Moscow Center for Continuous Mathematical Education

The Experimental Mathematics Club

Congruents

Scientific supervisor: G. B. Shabat
O. V. Karaseva

2019 - 2021

Contents

1 Introduction

This article discusses the Congruent number problem, that asks which numbers are the areas of rational Pythagorean triples. This problem was known to the Ancient Greeks, but still does not have a fully completed solution.

We will look at the connecting it with elliptic curves and tell how we can find more and more Pythagorean triangles with a given area, if we know at least one of them, without considering serious mathematical things, and just give the Tunnell's solution to the problem, proposed in the last century, which is based on the Birch and Swinnerton-Dyer conjecture, one of the unproven problems of the Millennium.

The text appeared in The Experimental Mathematics Club. George Borisovich Shabat [1] told me [2] about this problem, involved me in its study and helped me a lot. I would like to thank Grigory Merzon and all the members of The Experimental Mathematics Club, especially its supervisors.

[1] george.shabat@gmail.com
[2] karaseva_08@inbox.ru

2 Pythagorean triples

Definition. *The Pythagorean triple consists of three positive rational numbers a, b, c such that*

$$a^2 + b^2 = c^2$$

Theorem.
All Pythagorean triples are given by the formulas ($m > n$; m and n are coprime; m, n are positive integers; k is positive rational number):

$$a = k(2mn)$$
$$b = k(m^2 - n^2)$$
$$c = k(m^2 + n^2)$$

Proof.
Let us find general formula ($Euclid's\ formula$) for primitive Pythagorean triples (a, b, c). All Pythagorean triples can be obtained from primitive ones by multiplying by some rational number k.
We are looking for primitive Pythagorean triples, so a, b, c are pairwise coprime integers. Therefore c is odd. And let a is even, b is odd.

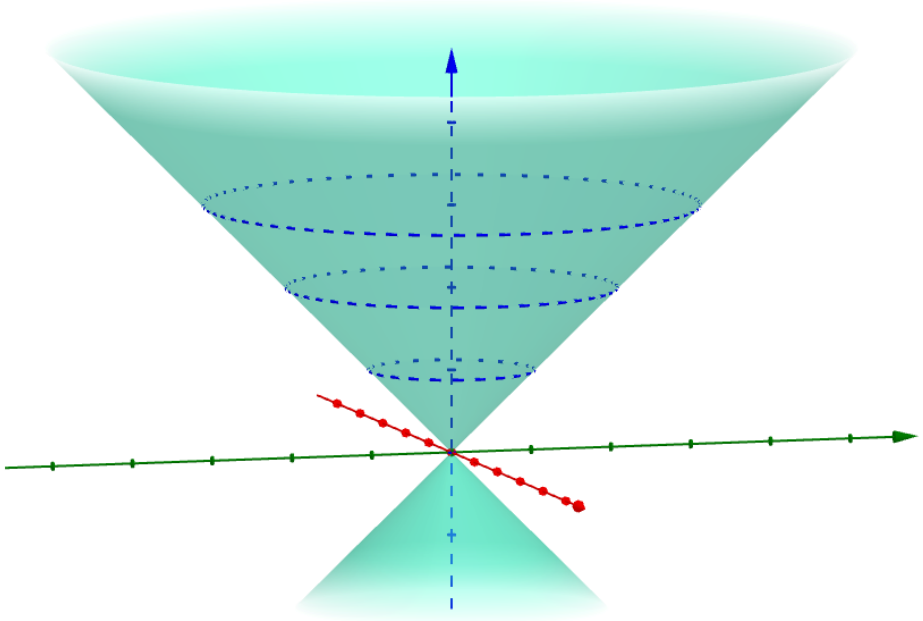
$$a^2 = c^2 - b^2$$
$$\left(\frac{a}{2}\right)^2 = \frac{c-b}{2} \cdot \frac{c+b}{2}$$

