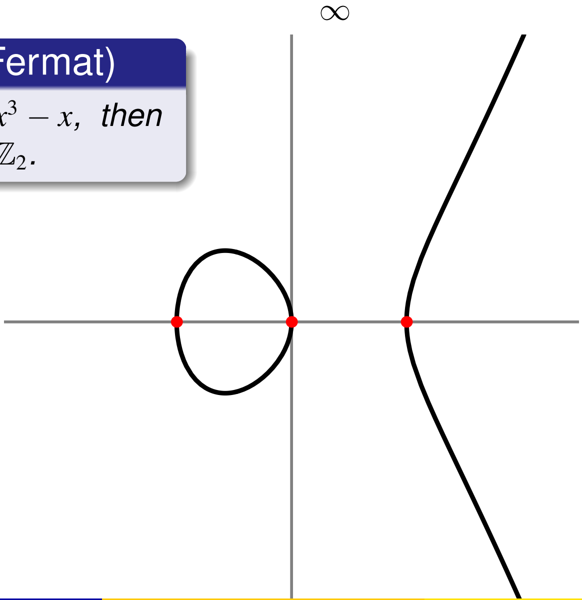
Elliptic curves



Elliptic curves

Example (Fermat)

If E *is* $y^2 = x^3 - x$, *then* $E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.



Elliptic curves

Theorem (Mordell, 1922)

The group $E(\mathbb{Q})$ is finitely generated.

In other words, although $E(\mathbb{Q})$ may be infinite, there is always a finite set of points $\{P_1, \ldots, P_r\}$ that generates all points in $E(\mathbb{Q})$ under the chord-and-tangent process.

In other other words,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$$

where

- r is a nonnegative integer, called the *rank* of E,
- $E(\mathbb{Q})_{\text{tors}}$ is a finite group, made up of all points that have finite order under the group law on E.

Points of finite order

Theorem (Nagell, Lutz, 1937)

If $(x, y) \in E(\mathbb{Q})_{\text{tors}}$, *then* $x, y \in \mathbb{Z}$ *and either* $y = 0$ *or* $y^2 \mid \Delta$.

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{\text{tors}}$ *is one of the following* 15 *groups:*

- $\mathbb{Z}_n$, $1 \le n \le 10$ *or* $n = 12$,
- $\mathbb{Z}_2 \times \mathbb{Z}_{2m}$, $1 \le m \le 4$

and each of these groups occurs infinitely often.

Points of finite order

Example

If E_d *is* $y^2 = x^3 - d^2x$ *then*

$$E_d(\mathbb{Q})_{\mathrm{tors}} = \{(0,0), (d,0), (-d,0), \infty\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Theorem

There is a rational right triangle with area d *if and only if* $E_d(\mathbb{Q})$ *is infinite.*

Corollary

If there is one rational right triangle with area d, *then there are infinitely many.*

Ranks

Equivalently, there is a rational right triangle with area d if and only if the rank of $E(\mathbb{Q})$ is nonzero.

Unfortunately, the rank is very mysterious.

- There is no known algorithm guaranteed to determine the rank.
- It is not known which ranks can occur.

How can we determine the rank, or at least determine whether $E(\mathbb{Q})$ is infinite?

Ranks

Another interpretation of the rank:

There is a constant $C \in \mathbb{R}^+$ *such that*

$$\#\{(x,y) \in E(\mathbb{Q}) : x = \tfrac{a}{b},\ h(a), h(b) < B\}$$

grows like $C \log(B)^{\mathrm{rank}(E)/2}$.

Rank 28 (Elkies)

Currently the largest known rank is (at least) 28:

$$E : y^2 = x^3 + ax + b$$

$$a = -321084198649208425360531331349416684014883684994863304027$$
$$b = 2206823154881955613890111083863921905341572013635896211771607846947800439724000275446$$

$$P_1 = (-2124150091254381073292137463, 259854492051899599030515511070780628911531)$$
$$P_2 = (2334509866034701756884754537, 18872004195494469180868316552803627931531)$$
$$P_3 = (-1671736054062369063879038663, 251709377261144287808506947241319126049131)$$
$$P_4 = (2139130260139156666492982137, 36639509171439729202421459692941297527531)$$
$$P_5 = (1534706764467120723885477337, 85429585346017694289021032862781072799531)$$
$$P_6 = (-2731079487875677033341575063, 262521815484332191641284072623902143387531)$$
$$P_7 = (2775726266844571649705458537, 12845755474014060248869487699082640369931)$$
$$P_8 = (1494385729327188957541833817, 88486605527733405986116494514049233411451)$$
$$P_9 = (1868438228620887358509065257, 59237403214437708712725140393059358589131)$$
$$P_{10} = (2008945108825743774866542537, 47690677880125552882151750781541424711531)$$
$$P_{11} = (2348360540918025169651632937, 17492930006200557857340332476448804363531)$$
$$P_{12} = (-1472084007090481174470008663, 246643450653503714199947441549759798469131)$$
$$P_{13} = (2924128607708061213363288937, 28350264431488878501488356474767375899531)$$
$$P_{14} = (5374993891066061893293934537, 286188908427263386451175031916479893731531)$$
$$P_{15} = (1709690768233354523334008557, 71898834974686089466159700529215980921631)$$

Counting points modulo p

Instead of trying to "count" $E(\mathbb{Q})$, for primes p count

$$E(\mathbb{Z}_p) := \{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\infty\}$$

