Exploring Number Theory via Diophantine Equations

Sunil Chetty

Department of Mathematics
Colorado College

Fall, 2009

Outline

Diophantus

Diophantine equations are named after the Greek mathematician Diophantus, c. 250, of Alexandria. In his *Arithmetica*, a treatise of several books, he studies some 200 equations in two or more variables with the restriction that the solutions be **rational** numbers.

(1570) Bombelli included translated parts in his *Algebra*.

(1575) Holzmann (a.k.a. Xylander) attempted a completed translation.

(1593) Viète reproduced a large part in his *Zetetica*.

(1621) Bachet published Diophantus' text in Greek, as well as a Latin translation with commentary.

Fermat, Euler, and Gauss

Weil, in his book *Number Theory*, remarks that the birth of modern number theory happens on two occassions.

> *... by 1636, as we learn from his correspondence, [Fermat] had not only studied [Bachet] but was already developing ideas of his own... In 1729... Euler reports that he has "just been reading Fermat" and that he has been greatly impressed by Fermat's assertion that every integer is a sum of four squares...*

In 1801, Gauss' *Disquisitiones Arithmeticae* marked the culmination of the work of Fermat, Euler, and others. Gauss also introduces fundamental concepts such as congruences and generalized integers.

Hilbert

In 1900, with the long history of mathematicians working on various Diophatine equations, David Hilbert challenged the mathematical community to find an algorithm which would determine, given a Diophantine equation, whether or not there is a solution in the integers.

Theorem (Davis-Putnam-Robinson, Matijasevič)

There is no such algorithm.

This theorem, in some sense, forces us to attack Diophantine equations in a more reserved manner, but also ensures that there is still work to do.

An Example

Suppose there is a piggy bank which contains only quarters, dimes, and nickels, with a total value of \$10. Can we determine *exactly* how many of each coin is inside?

A model we could use for answering this question is a "linear Diophantine equation"

$$25x + 10y + 5z = 1000,$$

with x representing the number of quarters, y the dimes, and z the nickels.

Two-Variable Linear Diophantine Equations

A **linear** Diophantine equation in **two variables** is of the form

$$ax + by + c = 0 \quad \text{or} \quad ax + by = c,$$

with a, b, and c integers, and for which the variables x and y can only have **integer** values.

Question

Can we determine when such an equation has *a* solution?

Example

Consider $30x + 14y = 1$.
We can rewrite this as $2(15x + 7y) = 1$, so the left side is *always* even and the right side is *never* even.

Greatest Common Divisor

The **greatest common divisor**, or GCD, of two integers a and b is the largest positive integer which divides both a and b. We denote it by (a, b).

Example

Let $a = 30$ and $b = 14$. Since

$$30 = 2 \cdot 15 = 2 \cdot 3 \cdot 5 \quad \text{and} \quad 14 = 2 \cdot 7,$$

the common divisors are ± 1 and ± 2. So $(30, 14) = 2$.

We can express the GCD as a "linear combination":

$$2 = 30 - 28 = 30(1) + 14(-2).$$

Existence of a Solution

In the example $30x + 14y = 1$, the GCD of 30 and 14 does not divide 1 and the equation has no solutions.

Consider $30x + 14y = 6$. With $x = 1$ and $y = -2$, we saw

$$30(1) + 14(-2) = 2.$$

Since $6 = 2 \cdot 3$, when we try $x = 3$, and $y = -2 \cdot 3 = -6$:

$$30(3) + 14(-6) = 3(\ 30(1) + 14(-2)\ ) = 3(2) = 6.$$

Theorem

For $ax + by = c$, there **is** a solution when c is divisible by (a, b), otherwise there are **none**.

All Solutions

We have explored when *a* solution exists, but in number theory we would like to understand *all* solutions.

We continue with $30x + 14y = 6$, and the solution $x = 3$, $y = -6$ above. Suppose u and v give another solution.

$$\begin{aligned} 30u + 14v = 30(3) + 14(-6) &\Rightarrow \quad 30(u-3) = 14(-6-v) \\ &\Rightarrow \quad 15(u-3) = 7(-6-v) \end{aligned}$$

This forces, for some integer k,

$$u = 3 - 7k \text{ and } v = -6 + 15k,$$

so our *one* explicit solution tells us how to get *all* the others.

