# The Right-Angled Triangle

Peng Tsu Ann
Department of Mathematics
National University of Singapore

A triangle whose sides are all rational numbers is called a *rational* triangle. The problem that I am going to discuss is the following :

What positive integer $A$ is the area of a rational right-angled triangle?

If $A$ is the area of a rational right-angled triangle, then it follows from Pythagoras' theorem that there are rational numbers $X, Y, Z$ such that

$$X^2 + Y^2 = Z^2,$$
$$\frac{1}{2}XY = A.$$

We call such an integer $A$ a *congruent* number. We know from antiquity that

$$3^2 + 4^2 = 5^2.$$

Thus $A = 6$ is a congruent number. Are there others? Are the integers 1, 2, 3, 4, 5 congruent numbers? Are there two or more rational right-angled triangles with the same area? We will try to answer these questions in the talk.

Let $B$ be a congruent number. We can write $B$ in the form $B = m^2 A$, where $m$ is a positive integer and $A$ is square-free (i.e. $A$ does not contain a factor of the form $n^2$ with $n > 1$). Since $B$ is congruent there are rational numbers $X$, $Y$, $Z$ such that

$$X^2 + Y^2 = Z^2,$$
$$\frac{1}{2}XY = B,$$

so that

$$\left(\frac{X}{m}\right)^2 + \left(\frac{Y}{m}\right)^2 = \left(\frac{Z}{m}\right)^2,$$

---

Presidential address delivered to the Singapore Mathematical Society on 9 March 1988.

$$\frac{1}{2}\left(\frac{X}{m}\right)\left(\frac{Y}{m}\right) = A.$$

Thus $A$ is also a congruent number. Clearly, if $A$ is congruent, so is $B = m^2 A$ for every integer $m$. So our problem is equivalent to the following :

What positive square-free integer $A$ is a congruent number?

This does not help us to determine whether 1, 2, 3 or 5 are congruent numbers. But it tells us that 4 is congruent if and only if 1 is; 8 is congruent if and only if 2 is; 12 is congruent if and only if 3 is; and so on. It can be proved (but not easily) that 1, 2, 3 are not congruent, so 4, 8, 12 are also not congruent. The triangle in Figure 1 shows that 5 is a congruent number.

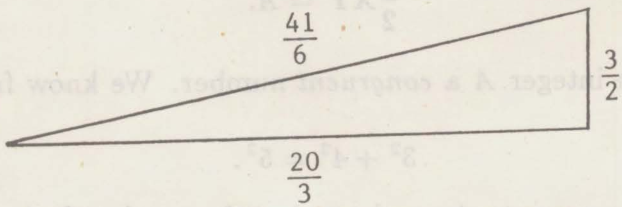


Figure 1

We already know that 6 is congruent. The integer 7 is also congruent because the following right-angled triangle has area 7 :

$$\left(\frac{35}{12}\right)^2 + \left(\frac{24}{5}\right)^2 = \left(\frac{337}{60}\right)^2.$$

The next congruent number after 7 is 13 :

$$\left(\frac{780}{323}\right)^2 + \left(\frac{323}{30}\right)^2 = \left(\frac{106921}{9690}\right)^2.$$

As a final example the triangle in Figure 2 shows that 157 is a congruent number. It is the "simplest" rational right-angled triangle of area 157.

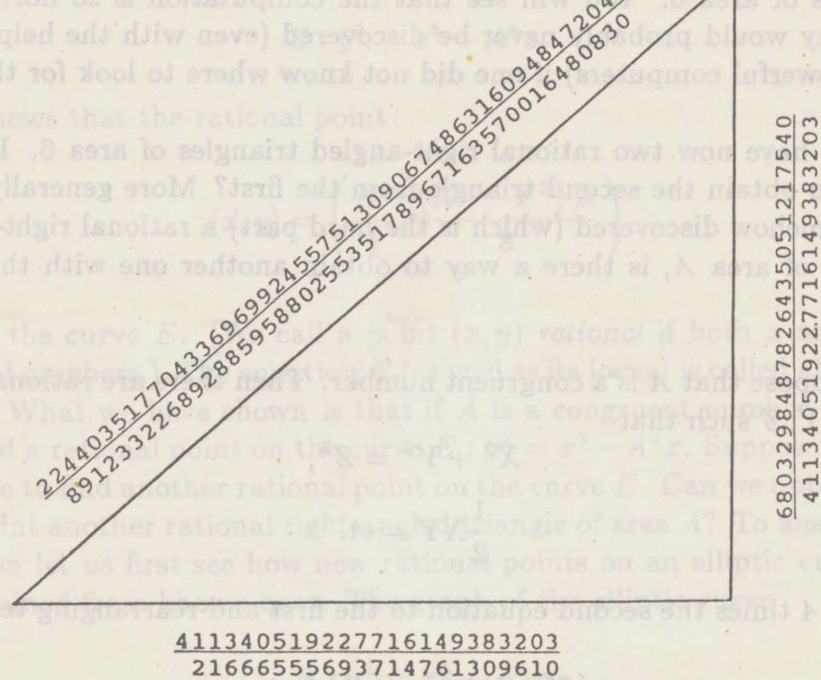


**Figure 2**

The simplest rational right-angled triangle of area 157
(computed by D.Zagier).