$\frac{c-b}{2}$ and $\frac{c+b}{2}$ are coprime because of b and c are coprime too. Also their product is a square number. Since the squareness of the product of coprime numbers implies the squareness of each, there exist m and n such that:

$$\frac{c-b}{2} = n^2; \quad \frac{c+b}{2} = m^2$$

Summing up these two equations, we get $c = m^2 + n^2$. Then $b = m^2 - n^2$, so $a^2 = c^2 - b^2 = (m^2 + n^2)^2 - (m^2 - n^2)^2 = 4m^2n^2$, hence $a = 2mn$
Therefore, for each Pythagorean primitive triple, m and n can be found. And for m, n (if they are coprime and are not both odd) can be find a primitive Pythagorean triple.

Q.E.D.



Pythagorean triples can be represented as a set of points in three-dimensional space (see above). They will form the straight circular cone with the vertice at the point $(0;0;0)$.

3 What are congruents?

Definition. *The numbers, which are the areas of the Pythagorean triples, are called congruents or congruent numbers.*
The areas of Pythagorean triangles with the legs a, b are given by the following formula (m and n are rational) by the theorem in the section 2:

$$A = \frac{a\,b}{2} = \frac{(2mn)(m^2 - n^2)}{2} = m^3n - mn^3$$

Note that considering natural congruents is equivalent to considering rational ones. For example, the Pythagorean triangle $\Big(9; 40; 41\Big)$, which is have the $A = 180$; it corresponds to the Pythagorean triangle $\left(\frac{3}{2}; \frac{20}{3}\frac{41}{6}\right)$, with area $A = 5$. So 5 is a congruent obtained from 180 by dividing by 6^2.

1, 2, 3 (see below) are not congruents, but, for example, 5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30 are.

If we look at the natural Pythagorean triples, that have one of the sides which is 1 less than the hypotenuse, the general formula for their areas is as follows:

$$A_1(k) = k(k+1)(2k+1)$$

If, for example, we look at the natural Pythagorean triples, that have a side, which is shorter than the hypotenuse by 2, for them the formula is as follows:

$$A_2(k) = k(k+1)(k+2)$$

There is the *Congruent Number Problem* that asks, which natural numbers can be congruents. This problem was known to the ancient Greeks, but this is still not fully resolved now. One of the first to study this problem was the Persian mathematician al-Karaji (who lived in the 10-11th centuries and based on the works of Diophantus). Later, Fibonacci (Leonardo of Pisa) established that 5 and 7 are congruents (in 1225 year). His hypothes, 1 is not a congruent number, was proved by Pierre Fermat in 1659 year. By the beginning of the 20th century, all congruent numbers, less than one hundred, were defined. An important breakthrough in this area was made in 1982 year by the American mathematician Jerrold Tunnel (see the next chapter) by connecting congruents and elliptic curves.

4 Tunnell's theorem

As an introduction, note that special attention is paid to congruents in the article by G. B. Shabat and G. A. Merzon "Areas of the Pythagorean triples" and in the Neal Koblitz's book "Introduction to Elliptic Curves and Modular Forms". In the book there is talking about the Tunnell's theorem, which gives the practically complete description of all congruent numbers. If the opposite statement of the Tunnel's theorem is true (it is not fully proven), the Birch and Swinnerton-Dyer conjecture (one of the problems of the Millennium) is true too.

Tunnell's theorem. *If n is an odd natural square-free congruent, then the number of solutions in the integers of the equation $A = 2x^2 + y^2 + 32z^2$ is equal to half the number of solutions in the integers of the equation $A = 2x^2 + y^2 + 8z^2$. If A is an even natural square-free congruent, then the number of solutions in the integers of the equation $A = 8x^2 + 2y^2 + 64z^2$ is equal to half the number of solutions in the integers of the equation $A = 8x^2 + 2y^2 + 16z^2$.*

Example. Let A be the area of the Pythagorean triangle $(20; 21; 29)$. Hence $A = 210$ is an even square-free congruent. The equation $210 = 8x^2 + 2y^2 + 64z^2$ has 8 solutions: $\left\{ \pm 4; \pm 3; \pm 1 \right\}$. And $210 = 8x^2 + 2y^2 + 16z^2$ has 16 solutions: $\left\{ \pm 2; \pm 9; \pm 1 \right\}$ and $\left\{ \pm 4; \pm 3; \pm 2 \right\}$. As we see, $8 \cdot 2 = 16$, which confirms the theorem.

