International Journal of Interdisciplinary Research in Arts and Humanities (IJIRAH)
Impact Factor: 4.675, ISSN (Online): 2456 - 3145
(www.dvpublication.com) Volume I, Issue I, 2016

A STUDY ON PYTHAGOREAN TRIPLES

A. Dinesh Kumar* & M. Vasuki**
* Head & Assistant Professor, Department of Science and Humanities, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu
** Assistant Professor, Department of Mathematics, Srinivasan College of Arts and Science, Perambalur, Tamilnadu

Cite This Article: A. Dinesh Kumar & M. Vasuki, "A Study on Pythagorean Triples", International Journal of Interdisciplinary Research in Arts and Humanities, Page Number 14-21, Volume 1, Issue 1, 2016.

Introduction:

The Pythagorean numbers play a significant role in the theory of higher arithmetic as they come in the majority of indeterminate problem. For the discovery of the law of the three squares (Pythagorean equation), really, one should be indebted to the Pythagorean who were the first Greeks with great intellectual perception. One may notice to his surprise that the Egyptians, the Chinese, the Babylonians and the Indians knew some knowledge of the property of right angled Pythagorean triangles or Pythagorean numbers .Since there is a 1−1 correspondence between Pythagorean numbers and Pythagorean triangles, we shall use them interchangeably. The only geometrical theorem with which the ancient Chinese were acquainted is that the area of the square described on the hypotenuse of a right angled triangle is equal to the sum of the areas of the squares described on the sides. A Pythagorean triangle is a right triangle whose sides are integral lengths.

Pythagorean Triples: Let(x,y,z) denote 3-tuple where x ,y and z are integer. (x,y,z) is a Pythagorean triple≡(1) x,y and z are positive. (2) $x^2+y^2=z^2$

Primitive Pythagorean Triple: Let(x,y,z)denote a 3-tuple where x,y,z and z are integers.(x,y,z) is a primitive Pythagorean triple Ξ (1)(x,y,z) is a Pythagorean triple. (2) GCD(x,y,z)=1.

Theorem 1:

If(x,y,z) is a Pythagorean triple such that GCD(x,y)=1 then(x,y,z)is a primitive Pythagorean triple.

Proof:

Without loss of generality,let us assume that, There exists a prime p such that p/x and p/z Then $p/(z^2-x^{2)}=y^2$ ⇨p/y^2 . Hence p/y, Where contradicts GCD(x,y)=1. ∴(x,y,z) is a primitive Pythagorean triple.

Theorem 2:

If(x,y,z) is a Pythagorean triple then there exists a primitive Pythagorean triple(a,b,c)and there exists an integer k≥1 such that(x,y,z)=(ka,kb,kc)

Proof:

Let k=GCD (x,y,z) and let a =x/k → (1)
b=y/k →(2)
and c=z/k →(3)

Then GCD (a,b,c)=1. Next T.P.T (a,b,c) is a Pythagorean triple. Square (1) & (2) and add $a^2+b^2=x^2/k^2+y^2/k^2$

$$= \frac{x^2+y^2}{k^2}$$

$=z^2/k^2$ ($\because x^2+y^2=z^2$)

$a^2+b^2=c^2$ (from (3))

∴ (a, b, c) is a Pythagorean triple. Thus (a,b,c) is a primitive Pythagorean triple.

Theorem 3:

If(x,y,z) is a primitive Pythagorean triple then exactly one of x and y is even and z must be odd.

Proof:

x and y cannot both be even . Since GCD(x,y)=1. Suppose that x and y are both odd. where x=2j+1} and y=2k+1→ (4).

Then, $x^2+y^2=z^2$. sub (2.4) in above equation, we get, $(2j+1)^2+(2k+1)^2=z^2$

$(4j^2+4j+1)+(4k^2+4k+1)=z^2$ →(5)

$4(j^2+j+k^2+k)+2=z^2$

Equation (5) implies z^2 is even. ∴z must be even. Assume that z=2m sub in (5)

$4(j^2+j+k^2+k)+2=4m^2$

Now 4 divides the R.H.S of this equation, but 4 does not divide the L.H.S. Which is contradiction to our assumption? One of these values must be even, and since GCD (x, y)=1, the other value must be odd. Thus exactly one of x and y is even, z must be odd.

Corollary 1:

Every Pythagorean triple consists of 2 odd integers and 1 even integers or else consists of 3 even integers.

Proof:

Let x and y are both odd. where x=2j+1 and y=2k+1 →(6)

Then, $x^2+y^2=z^2$, Substitution of (6) in above equations implies $(2j+1)^2+(2k+1)^2=z^2$

$$(4j^2+4j+1)+(4k^2+4k+1)=z^2$$
$$4(j^2+j+k^2+k)+2=z^2$$

This last equation implies z^2 is even. So z must be even. ∴Every Pythagorean triple consists of 2 odd integers and 1 even integer.

Convention:

If (x,y,z) denotes a Pythagorean triple ,then x will always denote an even integer.

Theorem 5:

If (x,y,z) is a primitive Pythagorean triple then there exists an integer k such that x=4k.

Proof:

By theorem 3 and convention, Let x=2r, y=2, s+1 and z=2t+1 Then, $x^2=z^2-y^2$

$$(2r)^2=(2t+1)^2-(2s+1)^2$$
$$4r^2=4t^2+4t+1-(4s^2+4s+1)$$
$$4r^2=4(t^2+t-s^2-s)$$
$$r^2=t(t+1)-s(s+1)$$

∴r^2 is the difference between two even integers. Hence r^2 must be even. ∴ r must be even. Assume r-2k Then x=2r =2.2k =4k

Theorem 6:

If $0 < n < m$ then (2mn, m2-n^2, m^2+n^2) is a Pythagorean triple.

