# Number Theory Section Summary: 11.1
## Pythagorean Triples

## 1. Summary

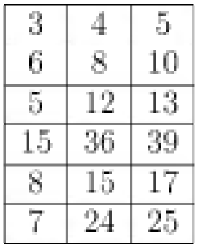
Here come those Pythagoreans again! The special right triangles related to Pythagorean triples had been studied and used by the Babylonians and the Egyptians long before Pythagoras, but those are the vagaries of history....

Pythagoras did find a formula for an infinite number of these, so there's some justification for the name.

## 2. Definitions

**Pythagorean triple**: a set of three integers $x$, $y$, $z$ such that $x^2+y^2=z^2$. The triple is said to be **primitive** if $\gcd(x,y,z)=1$.

Table 1: Examples of Pythagorean triples. Which are primitive?



| | | |
|---|---|---|
| 3 | 4 | 5 |
| 6 | 8 | 10 |
| 5 | 12 | 13 |
| 15 | 36 | 39 |
| 8 | 15 | 17 |
| 7 | 24 | 25 |

**Pythagorean triangle**: a right triangle whose sides are of integral length.

**Pythagorean theorem**: a famous theorem about right triangles (not necessarily Pythagorean triangles), infamously misstated by the scarecrow in the Wizard of Oz http://mathworld.wolfram.com/PythagoreanTheorem.html

: *After receiving his brains from the wizard in the 1939 film 'The Wizard of Oz', the Scarecrow recites the following mangled (and incorrect) form of the Pythagorean theorem, "The sum of the square roots of any two sides of an isosceles triangle is equal to the square root of the remaining side."*

## 3. Theorems

**Lemma 1**: If $x$, $y$, $z$ is a primitive Pythagorean triple, then one of the integers $x$ or $y$ is even, while the other is odd.

**Lemma 2**: If $ab = c^n$, where $\gcd(a, b) = 1$, then $a$ and $b$ are $n^{th}$ powers. That is, there exist positive integers $a_1$ and $b_1$ for which $a = a_1^n$ and $b = b_1^n$.

**Theorem 11.1**: All solutions of the Pythagorean equation

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

satisfying the conditions

$$\gcd(x, y, z) = 1 \quad 2|x \quad x, y, z > 0$$

are given by the formulas

$$x = 2st \quad y = s^2 - t^2 \quad z = s^2 + t^2.$$

For integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.

## 4. Properties/Tricks/Hints/Etc.

The radius of the inscribed circle of a Pythagorean triangle is always an integer (Theorem 11.2).

Proof of Lemma 1:

BWOC, assume that $x \equiv y \pmod 2$. If $x$ & $y$ are even, then $2 \mid z^2 \Rightarrow 2 \mid z \Rightarrow \gcd(x, y, z) \geq 2$. But this contradicts $\gcd(x, y, z) = 1$. So $x$ & $y$ must both be odd: let

$$x = 2m + 1$$
$$y = 2n + 1$$

Then $z^2 = x^2 + y^2 = (2m+1)^2 + (2n+1)^2 = 4(m^2 + n^2) + 4(m+n) + 2$

$$= 2\left[2\left[(m^2+n^2)+\ (m+n)\right] + 1\right]$$

$\therefore\ 2 \mid z^2 \Rightarrow 2 \mid z$, so $z = 2q$

$${}^{2}\cancel{4}q^2 = \cancel{2}\left[\qquad\qquad\right]$$

$$2q^2 = \underbrace{\left[2\left[\quad\right] + 1\right]}_{\text{odd}}, \Rightarrow \text{contradiction.}$$

---

$\therefore\ x \not\equiv y \pmod 2$ : one is even, the other odd.

---

Proof of Lemma 2: Given $ab = c^n$, $\gcd(a,b)=1$.

Let $\left.\begin{array}{l} a = \cancel{p}p_1^{k_1}\cdots p_r^{k_r} \\ c = c_1^{l_1}\cdots c_s^{l_s}\end{array}\right\}$ be the prime factorizations.

$$\therefore\ p_1^{k_1}\cdots p_r^{k_r}\, b = c^n = c_1^{l_1 n}\cdots c_s^{l_s n}$$

For each $p_i$, $p_i \mid c^n \Rightarrow p_i \mid c_j^{l_j n}$ for some $j$

$$\Rightarrow p_i = c_j$$

& the powers have to match up:

$$p_i^{k_i} = c_j^{l_j n} = p_i^{l_j n}$$

$$\therefore\ k_i = l_j n \qquad \therefore\ l_j = k_i/n \in \mathbb{Z}$$

So

$$a = p_1^{k_1}\cdots p_r^{k_r} = p_1^{(k_1/n)n}\cdots p_r^{(k_r/n)n}$$
$$= \left(p_1^{k_1/n}\cdots p_r^{k_r/n}\right)^n$$

$a$ is an $n^{\text{th}}$ power. By symmetry,
$b$ " " " ".

