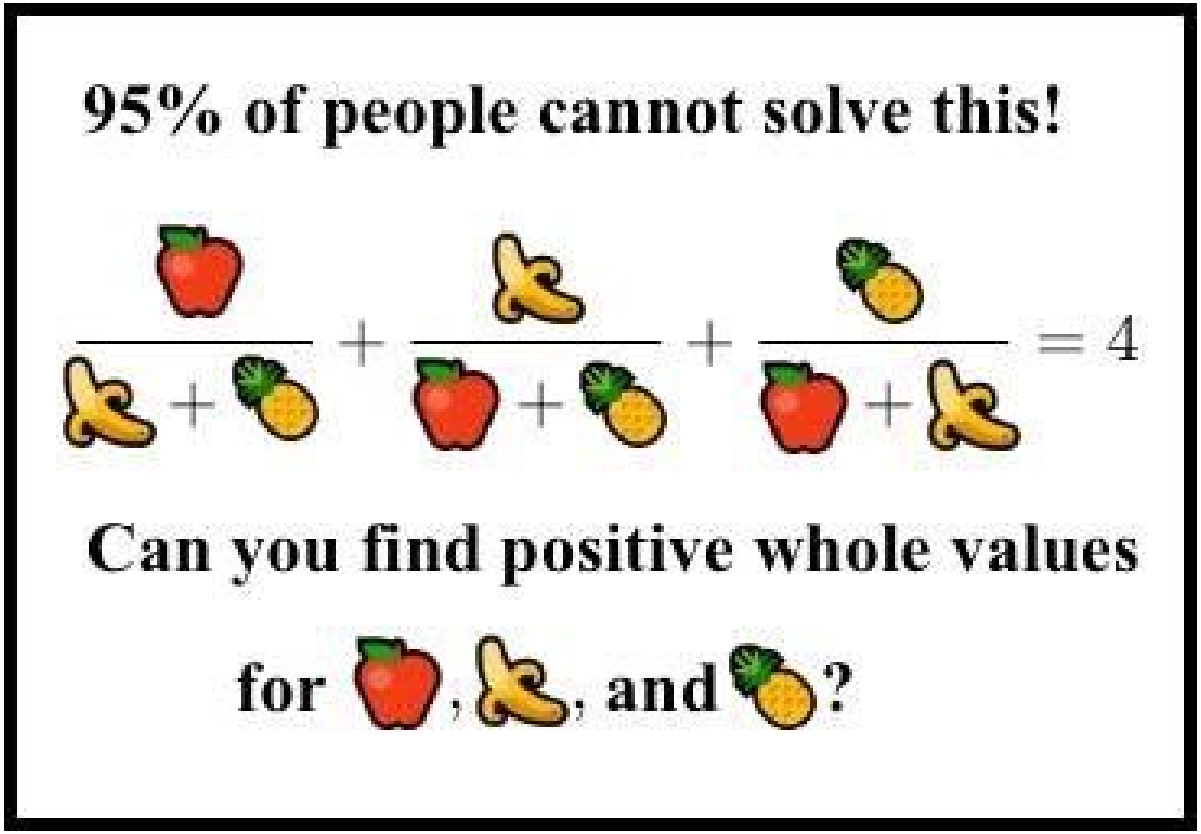
Elliptic Curves and a 95% Hard Problem

Richard Xu

Harvard University

September 16, 2020

The Problem



Take 1-2 minutes to think about this problem.