Proof:

Take x = 2mn, y = m^2-n^2 and z = m^2+n^2

T.P.T: $(2mn)^2+(m^2-n^2)^2=(m^2+n^2)^2$ Let $x^2+y^2=z^2$, Substitute the value of x and y in above equation

$$(2mn)^2+(m^2-n^2)^2 = 4m^2n^2+m^4-2mn^2+n^4 = m^4+2m^2n^2+n^4 = (m^2+n^2)^2$$

(2mn, m^2-n^2, m^2+n^2) is a Pythagorean triple

Corollary 2:

If 0<n<m and GCD (2mn, m^2-n^2) =1 then (2mn, m^2-n^2, m^2+n^2) is a primitive Pythagorean triple.

Proof:

By the Theorem 6, (2mn, m^2-n^2, m^2+n^2) is a Pythagorean triple. By Theorem 1, If (2mn, m^2-n^2, m^2+n^2) is a Pythagorean triple such that GCD (2mn, m^2-n^2) = 1. Then (2mn, m^2-n^2, m^2+n^2) is a primitive Pythagorean triple.

Theorem 7:

If (x, y, z) is a primitive Pythagorean triple then there exists integers m and n such that x=2mn, y= m^2-n^2, and z= m2+n^2

Proof:

By theorem 3 and convention, Let x=2k, y=2s+1 and z=2t+1

$$x^2=z^2-y^2$$
$$4k^2=(z+y).(z-y)$$
$$K^2=z+\frac{z+y}{2}.\frac{z-y}{2}=\frac{(2t+1)+(2s+1)}{2}.\frac{(2t+1)-(2s+1)}{2}=\frac{2t+2s+2}{2}.\frac{2t-2s}{2}=\frac{2(t+s+1)}{2}.\frac{2(t-s)}{2}$$
$$= (t+s+1).(t-s) \quad \rightarrow (7)$$

Claim: (t+s+1) and (t-s) have no common factor. For if there exists an integer r>1 such that

$$(t+s+1) = r.p \text{ and } (t-s) = r.q$$

Then r(p-q) = rp - rq = t+s+1-t+s = 2s+1= y

r (p+q) = rp+rq= t+s+1+t-s= 2t+1= z

Which shows is a common factor of x and z, an impossibility. Since (t+s+1) and (t-s) have no common factor. Yet their product is a perfect square, each must be a perfect square.

Let m = $\sqrt{t+s+1}$ and n = $\sqrt{t-s}$ Then $m^2+n^2=(t+s+1)+(t-s)=2t+1=z$

$m^2-n^2=t+s+1-t+s=2s+1=y$

$2mn = 2\sqrt{t+s+1}\sqrt{t-s} = 2(t+s+1)(t-s)1/2 = 2[k]1/2$ (by 7)

$= 2k = x$

Thus x = 2mn. y = m^2-n^2 and z = m^2+n^2

Theorem 8:

If (x,y,z) is a Pythagorean triple, then there exists integers k,m and n such that(2mn, m^2-n^2,m^2+n^2) is a primitive Pythagorean triple. Moreover,(x,y,z)=[k(2mn),k(m^2-n^2),k(m^2+n^2)]

Proof:

T.P.T: (2mn, m^2-n^2,m^2+n^2) is a primitive Pythagorean triple. Let k = GCD(x,y,z)

Let $2mn = x/k \quad \rightarrow (8)$

$m^2-n^2 = y/k \quad \rightarrow (9)$

and $m^2+n^2 = z/k \quad \rightarrow (10)$

Then GCD (2mn, m^2-n^2,m^2+n^2) =1. Next T.P.T (2mn, m^2-n^2,m^2+n^2) is a primitive Pythagorean triple.

Squaring and adding x (8) and (9).

$$4m^2n^2 + (m^2-n^2)^2 = \frac{x^2}{k^2} + \frac{y^2}{k^2} = \frac{x^2+y^2}{k^2} = \frac{z^2}{k^2} = (m^2+n^2)^2$$

∴ (2mn, m^2-n^2, m^2+n^2) is a Pythagorean triple. Thus (2mn, m^2-n^2, m^2+n^2) is a primitive Pythagorean triple.

Let x = k (2k), y = k (2s+1) and z = k (2t+1)

T.P.T: (x, y, z) = [k(2mn),k(m^2-n^2,m^2+n^2)]

$$X^2 = z^2-y^2$$

$$4k^4 = (z + y).(z-y)$$

$$k^4 = \frac{z+y}{2} \cdot \frac{z-y}{2} = \frac{k(2t+1)+k(2s+1)}{2} \cdot \frac{k(2t+1)-k(2s+1)}{2}$$

$$= \frac{2kt+k+2ks+k}{2} \cdot \frac{2kt+1-2ks-1}{2} = \frac{2k(t+s)+2k}{2} \cdot \frac{2k(t-s)}{2}$$

$$k4 = k (t+s+1).\ k(t-s)$$

Claim: k(t+s+1) and k(t-s) have no common factor. For if there exists an integer r >1 such that

$$k (t+s+1) = r.p \text{ and } k(t-s) = r.q$$

Then r.(p-q) = r.p - r.q = k (t + s + 1) – k (t-s) = tk + ks + k – kt + ks = k(2s+1) = y

r.(p+q) = r.p + r.q = kt + ks + k + kt – ks = k (2t+1) = z

Which shows r is a common factor of y and z an impossibility. Since k(t+s+1) and k(t-s) have no common factor Yet their product is a perfect square ,each must be a perfect square.