Pythagorean Triples

A familiar **non-linear** Diophantine equation is $x^2 + y^2 = z^2$.

We see $(3, 4, 5)$, $(6, 8, 10)$, and $(5, 12, 13)$ all satisfy the equation.

Questions

Are we in a situation as above? Does one solution produce others in a simple way? All others?

If (x, y, z) is Pythagorean, then so is (kx, ky, kz) since

$$(kx)^2 + (ky)^2 = k^2(x^2 + y^2) = k^2z^2 = (kz)^2.$$

So, $(3, 4, 5)$ produces $(6, 8, 10)$, $(9, 12, 15)$, $\ldots$, $(51, 68, 85)$, $\ldots$

Primitive Solutions

Let (x, y, z) be Pythagorean, with $(x, y) = (x, z) = (y, z) = 1$. (We may assume x, z are odd and y is even.)

Factoring, we get $y^2 = z^2 - x^2 = (z + x)(z - x)$, and since y is even,

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

Since $(x, z) = 1$, the terms on the right have no common factors. With a little algebra we get, for some integers r and s,

$$z + x = 2r^2, \quad z - x = 2s^2, \quad \text{and} \quad y = 2rs.$$

Gaussian Integers

Recall all complex numbers can be written as $a + ib$, where a and b are **real** numbers and $i := \sqrt{-1}$. If we only allow **integer** values for a and b we have the set $\mathbb{Z}[i]$ of "Gaussian integers."

Fact

$\mathbb{Z}[i]$ enjoys the property of unique factorization into "primes".

In $\mathbb{Z}[i]$, we can factor $z^2 = x^2 + y^2 = (x + iy)(x - iy)$, and then unique factorization leads to

$$x + iy = (r + si)^2 = (r^2 - s^2) + i(2rs).$$

Pell's Equation

Let d be an integer. A Pell equation is one of the form

$$x^2 - dy^2 = \pm 1.$$

In 1657, Fermat challenged the English mathematicians of the time to solve $x^2 - dy^2 = 1$ for general d, and if failing that to at least try $x^2 - 61y^2 = 1$ and $x^2 - 109y^2 = 1$, where he chose small coefficients "pour ne vous donner pas trop de peine" (so you don't have too much work).

d	60	61	62	108	109	110
x	31	1766319049	63	1351	158070671986249	21
y	4	226153980	8	130	15140424455100	2

Simple Cases

With any Pell equation $x^2 - dy^2 = 1$, there are the trivial solutions $x = \pm 1$, $y = 0$, and possibly $x = 0$, $y = \pm 1$.

Suppose $d = -1$. Then there can be no non-trivial solutions since

$$x^2 - (-1)y^2 = x^2 + y^2 \geq 1.$$

Now suppose $d = 4$ (a perfect square). Then

$$\begin{aligned} x^2 - 4y^2 = x^2 - (2^2)y^2 &= x^2 - (2y)^2 \\ &= (x - 2y)(x + 2y) = 1. \end{aligned}$$

Remaining Cases

From now on we assume $d > 0$ and is not a perfect square.

Fact

If $d > 0$ is not a perfect square then $\sqrt{d}$ is irrational.

Notice that for $x, y > 0$

$$x^2 - dy^2 = 1 \Rightarrow \left(\frac{x}{y}\right)^2 = d + \frac{1}{y^2} \approx d.$$

So, $\frac{x}{y}$ is a rational number which approximates $\sqrt{d}$.

Approximating Irrational Numbers

Let x be an irrational number. We define a sequence of integers $\{a_0, a_1, a_2, \ldots\}$ as follows.

- Set a_0 to be the largest integer $< x$, and $x_1 = 1/(x - a_0)$. Note that x_1 is irrational and $x_1 > 1$.
- Set a_1 to be the largest integer $< x_1$, and $x_2 = 1/(x_1 - a_1)$.

  $\ldots$
- Set a_i to be the largest integer $< x_i$, and $x_{i+1} = 1/(x_i - a_i)$.

