MATH 324 Summer 2012
Elementary Number Theory

Notes on Pythagorean Triples

Pythagorean Triples

In the following we present a brief introduction to Pythagorean triples, and we leave as exercises several questions which can be done as practice for the final examination.

Given a right triangle with legs of length a and b and hypotenuse of length c, the Pythagorean theorem tells us that

$$a^2 + b^2 = c^2 \tag{$*$}$$

and if a, b and c are positive integers, then the triplet (a, b, c) is called a **Pythagorean triple**.

The Pythagorean relationship was known even before Pythagoras. One of the Babylonian clay tablets in the G. A. Plympton Collection at Columbia University indicates that the Babylonians knew of the Pythagorean theroem more than 3500 years ago.

Note that $(3, 4, 5)$ is a Pythagorean triple, moreover, for any positive integer n, we have

$$(3n)^2 + (4n)^2 = 9n^2 + 16n^2 = 25n^2 = (5n)^2,$$

so that $(3n, 4n, 5n)$ is also a Pythagorean triple. Thus, there are infinitely many Pythagorean triples.

If (a, b, c) is a Pythagorean triple, then we say that it is a **primitive Pythagorean triple** if and only if a, b, and c have no common factors, that is,

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1.$$

There are many different ways to construct Pythagorean triples.

- We can use the **Fibonacci numbers**

F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	$\cdots$	F_n
0	1	1	2	3	5	8	13	21	$\cdots$	$F_{n-2} + F_{n-1}$

  where each term in the sequence is the sum of the previous two terms, to construct Pythagorean triples as follows. Let n be a positive integer and define

$$\begin{aligned} a &= F_n F_{n+3} \\ b &= 2F_{n+1}F_{n+2} \\ c &= F_{n+1}^2 + F_{n+2}^2, \end{aligned}$$

  where F_n is the n^{th} Fibonacci number, then it is easy to show that $a^2 + b^2 = c^2$, so that (a, b, c) is a Pythagorean triple. As an exercise, determine if it is a primitive Pythagorean triple.

  Also, show that we cannot generate all Pythagorean triples in this way.

- Another method, discovered by the **Pythagoreans**, is as follows. If n is any odd positive integer, and we define

$$a = n$$
$$b = \frac{n^2 - 1}{2}$$
$$c = \frac{n^2 + 1}{2}$$

then (a, b, c) is a Pythagorean triple. Verify this as an exercise, and show also that we cannot generate all Pythagorean triples in this way.

- Yet another method, discovered by the Greek philosopher **Plato**, is as follows. If n is any positive integer, and we define

$$a = 2n$$
$$b = n^2 - 1$$
$$c = n^2 + 1$$

then (a, b, c) is a Pythagorean triple. Again, verify that this is so, and that we cannot generate all Pythagorean triples this way.

- In 1934, **M. Willey** and **E. C. Kennedy** gave the following method for generating infinitely many Pythagorean triples.

a	b	c
21	220	221
201	20200	20201
2001	2002000	2002001
20001	200020000	200020001
200001	20000200000	20000200001
2000001	2000002000000	2000002000001
$\vdots$	$\vdots$	$\vdots$

You are invited to find a formula for these a, b and c, and show that it does indeed generate infinitely many Pythagorean triplets, but again, not all of them.

- In his book *The Elements*, **Euclid** gave the following method for generating Pythagorean triplets. For any positive integers m and n which are relatively prime, that is, $\gcd(m, n) = 1$, and of different parity, that is, one is even and the other is odd, if we define for $m > n$,

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

then (a, b, c) is a primitive Pythagorean triple. Moreover, *every* primitive Pythagorean triple arises in this way. In order to prove this, we need the following lemmas.

Lemma 1. If (a, b, c) is a primitive Pythagorean triple, then a and b are of different parity, that is, one is even and the other is odd.

Proof. If a and b are both even, then $\gcd(a, b) \geq 2$, which is a contradiction, since (a, b, c) is a primitive Pythagorean triple. If a and b are both odd, then

$$a^2 \equiv 1 \pmod 4 \qquad \text{and} \qquad b^2 \equiv 1 \pmod 4,$$

so that

$$c^2 = a^2 + b^2 \equiv 2 \pmod 4,$$

which is impossible, since the square of any integer is congruent to 0 or 1 modulo 4. Therefore, a and b have opposite parity.

□

Lemma 2. If u and v are relatively prime positive integers such that $u \cdot v$ is a perfect square, then both u and v are perfect squares.

Proof. Let p be a prime that divides u and let α be the exact power of p in u. (In symbols, we denote this by $p^\alpha || u$.) Since u and v are relatively prime, then p does not divide v, and therefore $p^\alpha || u \cdot v$. However, $u \cdot v$ is a perfect square, so that α must be even. Since this holds for all primes p dividing u, then u is a perfect square. Similarly, v is a perfect square.

□

Theorem. If (a, b, c) is a primitive Pythagorean triple, with b even, then there exist positive integers m and n which are relatively prime and of opposite parity with $m > n$ such that

$$\begin{aligned} a &= m^2 - n^2 \\ b &= 2mn \\ c &= m^2 + n^2 \end{aligned}$$

Proof. If (a, b, c) is a primitive Pythagorean triple with b even, then a is odd, and since $c^2 = a^2 + b^2$, then c is also odd. Therefore, $c - a$ and $c + a$ are both even, so that

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

Any common divisor of the two factors on the left divides both their sum c and their difference a, and since $\gcd(a, c) = 1$, then the two factors on the left have no common divisors except 1, that is, they are relatively prime. From the lemma, they must both be squares, so there exist positive integers m and n such that

$$\begin{aligned} \frac{c+a}{2} &= m^2 \\ \frac{c-a}{2} &= n^2 \\ \frac{b}{2} &= mn. \end{aligned}$$

We note that m and n are relatively prime since $c + a$ and $c - a$ are relatively prime, and that $m > n$. Also, since $c^2 = m^2 + n^2$ and c is odd, then m and n have different parity.

□