Let $m\sqrt{k} = \sqrt{k}$ (t+s+1) and $n\sqrt{k} = \sqrt{k}$ (t-s) Then k[m^2+n^2] = kt + ks + k + kt - ks= k(2t+1) = z

k[m^2-n^2] = kt + ks + k – kt + sks = k (2s+1) = y

k[2mn] = 2[k(t+s+1)k (t-s)]1/2 = 2[k^4]1/2 = $2k^2$ = x

∴ (x,y,z) = [k (2mn), k (m^2-n^2), k (m^2+n^2)]

Sums of Squares:

A Pythagorean triple (x,y,z) is a triple of positive integers satisfying $x^2+y^2=z^2$. If g = gcd(x,y,z) then (x/g,y/g,z/g) is also a Pythagorean triple. It follows that if g>1,(x,y,z) can be obtained from the "smaller" Pythagorean triple (x/g,y/g,z/g) by multiplying each entry by g. It is natural then to focus on Pythagorean triples(x,y,z) with gcd(x,y,z)=1 these are called primitive Pythagorean triples.

Theorem 9:

Let (x,y,z) be a primitive Pythagorean triple. Then gcd(x,y) = gcd (x,z) = gcd (y,z) = 1.

Proof:

T.P.T: gcd (x,y) =1, suppose gcd (x,y) >1 Then there is a prime p with p/x and p/y. Then $z^2= x^2+y^2 \equiv 0(\text{mod } p)$, As p/z^2 then p/z

∴ p/gcd (x,y,z), Which is a contradicting (x,y,z) being a primitive Pythagorean triple. Thus gcd (x,y) =1

T.P.T: gcd (x,z) =1, Suppose that gcd (x,z)>1, Then there is a prime p with p/x and p/z. Then $y^2=z^2-x^2\equiv 0(\text{mod } p)$

As p/y^2 then p/y, ∴ p/gcd(x,y,z), which is a contradicting(x,y,z) being a primitive Pythagorean triple. Thus gcd (x,z) =1.

T.P.T: gcd(y,z) =1, Suppose that gcd (y,z) >1, Then there is a prime p with p/y and p/z. Then $x^2= z^2-y^2 \equiv 0(\text{mod } p)$, As p/x^2 then p/x

∴ p/gcd(x,y,z), which is a contradicting (x,y,z) being a primitive Pythagorean triple. Thus gcd(y,z)=1.

Theorem 10:

Let (x,y,z) be a primitive Pythagorean triples with x odd. Then there are r,s∈N with r > s,gcd (r,s) =1 and r + s odd, such that $x=r^2-s^2$,y =2rs and $z = r^2+s^2$. Conversely, if r,s∈N with r>s, gcd(r,s) =1 and r + s odd, then ($r2-s^2$,2rs,r^2+s^2) is a primitive Pythagorean triple.

Part I: Given: Let (x,y,z) be a primitive a Pythagorean triples with x odd.

T.P.T: There are r,s ∈N with r > s ,gcd (r,s) =1 and r + s odd such that $x = r^2 – s^2$, y = 2rs, and $z = r^2+s^2$

Proof:

If x is odd, then y is even and z is odd. Let $a = \frac{z-x}{2}$, $b = \frac{z-x}{2}$ and $c = \frac{y}{2}$

Then a,b,c∈N, Also ,ab $= \frac{(z-x)(z+x)}{4} = \frac{z^2-x^2}{4} = \frac{y^2}{4} = c^2$

Let g = gcd (a,b). Then g/(a+b) and g/(b-a), (ie) g/z and g/x. As gcd (x,z), Then g =1 (ie) gcd(a,b) =1

Let p be a prime factor of a. Then p ∤ b,sov_p (b) = 0. Hence, $v_p(a) = v_p(a) + v_p(b) = v_p(ab) = v_p(c^2)$

$v_p(a) = 2v_p(c)$ is even. Then a is a square. Similarly b is a square. write $a = s^2$ and $b = r^2$ where r,s∈N. Then gcd (r,s)/a and gcd(r,s)/b as a and b are coprime, gcd(r,s) =1. Now,x = b-a = r^2-s^2

∴ r >s, Also, z = a +b = $r^2+ s^2$

As $c^2= ab$, $= {}^{r2s2}c = rs$ and ∴ y = 2rs. Finally as x is odd. Then 1 ≡ x = $r^2+s^2\equiv$ r + s. (ie) r + s is odd.

Part II: Given: Ifr,s∈N with r >s,gcd(r,s) =1 and r + s odd.
T.P.T: $(r^2-s^2, r^2+s^2, 2rs)$ is a primitive Pythagorean triple.

Proof:

Let $x = r^2- s^2$, $y = 2rs$, and $z = r^2+s^2$, Certainly $y,z \in N$ and also $x \in N$ as $r > s > 0$.

Also, $x^2+y^2 = (r^2-s^2)^2+(2rs)^2 = r^4- 2r^2 s^2 + s^4+4s r^2= r4+^{2r2s2}+s^4 = r^2+s^2=z^2$.

Hence(x,y,z) is a Pythagorean triple. Certainly y is even. $x = r^2-s^2 \equiv r - s \equiv r + s \pmod 2$, x is odd.
T.S.T: (x,y,z) is a primitive Pythagorean triple. Examine g = gcd(x,z)., As x is odd ,g is odd. Also $g/(x^2+z^2)$ and $g/(z^2-x^2)$ (ie) $g/2s^2$ and $g/2r^2$

As r and s are coprime. Then gcd $(2r^2,2s^2) = 2$, ∴ g/2

As g is odd g =1. Hence (x,y,z) is primitive Pythagorean triple.

Sums of Squares:

For k∈N, let $S_k=\{a_1^2+\ldots.+a_k^2 : a_1,\ldots.,a_k \in z\}$ be the set of sums of k squares. Note that zero is allowed. For example $1=1^2+0^2 \in S_2$.The sets S_2 and S_4 are closed under multiplication.