This gives a sequence of rational approximations to x

$$\frac{p_0}{q_0} = a_0, \quad \frac{p_1}{q_1} = a_0 + \frac{1}{a_1}, \quad \frac{p_2}{q_2} = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, \quad \ldots$$

An Example

Consider $x = \sqrt{2}$.

- First, $1 < x < 2$, so $a_0 = 1$ and $x_1 = 1/(\sqrt{2} - 1) = \sqrt{2} + 1$.
- Next, $2 < x_1 < 3$, so $a_1 = 2$ and then $x_2 = \frac{1}{(\sqrt{2}+1)-2} = \frac{1}{\sqrt{2}-1} = \sqrt{2} + 1$.
- Since $x_2 = x_1$, the process repeats and our sequence is $\{1, 2, 2, 2, \ldots\}$.

The sequence of rational approximations is then

$$\frac{p_0}{q_0} = 1, \quad \frac{p_1}{q_1} = 1 + \frac{1}{2} = \frac{3}{2}, \quad \frac{p_2}{q_2} = 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5}, \quad \cdots$$

Applications to Pell's Equation

Theorem

If $\left|\sqrt{2} - \frac{p}{q}\right| < \frac{1}{2q^2}$ then $\frac{p}{q}$ is one of the continued fraction rational approximations of $\sqrt{2}$.

What if we know $x, y > 0$ is a solution to $x^2 - 2y^2 = 1$?

Example: $d = 2$

Let $x = 17$, $y = 12$:

- $17^2 - 2 \cdot 12^2 = 289 - 2 \cdot 144 = 289 - 288 = 1.$
- $\left|\sqrt{2} - \frac{17}{12}\right| \approx .002453 < .003472 \approx \frac{1}{2 \cdot 12^2}.$

Generating New Solutions

If we allow ourselves to work with $\sqrt{d}$, we have

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$$

and multiplication formula

$$(x \pm y\sqrt{d})(u \pm v\sqrt{d}) = (xu + dyv) \pm (xv + uy)\sqrt{d}.$$

With these, if $x^2 - dy^2 = 1$ and $u^2 - dv^2 = 1$ then

$$\begin{aligned} 1 &= (x^2 - dy^2)(u - dv^2) \\ &= (x - \sqrt{d}y)(x + \sqrt{d}y)(u - \sqrt{d}v)(u + \sqrt{d}v) \\ &= (x - \sqrt{d}y)(u - \sqrt{d}v)(x + \sqrt{d}y)(u + \sqrt{d}v) \\ &= (xu + dyv)^2 - d(xv + uy)^2. \end{aligned}$$

An Example

Now, from one solution with $x > 0$ and $y > 0$, we have infinitely many solutions

$$x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n, \quad \text{for } n \geq 1.$$

Example: $d = 2$

We see that $x = 3$, $y = 2$ is a solution to $x^2 - 2y^2 = 1$.

- $(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2}$.
- $(3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2}$.
- $(3 + 2\sqrt{2})^4 = 577 + 408\sqrt{2}$.
- $(3 + 2\sqrt{2})^5 = 3363 + 2378\sqrt{2}$.

A Complete Solution

Theorem (Lagrange, 1768)

There exists a positive integer solution x_1, y_1 to the Pell equation $x^2 - dy^2 = 1$ such that all other positive integer solutions x_n, y_n are derived from it via the power rule