The problem of determining all congruent numbers has a long history. The examples 5 and 6 were given in an Arab manuscript written more than 1000 years ago [1]. The problem is not completely solved even today. In 1983, using very sophisticated methods in number theory Tunnell [4] discovered a characterization of congruent numbers (i.e. he found a necessary and sufficient condition for an integer to be congruent). (See [2] for a detailed account.) Unfortunately, Tunnell's result depends on a conjecture which has not been proved in general. All congruent numbers $< 2000$ are now known [3].

We now return to the right-angled triangle with sides 3,4 and 5. Its area is 6. Are there any other rational right-angled triangles of area 6? If you try hard enough you may discover that the following is such a triangle:

$$\left(\frac{7}{10}\right)^2+\left(\frac{120}{7}\right)^2=\left(\frac{1201}{70}\right)^2.$$

At the end of this talk I will show you a few more rational right-angled triangles of area 6. You will see that the computation is so horrendous that they would probably never be discovered (even with the help of the most powerful computers) if one did not know where to look for them.

We have now two rational right-angled triangles of area 6. Is there a way to obtain the second triangle from the first? More generally, if we have somehow discovered (which is the hard part) a rational right-angled triangle of area $A$, is there a way to obtain another one with the same area?

Suppose that $A$ is a congruent number. Then there are rational numbers $X, Y, Z$ such that

$$X^2 + Y^2 = Z^2,$$

$$\frac{1}{2}XY = A.$$

Adding 4 times the second equation to the first and rearranging terms we get

$$\left(\frac{X+Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 + A.$$

Subtracting instead of adding we get

$$\left(\frac{X-Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - A.$$

Multiplying the left and right sides of the last two equations we obtain

$$\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - A^2.$$

Putting $u = Z/2$ and $v = (X^2 - Y^2)/4$ we get

$$v^2 = u^4 - A^2.$$

Multiplying by $u^2$ gives

$$(uv)^2 = (u^2)^3 - A^2u^2.$$

Setting $x = u^2$ and $y = uv$ we obtain

$$E : y^2 = x^3 - A^2 x.$$

This shows that the rational point

$$(x, y) = \left( \frac{Z^2}{4}, \frac{(X^2 - Y^2) Z}{8} \right)$$

lies on the curve $E$. (We call a point $(x, y)$ *rational* if both $x$ and $y$ are rational numbers.) The equation $E$ (as well as its locus) is called an ***elliptic curve.*** What we have shown is that if $A$ is a congruent number then we can find a rational point on the curve $E : y^2 = x^3 - A^2 x$. Suppose that we are able to find another rational point on the curve $E$. Can we obtain from this point another rational right-angled triangle of area $A$? To answer this question let us first see how new rational points on an elliptic curve can be obtained from known ones. The graph of the elliptic curve

$$E : y^2 = x^3 - A^2 x$$

generally looks like this :

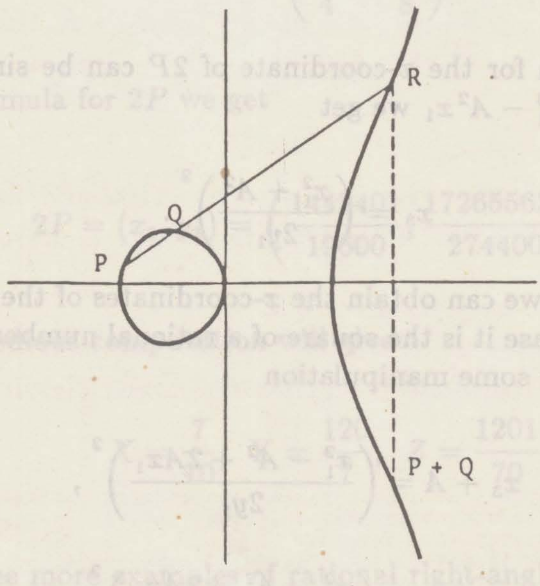


**Figure 3**

Let $P$ and $Q$ be two points on $E$. The line joining $P$ and $Q$ will intersect $E$ again at a point $R$. If $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, -y_3)$, we denote the point $(x_3, y_3)$ by $P + Q$. If the point $Q$ is the same as $P$, then we take the tangent at $P$ to be the line $PQ$ and the point $P + P$ will be denoted by $2P$. Let the equation of $PQ$ be $y = mx + a$. Substituting it in $y^2 = x^3 - A^2 x$ and solving for $x$ we will get the coordinates of $R$ and hence of $P + Q$ (or $2P$). If $P \neq Q$, we have

$$x_3 = -x_1 - x_2 + \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 ,$$

$$y_3 = -y_1 - \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) .$$

If $P = Q$, we have

$$x_3 = -2x_1 + \left( \frac{2x_1^2 - A^2}{2y_1} \right)^2 ,$$

$$y_3 = -y_1 + \left( \frac{3x_1^2 - A^2}{2y_1} \right) (x_1 - x_3) .$$

We see immediately that if $P$ and $Q$ are rational points, then so are $P + Q$ and $2P$.

