Triangle Numbers
MathCamp 2001

William A. Stein

July 28, 2001

Contents

1 Lecture 1: Triangle Numbers

Definition 1.1. A *triangle number* is an integer that is the area of some right triangle with rational side lengths.

The area of a right triangle with side lengths a, b, and c (with $a^2 + b^2 = c^2$) is $ab/2$. For example, $a = 3$, $b = 4$, and $c = 5$ are the lengths of the sides of a right triangle, so $6 = ab/2 = 3 \cdot 4/2$ is a triangle number.

Big Famous Ancient Problem:
Give a way to decide whether or not an integer n is a triangle number.

Idea:
Let's just list triangles and see what areas we get.

1.1 The Greeks' method to list the Pythagorean triples

There is a simple way to list all "primitive Pythagorean triples", that is triples of integers a, b, c with $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$.

Consider the unit circle $x^2 + y^2 = 1$. Let $v > u > 0$ be integers and draw a line of slope u/v through $(-1, 0)$; this line is defined by the equation $y = \frac{u}{v}(x + 1)$.

We now find the other point (x_0, y_0) of intersection of this line and the circle.

$$x^2 + \frac{u^2}{v^2}(x+1)^2 = 1$$

$$x^2 + \frac{u^2}{v^2}x^2 + \frac{u^2}{v^2}2x + \frac{u^2}{v^2} - 1 = 0$$
$$(u^2 + v^2)x^2 + 2u^2x + u^2 - v^2 = 0$$
$$x^2 + \frac{2u^2}{u^2+v^2}x + \frac{u^2 - v^2}{u^2+v^2} = 0$$

Now factor: $(x - (-1))(x - x_0) = 0$, so $x^2 - (x_0 - 1)x - x_0 = 0$, so

$$x_0 = \frac{v^2 - u^2}{u^2 + v^2},$$

and

$$y_0 = \frac{u}{v}\left(\frac{2v^2}{u^2+v^2}\right) = \frac{2uv}{u^2+v^2}.$$

We have

$$\left(\frac{v^2 - u^2}{u^2+v^2}\right)^2 + \left(\frac{2uv}{u^2+v^2}\right)^2 = 1.$$

Thus

$$a = v^2 - u^2, \quad b = 2uv, \quad c = u^2 + v^2$$

form a Pythagorean triple. Moreover, all primitive Pythagorean triples arise in this way. [1] The area of the cooresponding triangle is 1

$$A = ab/2 = uv(v^2 - u^2).$$

We can now list triangle numbers:

v	$>$	$u > 0$	$\triangle = ab/2 = uv(v^2 - u^2)$	square-free part
2		1	6	6
3		1	$6 \cdot 2^2$	6
4		1	$4 \cdot (16 - 1) = 2^2 \cdot 3 \cdot 5$	15
5		1	$5 \cdot (25 - 1) = 5 \cdot 3 \cdot 2^3$	30
3		2	$6 \cdot (9 - 4) = 30$	30
4		2	$8 \cdot (16 - 4) = 2^3 \cdot 2^2 \cdot 3$	6
4		3	$12 \cdot (16 - 9) = 12 \cdot 5$	15

If n is a square-free triangle number, then n would eventually appear in the right hand column of this list, perhaps after a few *billion* years.

Question: Is 1 on this list? Is 2 on this list? What about 5? What about your age? What about mine (27)? What about the year 2001?

The rest of these talks will be about how to answer such questions!

[1] Noam: It suffices to consider only u and v of opposite parity.

1.2 Congruent Numbers

In books, triangle numbers are usually called "congruent numbers". Here's why. Suppose n is the area of a right triangle with rational side lengths a, b, c, with $a \leq b < c$. Let $A = (c/2)^2$. Then

$$A - n, \quad A, \text{ and } A + n$$

are all perfect squares, and they are "congruent modulo n".

Proof. We have

$$\begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n \end{aligned}$$

Add or subtract 4 times the second equation to the first to get

$$\begin{aligned} a^2 \pm 2ab + b^2 &= c^2 \pm 4n \\ (a \pm b)^2 &= c^2 \pm 4n \\ \left(\frac{a \pm b}{2}\right)^2 &= \left(\frac{c}{2}\right)^2 \pm n \\ &= A \pm n \end{aligned}$$

□

1.3 A Cubic Connection

Multiply the together the two final equations in the last section for $+1$ and -1:

$$\begin{aligned} \left(\frac{a+b}{2}\right)^2 \cdot \left(\frac{a-b}{2}\right)^2 &= \left(\left(\frac{c}{2}\right)^2 + n\right) \cdot \left(\left(\frac{c}{2}\right)^2 - n\right) \\ \left(\frac{a^2 - b^2}{4}\right)^2 &= \left(\frac{c}{2}\right)^4 - n^2 \end{aligned}$$

so

$$u^4 - n^2 = v^2$$

has an interesting solution, namely

$$u = \frac{c}{2}, \quad v = \frac{a^2 - b^2}{4},$$

so

$$u^6 - n^2 u = v^2 u^2$$

also has an interesting solution, so

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

also has an interesting solution.

The curve defined by the equation

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

is an example of what is called an *elliptic curve*.

