Pythagorean Triples

Definition 1 (Pythagorean Triple)**.** *Given positive integers a, b, and c, we say that (a, b, c) is a* pythagorean triple *if $a^2 + b^2 = c^2$. If a, b, and c are mutually coprime we say that as a pythagorean triple, (a, b, c) is* primitive*.*

Proposition 1. *Let (a, b, c) be a pythagorean triple.*

1. *The following are equivalent. (1) (a, b, c) is primitive, (2) $\mathsf{gcd}(a, b) = 1$, (3) $\mathsf{gcd}(a, c) = 1$, (4) $\mathsf{gcd}(b, c) = 1$.*

2. *If (a, b, c) is primitive, then up to a swap of a and b, we can assume that b is even and a and c are odd.*

Proof. Note that the squares modulo 4 are 0 and 1; considering the equation $a^2 + b^2 \equiv c^2 \mod 4$ then gives only two possibilities: either $a^2 \equiv c^2 \equiv 1 \mod 4$ and $b^2 \equiv 0 \mod 4$, or $b^2 \equiv c^2 \equiv 1 \mod 4$ and $a^2 \equiv 0 \mod 4$. Without loss of generality, we can suppose the first case. Now b is even and a and c odd. $\square$

Lemma 2.

1. *If $a, b, c \in \mathbb{Z}$ such that $ab = c^2$ and $\mathsf{gcd}(a, b) = 1$, then $a = u^2$ and $b = v^2$ are squares.*

2. *If $a, b \in \mathbb{Z}$ are positive and $a^2 = b^2$, then $a = b$.*

Proof.

1. We can induct on the number of prime factors of a. If $a = 1$, then $a = 1^2$ and $b = c^2$. Now suppose p is a prime with $p|a$. Now $p|c^2$, so that $p|c$ (since p is prime) and thus $p^2|c^2$. So $p^2|ab$, and since p does not divide b, using Euclid's lemma we have $p^2|a$. Dividing out p^2 we get a similar equation $(a')b = (c')^2$ in which a has two fewer prime factors.

2. We have $(a + b)(a - b) = 0$, so either $a = -b$ or $a = b$. In the first case, a is both positive and negative, a contradiction. $\square$

Theorem 3 (Euclid's Parameterization of Pythagorean Triples)**.** *Let $a, b, c \in \mathbb{Z}$. Then (a, b, c) is a primitive pythagorean triple with b even if and only if there exist integers m and n such that the following hold.*

- *$m > n > 0$,*
- *$\mathsf{gcd}(m, n) = 1$,*
- *$m - n$ is odd, and*
- *$a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$.*

Proof. First suppose that m and n have these four properties. Certainly a, b, and c are positive, b is even, and

$$\begin{aligned} a^2+b^2 &= (m^2-n^2)^2+(2mn)^2 \\ &= m^4-2m^2n^2+n^4+4m^2n^2 \\ &= m^4+2m^2n^2+n^4 \\ &= (m^2+n^2)^2 \\ &= c^2, \end{aligned}$$

so that (a,b,c) is a pythagorean triple. It remains to be seen that (a,b,c) is primitive. To this end, suppose p is a prime dividing both $a=m^2-n^2=(m+n)(m-n)$ and $b=2mn$. If $p=2$, then 2 divides either $m+n$ or $m-n$. But $m+n\equiv m-n\equiv 1 \mod 2$, a contradiction. If $p\neq 2$, then either $p|m$ or $p|n$ and either $p|(m+n)$ or $p|(m-n)$. If $p|m$ and $p|(m+n)$, then $p|n$, so that $p|\mathsf{gcd}(m,n)$, a contradiction; similarly, in the other three cases we get a prime divisor of $\mathsf{gcd}(m,n)$. So in fact $\mathsf{gcd}(a,b)=1$, and thus (a,b,c) is a primitive pythagorean triple.

Conversely, suppose (a,b,c) is a primitive pythagorean triple with b even and a and c odd. Note that $c+a$ and $c-a$ are even (consider these equations mod 2). Let's write

$$c+a=2r, \quad c-a=2s, \quad \text{and } quadb=2t.$$

Now we have $b^2=c^2-a^2=(c+a)(c-a)$, so that $t^2=rs$.

We claim that $\mathsf{gcd}(r,s)=1$. To see this, suppose p is a prime such that $p|r$ and $p|s$. In particular, p divides $c+a$ and $c-a$, so p divides both $2a=(c+a)-(c-a)$ and $2c=(c+a)+(c-a)$. If $p\neq 2$, then $p|\mathsf{gcd}(a,c)$, so that $p=1$, a contradiction. Suppose $p=2$. In this case we have that $c+a=4r'$ and $c-a=4s'$, so that $2c=4(r'+s')$ and $2a=4(r'-s')$, and thus $2|\mathsf{gcd}(a,c)$, again a contradiction. So $\mathsf{gcd}(r,s)=1$.

Since $rs=t^2$ and $\mathsf{gcd}(r,s)=1$, both $r=m^2$ and $s=n^2$ are squares by the lemma. We can assume that m and n are both positive. Since a is positive, we have $m>n$. We can see that $a=m^2-n^2$ and $c=m^2+n^2$, and $b^2=(2mn)^2$, so that $b=2mn$ by the lemma. Since $\mathsf{gcd}(r,s)=1$, we also have $\mathsf{gcd}(m,n)=1$. Finally, if $m-n$ is even, then $a^2=(m-n)(m+n)$ is even, so that a is even, a contradiction; hence $m-n$ is odd. $\square$