An unusual cubic representation problem

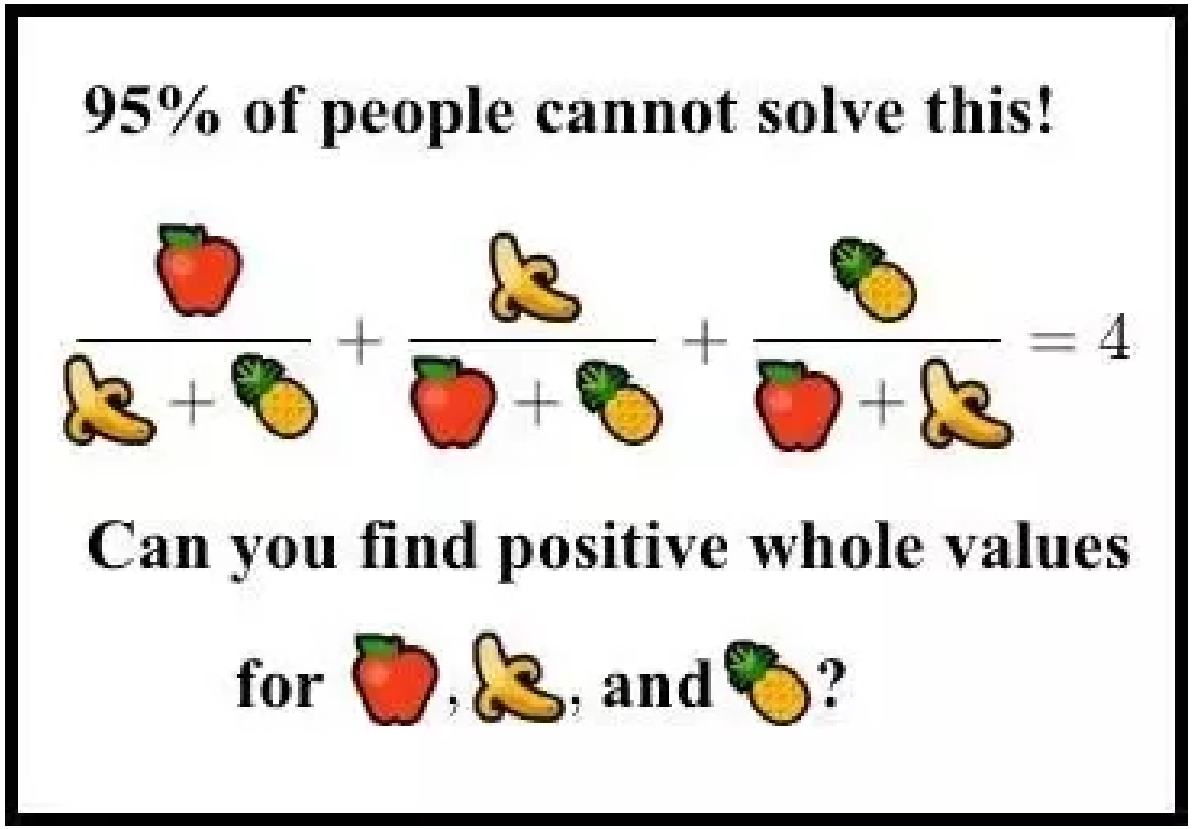
Undergraduate mathematics colloquium

David Kurniadi Angdinata

Imperial College London

Wednesday, 16 January 2019

An unusual cubic representation problem



$$\text{APPLE} = 154476802108746166441951315019919837485664325669565431700026634898253202035277999$$

$$\text{BANANA} = 368751317941299998271978115652254748254929799689719709962831374716372246340555 79$$

$$\text{PINEAPPLE} = 437361267792869725786125260237139015281653755816161361862143799337842346777 2036$$

A trivial cubic representation problem

95% of people cannot solve this!

Can you find values for  ,  , and  ?

$\mathbb{C}, \mathbb{R} : (a, b, c) = (2 + \sqrt{3}, 1, 0)$

$\mathbb{Q}, \mathbb{Z} : (a, b, c) = (11, 4, -1), (-11, -4, 1), (1, -4, -11), \ldots$

A less unusual cubic representation problem

$$\frac{a}{b+c}+\frac{b}{a+c}+\frac{c}{a+b}=4, \qquad a,b,c\in\mathbb{Z}.$$

- Require $a,b,c>0$.

Clear denominators:

$$a^3+b^3+c^3-5abc-3(a^2b+ab^2+a^2c+ac^2+b^2c+bc^2)=0.$$

Trivial solutions:

$$(a,b,c)=(11,4,-1),(-11,-4,1),(1,-4,-11),\ldots$$

Invalid solutions:

$$(a,b,c)=(1,-1,0),(-1,1,0),(-1,1,-1),\ldots$$

- Require $a+b,a+c,b+c>0$.