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad \text{for } n \geq 1.$$

Note: It not quite as simple to describe the solutions of

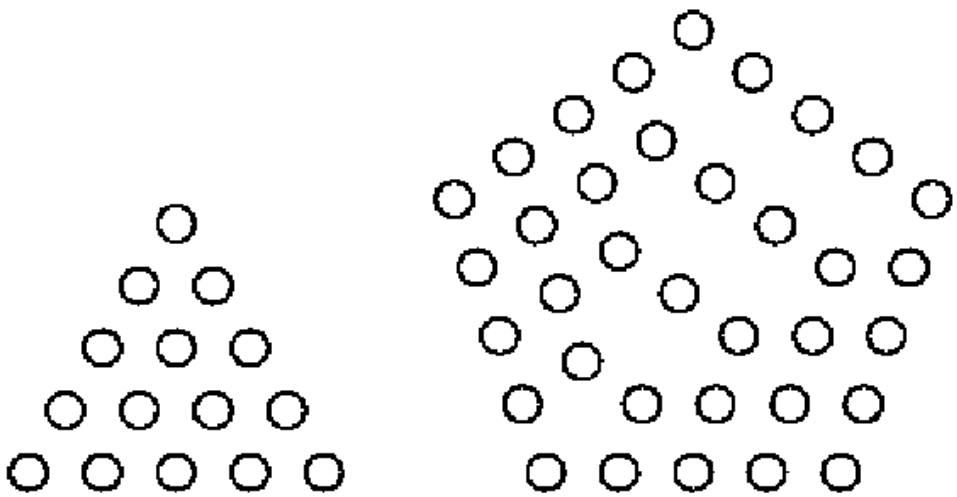
$$x^2 - dy^2 = -1,$$

but they will still come from the rational approximation process described above.

Polygonal Numbers

The d-gonal numbers are partial sums of the arithmetic progression with initial term 1 and common difference $d-2$.

$$\begin{aligned} T_n &= 1+2+\cdots+n = \tfrac{n(n+1)}{2} \\ S_n &= 1+3+\cdots+(2n-1) = n^2 \\ P_n &= 1+4+\cdots+(3n-2) = \tfrac{3n^2-n}{2} \end{aligned}$$



Triangular: 1, 3, 6, 10, 15

Pentagonal: 1, 5, 12, 22, 35

Triangular-Square Numbers

A triangular-square number: $T_m = S_n$ for some m and n.

Question

Are there any triangular-square numbers besides 1?

By the formulae above

$$\begin{aligned} T_m &= S_n \\ \tfrac{m^2+m}{2} &= n^2 \\ m^2 + m &= 2n^2 \\ \left(m + \tfrac{1}{2}\right)^2 - \tfrac{1}{4} &= 2n^2 \\ (2m+1)^2 - 1 &= 2(2n)^2 \end{aligned}$$

$$(2m+1)^2 - 2(2n)^2 = 1.$$

Triangular-Square Numbers

So, the question is reduced to solving $x^2 - 2y^2 = 1$ with $x, y > 0$ and x odd, y even.

It turns out that to satisfy this equation, x must be odd and y must be even.

x	3	17	99	577	3363	19601
y	2	12	70	408	2378	13860
$m = (x-1)/2$	1	8	49	288	1681	9800
$n = y/2$	1	6	35	204	1189	6930
$T_m = S_n$	1	36	1225	41616	1413721	48024900

Note $T_{49} = S_{35} = 1225$ means $1 + 2 + \cdots + 49 = 35 \cdot 35$.

(These numbers are Sloane's A001110.)

Square-Pentagonal Numbers

A square-pentagonal number: $S_m = P_n$ for some m and n.

Question

Are there any square-pentagonal numbers besides 1?

By the formulae above

$$\begin{aligned} S_m &= P_n \\ m^2 &= \frac{3n^2-n}{2} \\ 2m^2 &= 3n^2 - n \\ 2m^2 &= 3\left(\left(n-\tfrac{1}{6}\right)^2 - \tfrac{1}{36}\right) \\ 6(2m)^2 &= (6n-1)^2 - 1 \end{aligned}$$

$$(6n-1)^2 - 6(2m)^2 = 1.$$

Square-Pentagonal Numbers

This time the problem is reduced to solving $x^2 - 6y^2 = 1$, with $x, y > 0$, $x = 6n - 1$, and y even.

In $x^2 - 6y^2 = 1$, y is always even, $x = 6n \pm 1$, but not necessarily $x = 6n - 1$.

x	5	49	485	4801	47525	470449
y	2	20	198	1960	19402	192060
m	1		99		9701	
n	1		81		7921	
$S_m = P_n$	1		9801		94109401	

(These numbers are Sloane's A036353.)

Pythagorean Triples again

Are there other Pythagorean triples like $(3,4,5)$, i.e. with consecutive numbers in the first two variables?

We want to solve $m^2 + (m+1)^2 = n^2$.