2 Lecture 2: Elliptic Curves

Our Question: Which numbers are *triangle numbers*? That is, which numbers are the area of a right triangle with rational side lengths?

Last time: Given a triangle number n that is the area of a triangle with sides of length $a \leq b < c$, we observed that the equation

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

has an interesting solution:

$$x = \left(\frac{c}{2}\right)^2, \quad y = \frac{c(a^2 - b^2)}{8}.$$

Example 2.1. Suppose $a = 3$, $b = 4$, $c = 5$, $n = 6$. The elliptic curve is $y^2 = x^3 - 6^2 \cdot x$. The interesting solution is

$$\begin{aligned} x_0 &= \left(\frac{5}{2}\right)^2, \\ y_0 &= \frac{5 \cdot (9 - 16)}{8} = \frac{5 \cdot (-7)}{8}. \end{aligned}$$

(You can check that this is a solution easily enough by hand, or with a calculator.)

Theorem 2.2. *An integer n is a triangle number if and only if the equation $y^2 = x^3 - n^2 x$ has a solution with $y \neq 0$.*

(Hand out the "Some Triangle Numbers" handout.)

I won't tell you the proof of the theorem, which involves lots of algebra. I will tell you about elliptic curves! [2] 2

Definition 2.3. An *elliptic curve* is a curve defined by an equation of the form

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

(We assume that $x^3 + ax + b$ has distinct zeros.)

[Draw/insert a picture of $y^2 = x^3 - 36x$ from my mathcircles drawings.]

2.1 Points Spawn Even More Points

Given two points on an elliptic curve, you can "add them together" to get another point on the curve.

1. Draw the line that connects the two points. (Draw the tangent line if the two points are the same.)

[2] But, put the equation in the other direction in this (or a) handout.

2. Find *the* third intersection point
3. Reflect this point across the x axis.

[3] 3

Example 2.4.

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

[Draw the figure on page 7 of my notes.]

(Distribute the "elliptic curve" handouts and say:

- Elliptic curves are used for encryption for some bank transactions and digital mobile phones, and
- play a roll in trying to break cryptosystems.

(Do some examples on the computer.)

3 Lecture 3: The Birch and Swinnerton-Dyer Conjecture

Recall: An *elliptic curve* is defined by an equation

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

where $x^3 + ax + b$ has distinct zeros.

Two possibilities:

1. There are finitely many pairs (x_0, y_0) of rational numbers so that

$$y_0^2 = x_0^3 + ax_0 + b.$$

2. There are infinitely many pairs.

Question: Given an elliptic curve, which happens???

The Birch and Swinnerton-Dyer conjecture speculates that case 2 happens if and only if $L(E, s)$ takes the value 0 at 1. Here $L(E, s)$ is a "magic function" (kind of like sin or cos, but more complicated) attached to the elliptic curve E. If you could prove this conjecture, then you would be very famous.

[3] Noam: Remark: "getting points from other points was known for a long long time. But, reflecting and getting an abelian group was a more recent idea." I should say something about this, or omit step 3, depending on time.

3.1 Tunnell's theorem

Let n be *even* and squarefree. Let E be the elliptic curve

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

Then $L(E,1) = 0$ if and only if

$$\#\{(a,b,c) : 4a^2 + b^2 + 8c^2 = \frac{n}{2}\} = 2 \cdot \#\{(a,b,c) : 4a^2 + b^2 + 32c^2 = \frac{n}{2}\}.$$

[Or, as Noam points out]

$$\#\{(a,b,c) : 4a^2+b^2+8c^2 = \frac{n}{2} : c \text{ is even}\} = \#\{(a,b,c) : 4a^2+b^2+8c^2 = \frac{n}{2} : c \text{ is odd}\}.$$

When $n = 6$, we get

$$\#\emptyset = 2 \cdot \#\emptyset.$$

When $n = 2$, we get

$$\#\{(0,1,0)\} \neq 2 \cdot \#\{(0,1,0)\},$$

so the BSD conjecture predicts that $y^2 = x^3 - 4x$ has no interesting solutions and 2 is not a triangle number. [4] 4

In fact, this is true. The implication $L(E,1) \neq 0$ implies $y^2 = x^3 - n^2 x$ has no interesting solutions was proved by Coates and Wiles (this is the same Wiles who proved Fermat's Last Theorem).

The other implication:

$$L(E,1) = 0 \Longrightarrow y^2 = x^3 - n^2 x \text{ interesting (lots of solutions)}$$

is a fascinating *open problem*. For example, the Clay Math Institute (`www.claymath.org`) has offered a one million dollar reward for a proof of (a certain generalization of) this conjecture.

3.2 Summary

Question: Which numbers n are the area of a right triangle with rational side lengths?

Answer: Those for which $y^2 = x^3 - n^2 x$ has a solution with $y \neq 0$.

Question: Which $y^2 = x^3 - n^2 x$ have many solutions?

Conjectural Answer: Those for which "$L(E,1) = 0$".

Question: Huh??

Answer: (Tunnell) Those for which $\#\{\quad\} = 2 \cdot \#\{\quad\}$.

[4] Fermat, etc. proved this long long ago. But they didn't prove that 2001 isn't a congruent number...