Dimensionality of solution space

$$a^3 + b^3 + c^3 - 5abc - 3(a^2b + ab^2 + a^2c + ac^2 + b^2c + bc^2) = 0$$

Definition

A polynomial is **homogeneous** if its monomials have the same degree.

If (a_0, b_0, c_0) is a solution in $\mathbb{Z}$, then $(\lambda a_0, \lambda b_0, \lambda c_0)$ is a solution in $\mathbb{Q}$ for any $\lambda \in \mathbb{Q}^*$. Define the equivalence relation $\sim$ by

$$(a_0, b_0, c_0) \sim (a_0', b_0', c_0') \iff (a_0, b_0, c_0) = (\lambda a_0', \lambda b_0', \lambda c_0'), \qquad \lambda \in \mathbb{Q}^*.$$

Write the equivalence class as $[a_0, b_0, c_0]$.

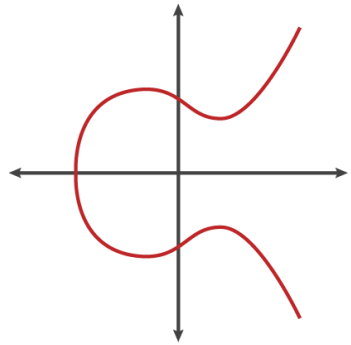
- Modulo $\sim$, the space of solutions is only two-dimensional.

If $c \neq 0$, the equation is equivalent to

$$a^3 + b^3 + 1 - 5ab - 3(a^2b + ab^2 + a^2 + a + b^2 + b) = 0, \qquad a, b \in \mathbb{Q}.$$

- Modulo $\sim$, the equation is cubic of two variables.

Elliptic curves: informally



An *elliptic curve* is the space of solutions to a cubic equation

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

where A and B are in some field such that $4A^3 + 27B^2 \neq 0$.

- Simplest non-trivial structures in algebraic geometry.
- Topic of the *Birch and Swinnerton-Dyer conjecture*.
- Tool in Wiles' proof of *Fermat's last theorem*.
- Methods for primality testing and integer factorisation.
- Applications in *elliptic curve cryptography*.

Elliptic curves: formally

Definition

An **elliptic curve** over a field K is a *smooth projective plane algebraic curve* E of *genus one* with a *K-rational base point* $\mathcal{O}_E$.

- *algebraic curve*: space of solutions to equation
- *plane*: two variables
- *projective*: consider equivalence classes of solutions
- *smooth*: no kinks
- *genus one*: degree three
- *K-rational base point*: coordinates in K

Theorem

An elliptic curve over $\mathbb{Q}$ is of the form

$$E = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

for some $A, B \in \mathbb{Q}$ such that $4A^3 + 27B^2 \neq 0$, where $\mathcal{O} = [0, 1, 0]$.

Weierstrass representations

$$a^3 + b^3 + c^3 - 5abc - 3(a^2b + ab^2 + a^2c + ac^2 + b^2c + bc^2) = 0$$

Proposition

The curve given by the equation is isomorphic to the following curves.

- $\{(x, y) \in \mathbb{Q}^2 : 6y^2 + 6xy + 6y = -91x^3 + 141x^2 + 15x - 1\} \cup \{\mathcal{O}\}$.
- $\{(x, y) \in \mathbb{Q}^2 : y^2 + xy - \frac{91}{6}y = x^3 + \frac{47}{2}x^2 - \frac{455}{12}x - \frac{8281}{216}\} \cup \{\mathcal{O}\}$.
- $\{(x, y) \in \mathbb{Q}^2 : y^2 + xy + y = x^3 - 234x + 1352\} \cup \{\mathcal{O}\}$.
- $\{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + \frac{1}{4}x^2 - \frac{467}{2}x + \frac{5409}{4}\} \cup \{\mathcal{O}\}$.
- $\{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - \frac{11209}{48}x + \frac{1185157}{864}\} \cup \{\mathcal{O}\}$.
- $\{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - 302643x + 63998478\} \cup \{\mathcal{O}\}$.

Let $A = -302643$ and $B = 63998478$. Overall invertible transformations:

$$\begin{cases} a = \frac{1}{72}x + \frac{1}{216}y - \frac{277}{24} \\ b = \frac{1}{72}x - \frac{1}{216}y - \frac{277}{24} \\ c = \frac{1}{6}x - \frac{95}{2} \end{cases} \qquad \begin{cases} x = \frac{1710a+1710b-831c}{6a+6b-c} \\ y = \frac{-9828a+9828b}{6a+6b-c} \end{cases}$$

A group law

$$E = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

Theorem

E is an abelian group $(E, +)$.