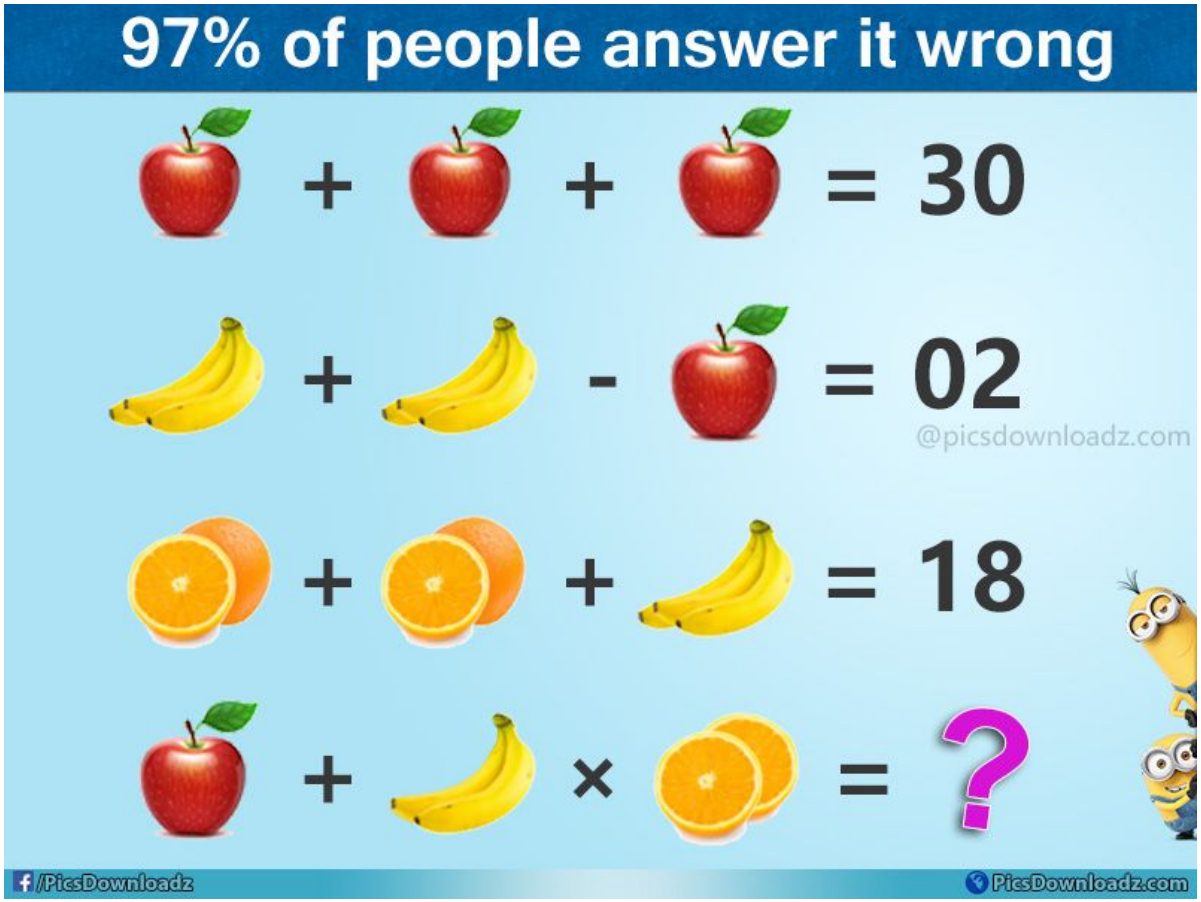
The Problem, cont.

Solution: $a \approx 1.54 \cdot 10^{80}$, $b \approx 3.69 \cdot 10^{79}$, $c \approx 4.37 \cdot 10^{78}$.

```
>>> from fractions import Fraction
>>> a=154476802108746166441951315019919837485664325669565431700026634898253202035277999
>>> b=368751317941299998271978115652254748254929799689719709962831374716372246340555 79
>>> c=437361267792869725786125260237139015281653755816161361862143799337842346777 2036
>>> Fraction(a,b+c)+Fraction(b,a+c)+Fraction(c,a+b)
Fraction(4, 1)
>>>
```

The origin

Back to 2017 and Viral Facebook Posts...