Theorem 11:

If $m,n \in S_2$ then $mn \in S_2$ & If $m,n \in S_4$ then $mn \in S_4$

Proof:

Let $m,n \in S_2$, Then $m=a^2+b^2$ and $n=r^2+s^2$ where a,b,r,s∈Z, By the two-square formula, $(a^2+b^2)(r^2+s^2) = (ar-bs)^2 + (as+br)^2$, it is immediate that $mn \in S_2$.

Let $m,n \in S_4$, Then $m=a^2+b^2+c^2+d^2$ and $n=r^2+s^2+t^2+u^2$ where a,b,c,d,r,s,t,u∈Z
By the four-square formula, $(a^2+b^2+c^2+d^2 (r^2+s^2+t^2+u^2) = (ar-bs-ct-du)^2 + (as+br+cu-dt)^2 + (at-bu+cr+ds)^2 + (au+bt-cs+dr)^2$,
it is immediate that $mn \in S_4$.

Remark: The two-square theorem comes from complex no: $(a^2+b^2)(c^2+d^2)= |a+ib|^2 |c+id|^2= |(a+ib)(c+id)|^2$
$= |(ac-bd)+(ad+bc)^2 = (ac-bd)+(ad+bc)^2$

Restrict the possible factorizations of a sum of two squares. If p is prime, and n is an integer, then vp(n) denotes the exponent of the largest power of p dividing n:p $vp(n) | n$ but $p^{v_p(n)|n \text{ but }} p^{v_p(n)+1}$**n**

Theorem 12:

Let p be a prime with p≡3(mod 4) and let n∈N. If $n \in S_2$ then $v_p(n)$ is even.

Proof:

Let $n=a^2+b^2$ with a,b∈Z, Suppose p/n, T.S.T: p/a and p/b. Suppose p/a. Then there is c∈Z with ac≡1(mod p). Then $0 \equiv c^2 n = c^2(a^2+b^2) = (ac)^2+(bc)^2 \equiv 1+(bc)^2 \pmod p$ ⇨ [-1/p]=1

But [-1/p]=1 when p≡3(mod 4), which is a contradiction. ∴ p/a

Similarly p/b, Thus $p^2/(a^2+b^2) = n$ and $n/p^2 = (a/p)^2 + (b/p)^2 \in S_2$ .Let $n \in S_2$and $k = v_p(n)$, If k > 0,then k ≥ 2 and $n/p^2 \in S_2$. Note that $v_p(n/p^2) = k - 2$, Similarly, if k-2>0(ie) if k>2), Then k-2≥2((ie)k≥4) and $n/p4 \in S_2$, Iterating this argument, find that if k = 2r+1 is odd. Then $n/p^{2r} \in S_2$ and $v(n/p^{2r}) = 1$, which is a contradiction. ∴ k is even. Hence $v_p(n)$ is even.

Remark: If n∈N, write $n= rm^2$ where m^2 is the largest square dividing n and r is square free,(ie) either r=1 (or) r is a product of distinct primes.

Theorem 13:

Let p be a prime with p≡1(mod 4). Then p∈S_2

Proof:

If p ≡ 1(mod 4), Then (-1/p) = 1, ∴ there is u∈Z with $u^2 \equiv -1 \pmod p$. Let $A = \{(m_1,m_2)/m_1,m_2 \in Z, 0 \le m_1,m_2 < \sqrt{p}\}$. Then A has $(1+s)^2$elements, where is the integer part of $\sqrt{p}$ (i.,e) $s \le \sqrt{p} < s + 1$

Hence |A|>p. Form $m=(m_1,m_2) \in R^2$, Define $\phi(m)=um_1+m_2$, Then ϕ is a linear map from R^2 to R. If $m \in Z^2$,then $\phi(m) \in Z$. As |A|>p, the ϕ (m) for m ∈ A cannot all be distinct modulo p. Hence there are distinct m,n∈A with $\phi(m) \equiv \phi(n) \pmod p$. Let α = m-n. Then $\phi(\alpha)=\phi(m)-\phi(n) \equiv 0 \pmod p$. Let α=(a,b), Then $a=m_1-n_1$ where $0 \le m_1,n_1 < \sqrt{p}$, ∴ $|a| < \sqrt{p}$, Similarly |b| $< \sqrt{p}$, Then $a^2+b^2 < 2p$.

As m≠n then α≠(0,0), ∴ $a^2+b^2>0$, But $0 \equiv \phi(\alpha) = ua + b \pmod p$, Hence $b \equiv -ua \pmod p$, ∴ $a^2+b^2 \equiv a^2 + (-ua)^2 \equiv a^2(1+u^2) \equiv 0 \pmod p$. ∴ a^2+b^2 is a multiple of p and $0<a^2+b^2<2p$, Then $a^2+b^2 =p$, ∴ p∈S_2

Theorem 14:

Let n∈N then n ∈S_2 iff $v_p(n)$ is even whenever p is a prime congruent to 3 modulo 4.

Proof:

Given: n∈S_2, To Prove that: $v_p(n)$ is even whenever p is a prime congruent to 3 modulo 4. If n∈S_2, p is prime p≡3(mod 4). Then $v_p(n)$ is even. Given: $v_p(n)$ is even whenever p is a primer congruent to 3modulo 4.

T.P.T: $n \in S_2$,If $v_p(n)$ is even ,then $p=rm^2$ where each prime factor p of r is either2(or) congruent to 1 modulo 4. By theorem 2.2.3,all such p lie in S_2. Hence $r \in S_2$. Hence $r = a2+b^2$ where $a,b \in Z$, $\therefore n = rm^2 = (am)^2+(bm)^2 \in S_2$

Theorem 15:

Let p be a prime .Then $p \in S_4$.

