FORMALIZED MATHEMATICS
Volume 9, Number 4, 2001
University 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.

The articles [6], [7], [2], [8], [5], [1], [3], [4], and [9] provide the terminology and notation 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 $p \nmid n$.

ISSN 1426–2630

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 observe that every number which is square is also natural.

Let n be a natural number. Observe that $n^{\mathbf{2}}$ is square.

Let us observe that there exists a natural number which is even and square.

One can check that there exists a natural number which is odd and square.

One can check that there exists a number which is even and square.

One can check that there exists a number which is odd and square.

Let m, n be square numbers. Observe that $m \cdot n$ is square.

We now 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. Observe that $i^{\mathbf{2}}$ is even.

Let i be an odd integer. Observe that $i^{\mathbf{2}}$ is odd.

Next we state three propositions:

(2) i is even iff $i^{\mathbf{2}}$ is even.

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

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

Let m, n be odd square numbers. Note that $m + n$ is non square.

One can prove the following two propositions:

(5) If $m^{\mathbf{2}} = n^{\mathbf{2}}$, then $m = n$.

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

3. Distributive Law for HCF

We now state two propositions:

(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

We now state the proposition

(9) For every set X such that for every m there exists n such that $n \geqslant m$ 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 $a^{\mathbf{2}} + b^{\mathbf{2}} = c^{\mathbf{2}}$ and a and b are relative prime and a is odd. Then there exist m, n such that $m \leqslant n$ and $a = n^{\mathbf{2}} - m^{\mathbf{2}}$ and $b = 2 \cdot m \cdot n$ and $c = n^{\mathbf{2}} + m^{\mathbf{2}}$.

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

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

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

In the sequel X is a Pythagorean triple.

Let us note 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 $m \leqslant n$ and it $= \{k \cdot (n^{\mathbf{2}} - m^{\mathbf{2}}), k \cdot (2 \cdot m \cdot n), k \cdot (n^{\mathbf{2}} + m^{\mathbf{2}})\}$.

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.

One can prove the following proposition

(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.

The following propositions are true:

(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. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[3] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.

[4] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[5] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[6] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[7] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[8] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[9] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received August 26, 2001