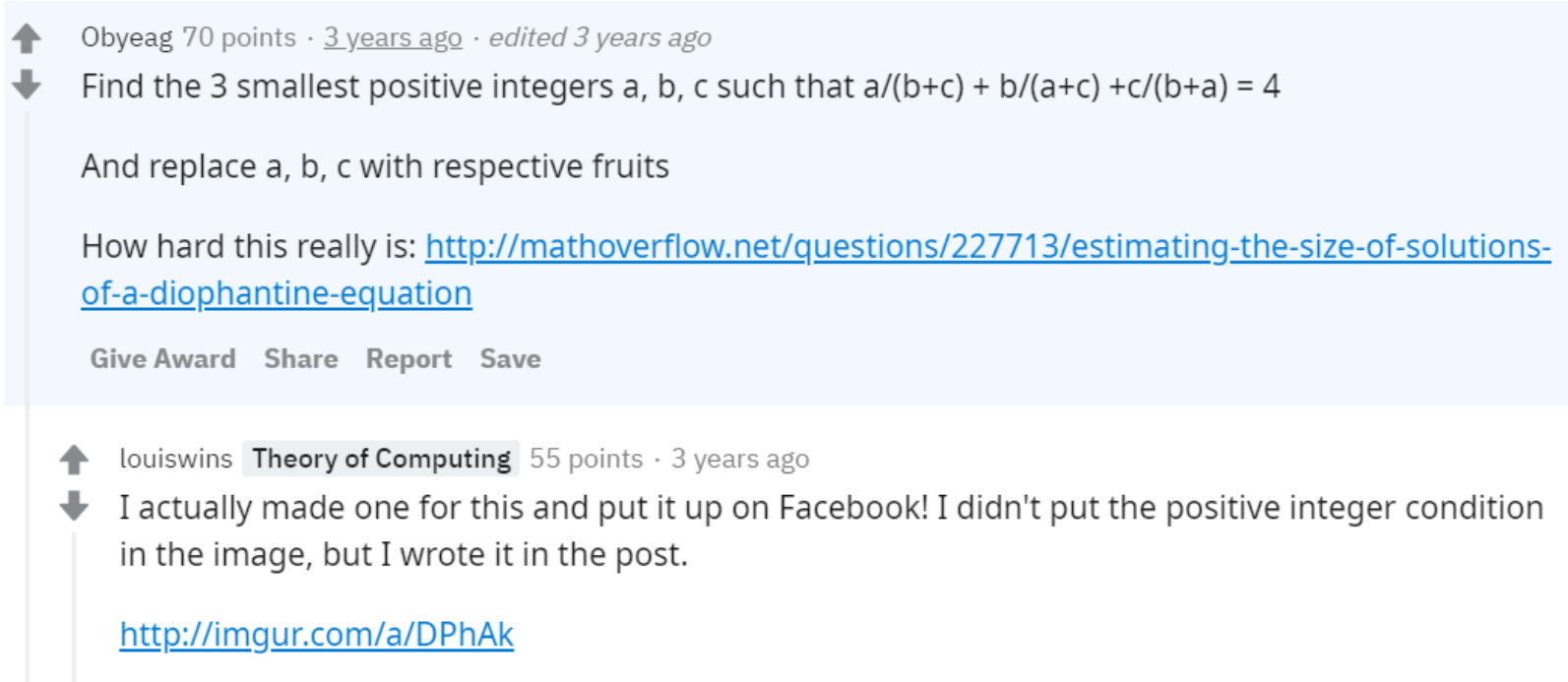
The origin, cont.

Someone had enough.

> **[request/fun] I'm really sick of all the facebook fruit math bull that's going on lately. Does anyone want to create a truly difficult math problem with pictures of fruit to counter this?**
>
> I bet you've encountered this already. If you haven't you can google *facebook fruit math* to get the idea. Basically shit like this or this.
>
> It's always accompanied with captions like "95% of people get this wrong", "only mathematicians know the answer" or "Albert Einstein designed this equation"....
>
> Can we make a problem out of this fruit so that only *actual* mathematicians or engineers can find the answer?