Proof:

If $p \equiv 1 \pmod 4$,then there are $a,b \in Z$ with $p = a^2+b^2+0^2+0^2$ so that $p \in S_4$ Also, $2=1^2+1^2+0^2+0^2 \in S_4$ and $3=1^2+1^2+1^2+0^2 \in S_4$, Assume that p>3 and that $p \equiv 3 \pmod 4$. As a consequence [-1/p]=-1, Let W be the smallest positive integer with [W/p]=-1 Then[W-1/p]=1 and [-W/p]=[-1/p][W/p]=1, Hence there are $u,v \in Z$ with $w\text{-}1 \equiv u^2 \pmod p$ and $-w \equiv v^2 \pmod p$. Then $1+ u^2 + v^2 \equiv 1 +(w\text{-}1) -w \equiv 0 \pmod p$.

Let $B=\{(m_1,m_2,m_3,m_4)/m_1,\ldots\ldots..,m_4 \in Z, 0 \le m_1,\ldots\ldots\ldots,m_4 < \sqrt{p}\}$ Then B has $(1+S)^4$elements ,where S is the integer part of $\sqrt{p}$ (i.e) $S \le \sqrt{p} < S+1$. Hence $|A| > p^2$, For $m = (m_1,nm_2,m_3,m_4)$. Define $\psi(m) = (um_1+vm_2+m_3\text{-}vm_1+um_2+m_4)$. Then ψ is a linear map from R^4 to R^2. If $m \in Z^4$ then $\psi(m) \in Z^2$, Write $(a,b) \equiv (a',b') \pmod p$. If $a \equiv a' \pmod p$ and $b \equiv b' \pmod p$. If a list$(a_1,b_1),\ldots,(a_N,b_N)$ of vectors in z^2 with $N > p^2$, Then there must be some i and j with$(a_i,b_i) \equiv (a_j,b_j) \pmod p$. This happens for the vectors $\psi(m)$ with $m \in B$. As $|B| > p^2$. There are distinct $m,n \in B$ with $\psi(m) \equiv \psi(n) \pmod p$. Let $\alpha = m\text{-}n$, Then $\psi(\alpha) = \psi(m)\text{-}\psi(n) \equiv 0 \pmod p$.

Let $\alpha=(a, b, c, d)$ then $a = m_1\text{-}n_1$, where $0 \le m_1,n_1 < \sqrt{p}$ $\therefore |a| < \sqrt{p}$, Similarly $|b|, |c|, |d| < \sqrt{p}$ then $a^2 + b^2 + c^2+ d^2 < 4p$, As $m \neq n$ then $\alpha \neq (0,0,0,0)$. $\therefore a^2+b^2+c^2+d^2 > 0$. Now $(0,0) \equiv \phi(\alpha)= (ua+ vb + c,- va+ub + d) \pmod p$. Hence $c \equiv - ua + vb \pmod p$ and $d \equiv va\text{-}ub \pmod p$. Then $a^2+b^2+c^2+d^2 \equiv a^2+b^2+ (- ua +vb)^2 + (va\text{-}ub)^2$

$= a^2+b^2+u^2a2+v^2b^2+2uvab+v^2a^2+u^2b^2\text{-}2uvab = (1+u^2+v^2)(a^2+b^2) \equiv 0 \pmod p$

As is a multiple of p and $0 < a^2+b^2+c^2+d^2 < 4p$ then $a^2+b^2+c^2+d^2 \in \{p,2p,3p\}$. when $a^2+b^2+c^2+d^2 = p$ then certainly $p \in S_4$. To consider the bother some cases where $a^2+b^2+c^2+d^2 = 2p$(or)3p. Suppose that $a^2+b^2+c^2+d^2 = 2p$.

Then $a^2+b^2+c^2+d^2 \equiv 2 \pmod 4$ $\therefore$ two of a, b, c, d are odd and other two even. Without loss of generality a and b are odd and c and d are even. then $\frac{1}{2}(a+b), \frac{1}{2}(a-b), \frac{1}{2}(c+d)$ *and* $\frac{1}{2}(c-d)$ are all integers. A simple computation gives $\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{a^2+b^2+2ab+a^2+b^2-2ab}{4} + \frac{c^2+d^2+2cd+c^2+d^2-2cd}{4}$

$= \frac{a^2+b^2+c^2+d^2}{2} = p \cdot \therefore p \in S_4$

Finally, suppose that $a^2+b^2+c^2+d^2 = 3p$. Then a2+b2+c2+d2 is a multiple of 3 but not 9. As $a^2 \equiv 0$ (or) $1 \pmod 3$ then either exactly one (or) all four of a, b, c and d are multiples of 3. But the latter case is impossible. (For then $a^2+b^2+c^2+d^2$ would be a multiple of 9). $\therefore$ without loss of generality 3/a and b, c, $d \equiv \pm 1 \pmod 3$. By replacing b by - b etc. If necessary, let us assume that $B \equiv c \equiv d \equiv 1 \pmod 3$. Then $\frac{1}{3}(b + c + d)$, $\frac{1}{3}(a + b - c)$, $\frac{1}{3}(a + c - d)$, $\frac{1}{3}$ $(a + d - b)$, Are all integers and a simple computation gives

$\left(\frac{b+c+d}{3}\right)^2 + \left(\frac{a+b-c}{3}\right)^2 + \left(\frac{a+c-d}{3}\right)^2 + \left(\frac{a+d-b}{3}\right)^2 = \frac{b^2+c^2+d^2+2bc++2cd+2bd}{9} + \frac{a^2+b^2+c^2+2ab-2bc-2ca}{9} + \frac{a^2+c^2+d^2+2ac-2cd-2ad}{9}$

$+ \frac{a^2+d^2+b^2+2ad-2bd-2ba}{9} = \frac{3(a^2+b^2+c^2+d^2)}{9} = p$

Units in Integral Group Rings:

Units in Z[D_4]:

In this section, we discuss V=V(Z[D_4]), the group of units of augmentation 1 in Z[D_4]. Let D_4 be generated by x, y with $X^2 = y^4 = c$ and $xyx = y^3$. Let $u \in Z[D_4]$ with $u = (a + by + cy^2 + dy3^3)+(e + fy + gy2^2+ hy^3)$ x, $u=\alpha+\beta x$. Since $\{c, y2\} - Z(D_4)$, the center of D_4. There is a ring homomorphism. λ: Z $[D_4] \to Z[D_4] / Z[Z(D_4)] \cong Z[C_2 \times C_2]$. Given by $\lambda(u) = (a + c) + (b + d) Y + (e + g) X + (f +h) XY$. Where X,Y are the images of x, y in the factor group $D_4/Z(D_4)=C_2xC_2$. Since $Z[C_2xC_2]$ has only trivial units, then have four possible cases for units with augmentation 1,namely one of a + c, b + d, e + g, f + h is 1 and the remaining 3 sums are 0.