---

Proof of the Theorem:

Assume we have a primitive triple $x, y, z$, /

$\gcd(x,y,z)=1$ & $x$ is even.

We know that $y$ is odd by lemma 1; let's show that $z$ is odd: $z^2$ = sum of an odd & an even $\Rightarrow$ $z^2$ is odd $\therefore$ $z$ is odd.

Consider

$$\boxed{\begin{aligned} z-y &= 2u \\ z+y &= 2v \end{aligned}}$$

Let's rewrite $x^2+y^2=z^2$ in terms of $u$ & $v$:

$$x^2 = z^2 - y^2 = (z-y)(z+y)$$

$$= 2u \cdot 2v = 4uv$$

so $\boxed{\left(\frac{x}{2}\right)^2 = uv}$; if only $\gcd(u,v)=1$!

We can use the lemma; so let's check: BWOC, assume they're not relatively prime: $\gcd(u,v)=d>1$.

$$\left.\begin{aligned} z &= u+v \\ y &= v-u \end{aligned}\right\} \Rightarrow d \mid z \text{ \& } d \mid y,$$

$$\Rightarrow d \mid x$$

(as $x^2=z^2-y^2$)

So $x,y,z$ wasn't primitive. Contradiction.

So $\gcd(u,v)=1$, & we can use the lemma: $u=t^2$ & $v=s^2$ $\exists\, s,t \in \mathbb{Z}^+$, & $s>t>0$

$$z = s^2+t^2$$

$$y = s^2-t^2$$

$$\left(\frac{x}{2}\right)^2 = uv \Rightarrow x = 2st$$

---

Left to show: $\gcd(s,t)=1$ & $s \not\equiv t \pmod 2$

BWOC assume $\gcd(s,t)=d>1$. $\Rightarrow d \mid z$ & $d \mid y \Rightarrow$

$d \mid x$, contradicting $\gcd(x,y,z)=1$. So $\gcd(s,t)=1$.

Need to show that $s \not\equiv t \pmod 2$. BWOC, assume $s \equiv t \pmod 2$.

Both even: contradicts $\gcd(s,t)=1$

Both odd: contradicts $y$ odd.

$\therefore$ $s \not\equiv t \pmod 2$.

$s=2$ & $t=1$ $\Rightarrow$ $$\boxed{\begin{aligned} x &= 2\cdot 2\cdot 1 = 4 \\ y &= 4-1 = 3 \\ z &= 4+1 = 5 \end{aligned}}$$

$(3,4,5)$

$s=3$, $t=2$ $\qquad$ $(5,12,13)$

$s=8$, $t=1$ $\qquad$ $(16,63,65)$

$\vdots$

---

#4 Primitive $(x,y,z)$ satisfies $12 \mid xy$ & $60 \mid xyz$

Start with $12 \mid xy$:

$x = 2st$ where $s$ or $t$ is even $\Rightarrow$ $4 \mid x$.

Need to show that $3 \mid x$ or $3 \mid y$.

BWOC, assume $3 \nmid x$ and $3 \nmid y$.

$x = 2st$

$y = s^2 - t^2$

$s,t$: one odd, one even relatively prime

$\gcd(y,3)=1$; $\therefore$ $y^2 \equiv 1 \pmod 3$.

Similarly for $x$. Since $3 \nmid x$, $3 \nmid s$ or $t$ either.

So

$$s^2 \equiv 1 \pmod 3$$
$$t^2 \equiv 1 \pmod 3$$

$y = s^2 - t^2 \equiv 0 \pmod 3$. Contradiction: $3 \nmid y$.

$\therefore$ Either $x$ or $y$ must be divisible by 3;

$\therefore$ $12 \mid xy$.

---

Part 2: $60 \mid xyz$. We need to show that $5 \mid$ one of $x, y,$ or $z$.

~~BWOC: assume not: $x^4 \equiv y^4 \equiv z^4 \equiv 1 \pmod 5$~~

~~$y = s^2 - t^2$~~

Direct: $xyz = 2st(s^2 - t^2)(s^2 + t^2)$

$= 2st(s^4 - t^4)$

$\gcd(5, s) = \gcd(5, t) = 1 \Rightarrow$ $s^4 \equiv 1 \pmod 5$
$t^4 \equiv 1 \pmod 5$

$xyz \equiv 0 \pmod 5$

$\therefore$ $5 \mid xyz$

---

#7 $3n, 4n, 5n$ are the only triples whose terms are in arithmetic progression.

$x - d$
$x$
$x + d$

$(x-d)^2 + x^2 = (x+d)^2$

$\Rightarrow$ $x = 4d$

$(3d, 4d, 5d)$

$(-1, 0, 1)$
What about that? *

* The definition in our text doesn't exclude these triples, but they're obviously not very interesting....

$$(-a)^2 + (0)^2 = (a)^2$$