The origin, cont.

Soon, we have a winner.



Obyeag 70 points · 3 years ago · *edited 3 years ago*

Find the 3 smallest positive integers a, b, c such that a/(b+c) + b/(a+c) +c/(b+a) = 4

And replace a, b, c with respective fruits

How hard this really is: http://mathoverflow.net/questions/227713/estimating-the-size-of-solutions-of-a-diophantine-equation

Give Award Share Report Save

louiswins **Theory of Computing** 55 points · 3 years ago

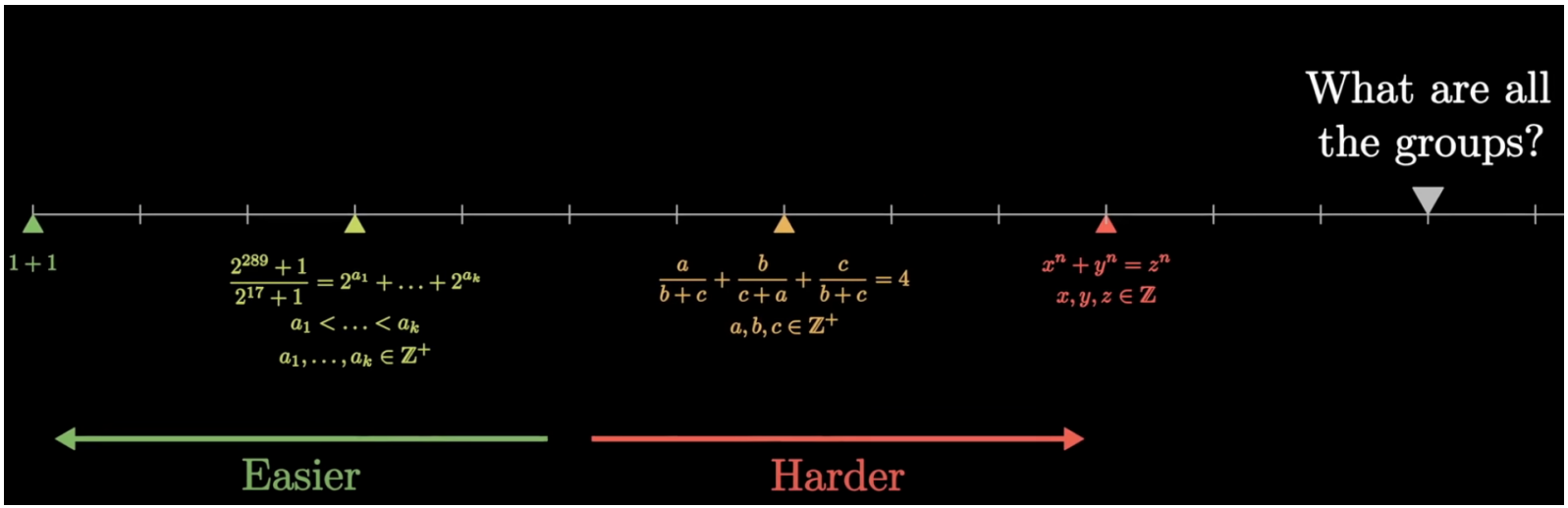
I actually made one for this and put it up on Facebook! I didn't put the positive integer condition in the image, but I wrote it in the post.

http://imgur.com/a/DPhAk

It is 1. not famous enough, 2. innocent looking and 3. has a solution.

Math culture reference

Recent reference in a 3Blue1Brown video:



Homogeneous Polynomials

Let's go back to the original equation:

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4.$$

Alternatively,

$$a^3 + b^3 + c^3 + abc - 3(a+b)(b+c)(c+a) = 0.$$

Homogeneous Polynomials

Let's go back to the original equation:

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4.$$

Alternatively,

$$a^3 + b^3 + c^3 + abc - 3(a+b)(b+c)(c+a) = 0.$$

If (a, b, c) is a solution, so is $(\lambda a, \lambda b, \lambda c)$.