Notice that here, n must be odd.

$$\begin{aligned} 2m^2 + 2m + 1 &= n^2 \\ 2(m^2 + m) + 1 &= n^2 \\ 2\left(\left(m + \tfrac{1}{2}\right)^2 - \tfrac{1}{4}\right) - 1 &= n^2 \\ (2m+1)^2 + 1 &= 2n^2 \end{aligned}$$

$$(2m+1)^2 - 2n^2 = -1$$

Pythagorean Triples again

$$m^2 + (m+1)^2 = n^2 \Leftrightarrow (2m+1)^2 - 2n^2 = -1.$$

So, we need to understand solutions to $x^2 - 2y^2 = -1$. It turns out x and y must be odd, so our condition on n is automatic.

x	1	7	41	239	1393	8119
y	1	5	29	169	985	5741
$m = (x-1)/2$	0	3	20	119	696	4059
$n = y$	1	5	29	169	985	5741

$3^2 + 4^2 = 5^2, \quad 20^2 + 21^2 = 29^2, \quad 119^2 + 120^2 = 169^2.$

Pythagorean Triples again

Are there Pythagorean triples with consecutive numbers in the last two variables?

We want $m^2 + n^2 = (n+1)^2$, which is equivalent to $m^2 = 2n + 1$. So, m needs to be odd, i.e. $m = 2k + 1$. This makes

$$n = (m^2 - 1)/2 = 2k^2 + 2k.$$

k	1	2	3	4	5	6
$2k+1$	3	5	7	9	11	13
$2k^2+2k$	4	12	24	40	60	84
$2k^2+2k+1$	5	13	25	41	61	85

This has nothing to do with Pell's equation.

An Example

In the 17^{th} century, Bachet and Fermat studied the equation $y^2 = x^3 - 2$. We will see that this equation has a finite number of solutions in the integers.

We can start by simple trial-and-error:

- $x = 1$: $1^3 - 2 = 1 - 2 = -1$, no possible (real) y.
- $x = 2$: $2^3 - 2 = 8 - 2 = 6$, no possible (integer) y.
- $x = 3$: $3^3 - 2 = 27 - 2 = 25 = 5^2$, so $y = \pm 5$ works.

So far, $(3, \pm 5)$ are two integral solution of the equation.

Integral Solutions of $y^2 = x^3 - 2$

Recall: $\mathbb{Z}[i]$ consists of complex numbers $x + iy$, with x, y restricted to the integers.

If we denote $\alpha = \sqrt{-2}$, we can define a set $\mathbb{Z}[\alpha]$ of complex numbers of the form $x + \alpha y$, again with x, y restricted to the integers.

Fact

$\mathbb{Z}[\alpha]$ also has the property of unique factorization into "primes."

In $\mathbb{Z}[\alpha]$, the equation $y^2 = x^3 - 2$ can be factored

$$(y + \alpha)(y - \alpha) = x^3.$$

Integral Solutions of $y^2 = x^3 - 2$

From $(y+\alpha)(y-\alpha) = x^3$ and unique factorization, one obtains

$$y + \alpha = (u + \alpha v)^3, \quad u, v \text{ integers.}$$

Expanding the right-hand side and collecting terms gives

$$\begin{aligned} y = \quad & u^3 - 6uv^2 \quad \text{and} \quad 1 = \quad 3u^2 - 2v^3 \\ & = \quad v(3u^2 - 2v^2), \end{aligned}$$

so it must be that $u = v = 1$.

Thus, the *only* integral solutions to $y^2 = x^3 - 2$ are $(3, \pm 5)$.

Elliptic Curves

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

More generally, an elliptic curve is the set of solutions to an equation of the form