The expression for the $x$-coordinate of $2P$ can be simplified. Using the relation $y_1^2 = x_1^3 - A^2 x_1$ we get

$$x_3 = \left( \frac{x_1^2 + A^2}{2y_1} \right)^2 .$$

Using this formula we can obtain the $x$-coordinates of the points $4P$, $8P$, $16P$, etc. In each case it is the square of a rational number. Furthermore, we can obtain after some manipulation

$$x_3 + A = \left( \frac{x_1^2 - A^2 + 2Ax_1}{2y_1} \right)^2 ,$$

$$x_3 - A = \left( \frac{x_1^2 - A^2 - 2Ax_1}{2y_1} \right)^2 .$$

It can easily be verified that

$$X = \sqrt{x_3 + A} - \sqrt{x_3 - A},$$
$$Y = \sqrt{x_3 + A} + \sqrt{x_3 - A},$$
$$Z = 2\sqrt{x_3},$$

is a rational right-angled triangle of area $A$.

This shows that each of the points $2P$, $4P$, $8P$, $16P$, etc., will give a rational right-angled triangle of area $A$. (So will the points $3P$, $5P$, $7P$, etc., if $P$ is obtained as above from a rational right-angled triangle; for in this case it can be shown that there is a point $Q$ on $E$ such that $P = 2Q$.)

Let us now do some numerical computation starting with the rational point on $y^2 = x^3 - 36x$ obtained from the triangle with sides 3,4 and 5. We have

$$P = (x_1, y_1) = \left( \frac{Z^2}{4}, \frac{(X^2 - Y^2)\, Z}{8} \right)$$
$$= \left( \frac{25}{4}, -\frac{35}{8} \right).$$

Using the formula for $2P$ we get

$$2P = (x_3, y_3) = \left( \frac{1442401}{19600}, \frac{1726556399}{2744000} \right).$$

Then some tedious computation will give

$$X = \frac{7}{10},\ Y = \frac{120}{7},\ Z = \frac{1201}{70}.$$

Here are three more examples of rational right-angled triangles of area 6 (where $X(nP)$ is the $x$-coordinate of the point $nP$, etc.) :

n = 4

X(4P) = 4386303618090112563849601/233710164715943220558400

Y(4P) = 8704369109085580828275935650626254401/
112983858512463619737216684496448000

X = 2017680/1437599

Y = 1437599/168140

Z = 2094350404801/241717895860

n = 8

X(8P) =
4496942370608668437623803491688144746516812121832330220353135940482871736595521
11551208111024678401/
7082917623688115705702885778631234291517597814239535872288521683692758683605423
0045112363033913600

Y(8P) =
3118154486813851238899642161252972821225801012340423649225929522582870935867066
195274856756888461030478038344334168538500820972923996262168784697601/
5960988531670318971742139522154247624640309205263747167798104038800248842470784
59473944414450509794818074644311492325830884147807754542795600384000

X = 12149807353008887088572640/4156118808548967941769601

Y = 4156118808548967941769601/1012483946084073924047720

Z = 21205995309366331267522543206350800799677728019201/
4208003571673898812953630313884276610165569359720

n = 16

X =

1470411759186146228788346097638447378632385096234322169830177025825102284298993
19383526553807398401/
1784698080054269335747720824248147353187892880150466352162930585411147359826919
61198186826871967440

Y =

2141637696065123202897264989097776823825471456180559622595516702493376831792303
534378241922463609280/
1470411759186146228788346097638447378632385096234322169830177025825102284298993
19383526553807398401

Z =

3828287062759812405802726343647345407154268148992470182031493604127936838241944
4429672863024221282048102305307683054675504581663755927841276758115720421459124
2529333839972242849326273684407014476801/
2624241043508735806564471796442764583007444503849646529252803997087695760054570
3388470868564070209377973721184752836684902119972667419272581210782713600783726
447319119019353356892707124662780063440

As you can see, the computation is horrendous. I have not shown you the coordinates of the point $16P$. The numerator of the $x$-coordinate of $16P$ has 396 digits and the denominator 394 digits. Is there an easier way to obtain these rational right-angled triangles of area 6? I do not know.

What I have tried to show in this talk is that even a very simple question about the integers can lead to very interesting and beautiful mathematics – the theory of elliptic curves in this case. It is a vast and difficult subject. The techniques used to study elliptic curves are among the most advanced and sophisticated in all of mathematics. The theory of elliptic curves has in recent years found application in crytography, but that is another subject (or should I say another enigma).

## References

[1] L. E. Dickson, *History of the Theory of Numbers*, Vol.2, Stechert, 1934.

[2] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics 97, Springer-Verlag, 1984.

[3] G. Kramarz, All congruent numbers less than 2000, *Math. Ann.*, **273** (1986), 337-340.

[4] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.*, **72** (1983), 323-334.