Projective Space

We will work over $\mathbb{R}$.
The projective 2-space over $\mathbb{R}$, denoted $\mathbb{RP}^2$ or $\mathbb{P}^2$, is the set of all lines through the origin in $\mathbb{R}^3$.
An element $p \in \mathbb{P}^2$ has the form $[X : Y : Z]$, and
$[X : Y : Z] \sim [\lambda X : \lambda Y : \lambda Z]$.

Projective Space

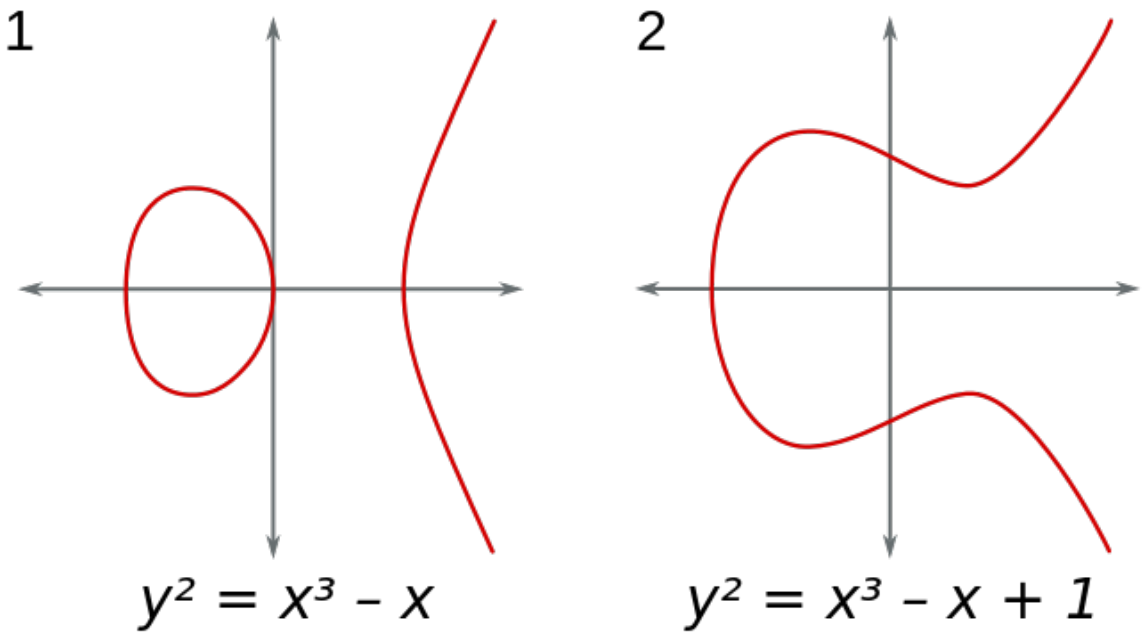
We will work over $\mathbb{R}$.
The projective 2-space over $\mathbb{R}$, denoted $\mathbb{RP}^2$ or $\mathbb{P}^2$, is the set of all lines through the origin in $\mathbb{R}^3$.
An element $p \in \mathbb{P}^2$ has the form $[X : Y : Z]$, and
$[X : Y : Z] \sim [\lambda X : \lambda Y : \lambda Z]$.
Define $U_3 = \{[X : Y : Z] | Z \neq 0\} \subset \mathbb{P}^2$, then each element $p \in U_3$ can be written uniquely as $P = [x : y : 1]$.

Elliptic Curves

We have a *cubic* polynomial

$$a^3 + b^3 + c^3 + abc - 3(a+b)(b+c)(c=a)$$

on the *projective plane*. Next, notice that our polynomial has some easy rational solutions: $[1 : -1 : 0]$ and its 6 permutations. So, we have an *elliptic curve over* $\mathbb{Q}$!