- *The identity point is $\mathcal{O} \in E$.*
- *The inverse of a point is obtained by reflecting the point vertically.*
- *The sum of two points is obtained by inverting the third point of intersection between the curve and the line joining the two points:*

$$P + Q = \begin{cases} S & \text{if } P = (x, y),\ Q = (x', y'),\ x \neq x', \\ R & \text{if } P = Q = (x, y),\ y \neq 0, \\ P & \text{if } Q = \mathcal{O}, \\ \mathcal{O} & \text{if } P = Q = (x, 0), \end{cases}$$

$$S = \left(\frac{(A+xx')(x+x')+2(B-yy')}{(x-x')^2}, \frac{(Ay'-x'^2y)(3x+x')+(x^2y'-Ay)(x+3x')-4B(y-y')}{(x-x')^3} \right),$$

$$R = \left(\frac{x^4-2Ax^2-8Bx+A^2}{4y^2}, \frac{x^6+5Ax^4+20Bx^3-5A^2x^2-4ABx-A^3-8B^2}{8y^3} \right).$$

Proof of the group law

$$E = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

Lemma (Bézout's theorem)

Let C and D be projective algebraic curves over an algebraically closed field $\overline{K}$. Then C and D intersect at exactly $\deg C \deg D$ *points counted with intersection multiplicity.*

Lemma (Cayley–Bacharach theorem)

Let C, D, E be projective algebraic cubic curves over an algebraically closed field $\overline{K}$ such that

$$C \cap E = \{P_1, \ldots, P_8, Q\}, \qquad D \cap E = \{P_1, \ldots, P_8, R\},$$

counted with intersection multiplicity. Then $Q = R$.

- Well-definition of addition in K holds by explicit equations.
- Commutativity of addition holds by symmetry.
- Associativity of addition holds by intimidation.

Procedure

Algorithm

Generate new solutions from old solutions.

- *Choose an initial solution* (a, b, c).
- *Apply the change of variables:*

$$\begin{cases} x = \frac{1710a+1710b-831c}{6a+6b-c} \\ y = \frac{-9828a+9828b}{6a+6b-c} \end{cases}$$

- *Compute multiples of the point* (x, y).
- *Apply the change of variables:*

$$\begin{cases} a = \frac{1}{72}x + \frac{1}{216}y - \frac{277}{24} \\ b = \frac{1}{72}x - \frac{1}{216}y - \frac{277}{24} \\ c = \frac{1}{6}x - \frac{95}{2} \end{cases}$$

- *Terminate or repeat.*

Computation: failure

Choose an invalid solution:

$$(a, b, c) = (-1, 1, -1).$$

Apply the change of variables:

$$(x, y) = (831, 19656).$$

Compute multiples of point:

- $2(x, y) = (363, 1404)$.
- $3(x, y) = (327, 0)$.
- $4(x, y) = (363, -1404)$.
- $5(x, y) = (831, -19656)$.
- $6(x, y) = \mathcal{O}$.

This is a cyclic subgroup of order six.

Computation: success

Choose a trivial solution:

$$(a, b, c) = (11, 4, -1).$$

Apply the change of variables:

$$(x, y) = (291, -756).$$

Compute multiples of point:

- $2(x, y) = (\frac{22107}{49}, -\frac{1506492}{343})$. Apply the change of variables:

$$(a, b, c) = (-8784, 5165, 9499).$$

- $3(x, y) = (-\frac{2694138}{11881}, -\frac{14243306490}{1295029})$. Apply the change of variables:

$$(a, b, c) = (679733219, -375326521, 883659076).$$

- $9(x, y) = (\frac{3823387580080160076063605209061052603963389916327719142}{13514400292716288512070907945002943352692578000406921}, \dots)$. Apply the change of variables:

$$(a, b, c) = (\text{APPLE}, \text{BANANA}, \text{PINEAPPLE}).$$

Further facts

The general equation is

$$\frac{a}{b+c}+\frac{b}{a+c}+\frac{c}{a+b}=N, \qquad a,b,c\in\mathbb{N}^*, \qquad N\in\mathbb{Z}.$$

- The elliptic curve is

$$E\cong\mathbb{Z}^r\oplus\begin{cases}\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z} & \text{if } N=2,\\ \mathbb{Z}/6\mathbb{Z} & \text{otherwise,}\end{cases} \qquad r\in\mathbb{N}^*.$$

- The smallest solution for $N=4$ is $(a,b,c)=(\text{APPLE},\text{BANANA},\text{PINEAPPLE})$.
- The smallest solution for $N=178$ has four hundred million digits.
- There are no solutions for N is odd.
- There may also be no solutions if N is even.
- There are infinitely many even N with solutions.

Further references

- A Amit's 2017 Quora answer on *How do you find the positive integer solutions to*

$$\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}=4?$$

- A Bremner and A Macleod's 2014 paper on *An unusual cubic representation problem*
- J Silverman's 1986 book on *The arithmetic of elliptic curves*
- R Hartshorne's 1977 book on *Algebraic geometry*
- N Duif's 2011 implementation on *Transforming a general cubic elliptic curve equation to Weierstrass form*
- M Laska's 1982 paper on *An algorithm for finding a minimal weierstrass equation for an elliptic curve*