Example

$E : y^2 = x^3 + 2x + 1$
$p = 5$

x	$x^3 + 2x + 1 \pmod{5}$	y
0	1	$1, 4$
1	4	$2, 3$
2	3	–
3	4	$2, 3$
4	3	–

so $E(\mathbb{Z}_5)$ *has* 7 *points.*

Counting points modulo p

Theorem (Gauss)

If E_d *is the elliptic curve* $y^2 = x^3 - d^2x$ *and* $p \nmid 2d$, *then*

- $\#(E(\mathbb{Z}_p)) = p + 1$ *if* $p \equiv 3 \pmod 4$,
- $\#(E(\mathbb{Z}_p)) = p + 1 - 2\left(\frac{d}{p}\right)u$ *if* $p \equiv 1 \pmod 4$, *where*
  $\left(\frac{d}{p}\right)$ *is the Legendre symbol,*
  $p = u^2 + v^2$, v *is even, and* $u \equiv v + 1 \pmod 4$.

Idea of Birch and Swinnerton-Dyer

There is a “reduction map”

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{Z}_p).$$

Birch and Swinnerton-Dyer suggested that the larger $E(\mathbb{Q})$ is, the larger the $E(\mathbb{Z}_p)$ should be “on average”.

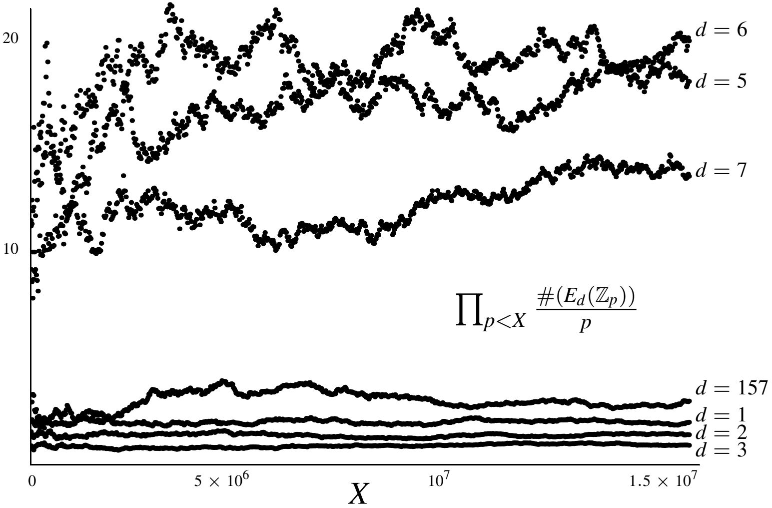
How can we measure this?

Birch and Swinnerton-Dyer computed

$$\prod_{p<X} \frac{\#(E(\mathbb{Z}_p))}{p}$$

as X grows.

Data for $y^2 = x^3 - d^2x$



Better idea

Define the *L-function of E*

$$L(E,s) := \prod_p \left(1 - \frac{1+p-\#(E(\mathbb{Z}_p))}{p^s} + \frac{p}{p^{2s}}\right)^{-1}.$$

As a function of the complex variable s, this product converges on the half-plane $\mathrm{Re}(s) > 3/2$.

If we set $s = 1$ (!!!)

$$L(E,1) \text{ “} = \text{”} \prod_p \left(\frac{\#(E(\mathbb{Z}_p))}{p}\right)^{-1}.$$

This is (the inverse of) what Birch and Swinnerton-Dyer were computing.

Better idea

The Birch and Swinnerton-Dyer “heuristic” predicts that $L(E,1)$ should tell us how big $E(\mathbb{Q})$ is.

Theorem (Wiles et al., 1999)

$L(E,s)$ *has an analytic continuation to the entire complex plane.*

Conjecture (Birch and Swinnerton-Dyer)

$E(\mathbb{Q})$ *is infinite if and only if* $L(E,1) = 0$*.*

(In fact, they conjecture that $\mathrm{rank}(E) = \mathrm{ord}_{s=1} L(E,s)$.)

Theorem

Theorem (Coates & Wiles, Kolyvagin, Kato, . . .)

If $E(\mathbb{Q})$ *is infinite, then* $L(E,1) = 0$*.*

Now let E_d be the elliptic curve $y^2 = x^3 - d^2x$, where d is a positive squarefree integer.

Corollary

If there is a right triangle with rational sides and area d*, then* $L(E_d,1) = 0$*.*

We need a way to evaluate $L(E_d,1)$.

$L(E_d, 1)$

Theorem (Tunnell)

Let E_d be the elliptic curve $y^2 = x^3 - d^2x$. Then

$$L(E_d, 1) = \frac{a(n-2m)^2}{16\sqrt{d}} \int_1^\infty \frac{dx}{\sqrt{x^3 - x}}$$

where $a = 1$ if d is odd, and $a = 2$ if d is even,

$$n = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 2ay^2 + 8z^2 = d/a\},$$
$$m = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 2ay^2 + 32z^2 = d/a\}.$$

Corollary

If there is a right triangle with rational sides and area d, then $n = 2m$.

Open questions

1. Prove the converse: if $n = 2m$, then there is a rational right triangle with area d.
2. If $n = 2m$, *find* a rational right triangle with area d. (There is a method that works “most”(?) of the time, including $d = 157$, but not always.)
3. How often is there a rational right triangle with area d, if $d \equiv 1, 2,$ or $3 \pmod 8$? (Guess: the number of such $d < X$ is about $X^{3/4}$).

Right triangles and elliptic curves

Karl Rubin

UCIrvine
UNIVERSITY OF CALIFORNIA, IRVINE

Ross Reunion July 2007