$$y^2 = x^3 + ax^2 + bx + c.$$

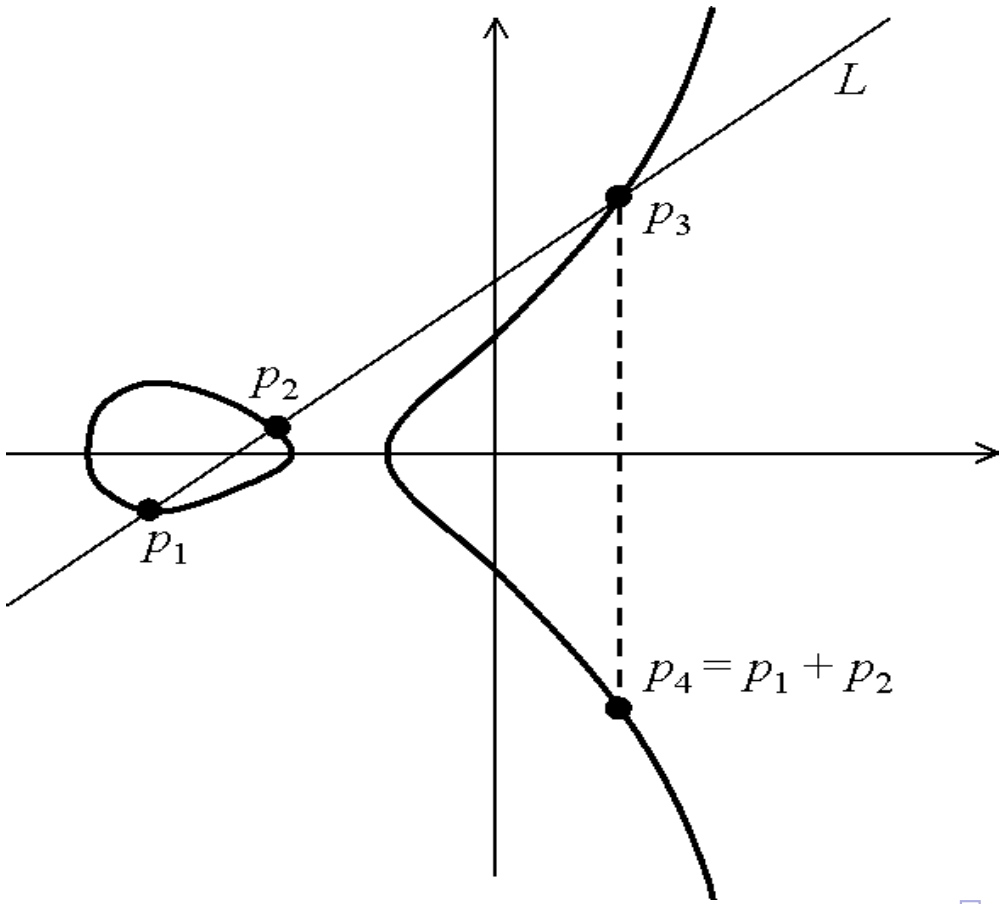
For **integral** solutions there is a nice theorem.

Theorem (Siegel, 1926)

If a, b, and c are integers, then there are only finitely many integral solutions to $y^2 = x^3 + ax^2 + bx + c$.

Adding Solutions

For elliptic curves, understanding all of the solutions in the **rational numbers** is a much more complicated problem.



Mordell-Weil Theorem

In 1922, Mordell used Fermat's idea of "descent" to prove

Theorem (Mordell, 1922)

For $y^2 = x^3 + ax^2 + bx + c$, with a, b, and c integers, there exists a finite set of rational solutions $(x_1, y_1), \ldots, (x_r, y_r)$ such that all other rational solutions can be obtained from these by repeated application of the chord-tangent process.

Problem

This proof only gives *existence*. Currently, there is no method to generate this finite set, nor a way to determine just how many points (the **rank**) are needed in this finite set.

The Statement

In his copy of Bachet, Fermat stated:

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.

I.e., the equation $x^n + y^n = z^n$ has no **integer** solutions.

Frey, Ribet, and Wiles

In 1985, Frey suggested that one consider the elliptic curve

$$E_{a,b,c}: \ y^2 = x(x - a^n)(x + b^n)$$

where $a^n + b^n = c^n$. A conjecture of Taniyama and Shimura states that such an elliptic curve should be "modular."

Theorem (Ribet)

$E_{a,b,c}$ is *not* modular.

Theorem (Wiles-Taylor)

$E_{a,b,c}$ *is* modular.

So, assuming there exist integers a, b, c with $a^n + b^n = c^n$ leads to a contradiction by way of a strange elliptic curve.

The End

Thank you for your attention.