Denote the subsets of these units in V by V_i with $1 \le i \le 4$ respectively. Note that y^2 $v^i=V_i$ for all I and also $V_2=yV_1=V_1y$; $V_3=xV_1=V_1x$; $V_4=yxV_1=V_1y$. Thus these sets are in Bijective correspondence. $\therefore$ Up to multiplication with a trivial unit. Assume that elements of V lie in V_1, (ie) $a + c = 1$ & $b + d = e + g = f + h = 0$. For $u \in V$, it follows directly from above equation that $u \in V_1$ iff $u=1+\gamma(1\text{-}y^2)$, γ=-c+by+ex+fyx. Now let $u=\alpha+\beta x \in V_1$. $\alpha\bar{\alpha} - \beta\bar{\beta}$is a unit in Z[$C_4$] fixed by the action of x. Since Z[C_4] has only trivial units, $\alpha\bar{\alpha} - \beta\bar{\beta} = \pm 1$ (or) $\pm y^2$. By (3.4), $\alpha\bar{\alpha} - \beta\bar{\beta} = (1+2\delta) - (2\delta)\, y^2$. Where $\delta = b^2+c^2\text{-}e^2\text{-}f^2\text{-}c$. Since δ is an integer, we must have that $\delta=0$, (ie) $\alpha\bar{\alpha} - \beta\bar{\beta} = \det(\phi(u)=1)$ and $e^2+f^2\text{-}b^2=c(c-1) = - ac \to (3.5)$

Remark: $\phi(y) = \begin{pmatrix} y & 0 \\ 0 & y^3 \end{pmatrix}$ and $\phi(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Thus for $u \in V_1 \cup V_2$, $\det(\phi(u))=1$ and $V_1 \cup V_2$ is a normal subgroup of V of index 2.

Similarly, det (ϕ(u) for u in V3 (or) V_4 is -1. Since, - ac ≥ 0, (3.5) shows that all units in V_1 lie on a surface, $X^2+Y^2-Z^2$ = -ac. which is a hyperboloid of one sheet if ac≠0 and a cone if ac=0. Let H_k denote the set of integer points on the hyperboloid $X^2+Y^2=Z^2+k$. Let H_n denote the units with c=n on $H_{n(n-1)}$. A point (e, f, b) in H_c is identified with the unit $u=1+\gamma(1-y^2)$ with γ=-c+ by + ex + fyx as in above equation. Given any value of c, H_c is non empty. Since c(1-c)=2mn for integers m, n then b = m + n, c = m & f = n. Then we may identify V_1 with $\cup_{c\in Z} H_c$, (ie) V_1 is identified with the set of two copies of each hyperboloid $H_{n(n-1)}$. One copy of $H_{n(n-1)}$ corresponds to the units with c=n and the other to the units with c=1-n. The following remark gives the multiplication for units in V_1.

Remark: Let u = (e, f, b)∈H_c and v = (e′, f′, b′) ∈ $H_{c'}$ then uv = (e″, f″, b″)∈$H_{c''}$ where c″=c+c′+2bb′-2cc′-2ee′-2ff′=(b + b′)²+(c - c′) ² - (e + e′)²- (f + f′)²; b″=(1-2c′)b+(1-2c)b′+2fe′-2ef′; e″=(1-2c′)e+(1-2c)e′+2b′f-2bf′; f″=(1-2c′)f+(1-2c)f′+2be′ – 2eb′;

The multiplication formula may be interpreted as

$$\begin{bmatrix} e'' \\ f'' \\ b'' \end{bmatrix} = (1-2c') \begin{bmatrix} e \\ f \\ b \end{bmatrix} + (1-2c) \begin{bmatrix} e' \\ f' \\ b' \end{bmatrix} + 2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \left(\begin{bmatrix} e \\ f \\ b \end{bmatrix} \times \begin{bmatrix} e' \\ f' \\ b' \end{bmatrix} \right)$$

Thus u, v∈v_1 commute if they represent parallel vectors in Z^3.

Theorem 16:

Let u=(e, f, b)∈H_c and let un=(e_n,f_n,b_n)∈H_{cn}. For n a positive integer,(e_n,f_n,b_n)=α_n(e ,f ,b,) for some integer α_n with α_1=1, α_2 =2(1-2c),etc. Furthermore the sequence $|\alpha_1|, |\alpha_2|$,….. is strictly increasing. For n a positive integer, $c_n=\beta_n c$ for some integer β_n where β_1=1,β_2=4a, etc. If ac≠0, then the sequence $|\beta|, |\beta|$,…… is strictly increasing. If e=0,then e_n=0 for all n.if a=0,c=1 then c_n=0 if n is even, and c_n=1 if n is odd.