5 From congruents to Square progressions

Let's consider the relations between the congruents and the Square progressions. Let we have a Pythagorean triangle with sides $a > b$ and a hypotenuse c. Then these numbers form an arithmetic progression with the difference $2ab$:

$$(a-b)^2, \quad a^2+b^2, \quad (a+b)^2$$

All the members of this short progression are squares, so we will call this progression a **Square progression.** Let

$$x = a^2 + b^2, \quad S = 2ab.$$

Note that if we know x and S, we can find a, b and c:

$$a = \frac{\sqrt{x+S} + \sqrt{x-S}}{2}; \quad b = \frac{\sqrt{x+S} - \sqrt{x-S}}{2}; \quad c = \sqrt{x}$$

It means that for a and b to be rational, the numbers $x - S$, x and $x + S$ must be squares of some rational numbers. Then S is 4 times the congruent.

Look at all of the above with an example of the Egyptian triangle: $a = 4$, $b = 3$, $c = 5$. In this case $x = 4^2 + 3^2 = 25$ and $S = 2 \cdot 4 \cdot 3 = 24$. Also we can check the formulas for a, b and c:

$$a = \frac{\sqrt{25+24} + \sqrt{25-24}}{2} = 4; \quad b = \frac{\sqrt{25+24} - \sqrt{25-24}}{2} = 3; \quad c = \sqrt{25} = 5$$

That's right, we got Egyptian triangle. We can write down the Square progression itself: $\Big(1, 25, 49\Big)$.

6 From Square progressions to elliptic curves

In the previous section, we looked at Square progressions and noticed that the numbers $x - S$, x, and $x + S$ are squares. If we multiply all these three numbers, we also get the square of some rational number (y):

$$y^2 = (x - S)\, x\, (x + S)$$

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

We obtained the equation of a cubic curve with trivial points $(-S; 0)$, $(0; 0)$ and $(S; 0)$.

Note that if we know at least one rational (not trivial) point of this cubic curve, then we can get another one by:

1) The Diophantus secant method. If we know such a point, we can draw a straight line through it and through any of the trivial or previously found other rational points on this curve. Then the other intersection points of this straight line and the cubic curve will be rational.
The line that we will draw through the points $(x_1; y_1)$ and $(x_2; y_2)$ will be given by the equation ($x_1 \neq x_2$ and $y_1 \neq y_2$):

