MEM204-Number Theory

13th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 15/05/2020

University of Crete

Pythagorian triples

Introduction

Let $x, y, z > 0$ be integers. Then (x, y, z) is called a Pythagorian triple (Πυθαγόρεια τριάδα) if

$$x^2 + y^2 = z^2.$$

They are named after the *Pythagorian theorem*, that implies that these numbers can be the lengths of the edges a (non-degenerate) right triangle.

Primitive Pythagorian triples

Definition

The Pythagorian triple (x, y, z) is called primitive (αρχική) if $\gcd(x, y, z) = 1$.

Let (x, y, z) be a non-primitive Pythagorian triple. Then $1 \neq d = \gcd(x, y, z)$. However, one can easily check that (x', y', z'), where $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ and $z' = \frac{z}{d}$, is a primitive Pythagorian triple.

Inversely, given a primitive Pythagorian triple (x, y, z), every triple of the form (dx, dy, dz) (where $d > 1$) is a (non-primitive) Pythagorian triple.

It follows that, the problem of identifying all the Pythagorian triples can be reduced to identifying all the primitive Pythagorian triples.

Primitive Pythagorian triples

Proposition

The primitive Pythagorian triples are given by the formulas

$$x = 2uv,\ y = u^2 - v^2,\ z = u^2 + v^2$$

and

$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2,$$

where $u, v \in \mathbb{Z}$*, such that* $0 < v < u$*,* $(u, v) = 1$ *and not both of them are odd.*

Proof

Let (x, y, z) be a primitive Pythagorian triple. It is not hard to check that x, y, z are pairwise co-prime (why?). Now, assume that x and y are both odd. Then $x^2 \equiv y^2 \equiv 1 \pmod 4$, hence $z^2 \equiv 2 \pmod 4$, which is impossible. It follows that x, y, z are pairwise co-prime and exactly one of x, y is odd. It follows directly that z is odd.

W.l.o.g. we assume that x is even and y is odd. Then

$$x^2 = z^2 - y^2 = (z+y)(z-y) \Rightarrow \frac{x^2}{4} = \frac{z+y}{2} \cdot \frac{z-y}{2},$$

where all the fractions above are, in fact, integers.

Proof

Now, let $d = (\frac{z+y}{2}, \frac{z-y}{2})$. Then $d \mid \frac{z+y}{2} \pm \frac{z-y}{2}$, that is $d \mid z$ and $d \mid y$. Hence $d \mid (z, y) = 1$, i.e., $d = 1$. We proved that the numbers $\frac{z+y}{2}$ and $\frac{z-y}{2}$ are co-prime and we have that their product is a square. It follows that each of them is a square. So, we may write

$$\frac{z+y}{2} = u^2 \text{ and } \frac{z-y}{2} = v^2,$$

for some u, v.

It follows that $x = 2uv$, $y = u^2 - v^2$ and $z = u^2 + v^2$. Moreover, since $(\frac{z+y}{2}, \frac{z-y}{2}) = 1$, we get that $(u, v) = 1$. If u and v were both odd, we would have z even, a contradiction, hence u and v are not both odd. Finally, it is clear that $0 < v < u$.

Proof

If we assumed that x is odd and y is even, we would similarly get $x = u^2 - v^2$, $y = 2uv$ and $z = u^2 + v^2$, with the same restrictions on u, v.

Now, it remains to show the inverse, that is, that a triple of the described form is, in fact, a primitive Pythagorian triple.

Take two co-prime numbers $0 < v < u$, such that not both of them are odd. Then

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2,$$

hence the triples $(u^2 - v^2, 2uv, u^2 + v^2)$ and $(2uv, u^2 - v^2, u^2 + v^2)$ are Pythagorian triples. It remains to show that they are primitive.

Proof

Let $d' = (u^2 - v^2, u^2 + v^2)$. We get that $d' \mid (u^2 - v^2) \pm (u^2 + v^2)$, that is, $d' \mid 2u^2$ and $d' \mid 2v^2$. Since $(u, v) = 1$ the latter implies $d' \mid 2$, thus $d' = 1$ or 2. However, since exactly one of u and v is odd, we get that $u^2 - v^2$ and $u^2 + v^2$ are odd, hence d' is odd, hence $d' = 1$. It follows that $(2uv, u^2 - v^2, u^2 + v^2) = 1$ and the result follows.

A complete characterization

Corollary

The integer solutions of the equation

$$x^2 + y^2 = z^2$$

are described by the rules

$$x = \pm d(u^2 - v^2),\ y = \pm d2uv,\ z = \pm d(u^2 + v^2)$$

or

$$x = \pm d2uv,\ y = \pm d(u^2 - v^2),\ z = \pm d(u^2 + v^2),$$

where $d \in \mathbb{Z}$*,* $0 \leq v < u$*,* $(u, v) = 1$ *and not both of* u *and* v *are odd.*

Some examples

- For $d = 1$, $u = 2$ and $v = 1$, we get the most well-known Pythagorian triple, $(3, 4, 5)$.
- For $d = 1$, $u = 3$ and $v = 2$, we get $(5, 12, 13)$.
- For $d = 2$, $u = 4$ and $v = 3$, we get the (non-primitive) triple $(14, 48, 50)$.

Fermat's last theorem

A famous text

In 1637, inspired by the Pythagorian triples, Fermat wrote the following on the margin of his personal copy of Diophantus' *Arithmetica*:

> *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 marvelous proof of this, which this margin is too narrow to contain.*

In other words, Fermat claimed to have proved that the Diophantine equation $x^n + y^n = z^n$ has no integer non-trivial solutions if $n \geq 3$ (where non-trivial means $x, y, z \neq 0$).

A historical theorem

It is now considered unlikely that Fermat had actually proved his claim. Instead it took almost 360 years for mathematicians to actually prove it. The result is now known as *Fermat's last theorem*.

Theorem (Fermat's last theorem)

The equation $x^n + y^n = z^n$ has no integer non-trivial solutions if $n \geq 3$.

A historical theorem

- Partial proofs (for certain n's) were given by numerous scholars, with the case $n = 4$ deriving directly from another result of Fermat.
- After working on this problem for 7 years, Andrew Wiles, presented a proof in 1994. The proof was published in two papers in *Annals of Mathematics* and its total length is 129 pages.
- For this result, Wiles won several awards, including a knighthood and an Abel prize.
- Before Wiles's proof, the conjecture was notorious for its numerous false proofs. In fact, the first proof of Wiles also contained an error, that he quickly corrected.

Stay safe!