Proof:

First show that (e_n, f_n, b_n)=α_n(e, f, b) and $e_n=\beta_n c$ for integers α_n,β_n. The proof is by induction on n. If n=2, then α_2=2(a-c) =2(1-2c). Now suppose that for n=k-1, (e_{k-1},f_{k-1},b_{k-1})=α_{k-1}(e,f,b). Then (e_k,f_k,b_k)=((1-2c_{k-1})+(1-2c)α_{k-1})(e,f,b), Similarly, since c_2=4ac. Again using induction on n, suppose that $c_{k-1}=\beta_{k-1}c$. Then $c_k=c+\beta_{k-1}(1-2c)c+2\alpha_{k-1}ac$, so that, $\beta_k=1+\beta_{k-1}(1-2c)+2a\alpha_{k-1}$. Now suppose that ac≠0, so that |a-c|>1. Note that we have shown that $\alpha_n=1-2\beta_{n-1}c+(1-2c)\alpha_{n-1}$; $\beta_n=1+\beta_{n-1}(1-2c)+2a\alpha_{n-1}$ Next to claim that for n≥2,α_n&β_n have the same sign and $|\alpha_n|>|\alpha_{n-1}|$, $|\beta_n|>|\beta_{n-1}|$, Note that α_1=1, β=1, α_2=2(a-c), β_2 =4a and proceed by induction. Suppose that α_{k-1}andβ_{k-1}hae the same sign. Since -2c,a-c and 2a all have the same sign. Then the summands $2c\beta_{k-1}$,(a-c)α_{k-1},(a-c)β_{k-1},$2a\alpha_{k-1}$ in(3.6),(3,7) have same sign. If these are positive. Then clearly α_k,β_k are positive and greater than $|\alpha_{k-1}|$,$|\beta_{k-1}|$. If the summands are all negative. Then since $|2c\beta_{k-1}|$>1 and $|2a\alpha_{k-1}|$>1. Still have that $|\alpha_k|$,$|\beta_k|$ are greater than $|\alpha_{k-1}|$, $|\beta_{k-1}|$ respectively. Now let ac=0. If c=0, then the multiplication formula immediately yields that α_n=n. c_n=0 for all n. If c=1, then again by Remark 3.1.2 and a simple induction argument, the sequence of$\alpha_n$is 1,-2,3,-4,….. and the sequence of integers c_n is 1,0,1,0,1,……

Theorem 17:

- ✓ The set $V_2=yV_1$ has no units of order 2, but has non –trivial units of order 4. A unit u∈V_2, $u=y^3+\gamma(1-y^2)$ with γ=a + by + ex + fyx is of order 4. iff a=0 and (e, f) is an integer point on the circleX2+Y2=b(b-1).
- ✓ The sets V_3 &V_4 have no units of order 4,but have non-trivial units of order 2.For $u=^{y2x}+\gamma(1-y^2)$ in V_3,γ as above, then u has order 2 iff a=0,and (b,f) is a point on the hyperpola $X^2-Y^2=e^2$-e.For u= y3x+γ(1-y^2) in V_4. γ as above, then u has order 2 iff a=0, and(b,e) is a point on$X^2-Y^2=f^2$-f

Proof:

Let u=α+βx∈V_2. Suppose first that u^2=1. By the theorem ”Let D be the image of Z[G] under ϕ so that the unit group of Z[G] is isomorphic to the group of matrices in D with determinant a unit in Z[H], (ie) ű(Z[G])={$u = \alpha + \frac{\beta x}{\alpha\bar{\alpha}} - \beta\bar{\beta} \in u(Z[H])$}. If u=α+βx∈u(Z[G]) with $\alpha\bar{\alpha} - \beta\bar{\beta} = w \in \ddot{u}(Z[H])$ then u-1=W-1(α-βX)” ⇨α = $\bar{\alpha}$, β=-β Thus b=d, contradicting b + d=1. Now let $u^2=y^2=u^{-2}$, ⇨$\alpha^2=\bar{\alpha}^2$ So that either b=d, a contradiction. (or) a=c=0. Straight forward computation shows that if a=c=0,$u^2=y^2$ iff$e^2+f^2=b^2$-b. Now let u=α+βx∈V_3

Suppose first that $u^2=y^2$. For u∈V_3,det(ϕ(u))=-1, / u-1=-$\bar{\alpha}$ + βx. Then $u^2=u^{-2}$, ⇨either b=d=0 (or) a=c=0. If a=e=0, again as above, E^2+f^2=b (b-1). But the left side of this equation is odd and the right side is even. Which is a contradiction. A Similar contradiction arises if b=d=0. Now suppose that u=u-1. Then α=$-\bar{\alpha}$ or equivalently a=0. Now let $u^2=y^2$=u-2, ⇨α2=$\bar{\alpha}$2 so that either b=d, a contradiction, (or) a=c=0. Straight forward computation shows that if a=c=0, $u^2=y^2$ iff $e^2+f^2=b^2$-b. Now let u=α+βx∈V_3. Suppose first that $u^3=y^2$. For u∈V_3, Let(ϕ(u))=-1, / u-1=-$\bar{\alpha}$+βx, Then $u^2=u^{-2}$, ⇨either b=d=0 (or) a=c=0. If a=c=0, again as above, e^2+f^2=b(b-1). But the left side of this equation is odd and the right side is even. Which is a contradiction. A

similar contradiction arises if b=d=0. Now suppose that $u=u^{-1}$. Then $\alpha=\bar{\alpha}$ or equivalently a=0 and $\alpha\bar{\alpha}=\beta\bar{\beta}+1$ or equivalently $b^2=f^2+e^2-e$. The argument for V_4 is similar.

Remark: A subgroup of $V(Z[D_4])$ isomorphic to the Klein 4-group k must be generated by y^2 and a unit of order 2 in V_3 (or)V_4. For suppose u,v generate a copy of k with $u\in V_3$ and $v\in V_4$.Then $uv\in V_2$ which has no units of order 2.Thus u,v both lie in V_3 (or)V_4 , and $uv=y^2$.