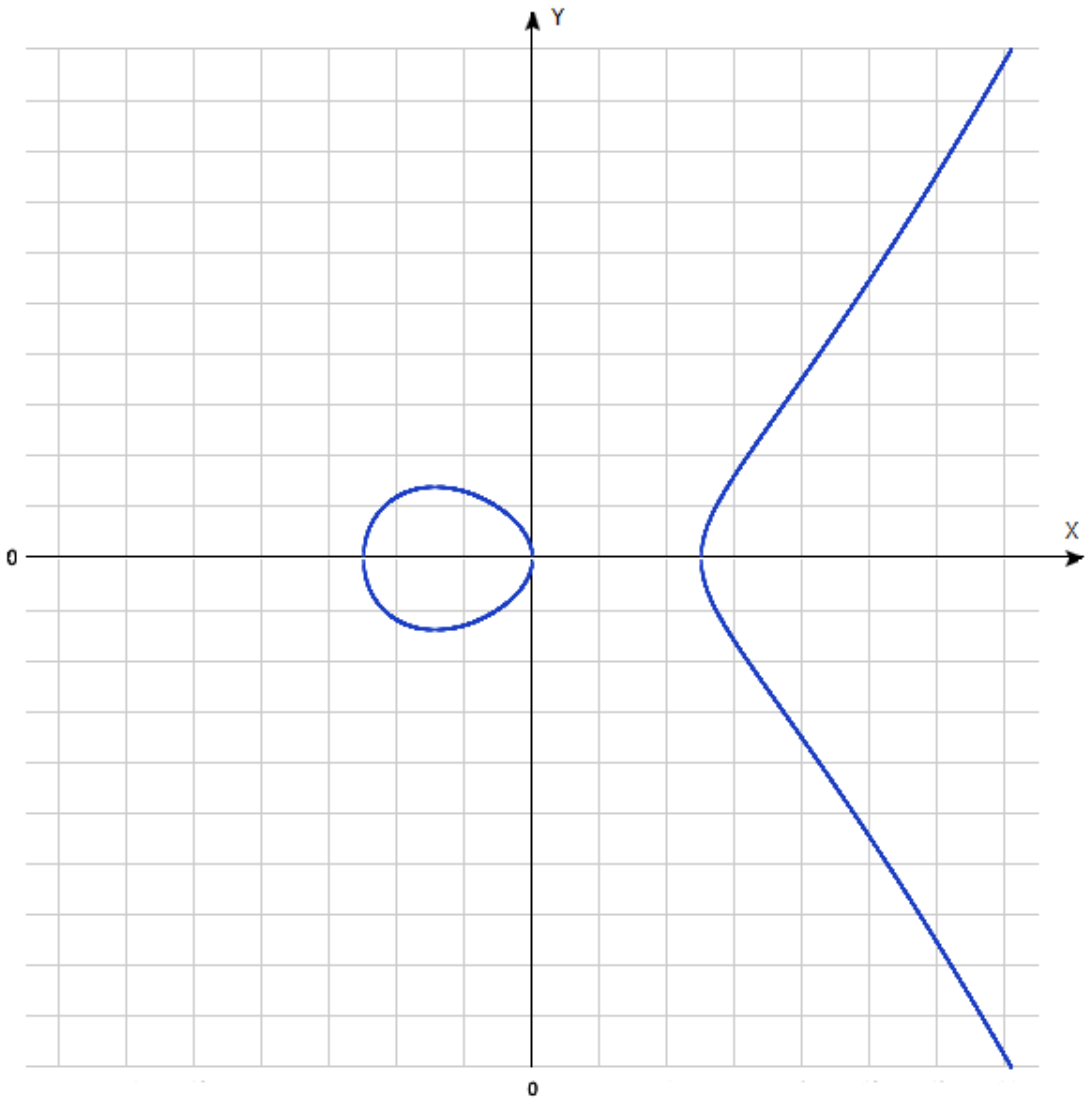
$$y = y_1 + \frac{(y_2 - y_1)(x - x_1)}{x_2 - x_1}$$

2) ***The Diophantus tangent method. In this case, we draw the tangent through a non-trivial point on the elliptic curve. The intersection points of the curve and the tangent will be also rational.
To do this, we can write the equation of all lines passing through a given point $(x_0; y_0)$ (through which we want to draw a tangent): $y = y_0 + k(x - x_0)$. And substitute it in the cubic equation:

$$\Big(y_0 + k(x - x_0)\Big)^2 - (x - S)\,x\,(x + S) = 0$$

The left side of the equation can be represented as two brackets. The first one will be $(x - x_0)$, and the second one will form some polynomial $F(x, k)$. By substituting in $F(x, k)$ $x = x_0$ (the equation becomes linear), we can find one value of k and therefore the tangent equation.