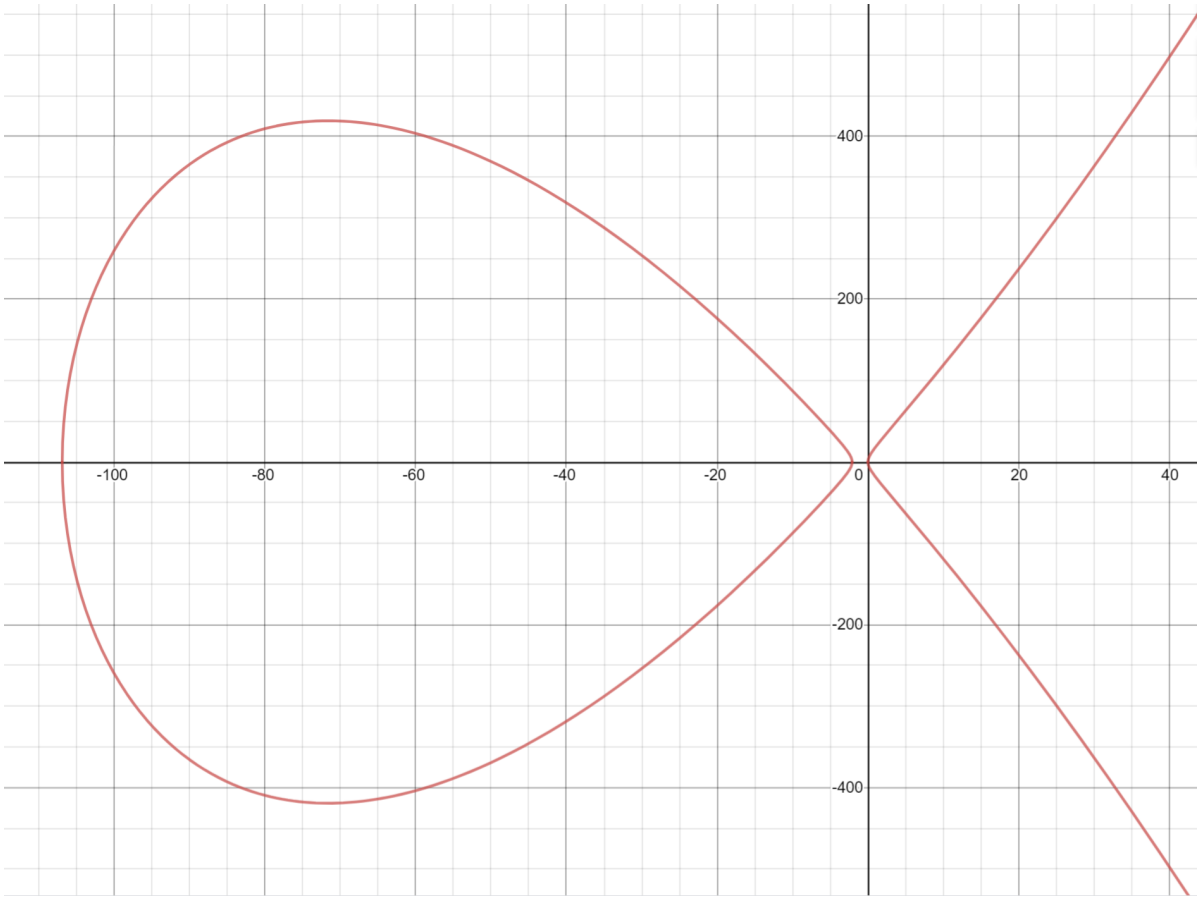
Weierstrass Normal Form

The form $y^2 = x^3 + ax^2 + bx + c$ is known as the Weierstrass normal form, and we can get to it with some (tedious) transformations.
We dehomogenize w.r.t c and do some long math to get
$y^2 = x^3 + 109x^2 + 224x$, with the relations

$$x = \frac{-28(a+b+c)}{6a+6b-c}, y = \frac{364(a-b)}{6a+6b-c}.$$

Weierstrass, cont.