Integer Points on a Hyperoloid:

Now describe a method for finding integer points on H_k for various k based on "growing the tree of primitive Pythagorean triples from (3,4,5)". A point $p=(a,b,c)\in H_0$ satisfies $x^2+y^2=z^2$. If a,b,c are positive, then (a,b,c) is called a Pythagorean triple. Every Pythagorean tripled is a multiple of a primitive Pythagorean triple, (ie) one in which gcd(p)=gcd(a,b,c)=1. In order to construct all primitive Pythagorean triples , it suffices to find all primitive Pythagorean triples (a,b,c) with a,c odd and b even, since all others are obtained by switching a,b. The "tree" of such triples with a,b,c positive grown from the "seed" (3,4,5) is well known ;review its construction. Let I_i,i=1,2,3 and $I_{1.2}$ be the matrices representing reflections in the planes X=0,Y=0,Z=0 and X=Y respectively. Let, U,A,D be the transformations with matrices

$$A=\begin{pmatrix}1&2&2\\2&1&2\\2&2&3\end{pmatrix}$$

Remark: Construct the integer points on H_k,k≠0, in a similar manner. Let $\mathcal{G}$ be a group of linear transformations on Z3 which maps H_k to itself. Define an equivalence relation $\sim_{\mathcal{G}}$ on H_k by $p\sim_{\mathcal{G}}$ QiffQ=T(p) for some $T\in\mathcal{G}$. Denote the equivalence class of p by $[p]_{\mathcal{G}}$. Now define groups of transformations on H_k as follows

- ✓ Let R be generated by $I_{1.2}$,I_i,i=1,2,3.R≅D_4XC_2.
- ✓ Let R be generated by$I_3$and $I_{i.2}$ R′≅C_2XC_2.
- ✓ Let S be generated by the U,A,D or equivalently by A,I_1,I_2
- ✓ Let S be generated by S and R′.

Let $(x,y,z)\in H_k$ with k not a square and x=2m+1 odd. Then o≠t=z-y, Letting s=z+y we have ts=x2-k. We identify points with x odd in H_k with the set of pairs $P_k=\{m,t\}/m\in Z$,t divides(2m+1)2-k} via.

$$\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}2m+1\\\frac{(2m+1)^2-k-t^2}{2t}\\\frac{(2m+1)^2-k+t^2}{2t}\end{pmatrix}=\begin{pmatrix}2m+1\\\frac{s-t}{2}\\\frac{s+t}{2}\end{pmatrix}$$

Now identify points $(x, y, z)\in H_k$ with x=2m even,k not a square, in a similar way with the set of pairs $2_k=\{(m, t)/m\in Z$,t divides (2m)2-k} via

$$\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}2m+1\\\frac{(2m)^2-k-t^2}{2t}\\\frac{(2m)^2-k+t^2}{2t}\end{pmatrix}=\begin{pmatrix}2m\\\frac{s-t}{2}\\\frac{s+t}{2}\end{pmatrix}$$

The linear transformations U,A,D on H_k define maps (which we also denote U,A,D) on P_k and 2_k, y

U(m,t)=(m+t,t)

and A(m,t)=(m+s,s) for $(m,t)\in P_k$(or)2_k

D(m,t)=(s-m-1,s) for$(m,t)\in p_k$

D(m,t)=(s-m,s) for$(m,t)\in 2_k$

Remark: If $(m, t)\in P_k$ (or) 2_k corresponds to $(x, y, z)\in H_k$, then (m,s) corresponds to (x,-y,z), (m,-t) corresponds to(x,-y,-z).

Remark: If k is a square, say $k=K^2$, then any point (±K,y,y) lies on H_k so that the bijective correspondence between H_k and $P_k\cup 2_k$ fails.

Remark: Let $p=(x, y, z)\in H_k$.

- ✓ If k≡0 mod 4,then either x, y, z are all even (and thus gcd(p)≥2).(or)z is odd, and x, y have different parity, then
- ✓ If k≡1 mod 4, then either x, y, z are all odd, (or) z is even and x,y have different parity.
- ✓ If k≡2 mod 4, then z must be even and x, y both odd.
- ✓ If k≡3 mod 4, then z must be odd and x, y other even.

Theorem 18:

If $P_k\neq\phi$, then for any $m\in Z$, there exists t such that$(m,t)\in P_k$. & If $2_k\neq\phi$, then for any $m\in Z$, there exists t such that $(m,t)\in 2_k$.

Proof:

Let $P_k=\phi$,$m\in Z$,x=2m+1. If k is even. Then $st=x^2-k$ is odd ∴ Let t=1, $S=x^2-k$, To obtain values of y, z. If k is odd, Then k≡1 mod 4, ∴ 4 divides $z^2=y^2$

Choose t = 2and s even. The proof of (ii) is similar and use the fact that here cannot have k≡2mod4.

Conclusion:

This paper deals with Pythagorean Triples and primitive Pythagorean triples. Some theorems based on these are also discussed. Also it deals with characterization of primitive Pythagorean triples and lagrange's square theorem. And then describes a simple method for finding units of group rings of the form Z[G]=Z[H] =Z[C_2] for H an Abelian group and apply this to the case G=D_4 ,the dihedral group of order 8.

References:

1. Barnad and child, "Higher algebra", Mac Millian Company, London.
2. M. Beattie and Weatherby, "Pythagorean Triples and units in integral group", Journal of Algebra and its applications, 2003.
3. David M. Byrton, "Elementary Number theory", Universal Book stall, 1991.
4. L E. Dickson, "History of theory of numbers". Chelsea publishing company, New York, 1952.
5. John Kennedy, "Pythagorean Triples", pacific journal of mathematics, 2002.
6. Robin Chapman, "Pythagorean Triples and Sums of squares", Journal of number theory, 2004.
7. S. G Telang, "Number theory", Tata McGraw-Hill publishing Company Limited, New Delhi.