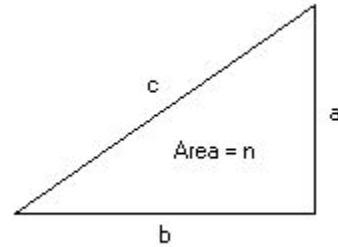


The Congruent Number Problem

Notes from Ed Eikenberg's talk on November 9, 2000

Let n be a positive integer. Does there exist a right triangle with rational sides whose area is n ? If so, then n is called a congruent number. For example, the familiar 3-4-5 right triangle has area 6, so $n=6$ is a congruent number. But what about other values of n , like $n=5$ or $n=157$? We could try listing pythagorean triples (x, y, z) until we find one with area $xy/2=5k^2$. Then the right triangle with sides $a=x/k, b=y/k, z=c/k$ will have area 5. But we have no idea how long this would take, or even whether or not one actually exists. For example, $n=157$ is a congruent number and the simplest right triangle (in terms of number of digits) with area 157 has hypotenuse



$$c = \frac{2244035177043369699245575130906674863160948472041}{8912332268928859588025535178967163570016480830}$$

Obviously searching through all possible pythagorean triples is not the answer. So we will make a change of variables:

$$x = (c/2)^2$$

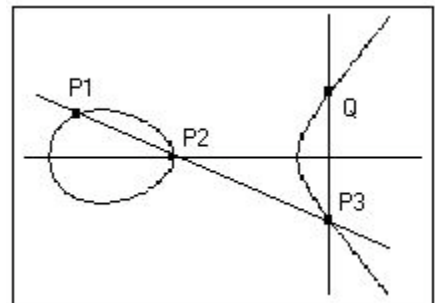
$$y = (b^2 - a^2)c/8$$

Then using the fact that $c^2 = a^2 + b^2$ and $n = ab/2$, it is easy to show that x and y satisfy the equation

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

For example, when $n=6$, the 3-4-5 right triangle will give us the point $(x, y) = (25/4, 35/8)$ on the curve $y^2 = x^3 - 36x$.

An equation of the form $y^2 = Ax^3 + Bx^2 + Cx + D$ is called an **elliptic curve**. Elliptic curves have both algebraic and geometric properties, and for this reason are very interesting curves. We can use the geometric structure of this curve to define a technique of "adding" rational points on the curve. Given two points P_1 and P_2 with rational coordinates, construct the line through these points and find the third point of intersection that this line has with the curve. Call this point P_3 , and let Q be the mirror image of this



point with respect to the x-axis. We then define $P_1 + P_2 = Q$. This may seem unusual, but with a point \mathcal{O} at infinity (which is considered to be on every vertical line) this addition law satisfies the following properties:

$$\begin{aligned} P_1 + P_2 &= P_2 + P_1 \\ \mathcal{O} + P &= P \\ P + (-P) &= \mathcal{O} \\ (P_0 + P_1) + P_2 &= P_0 + (P_1 + P_2) \end{aligned}$$

These properties make the rational points on an elliptic curve along with the point \mathcal{O} at infinity into an abelian group with \mathcal{O} as the identity element. This gives a method of adding two points to construct another point. Note that if the P_1 and P_2 are the same point, then the line through both of them is actually the line tangent to the curve at that point. This gives a method of doubling a point.

Let us consider the case where $n=5$ and attempt to find a solution. This amounts to finding a point on $y^2 = x^3 - 25x$ which can be pulled back to a triangle (a, b, c) . Since $x = (c/2)^2$, we need x to be the square of a rational number. A quick glance at the curve gives the obvious points $(-5,0)$, $(0,0)$, and $(5,0)$, and a little more work gives the point $(-4,6)$. But none of these points will give us a solution. So we need to look for other points by adding these points. If we take $P_1 = (-5,0)$ and $P_2 = (-4,6)$, we get the line $y = 6(x + 5)$, and substituting this into the equation for the elliptic curve gives $36(x + 5)^2 = x^3 - 25x$. This gives a cubic equation whose three roots are the three points of intersection of the line and the elliptic curve (and we know P_1 and P_2 are two of these points). So we can rewrite this as $0 = x^3 - 36x^2 + \dots$ where the coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $P_3 = (45,300)$, and this still does not give a solution since the x value is not a square.

It turns out that the only way to get a point which actually gives a solution is to take two times a point. This fact follows from some of the more advanced properties of elliptic curves. If we take $P_1 = (-4,6) = P_2$, we need to find the tangent line to the curve at this point. By differentiating implicitly, we get $2y \frac{dy}{dx} = 3x^2 - 25$, or $\frac{dy}{dx} = \frac{23}{12}$ at the point $(-4,6)$. This gives us the tangent line $y = \frac{23}{12}x + \frac{41}{3}$. Substituting this into the elliptic curve equation gives $(\frac{23}{12}x + \frac{41}{3})^2 = x^3 - 25x$. This gives us $0 = x^3 - (\frac{23}{12})^2 x^2 + \dots$ which gives $(\frac{23}{12})^2 = (-4) + (-4) + x$, or $x = \frac{1681}{144} = (\frac{41}{12})^2$. We now have a solution to the original problem, namely $c = \frac{41}{6}$, $a = \frac{3}{2}$, $b = \frac{20}{3}$. This gives a right triangle with area $n=5$. Thus $n=5$ is a congruent number.

