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.

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).

Lemma 1:

One of x + y is odd, one even;
if x + y are part of a primtive triple.

Assume not;

They can't both be even; otherwise 2
would be even or we could divide them

all by 2.

They must both be odd:

$$\left.\begin{aligned} x &= 2m+1 \\ y &= 2n+1 \end{aligned}\right\} \text{ for integers } m \text{ and } n.$$

$$\begin{aligned} x^2+y^2 &= (2m+1)^2 + (2n+1)^2 \\ &= 4(m^2+n^2) + 4(m+n) + 2 \qquad (\text{even}) \end{aligned}$$

So z^2 is even: $2 \mid z^2 \Rightarrow 2 \mid z$, so

z is even: $2v = z$

$$\begin{aligned} x^2+y^2 &= 2\left[2(m^2+n^2) + 2(m+n) + 1\right] \\ &= 2^2 v^2 \end{aligned}$$

Dividing by 2, we have

$$2v^2 = \underbrace{\left[2(m^2+n^2) + 2(m+n) + 1\right]}_{\text{odd!}}$$

Contradiction: $2 \neq$ odd, so one of $x+y$ is odd, the other even ($\Leftarrow$ z is odd!).

Lemma 2: If $ab = c^n$ and $\gcd(a,b) = 1$, then $a = a_1^n$ and $b = b_1^n$ for some integers a_1 and b_1

Proof (using symmetry):

Let $a = p_1^{k_1} \cdots p_r^{k_r}$, $c = c_1^{l_1} \cdots c_s^{l_s}$ } be the prime factorizations

Then

$$p_1^{k_1} \cdots p_r^{k_r} b = (c_1^{l_1} \cdots c_s^{l_s})^n$$
$$= c_1^{nl_1} \cdots c_s^{nl_s}$$

So $p_i = c_j$ for some j, by Corollary 2 and $p_i \nmid b$, since $\gcd(a, b) = 1$. [41]

Furthermore

$$p_i^{k_i} = c_j^{nl_j} = p_i^{nl_j} = (p^{l_j})^n$$

(since prime powers have to match). So

$$a = p_1^{k_1} \cdots p_r^{k_r} = (p^{k_1/n})^n \cdots (p^{k_r/n})^n$$
$$= [\underbrace{p_1^{k_1/n} \cdots p_r^{k_r/n}}_{a_1}]^n$$

(since every k_i is divisible by n).

By symmetry $b = b_1^n$ for some integer b_1.

Proof of 11.1 (treat it as an if and only if proof):

$\Rightarrow$

(1) $y+z$ are both odd; y is odd by lemma 1, & z is odd because $\gcd(x,y,z)=1$, so $2 \nmid z$.

(2) $z-y$ and $z+y$ are both even, as the sum or difference of odds; hence

$$\left.\begin{aligned} z-y &= 2u \\ z+y &= 2v \end{aligned}\right\} \text{ for some } u, v$$

(3) Rewrite $x^2+y^2=z^2$ as

$$x^2 = z^2 - y^2 = (z-y)(z+y)$$
$$= 2u \cdot 2v = 2^2 uv$$

or

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

(4) Invoke Lemma 2: if $\gcd(u,v)=1$, then $u+v$ are perfect squares by Lemma 2.

Suppose $u+v$ aren't relatively prime, so that $d = \gcd(u,v) \neq 1$.

By definition

$$z-y = 2u$$
$$z+y = 2v$$

so

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

So $d \mid z$ + $d \mid y$; but $\gcd(z,y)=1$, so Contradiction! $\gcd(u,v)=1$

Hence u + v are perfect squares.

Let $u = t^2$ and $v = s^2$.

(5) Conclusion:

$$z = u + v = s^2 + t^2$$
$$y = v - u = s^2 - t^2 \quad (\Rightarrow s > t)$$

and

$$x^2 = 4uv = 2^2 \cdot t^2 \cdot s^2 = (2st)^2, \text{ so}$$

$$x = 2st.$$

(6) Let's check that $\gcd(s,t) = 1$. Suppose not:

$$\gcd(s,t) = d \neq 1.$$

Then $d \mid z$ and $d \mid y$ (in fact, $d^2 \mid z + y$!);
contradiction, as $\gcd(z,y) = 1$.

(7) Let's check that $s \not\equiv t \pmod 2$.

They can't both be even, or they wouldn't be relatively prime. Are they both odd? Then y would be even, as the difference of odds. But y is odd! Contradiction.

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

$\Leftarrow$ We've got $s > t$, $s > t > 0$, $s \not\equiv t \pmod 2$.

(1) Check that

$$x = 2st > 0, \quad 2 \mid x$$
$$y = s^2 - t^2 > 0$$
$$z = s^2 + t^2 > 0$$

yields a Pythagorean triple!

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

$$4s^2t^2 + s^4 - 2s^2t^2 + t^4 =$$

$$s^4 + 2s^2t^2 + t^4 =$$

$$(s^2+t^2)^2 \quad \checkmark$$

(2) Check that $\gcd(x,y,z) = 1$. Suppose not:

$\gcd(x,y,z) = d \neq 1$,

& d has a prime divisor p.

a) $p \neq 2$, since $p \nmid \underbrace{s^2+t^2}_{\text{odd}} = z^2$, so $p \nmid z$.

b) If $p \mid y$ and $p \mid z$, then

$p \mid z-y$ and $p \mid z+y$, so

$p \mid 2t^2$ and $p \mid 2s^2$.

Therefore $p \mid t^2$ and $p \mid s^2 \Rightarrow$

$p \mid t$ and $p \mid s$; but $\gcd(t,s)=1$.

Contradiction.

Q.E.D.

#4 Prove that in Pyth. triple (x,y,z)

$12 \mid xy$ and $60 \mid xyz$.

We certainly know that $2 \mid x$ (WLOG).

$x = 2st$

one is even, hence $4 \mid x$.

Assume $3 \nmid x$ and $3 \nmid y$.

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

$3 \nmid s$ & $3 \nmid t$, since $3 \nmid x$.

Fermat's Little Theorem: $x^2 \equiv 1 \pmod 3$
$y^2 \equiv 1 \pmod 3$
$s^2 \equiv 1 \pmod 3$
$t^2 \equiv 1 \pmod 3$

$$s^2 - t^2 \equiv 1 - 1 \equiv 0 \pmod 3$$
$$\not\equiv 1 \pmod 3$$

Contradiction!

One of x & y must be divisible by 3.

So $4 \mid x$ and $3 \mid x$ or y, so

$$12 \mid x \cdot y$$

Show that $5 \mid x$ or y or z.

If $\gcd(a,5) = 1$, then $a^4 \equiv 1 \pmod 5$.

$a^2 \equiv \underline{1 \text{ or } 4} \pmod 5$

Suppose x & y are relatively prime to 5:

$$x^2 + y^2 \equiv z^2 \equiv 0, 2, 3 \pmod 5$$

So z is not relatively prime to 5.

Hence they can't all be relatively prime to 5:

$$5 \mid xyz.$$

$\therefore \quad 60 = 12.5 \mid xyz.$

#7 $\quad (\underbrace{x-d}_{y},\ x,\ \underbrace{x+d}_{z})$

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

$$x^2 - 2xd + \cancel{d^2} + \cancel{x^2} = \cancel{x^2} + 2xd + \cancel{d^2}$$

$$x^2 = 4xd$$

$$x = 4d$$

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