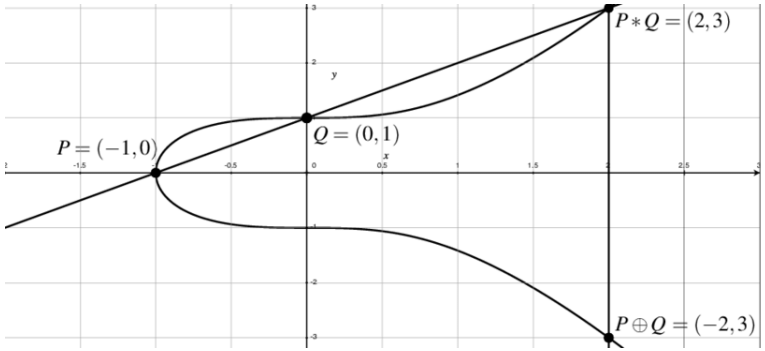
Here's a nice Desmos picture of it!



Group Law on Elliptic Curve

The points on an elliptic curve E form a *group*, with addition defined as follows:
Given two points P and Q,

1. Define $O = [0 : 1 : 0]$.
2. Draw the line going through P and Q, intersects the curve at another point (why?). Call that point R.
3. Define $P + Q := -R$.



Rational Points

1. The rational points on E form a subgroup $E(\mathbb{Q}) \subset E$.
2. Take an small (negative) solution, e.g. $(a, b, c) = (4, -1, 11)$ and drag it through the affine transformations to get $P = (-100, 260)$ is a rational point.
3. Check on each step whether we get a positive solution (a, b, c).

At $9P \approx (-4.8986, 37.4273)$, we find our 80-digit solution from before.

Is this the smallest?

This 80-digit solution feels big. Is there a smaller one?

1. Define a height function $h(P) = \log \max(|p|, |q|)$, $P = (x, y), x = p/q$. This represents how "complicated" a point is.
2. Notice that for a finite n, there are only finitely many points P with $h(P) < n$.
3. If another family of solutions Q were to exist, we can use infinite descent to find a point $P' = aP + bQ$ with small height, but checking all the points leave us empty handed.

Extension: Mordell-Weil

The Mordell-Weil theorem: the group $E(\mathbb{Q})$ is a finitely generated Abelian group.

1. How big can the *rank* of $E(\mathbb{Q})$ be? Open question. It is at least 28 (Elkies 2006), and we have a curve with rank exactly 20 (Elkies-Klagsbrun 2020).
2. The rank of $E(\mathbb{Q})$ seems connected to the HasseWeil zeta function. Is this always the case? This is the Birch and Swinnerton-Dyer conjecture.
3. \$1,000,000

What about other n?

You may think other cases are simpler. However, $n = 4$ is one of the *simplest* cases.

Bremner, Macleod 2014:

N	m	# digits	N	m	# digits	N	m	# digits
4	9	81	48	311	418086	136	65	26942
6	11	134	58	221	244860	146	307	259164
10	13	190	60	61	9188	156	353	12046628
12	35	2707	66	107	215532	158	1211	15097279
14	47	1876	76	65	23662	162	457	1265063
16	11	414	82	157	85465	178	2945	398605460
18	49	10323	92	321	252817	182	853	2828781
24	107	33644	102	423	625533	184	851	20770896
28	121	81853	112	223	935970	186	643	5442988
32	65	14836	116	101	112519	196	701	11323026
38	659	1584369	126	75	196670	198	121	726373
42	419	886344	130	707	8572242	200	2957	71225279
46	201	198771	132	461	3607937			

Table 2: The maximum number of digits in a, b, c in the range $1 \leq N \leq 200$

References

The talk is inspired by Alon Amit's post on Quora. Much of the algebraic geometry background are from Brooke Ullery's Math 137 course, Silverman *The Arithmetic of Elliptic Curves* and Wikipedia.