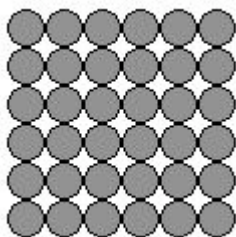
Note that this solution does come from a Pythagorean triple, namely $(40, 9, 41)$, which would not have been that difficult to find, but clearly this process would not have worked for $n=157$, as the Pythagorean triple would contain numbers at least 48 digit long.

Now that we have shown $n=5$ is a congruent number, what can we do about other values of n ? In particular, is there a way to determine whether or not a given value of n is a congruent number? A theorem by Mordell and Weil states that for any elliptic curve there exists a finite set of points on the curve which can be used to generate all other points with rational coordinates. This tells us that there is an isomorphism between the group of points on an elliptic curve and a group of the form $\mathbf{Z}^r \times F$, where \mathbf{Z} represents the integers, F is a finite group, and r is called the rank. In the case $n=5$, the points on the curve form a group isomorphic to $\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$, which is generated by the points $(-4,6)$, $(-5,0)$, and $(0,0)$. Notice that the three roots of the curve are points of order 2 since the tangent line to each of these points is a vertical line, and the point \mathcal{O} at infinity is the third point of intersection.

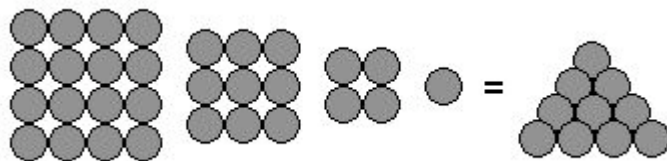
In the general case for the congruent number problem, the elliptic curve $y^2 = x^3 - n^2x$ always has three points of order two, and in fact, these are the only points of finite order. So the group of rational points on the curve is isomorphic to $\mathbf{Z}^r \times (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$, and the rank r will determine whether or not n is a congruent number. If $r = 0$, then the only rational points on the curve are the 3 roots, and none of these will pull back to a solution. This means that n is not a congruent number, so there is no right triangle with area n where all three sides are rational. If $r > 0$, then there is a point on the curve which we can double to find a solution. This will imply that n is a congruent number.

By relating these elliptic curves to a certain class of functions called L-functions, and assuming that the widely-accepted conjecture of Birch and Swinnerton-Dyer holds, it is possible to show that n is a congruent number if it has a certain form. If n is a squarefree integer of the form $8k+5$, $8k+6$, or $8k+7$ for some nonnegative integer k , then it can be shown that the elliptic curve $y^2 = x^3 - n^2x$ must have a point of infinite order, and thus n must be a congruent number. For more information on the Birch and Swinnerton-Dyer Conjecture, check out the [Clay Mathematics Institute](#). They are offering \$1,000,000 for a proof of this conjecture, as well as for six other famous unsolved problems.

Here's another interesting problem: Is it possible to find a number of cannonballs which can be arranged in the shape of a square and also a pyramid with a square base? For example, 36 cannonballs can be arranged in a 6 by 6 square, but cannot be arranged in the shape of a pyramid with a square base. If the base of the pyramid is 4 by 4, then the pyramid has 30 cannonballs, and if the base is 5 by 5, the pyramid has 55 cannonballs.



$$6^2 = 36$$



$$4^2 + 2^2 + 1 = 30$$

If we can find such a number of cannonballs, it would mean that we can find integers x and y such that

the number of cannonballs is $1^2 + 2^2 + 3^2 + \dots + x^2$ and also y^2 . Using the formula for the sum of consecutive squares, we get the following equation:

$$y^2 = x(x+1)(2x+1)/6 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$$

This is another elliptic curve, and we are now seeking a solution where x and y are positive integers. There are a few obvious points on the curve, namely the three roots $(0,0)$, $(-1,0)$, $(-1/2,0)$, as well as the points $(1,1)$ and $(1,-1)$. If we add the points $P_1 = (0,0)$ and $P_2 = (1,1)$ using the addition law on the curve (computations left to the reader), we get $P_3 = (1/2, 1/2)$, which gives us $Q = P_1 + P_2 = (1/2, -1/2)$. Adding this point to the point $P_2 = (1,1)$ again will give $Q + P_2 = (24, -70)$. This means that $x=24$, $y=70$ is a point on the curve which gives a solution to the problem. So 4900 cannonballs can be arranged in a 70 by 70 square and can also be arranged in a pyramid with base 24 by 24. In fact, it is possible to use some other properties of elliptic curves to show that this is the only integer solution to the problem other than 0 and 1.

Hopefully by now you are convinced that elliptic curves are very interesting. If you would like to learn more about elliptic curves, I recommend [An Introduction to Elliptic Curves and Modular Forms](#) by Neil Koblitz. If you have any questions, feel free to send me an e-mail at eve@math.umd.edu or check out my [home page](#).