JOURNAL OF FORMALIZED MATHEMATICS
Volume 13, Released 2001, Published 2003
Inst. of Computer Science, Univ. of Białystok

Pythagorean Triples

Freek Wiedijk
University of Nijmegen

Summary. A Pythagorean triple is a set of positive integers $\{a,b,c\}$ with $a^2+b^2=c^2$. We prove that every Pythagorean triple is of the form

$$a=n^2-m^2 \qquad b=2mn \qquad c=n^2+m^2$$

or is a multiple of such a triple. Using this characterization we show that for every $n>2$ there exists a Pythagorean triple X with $n \in X$. Also we show that even the set of *simplified* Pythagorean triples is infinite.

MML Identifier: PYTHTRIP.

WWW: http://mizar.org/JFM/Vol13/pythtrip.html

The articles [11], [15], [5], [3], [12], [7], [14], [8], [1], [13], [9], [6], [10], [16], [4], and [2] provide the notation and terminology for this paper.

1. Relative Primeness

We follow the rules: a, b, c, k, m, n are natural numbers and i is an integer.

Let us consider m, n. Let us observe that m and n are relative prime if and only if:

(Def. 1) For every k such that $k \mid m$ and $k \mid n$ holds $k=1$.

Let us consider m, n. Let us observe that m and n are relative prime if and only if:

(Def. 2) For every prime natural number p holds $p \nmid m$ or $p \nmid n$.

2. Squares

Let n be a number. We say that n is square if and only if:

(Def. 3) There exists m such that $n=m^{\mathbf{2}}$.

Let us note that every number which is square is also natural.
Let n be a natural number. Note that $n^{\mathbf{2}}$ is square.
Let us observe that there exists a natural number which is even and square.
Let us observe that there exists a natural number which is odd and square.
Let us mention that there exists a number which is even and square.
One can verify that there exists a number which is odd and square.
Let m, n be square numbers. Observe that $m \cdot n$ is square.
Next we state the proposition

(1) If $m \cdot n$ is square and m and n are relative prime, then m is square and n is square.

Let i be an even integer. Note that i^2 is even.
Let i be an odd integer. One can verify that i^2 is odd.
We now state three propositions:

(2) i is even iff i^2 is even.

(3) If i is even, then $i^2 \bmod 4 = 0$.

(4) If i is odd, then $i^2 \bmod 4 = 1$.

Let m, n be odd square numbers. Note that $m+n$ is non square.
We now state two propositions:

(5) If $m^2 = n^2$, then $m = n$.

(6) $m \mid n$ iff $m^2 \mid n^2$.

3. Distributive Law for HCF

The following propositions are true:

(7) $m \mid n$ or $k = 0$ iff $k \cdot m \mid k \cdot n$.

(8) $\gcd(k \cdot m, k \cdot n) = k \cdot \gcd(m,n)$.

4. Unbounded Sets are Infinite

Next we state the proposition

(9) For every set X such that for every m there exists n such that $n \geq m$ and $n \in X$ holds X is infinite.

5. Pythagorean Triples

We now state three propositions:

(10) If a and b are relative prime, then a is odd or b is odd.

(11) Suppose $a^2 + b^2 = c^2$ and a and b are relative prime and a is odd. Then there exist m, n such that $m \leq n$ and $a = n^2 - m^2$ and $b = 2 \cdot m \cdot n$ and $c = n^2 + m^2$.

(12) If $a = n^2 - m^2$ and $b = 2 \cdot m \cdot n$ and $c = n^2 + m^2$, then $a^2 + b^2 = c^2$.

A subset of $\mathbb{N}$ is called a Pythagorean triple if:

(Def. 4) There exist a, b, c such that $a^2 + b^2 = c^2$ and it $= \{a,b,c\}$.

In the sequel X is a Pythagorean triple.
Let us observe that every Pythagorean triple is finite.
Let us note that the Pythagorean triple can be characterized by the following (equivalent) condition:

(Def. 5) There exist k, m, n such that $m \leq n$ and it $= \{k \cdot (n^2 - m^2), k \cdot (2 \cdot m \cdot n), k \cdot (n^2 + m^2)\}$.

Let us consider X. We say that X is degenerate if and only if:

(Def. 6) $0 \in X$.

We now state the proposition

(13) If $n > 2$, then there exists X such that X is non degenerate and $n \in X$.

Let us consider X. We say that X is simplified if and only if:

(Def. 7) For every k such that for every n such that $n \in X$ holds $k \mid n$ holds $k = 1$.

Let us consider X. Let us observe that X is simplified if and only if:

(Def. 8) There exist m, n such that $m \in X$ and $n \in X$ and m and n are relative prime.

The following proposition is true

(14) If $n > 0$, then there exists X such that X is non degenerate and simplified and $4 \cdot n \in X$.

Let us note that there exists a Pythagorean triple which is non degenerate and simplified.
We now state two propositions:

(15) $\{3,4,5\}$ is a non degenerate simplified Pythagorean triple.

(16) $\{X : X \text{is non degenerate} \wedge X \text{is simplified}\}$ is infinite.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[3] Grzegorz Bancerek. Sequences of ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal2.html.

[4] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[5] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finset_1.html.

[6] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Journal of Formalized Mathematics*, 10, 1998. http://mizar.org/JFM/Vol10/pepin.html.

[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/real_1.html.

[8] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_2.html.

[9] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Journal of Formalized Mathematics*, 9, 1997. http://mizar.org/JFM/Vol9/abian.html.

[10] Andrzej Trybulec. Domains and their Cartesian products. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/domain_1.html.

[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[12] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[13] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers operations: min, max, square, and square root. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/square_1.html.

[14] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_1.html.

[15] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[16] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

Received August 26, 2001

Published January 2, 2004