Our curve $y^2 = (x - S)\,x\,(x + S)$ will have approximately the following form:



The graphs of curves $y^2 = (x - S)\,x\,(x + S)$ for $S \in \mathbb{N}$ in the interval $[1; 5]$ are also presented a little below.

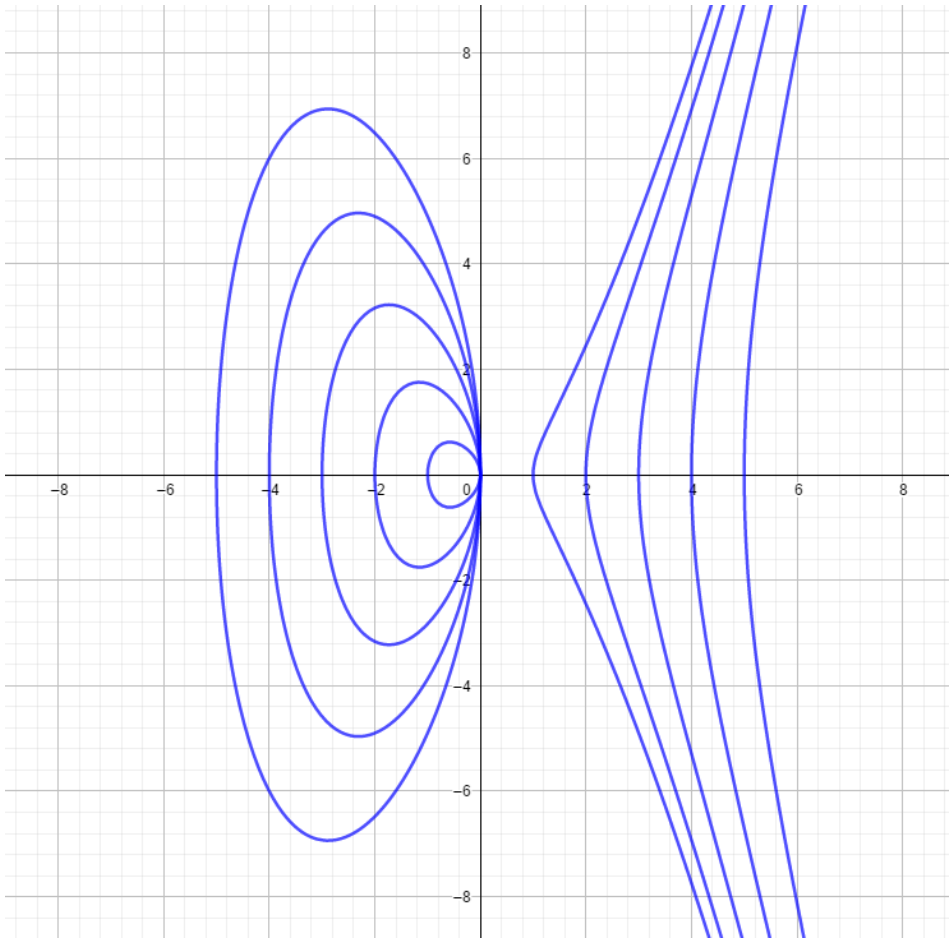
As we can see, each rational Pythagorean triple corresponds to a rational points $(x; y)$ and $(x; -y)$ on the cubic curve under consideration. But the point corresponds to a rational (!) triangle if $x - S$, x and $x + S$ are square numbers.

This can also be written as two other conditions (we assume that $n = \frac{S}{4}$ is a positive square-free integer, otherwise we can multiply or divide it by some square integer; x is represented as a reduced fraction):

(1) x is the square of some rational number.
This is an obvious condition, since by assumption $x^2 = a^2 + b^2 = c^2$. For example, there is a point $(72; 576)$ on the curve $y^2 = (x-24)\,x\,(x+24)$, because of $576^2 = (72-24)\,72\,(72+24) = 331\,776$. This cannot correspond to a rational Pythagorean triangle (with area of 6), because of $\sqrt{72} = 6\sqrt{2}$ is an irrational number (in fact conditions (1) and (2) are incorrect in this case).

(2) the numerator of x must not have common divisors more than one with S.
First, note that the numerator of x must be odd. Let's imagine that a rational point with an abscissa equal to x corresponds to some rational Pythagorean triangle with sides a, b, c. Then $c = \frac{c'}{k}$, where the integers a', b', c' form a primitive Pythagorean triple (a, b, c can be obtained from them by dividing by k). $\Rightarrow x = c^2 = \left(\frac{c'}{k}\right)^2$. Because of c' is odd in the integer primitive Pythagorean triple, the numerator of x will also be odd. Now let the numerator of x and S have an odd common divisor $p > 2$. Then the numerators of the numbers $x + S = (a+b)^2$ and $x - S = (a-b)^2$ are divided by p. Therefore, $\left(a+b\right) \vdots\, p$ and $\left(a-b\right) \vdots\, p$. This means that odd number p is also a divisor of a and b. But in this case $n = \left(\frac{ab}{2}\right) \vdots\, p^2$. We received, that n is not square-free (which contradicts the assumption).

For example, points $(100; 960)$ in $y^2 = (x-28)\,x\,(x+28)$, $(289; 4335)$ in $y^2 = (x-136)\,x\,(x+136)$ or $(25; 75)$ in $y^2 = (x-20)\,x\,(x+20)$ don't satisfy this condition and therefore don't form a rational triangle.



Conditions (1) and (2) are necessary. It turns out that they are also sufficient.

Prove it. Let $\sqrt{x} = u$, where u is rational, and $v = \dfrac{y}{u}$ ($x > 0$, $y > 0$ and $y^2 = (x - S)\,x\,(x + S)$).

$$v^2 = \frac{y^2}{u^2} = \frac{y^2}{x} = (x - S)(x + S) = x^2 - S^2 \quad \Rightarrow v^2 + S^2 = x^2$$

Consider the last equality. Let r be the denominator of u. Then the denominators of x^2 and v^2 must match and equal r^2, since S^2, as S, is a natural number. In this case, r^2v, r^2S and r^2x is a primitive Pythagorean triple, because of $\gcd(r^2S;\, r^2x) = 1$, which follows from $\gcd(r^2x;\, r^2) = 1$ (r^2 is the smallest number such that r^2x is integer, and x is represented as irreducible fraction) and $\gcd(r^2x;\, S) = 1$ (second condition).

$$\Big(r^2v\Big)^2 + \Big(r^2S\Big)^2 = \Big(r^2x\Big)^2$$

It means that r^2x is odd. One of the numbers r^2v and r^2S is even, and it is r^2S, because of $S = 4n$. Then:

$$\begin{cases} r^2S = 2pq \\ r^2v = p^2 - q^2 \\ r^2x = p^2 + q^2 \end{cases}$$

It turns out that a right triangle with sides

$$\left\{\frac{p}{r};\ \frac{q}{r};\ u\right\}$$

has an area equal to n:

$$\sqrt{\left(\frac{p}{r}\right)^2 + \left(\frac{q}{r}\right)^2} = \sqrt{\frac{p^2 + q^2}{r^2}} = \sqrt{\frac{r^2x}{r^2}} = \sqrt{x} = u$$

$$\frac{\frac{p}{r} \cdot \frac{q}{r}}{2} = \frac{\frac{2pq}{r^2}}{4} = \frac{S}{4} = n$$

As we can see, if the two conditions considered earlier are true for a point, there always is a corresponding to it a rational Pythagorean triangle.

Example.
Consider the Pythagorean triangle $(9; 40; 41)$. Its area equals to 180 and it corresponds to a triangle $\left(\frac{3}{2}; \frac{20}{3}; \frac{41}{6}\right)$ with an area of 5 and $S = 20$.

$$x_0 = \left(\frac{41}{6}\right)^2 = \frac{1681}{36}$$

$$y_0 = \sqrt{\left(\frac{1681}{36} - 20\right)\frac{1681}{36}\left(\frac{1681}{36} + 20\right)} = \frac{62\,279}{216}$$

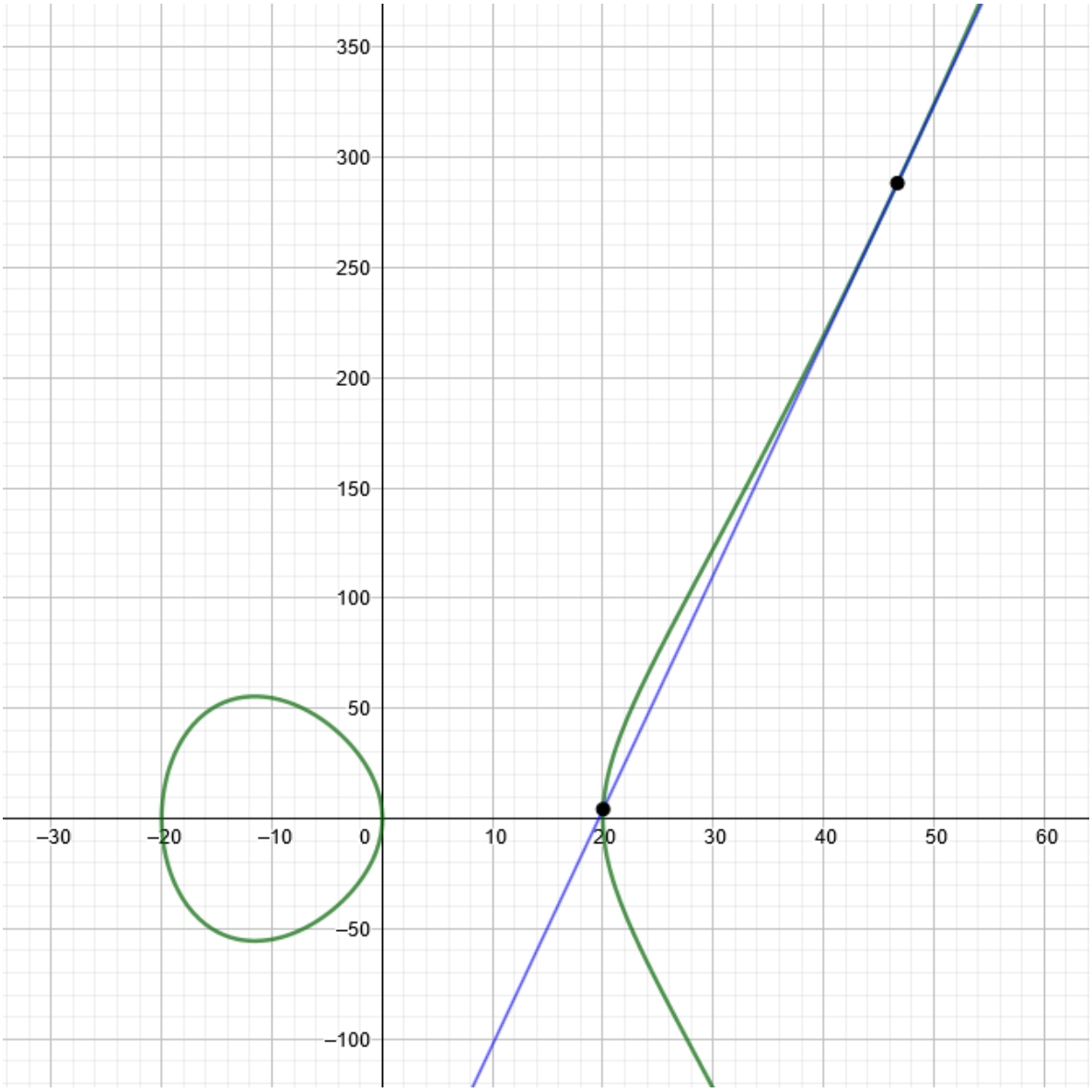
$$y^2 = (x - 20)\,x\,(x + 20)$$

We will draw a tangent $y = y_0 + k\,(x - x_0)$ through the point $(x_0; y_0)$ to the curve $y^2 = (x - 20)\,x\,(x + 20)$.

$$\Big(y_0 + k\,(x - x_0)\Big)^2 - (x - 20)\,x\,(x + 20) = 0$$

$$\left(\frac{62\,279}{216} + k\left(x - \frac{1681}{36}\right)\right)^2 - (x - 20)\,x\,(x + 20) = 0$$

$$\frac{\Big(36x - 1681\Big)\Big(1296k^2x - 60516k^2 + 747348k - 1296x^2 - 60516x - 2307361\Big)}{46656} = 0$$



The expansion into brackets indicates that x_0 is the root of this equation. To find k, and hence the tangent equation, put $x = x_0$ in the second bracket:

$$1296k^2x - 60516k^2 + 747348k - 1296x^2 - 60516x - 2307361 = 0, \quad x = \frac{1681}{36}$$

As a result, we get a linear (!) equation with k:

$$-7958883 + 747348k = 0$$

$$k = \frac{2652961}{249116}$$

Now we can find the equation of the tangent:

$$y = -\frac{137110601}{656208} + \frac{2652961}{249116}\,x$$

Finally, we need to find the intersection points of the tangent and the curve:

$$(x-20)\,x\,(x+20) = \left(-\frac{137110601}{656208} + \frac{2652961}{249116}\,x\right)^2$$

Solving this equation, we find $x = \dfrac{1681}{36}$ and $x = \dfrac{11183412793921}{558529033104}$, $y = \pm\dfrac{1791076534232245919}{417415555832208192}$.

As we can see, $\sqrt{x} = \sqrt{\dfrac{11183412793921}{558529033104}} = \dfrac{3344161}{747348}$ and $\gcd\Big(11183412793921; 20\Big) = 1$.

So, the corresponding Pythagorean triangle exists in the second case too:

$$a = \frac{\sqrt{x+S} + \sqrt{x-S}}{2} = \frac{4920}{1519}, \quad b = \frac{\sqrt{x+S} - \sqrt{x-S}}{2} = \frac{1519}{492}, \quad c = \sqrt{x} = \sqrt{a^2+b^2} = \frac{3344161}{747348}$$

$$A = \frac{1}{2}\,a\,b = \frac{1}{2}\cdot\frac{4920}{1519}\cdot\frac{1519}{492} = 5$$

There are other Pythagorean triples with area of 5. For example:

$$a = \frac{624251547806280259604941031245951878706007939991283 19}{133775751189161858824782767322253868196963922972996 8}$$

$$b = \frac{133775751189161858824782767322253868196963922972996 80}{624251547806280259604941031245951878706007939991283 19}$$

$$c = \frac{3896941041458487485320832722469963686366256264486004169772710584821176712668535259971051251201565099266561}{8350971973878212740240966684609875823763478548941220175986085114112953507390442401963656930118175176379 2}$$

7 Conclusion

So we talked about the connection between the rational areas of right triangles and elliptic curves, and gave the formulation of Tunnell's theorem. But at the moment the general Congruent Number Problem still does not have a complete solution.

One of the generalizations of congruents are Geron triangles, that are triangles with an integer area and rational sides. It turns out that there is an exact formula for their sides and they are closely related to another elliptic curve $y^2 = x\,(x - n\tau)\,(x + \frac{n}{\tau})$.

1. George Shabat and Grigory Merzon, *Areas of Pythagorean triangles*
2. Neal Koblitz, *Introduction to elliptic curves and modular forms*
3. Edray Herber Goins and Davin Maddbox, *Heron triangles via elliptic curves*